

GIT HAPPENS

Welcome to my writeup where I am gonna be pwning the **GitHappens** from TryHackMe.
This challenge has 1 flag. Let's get started!

GETTING STARTED

To access the challenge, click on the link given below:

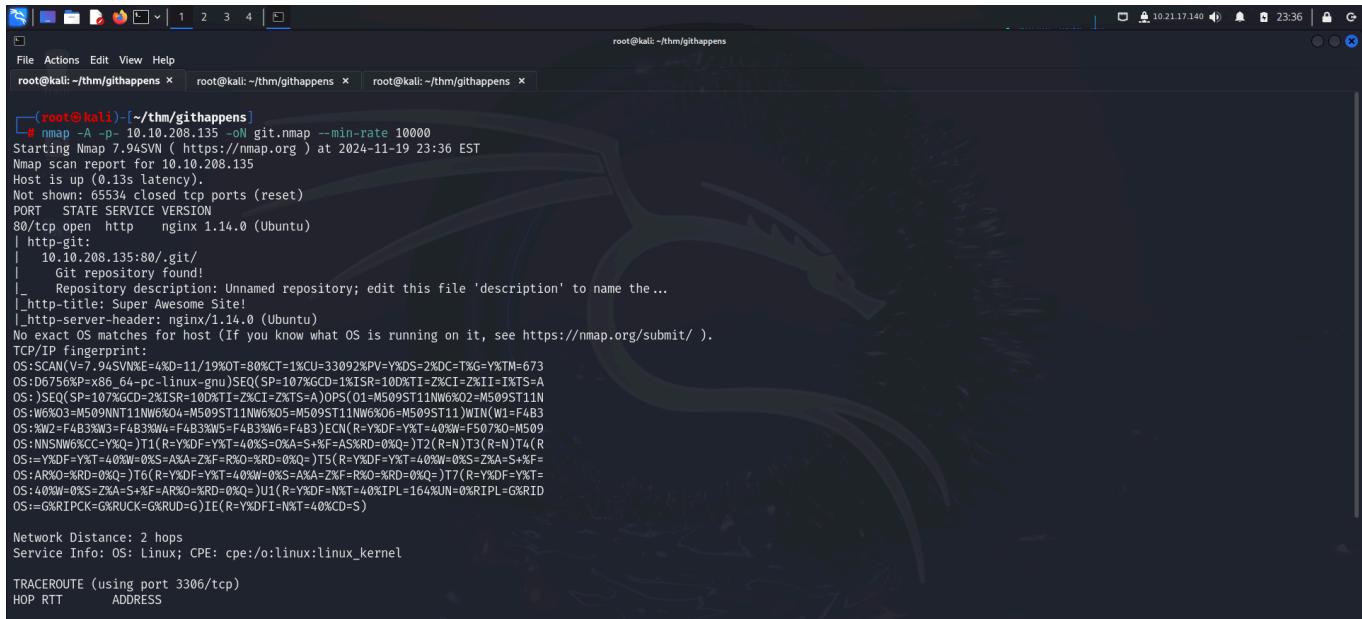
<https://tryhackme.com/r/room/githappens>

Note

This writeup documents the steps that successfully led to pwnage of the machine. It does not include the dead-end steps encountered during the process (which were numerous). This is just my take on pwning the machine and you are welcome to choose a different path.

RECONNAISSANCE

I started off by performing an **nmap** aggressive scan to find open ports and services running on the machine.



The screenshot shows a terminal window with three tabs. The current tab is titled "root@kali: ~/thm/githappens". The command entered is "# nmap -A -p- 10.10.208.135 -oN git.nmap --min-rate 10000". The output of the scan is displayed, showing an open port 80/tcp on http://10.10.208.135:80, running nginx 1.14.0 (Ubuntu). The service is identified as "Super Awesome Site!". The terminal also shows the user is root on a Kali Linux system.

```
# nmap -A -p- 10.10.208.135 -oN git.nmap --min-rate 10000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 23:36 EST
Nmap scan report for 10.10.208.135
Host is up (0.13s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.14.0 (Ubuntu)
| http-git:
|_ 10.10.208.135:80/.git/
|   Git repository found!
|_ Repository description: Unnamed repository; edit this file 'description' to name the ...
|_ http-title: Super Awesome Site!
|_ http-server-header: nginx/1.14.0 (Ubuntu)
No exact OS matches for host (if you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

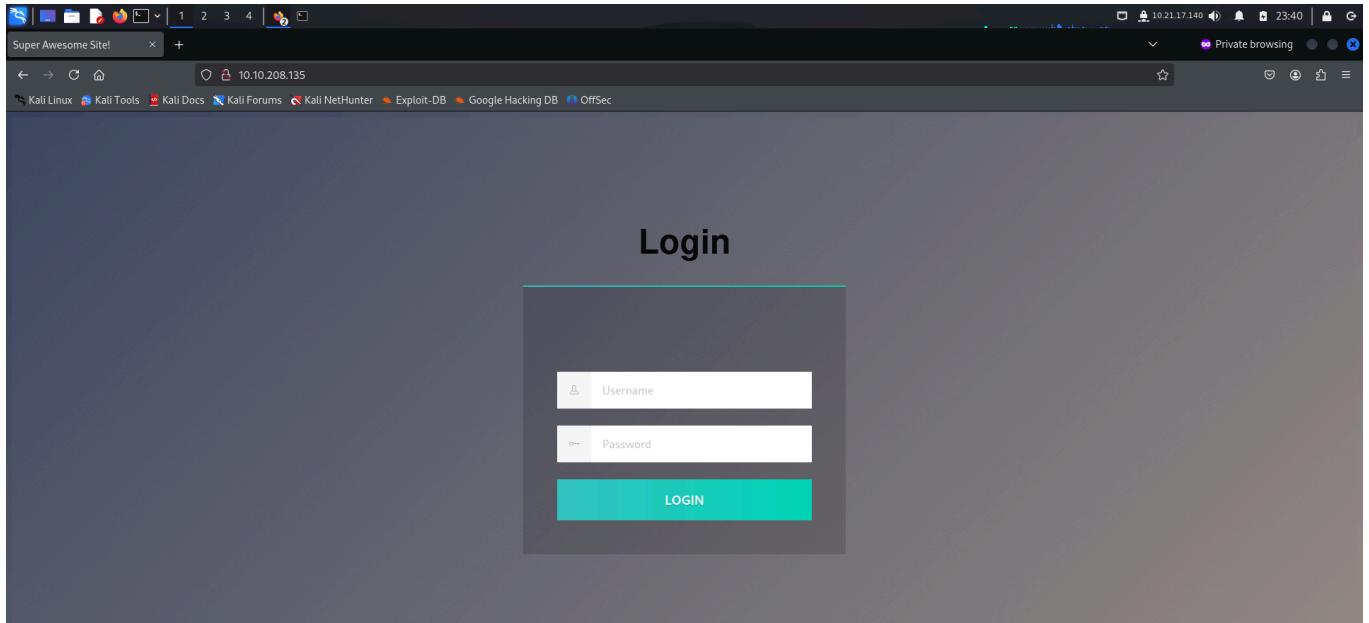
```
OS:SCAN(V=7.94SVN E=4K0-11/19K0T=80%CT=1%CU=33092%PV=Y%OS=2%DC=T%G=Y%TM=673
OS:D6756%P=x86_64-pc-linux-gnu)SEQ(SP=107%CD=1%SR=10D%TI=Z%CI=Z%II=I%TS=A
OS:SEQ(SP=107%CD=2%ISR=10D%TI=Z%CI=Z%TS=A)OPS(01=M509ST11NW6X02+M509ST11N
OS:W6X03+M509NT11NW6X04+M509ST11NW6X05+M509ST11NW6X06+M509ST11J)WIN(W1=F4B3
OS:W3D=F4B3XW3+FA83XW4=F4B3XW6+F4B3)ECN(R=Y8DF=Y8T+408W+F507%O+M509
OS:NNSNW6X0C=Y8Q=)T1(R=Y8DF=Y8T+408S+0%A+S+RF=ASRD=0%)T2(R=N)T3(R=N)T4(R
OS:=Y8DF=Y8T+408W+0%S+0%A+Z%F=R80-%RD=0%)T5(R=Y8DF=Y8T+408W+0%S+Z%A+S+RF=
OS:AR80-%RD=0%)T6(R=Y8DF=Y8T+408W+0%S+0%A+Z%F=R80-%RD=0%)T7(R=Y8DF=Y8T+
OS:+408W+0%S+Z%A+S+%F=AR80-%RD=0%)U1(R=Y8DF=N%T+40%IPL=164%UN=0%RIPL=G%RID
OS:=G%RIPLCK=G%RUCK=G%RID=G)IE(R=Y8DFI=40%CD=S)
```

Network Distance: 2 hops
Service Info: OS: Linux; CPE:cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3306/tcp)
HOP RTT ADDRESS

CAPTURING THE FLAG

The scan revealed port 80 to be up and running. It also found a directory `/.git` on the website. I visited the website from my browser.



To find more directories, I performed a web fuzzing using **ffuf**

```
File Actions Edit View Help
root@kali:~/thm/githappens x root@kali:~/thm/githappens x root@kali:~/thm/githappens x
└─(root@kali)-[~/thm/githappens]
# ffuf -u http://10.10.208.135/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt


```

Login

v2.1.0-dev

```
-- Method : GET
:: URL   : http://10.10.208.135/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
```

```
index.html      [Status: 200, Size: 6890, Words: 541, Lines: 61, Duration: 137ms]
.               [Status: 301, Size: 194, Words: 7, Lines: 8, Duration: 131ms]
.git            [Status: 301, Size: 194, Words: 7, Lines: 8, Duration: 155ms]
dashboard.html [Status: 200, Size: 3775, Words: 106, Lines: 17, Duration: 138ms]
:: Progress: [37050/37050] :: Job [1/1] :: 201 req/sec :: Duration: [0:02:13] :: Errors: 0 ::
```

```
└─(root@kali)-[~/thm/githappens]
```

The fuzz scan revealed another page `dashboard.html`. I then navigated to `/.git` and found contents of a git repository.

```

../
branches/
hooks/
info/
logs/
objects/
refs/
HEAD
config
description
index
packed-refs

```

23-Jul-2020 22:39 -
23-Jul-2020 22:39 23
24-Jul-2020 06:25 110
23-Jul-2020 22:39 -
23-Jul-2020 22:39 -
23-Jul-2020 22:39 645
24-Jul-2020 06:25 102

In order to make working with it more convinient, I used [gittools](#).

It contains a script called **gitdumper**. This tool can be used to download as much as possible from the found `.git` repository from webservers which do not have directory listing enabled. I used it to copy the contents from the site to my local machine.

```

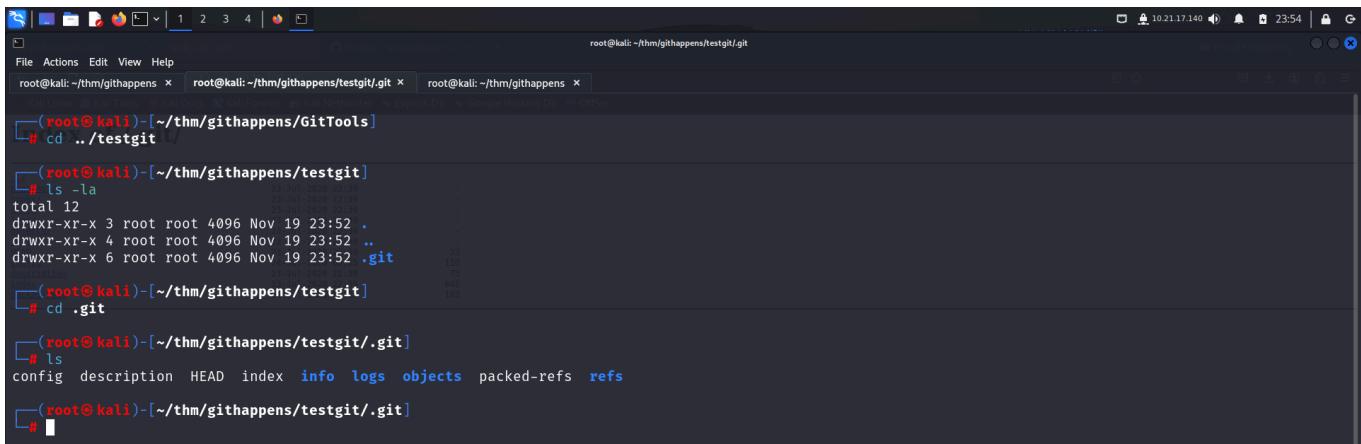
File Actions Edit View Help
root@kali: ~/thm/githappens/GitTools/Dumper x root@kali: ~/thm/githappens/GitTools/Dumper x root@kali: ~/thm/githappens
root@kali: ~/thm/githappens/GitTools x root@kali: ~/thm/githappens/GitTools/Dumper x root@kali: ~/thm/githappens
└─(root@kali)-[~/thm/githappens/GitTools]
# ls Products Solutions OpenSource Enterprise ...
Dumper Extractor Finder LICENSE.md README.md
└─(root@kali)-[~/thm/githappens/GitTools]
# cd Dumper
└─(root@kali)-[~/thm/githappens/GitTools/Dumper]
# ls
gitdumper.sh README.md
└─(root@kali)-[~/thm/githappens/GitTools/Dumper]
# ./gitdumper.sh
#####
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehexelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
#####
[*] USAGE: http://target.tld/.git/ dest-dir [--git-dir=otherdir]
      --git-dir=otherdir          Change the git folder name. Default: .git
└─(root@kali)-[~/thm/githappens/GitTools/Dumper]
# 
Completing executable file

```

```

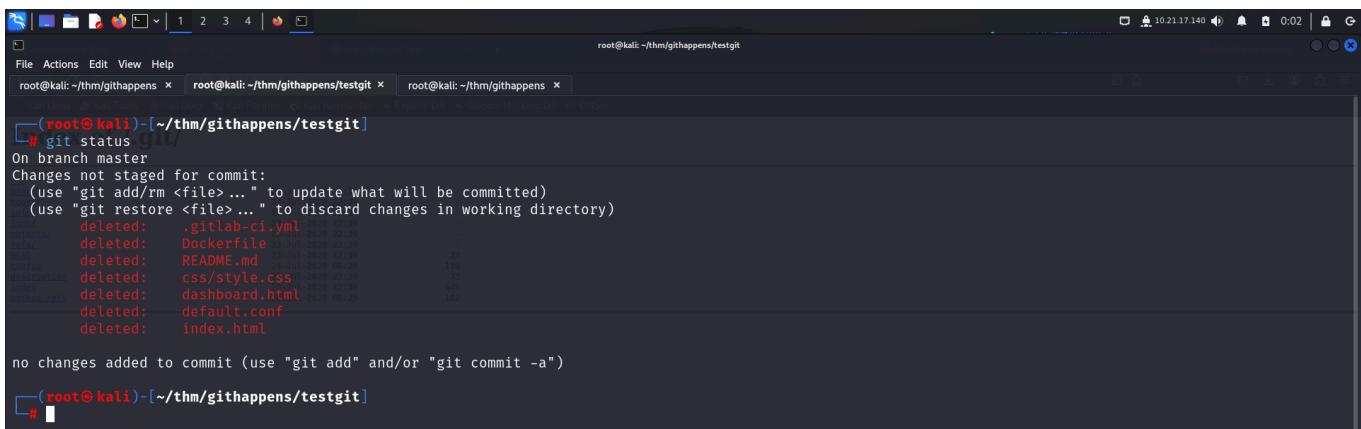
File Actions Edit View Help
root@kali: ~/thm/githappens/GitTools/Dumper x root@kali: ~/thm/githappens
root@kali: ~/thm/githappens/GitTools/Dumper x root@kali: ~/thm/githappens
└─(root@kali)-[~/thm/githappens/GitTools/Dumper]
# ./gitdumper.sh http://10.10.208.135/.git/ ~/thm/githappens/testgit/
#####
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehexelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
#####
[*] Destination folder does not exist
[+] Creating /root/thm/githappens/testgit/.git/
[+] Downloaded: HEAD
[-] Downloaded: objects/info/packs
[+] Downloaded: description
[+] Downloaded: config
[-] Downloaded: COMMIT_EDITMSG
[+] Downloaded: index
[+] Downloaded: packed-refs
[+] Downloaded: refs/heads/master
[-] Downloaded: refs/remotes/origin/HEAD
[-] Downloaded: refs/stash
[+] Downloaded: logs/HEAD
[+] Downloaded: logs/refs/heads/master
[-] Downloaded: logs/refs/remotes/origin/HEAD
[-] Downloaded: info/refs
[+] Downloaded: info/exclude

```



```
root@kali:~/thm/githappens/testgit/git
File Actions Edit View Help
root@kali:~/thm/githappens x root@kali:~/thm/githappens/testgit.git x root@kali:~/thm/githappens x
(boot@kali)-[~/thm/githappens/GitTools]
# cd .. /testgit
(boot@kali)-[~/thm/githappens/testgit]
# ls -la
total 12
drwxr-xr-x 3 root root 4096 Nov 19 23:52 .
drwxr-xr-x 4 root root 4096 Nov 19 23:52 ..
drwxr-xr-x 6 root root 4096 Nov 19 23:52 .git
(boot@kali)-[~/thm/githappens/testgit]
# cd .git
(boot@kali)-[~/thm/githappens/testgit/.git]
# ls
config description HEAD index info logs objects packed-refs refs
(boot@kali)-[~/thm/githappens/testgit/.git]
#
```

I viewed the status of the repo using `git status` and found a lot of files had been deleted.

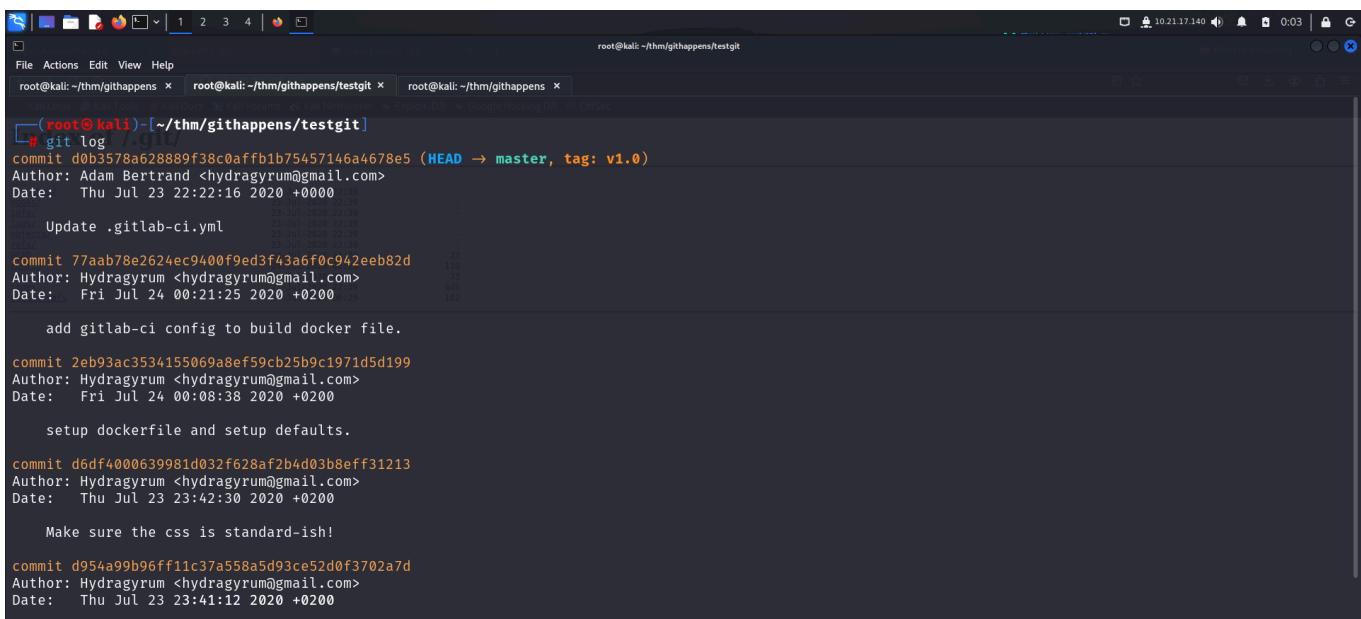


```
root@kali:~/thm/githappens/testgit
File Actions Edit View Help
root@kali:~/thm/githappens x root@kali:~/thm/githappens/testgit x root@kali:~/thm/githappens x
(boot@kali)-[~/thm/githappens/testgit]
# git status
On branch master
Changes not staged for commit:
  (use "git add/rm <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
deleted:   .gitlab-ci.yml
deleted:   Dockerfile
deleted:   README.md
deleted:   css/style.css
deleted:   dashboard.html
deleted:   default.conf
deleted:   index.html

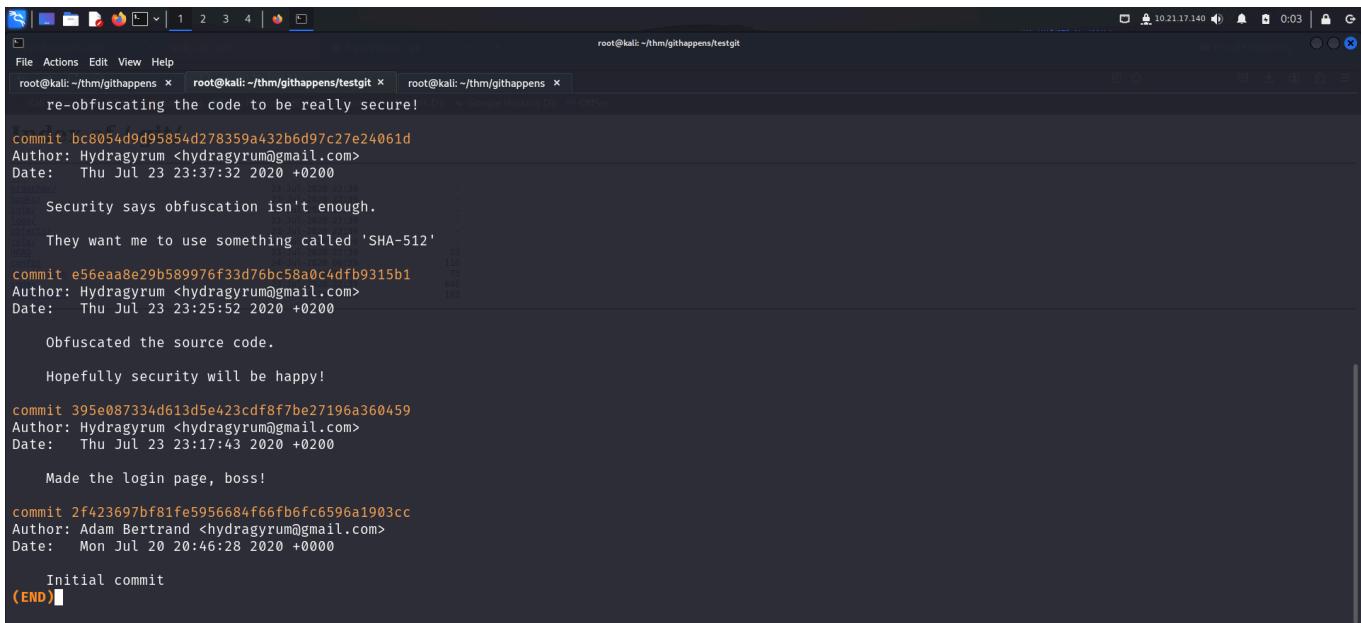
no changes added to commit (use "git add" and/or "git commit -a")

(boot@kali)-[~/thm/githappens/testgit]
#
```

I then viewed logs to find information about the commits that were made using `git log` command.



```
root@kali:~/thm/githappens/testgit
File Actions Edit View Help
root@kali:~/thm/githappens x root@kali:~/thm/githappens/testgit x root@kali:~/thm/githappens x
(boot@kali)-[~/thm/githappens/testgit]
# git log / .git/
commit d0b3578a628889f38c0affb1b75457146a4678e5 (HEAD -> master, tag: v1.0)
Author: Adam Bertrand <hydragyrum@gmail.com>
Date:   Thu Jul 23 22:16 2020 +0000
        Update .gitlab-ci.yml
commit 77aab78e2624ec9400f9ed3f43a6f0c942eeb82d
Author: Hydragryum <hydragyrum@gmail.com>
Date:   Fri Jul 24 00:21:25 2020 +0200
        add gitlab-ci config to build docker file.
commit 2eb93ac353a15506948ef59cb25b9c1971d5d199
Author: Hydragryum <hydragyrum@gmail.com>
Date:   Fri Jul 24 00:08:38 2020 +0200
        setup dockerfile and setup defaults.
commit d6df4000639981d032f628af2b4d03b8eff31213
Author: Hydragryum <hydragyrum@gmail.com>
Date:   Thu Jul 23 23:42:30 2020 +0200
        Make sure the css is standard-ish!
commit d954a99b96ff11c37a558a5d93ce52d0f3702a7d
Author: Hydragryum <hydragyrum@gmail.com>
Date:   Thu Jul 23 23:41:12 2020 +0200
```



```
re-obfuscating the code to be really secure!
commit bc8054d9d95894d278359a432b6d97c27e24061d
Author: Hydragryum <hydragryum@gmail.com>
Date: Thu Jul 23 23:37:32 2020 +0200

    Security says obfuscation isn't enough.

They want me to use something called 'SHA-512'
commit e56ea8e29b589976f33d76bc58a0c4dfb9315b1
Author: Hydragryum <hydragryum@gmail.com>
Date: Thu Jul 23 23:25:52 2020 +0200

    Obfuscated the source code.

    Hopefully security will be happy!

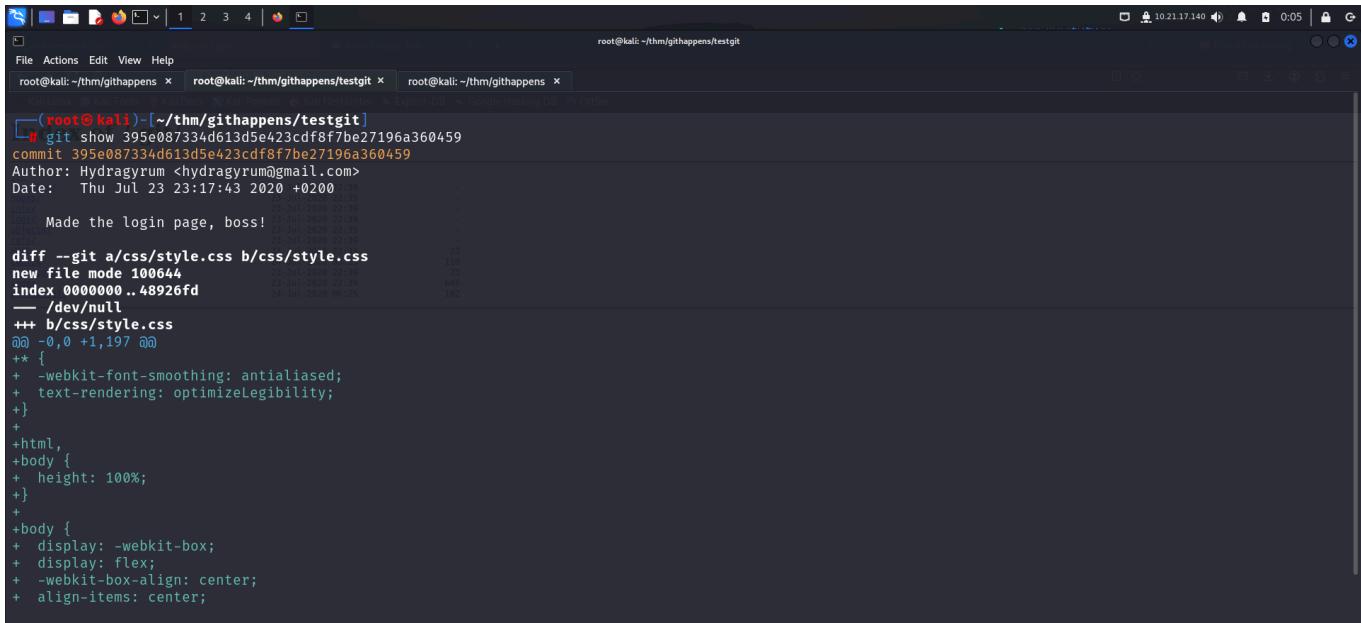
commit 395e087334d613d5e423cdf8f7be27196a360459
Author: Hydragryum <hydragryum@gmail.com>
Date: Thu Jul 23 23:17:43 2020 +0200

    Made the login page, boss!

commit 2f423697bf81fe5956684f66fb6fc6596a1903cc
Author: Adam Bertrand <hydragryum@gmail.com>
Date: Mon Jul 20 20:46:28 2020 +0000

    Initial commit
(END)
```

The commit with `Made the login page, boss!` comment looked interesting. So I viewed the information that was sent in that commit using `git show` command.



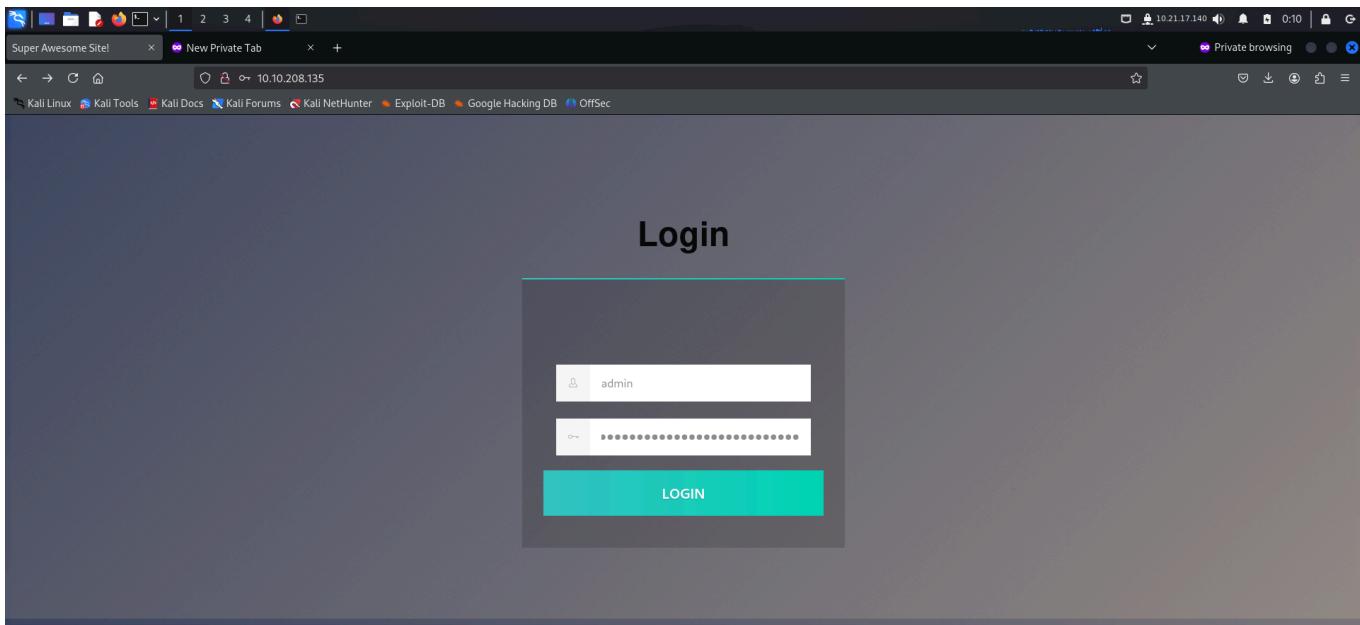
```
(root@kali)-[~/thm/githappens/testgit]
# git show 395e087334d613d5e423cdf8f7be27196a360459
commit 395e087334d613d5e423cdf8f7be27196a360459
Author: Hydragryum <hydragryum@gmail.com>
Date: Thu Jul 23 23:17:43 2020 +0200

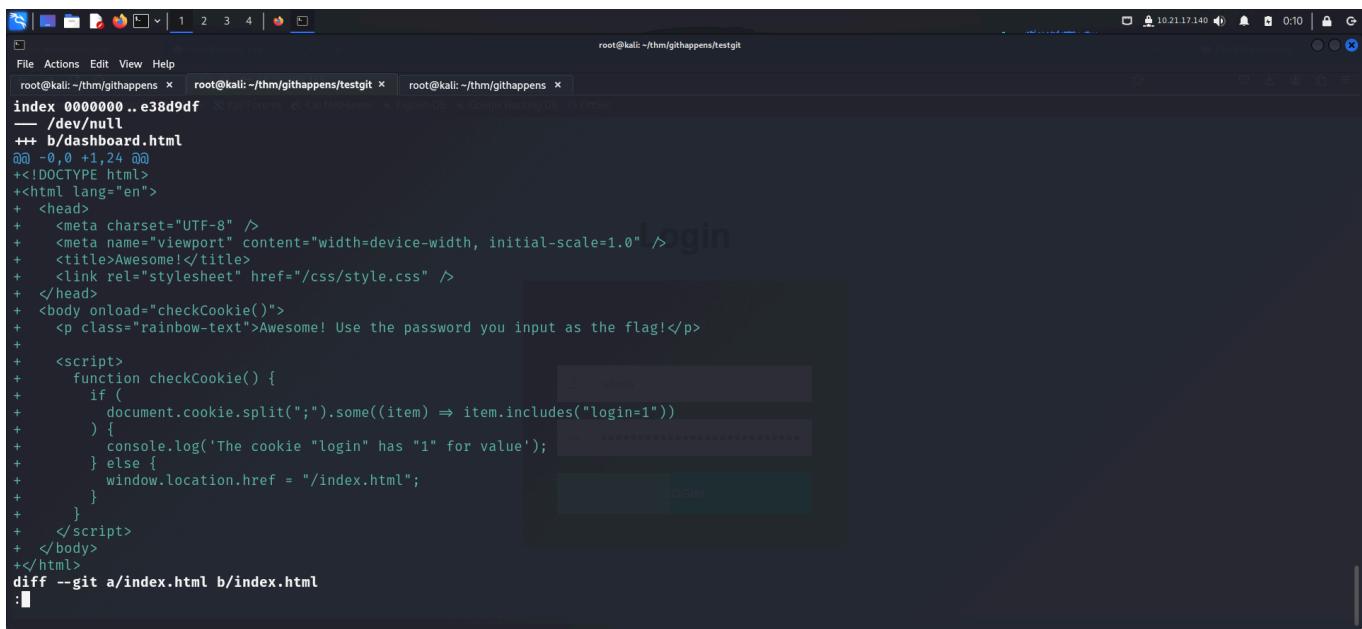
    Made the login page, boss!

diff --git a/css/style.css b/css/style.css
new file mode 100644
index 000000..48926fd
--- /dev/null
+++ b/css/style.css
@@ -0,0 +1,197 @@
+{
+    -webkit-font-smoothing: antialiased;
+    text-rendering: optimizeLegibility;
+}
+
+html,
+body {
+    height: 100%;
+}
+
+body {
+    display: -webkit-box;
+    display: flex;
+    -webkit-box-align: center;
+    align-items: center;
```

Here I found the hardcoded credentials for the **login** page.

I entered these credentials and tried logging in but I didn't get any response from the website. So I revisited the commit to look for more information.





```
root@kali:~/thm/githappens/testgit
index 0000000..e38d9df
--- /dev/null
+++ b/dashboard.html
@@ -0,0 +1,24 @@
+<!DOCTYPE html>
+<html lang="en">
+<head>
+  <meta charset="UTF-8" />
+  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
+  <title>Awesome!</title>
+  <link rel="stylesheet" href="/css/style.css" />
+</head>
+<body onload="checkCookie()">
+  <p class="rainbow-text">Awesome! Use the password you input as the flag!</p>
+
+<script>
+  function checkCookie() {
+    if (
+      document.cookie.split(";").some((item) => item.includes("login=1"))
+    ) {
+      console.log('The cookie "login" has "1" for value');
+    } else {
+      window.location.href = "/index.html";
+    }
+  }
+</script>
+</body>
+</html>
diff --git a/index.html b/index.html
:|
```

I found another message that I had skipped previously. The flag was the password used to log in. So I submitted the password on **tryhackme** and solved the challenge.

Thats it from side :)

Until next time
