Academy

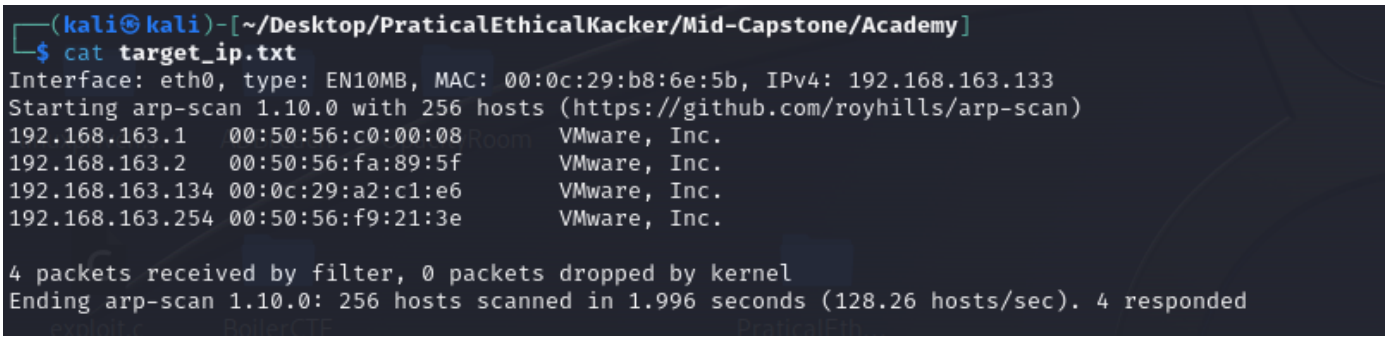
Links for reference:

FTP - https://www.linkedin.com/pulse/pentesting-exploiting-ftp-servers-kubotor ,

I have no idea on what to expect in this machine!

Lets get started with enumeration.

Target Ip_Address: 192.168.163.134



Nmap scan:

```
┌──(kali㉿kali)-[~/Desktop/PraticalEthicalKacker/Mid-Capstone/Academy]
└─$ sudo nmap -T4 -A -p- 192.168.163.134 -oN academy_nmap_scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-07 15:17 EDT
Nmap scan report for 192.168.163.134
Host is up (0.00041s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.163.133
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 c7:44:58:86:90:fd:e4:de:5b:0d:bf:07:8d:05:5d:d7 (RSA)
|   256 78:ec:47:0f:0f:53:aa:a6:05:48:84:80:94:76:a6:23 (ECDSA)
|_  256 99:9c:39:11:dd:35:53:a0:29:11:20:c7:f8:bf:71:a4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:0C:29:A2:C1:E6 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.41 ms 192.168.163.134

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.84 seconds
```

After the Nmap scan, I retrieved the "note.txt" file, and that particular file disclosed some very sensitive information. We now have credentials for the website admin.

```
┌──(kali㉿kali)-[~/Desktop/PraticalEthicalKacker/Mid-Capstone/Academy]
└─$ cat note.txt
Hello Heath !
Grimmie has setup the test website for the new academy.
I told him not to use the same password everywhere, he will change it ASAP.


I couldn't create a user via the admin panel, so instead I inserted directly into the database with the following command:

INSERT INTO `students` (`StudentRegno`, `studentPhoto`, `password`, `studentName`, `pincode`, `session`, `department`, `semester`, `cgpa`, `creati
ondate`, `updationDate`) VALUES
('10201321', '', 'cd73502828457d15655bbd7a63fb0bc8', 'Rum Ham', '777777', '', '', '', '7.60', '2021-05-29 14:36:56', '');

The StudentRegno number is what you use for login.


Le me know what you think of this open-source project, it's from 2020 so it should be secure... right ?
We can always adapt it to our needs.

-jdelta

┌──(kali㉿kali)-[~/Desktop/PraticalEthicalKacker/Mid-Capstone/Academy]
```

findings.txt | possible_exploits.txt

```
7/7/2024 Findings for "Academy" virtual machine.

FTP/21 - vsFTPd 3.0.3 :
                - anonymous login allowed.
                - information disclosure. Note.txt discloses info about same password being used throughout the website. And we have credentials for login in an account. They provided the SQL syntax code which was used to add the admin user into the databased of the website. We have a "username" which in this case it is called "StudentRegno number", and a password hash. It also mentions that the website is an open-source project, which means they are using a public framework.


```

I also searched if there was any available exploits for "vsFTPd 3.0.3", but there does not seem to have one specific. It looks like a bunch of different techniques that could work, but not a vulnerability in specific for the version. At this point, I think we have a better chance login to this admin account, and see if we have write and/or execute to some file in the machine. Lets stick with the low hanging fruits first. Path to login is "/academy".

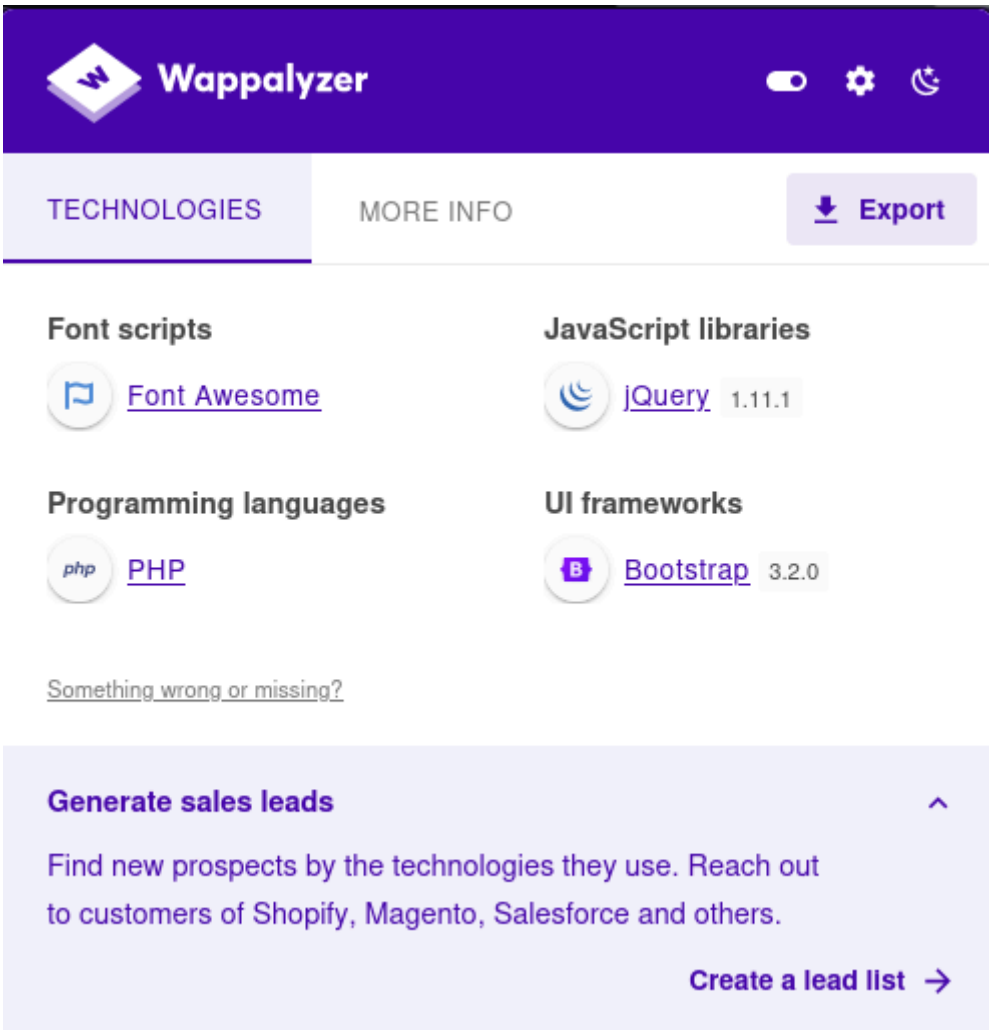
Credential: Reg no: "10201321" ;

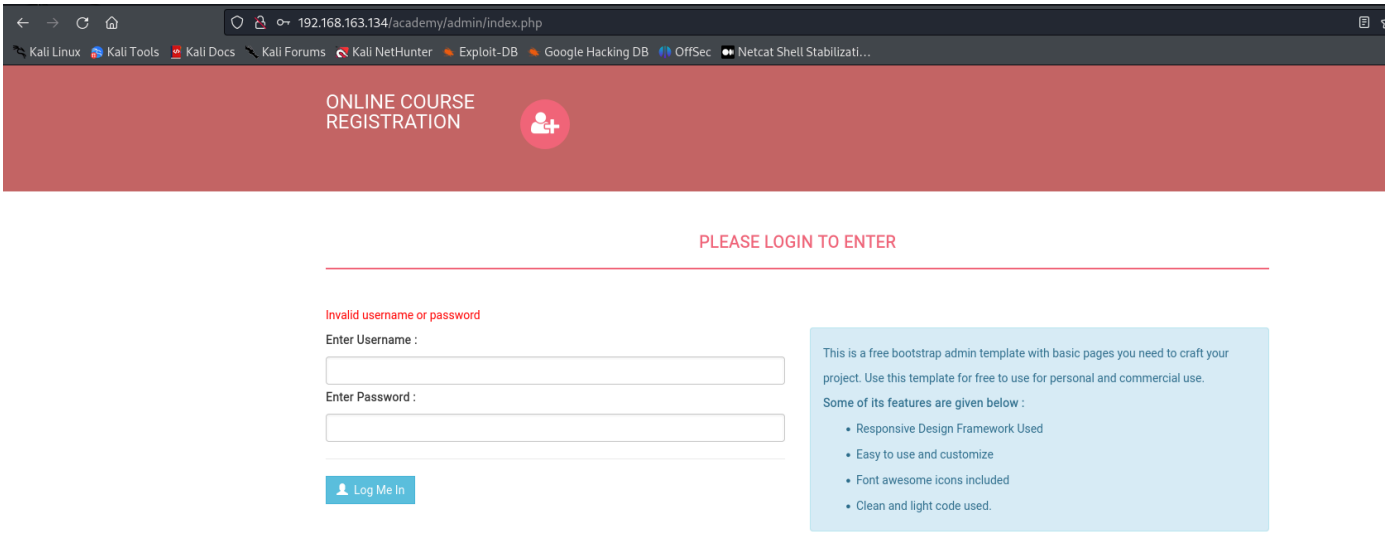
Password: "student" ; quotation signs are should not be included.

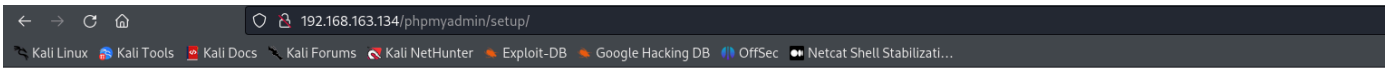
Updated to: "Password123!" ;

Potential username: jdelta ;

Website technologies:


Wappalyzer
TECHNOLOGIES
MORE INFO
Export
Font scripts
Font Awesome
JavaScript libraries
jQuery 1.11.1
Programming languages
PHP
UI frameworks
Bootstrap 3.2.0
Something wrong or missing?
Generate sales leads
Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.
Create a lead list


192.168.163.134/academy/admin/index.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Netcat Shell Stabilizati...
ONLINE COURSE REGISTRATION
PLEASE LOGIN TO ENTER
Invalid username or password
Enter Username :
Enter Password :
Log Me In
This is a free bootstrap admin template with basic pages you need to craft your project. Use this template for free to use for personal and commercial use.
Some of its features are given below :
Responsive Design Framework Used
Easy to use and customize
Font awesome icons included
Clean and light code used.



Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator at webmaster@localhost to inform them of the time this error occurred, and the actions you performed just before this error.

More information about this error may be available in the server error log.

Apache/2.4.38 (Debian) Server at 192.168.163.134 Port 80

IMPORTANT TAKE ON IMAGE UPLOAD:

When trying to exploit "image upload", start by trying with the regular malicious file extension only, and then move up to trying to bypass filters. There might be no filters, and trying to bypass something that is not there might break things, and get in the way of a successful exploitation.

We successfully exploit the Image Upload after watching the walkthrough, and now we need to escalate privileges to get root.

```
$ find / -type f -perm -04000 -ls 2>/dev/null
   12774     52 -rwsr-xr--   1 root     messagebus    51184 Jul  5  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
  135600     12 -rwsr-xr-x   1 root     root          10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
   16121    428 -rwsr-xr-x   1 root     root         436552 Jan 31  2020 /usr/lib/openssh/ssh-keysign
      52     56 -rwsr-xr-x   1 root     root          54096 Jul 27  2018 /usr/bin/chfn
    3908     52 -rwsr-xr-x   1 root     root          51280 Jan 10  2019 /usr/bin/mount
    3436     44 -rwsr-xr-x   1 root     root          44440 Jul 27  2018 /usr/bin/newgrp
    3910     36 -rwsr-xr-x   1 root     root          34888 Jan 10  2019 /usr/bin/umount
      53     44 -rwsr-xr-x   1 root     root          44528 Jul 27  2018 /usr/bin/chsh
      56     64 -rwsr-xr-x   1 root     root          63736 Jul 27  2018 /usr/bin/passwd
    3583     64 -rwsr-xr-x   1 root     root          63568 Jan 10  2019 /usr/bin/su
      55     84 -rwsr-xr-x   1 root     root          84016 Jul 27  2018 /usr/bin/gpasswd
$
```

```
        33      84 -rwsr-xr-x   1 root     root          84016 Jul 27  2018 /usr/bin/gpasswd
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:107:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
grimmie:x:1000:1000:administrator,,,:/home/grimmie:/bin/bash
$
```

```
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#

* * * * * /home/grimmie/backup.sh
www-data@academy:/home/grimmie$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
echo $PATH
www-data@academy:/home/grimmie$
```