

Pentest-24-04-23


Target

<https://cuportal.covenantuniversity.edu.ng>

Procedure

Ip and Host Discovery

- Get IP address of cuportal server using nslookup command

A screenshot of a terminal window with a dark blue background and a light blue border. The terminal has three colored window control buttons (red, yellow, green) in the top left corner. The command `nslookup cuportal.covenantuniversity.edu.ng` is entered in a light green monospace font.

```
nslookup cuportal.covenantuniversity.edu.ng
```

- The IP address of the server is `151.106.35.195`
- Query location of the server by finding it's name-server
 - this can be done using nslookup



```
nslookup 151.106.35.195
```

- From the results the ip address links european name servers [eu] this can be further confirmed by passing the ip address through the <https://iplocation.net> website

Geolocation data from IP2Location (Product: DB6, 2023-4-1)



IP ADDRESS: 151.106.35.195



ISP: Host Europe GmbH



COUNTRY: France 



ORGANIZATION: Not available



REGION: Hauts-de-France



LATITUDE: 50.6937



CITY: Roubaix



LONGITUDE: 3.1744

Port Scanning and Enumeration

- Scan all ports on the system using the nmap port scanner



```
nmap -sV -sC -sS -A 151.106.35.195 --open
```

- **Flags**
-

- sV → checks for running services and version on each port
- sC → runs default nmap scripts
- sS → runs scan in stealth mode
- A → checks for running operating system and device type
- p- → runs scan on all ports
- --open → only shows results for open ports

- **Results**

- **Services**

- FTP - PureFTPd - 21
- ssh - OpenSSH7.4 - 22
- smtp - Exim smtpd 4.96 - 25, 573
- DNS - PowerDNS Authoritative Server - 53
- http - Apache httpd - 80,443,8080
- http - Cpanel httpd - 2078
- mysql - Mysql 5.7.42 - 3306

- **Os/Device Scan**

- Running Linux Kernel 4.X
- General purpose device

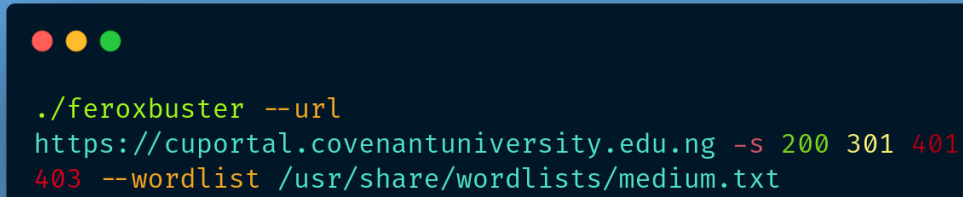
- **Server Distance**

- 16 hops

Directory Fuzzing

- Test for available directories on the cuportal website using feroxbuster(feroxbuster is chosen in this case because it is

significantly faster than its alternatives)

A terminal window with a dark background and three colored window control buttons (red, yellow, green) in the top left corner. The terminal displays a command to run feroxbuster on a specific URL with a wordlist.

```
./feroxbuster --url  
https://cuportal.covenantuniversity.edu.ng -s 200 301 401  
403 --wordlist /usr/share/wordlists/medium.txt
```

- **Results**

- **Fuzzing using common-php-filenames**

200 GET 142l 288w 3403c

https://cuportal.covenantuniversity.edu.ng/pwordreset.php

200 GET 50l 272w 25328c

https://cuportal.covenantuniversity.edu.ng/assets/img/logo.png

200 GET 4l 66w 31000c

https://cuportal.covenantuniversity.edu.ng/assets/css/font-awesome.min.css

200 GET 1l 3w 52c

https://cuportal.covenantuniversity.edu.ng/logout.php

200 GET 0l 0w 0c

https://cuportal.covenantuniversity.edu.ng/assets/img/index.php

200 GET 0l 0w 0c

https://cuportal.covenantuniversity.edu.ng/assets/img/

200 GET 0l 0w 0c

https://cuportal.covenantuniversity.edu.ng/assets/js/

200 GET 0l 0w 0c

https://cuportal.covenantuniversity.edu.ng/assets/js/index.php

200 GET 0l 0w 0c

https://cuportal.covenantuniversity.edu.ng/assets/

200 GET 0l 0w 0c

https://cuportal.covenantuniversity.edu.ng/assets/index.php

200 GET 0l 0w 0c
https://cuportal.covenantuniversity.edu.ng/assets/css/index
.ph
p

200 GET 0l 0w 0c
https://cuportal.covenantuniversity.edu.ng/assets/css/

200 GET 296l 1242w 136540c
https://cuportal.covenantuniversity.edu.ng/assets/img/CU_LO
G0.jpg

200 GET 7l 1163w 99554c
https://cuportal.covenantuniversity.edu.ng/assets/css/boots
trap.min.css

200 GET 4235l 11419w 104476c
https://cuportal.covenantuniversity.edu.ng/assets/css/style
.css

200 GET 11008l 45042w 293430c
https://cuportal.covenantuniversity.edu.ng/assets/js/jquery
.js

200 GET 949l 7159w 559132c
https://cuportal.covenantuniversity.edu.ng/assets/img/CU4.j
pg

200 GET 75l 316w 3765c
https://cuportal.covenantuniversity.edu.ng/login.php

200 GET 0l 0w 0c
https://cuportal.covenantuniversity.edu.ng/testmail.php

200 GET 1l 10w 48c
https://cuportal.covenantuniversity.edu.ng/right.php###
Using dirbuster-medium-wordlist

- **Fuzzing using dirbuster-medium-wordlist**

301 GET 7l 20w 259c
https://cuportal.covenantuniversity.edu.ng/cgi-bin ⇒
https://cuportal.covenantuniversity.edu.ng/cgi-bin/

301 GET 7l 20w 258c
https://cuportal.covenantuniversity.edu.ng/assets ⇒
https://cuportal.covenantuniversity.edu.ng/assets/

301 GET 7l 20w 259c

<https://cuportal.covenantuniversity.edu.ng/mailman> ⇒
<https://cuportal.covenantuniversity.edu.ng/mailman/>

301 GET 7l 20w 268c

<https://cuportal.covenantuniversity.edu.ng/mailman/archives>
⇒
<https://cuportal.covenantuniversity.edu.ng/mailman/archives/>

301 GET 7l 20w 265c

<https://cuportal.covenantuniversity.edu.ng/assets/images> ⇒
<https://cuportal.covenantuniversity.edu.ng/assets/images/>

301 GET 7l 20w 262c

<https://cuportal.covenantuniversity.edu.ng/assets/img> ⇒
<https://cuportal.covenantuniversity.edu.ng/assets/img/>

301 GET 7l 20w 261c

<https://cuportal.covenantuniversity.edu.ng/pipermail> ⇒
<https://cuportal.covenantuniversity.edu.ng/pipermail/>

301 GET 7l 20w 264c

<https://cuportal.covenantuniversity.edu.ng/applications> ⇒
<https://cuportal.covenantuniversity.edu.ng/applications/>

200 GET 21l 31w 442c

<https://cuportal.covenantuniversity.edu.ng/mailman/subscribe>

301 GET 7l 20w 267c

<https://cuportal.covenantuniversity.edu.ng/assets/img/user>
⇒
<https://cuportal.covenantuniversity.edu.ng/assets/img/user/>

200 GET 44l 137w 1677c

<https://cuportal.covenantuniversity.edu.ng/mailman/listinfo>

200 GET 45l 145w 1746c

<https://cuportal.covenantuniversity.edu.ng/mailman/admin>

301 GET 7l 20w 262c

<https://cuportal.covenantuniversity.edu.ng/assets/css> ⇒
<https://cuportal.covenantuniversity.edu.ng/assets/css/>

301 GET 7l 20w 270c

<https://cuportal.covenantuniversity.edu.ng/applications/adm>

in ⇒
<https://cuportal.covenantuniversity.edu.ng/applications/admin/>

301 GET 7l 20w 259c
https://cuportal.covenantuniversity.edu.ng/include ⇒
<https://cuportal.covenantuniversity.edu.ng/include/>

301 GET 7l 20w 269c
https://cuportal.covenantuniversity.edu.ng/assets/css/images ⇒
<https://cuportal.covenantuniversity.edu.ng/assets/css/images/>

301 GET 7l 20w 276c
https://cuportal.covenantuniversity.edu.ng/applications/admin/users ⇒
<https://cuportal.covenantuniversity.edu.ng/applications/admin/users/>

301 GET 7l 20w 277c
https://cuportal.covenantuniversity.edu.ng/applications/admin/assets ⇒
<https://cuportal.covenantuniversity.edu.ng/applications/admin/assets/>

301 GET 7l 20w 261c
https://cuportal.covenantuniversity.edu.ng/assets/js ⇒
<https://cuportal.covenantuniversity.edu.ng/assets/js/>

200 GET 22l 34w 452c
<https://cuportal.covenantuniversity.edu.ng/mailman/private>

301 GET 7l 20w 278c
https://cuportal.covenantuniversity.edu.ng/applications/admin/reports ⇒
<https://cuportal.covenantuniversity.edu.ng/applications/admin/reports/>

200 GET 329l 768w 34115c
<https://cuportal.covenantuniversity.edu.ng/webmail>

301 GET 7l 20w 281c
https://cuportal.covenantuniversity.edu.ng/applications/admin/assets/img ⇒

`https://cuportal.covenantuniversity.edu.ng/applications/admin/assets/img/`

Notable Directories

- `https://cuportal.covenantuniversity.edu.ng/right.php`
- `https://cuportal.covenantuniversity.edu.ng/testmail.php`
- `https://cuportal.covenantuniversity.edu.ng/pipermail.php`
- `https://cuportal.covenantuniversity.edu.ng/applications/*`
- `https://cuportal.covenantuniversity.edu.ng/applications/admin/users`

Other

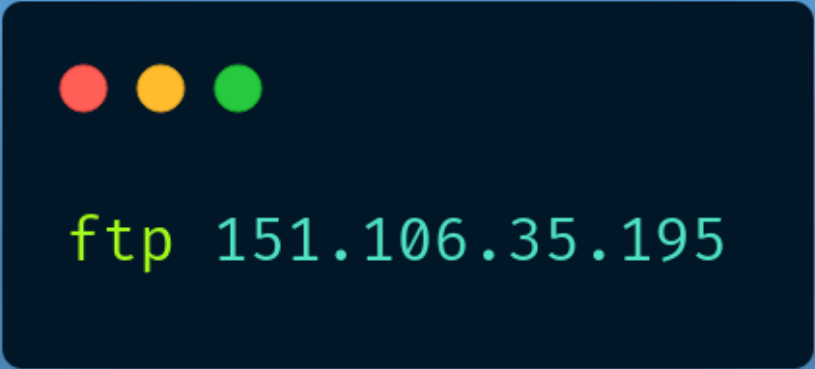
- `https://cuportal.covenantuniversity.edu.ng/applications/*` ⇒ returns blank page

Enumerating Services

FTP

- try to connect to the Pure-FtpD server running on port 21 using ftp command

#

A terminal window with a dark blue background and three colored window control buttons (red, yellow, green) at the top left. The text 'ftp 151.106.35.195' is displayed in a light green monospace font.

```
ftp 151.106.35.195
```

- Doesn't not have anonymous credentials
- Default credentials do not work

MySQL

- testing for sql injection on the login page using sqlmap

A terminal window with a dark blue background and three colored window control buttons (red, yellow, green) at the top left. The text shows a sqlmap command in a light green monospace font.

```
python sqlmap.py -v -u  
https://cuportal.covenantuniversity.edu.ng --level=2 --dbms  
=mysql --risk=2 --all --data="userid=&inputpassword1=&  
signin=Sign%20In"
```

- All the parameters are non injectable
- using old auth plugin(mysql_native_password)
 - Security Risk
 - Suggestion use a more secure authentication plugin such as (caching_sha2_password)

Http

- Testing http endpoints running on port 443 and 8080
- both pages appear to be inactive

Cookie Security risks

- Insecure cookie setting: Missing Secure Flag on the PHPSESSID cookie
- Risk
 - Since the `Secure` flag is not set on the cookie, the browser will send it over an unencrypted channel (plain HTTP) if such a request is made. Thus, the risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.
- Recommendation
 - set the `Secure` flag for the PHPSESSID cookie
- Insecure cookie setting: Missing HttpOnly flag
 - Risk
 - The PHPSESSID cookie has been set without the `HttpOnly` flag, which means that it can be accessed by the JavaScript code running inside the web page. If an attacker manages to inject malicious JavaScript code on the page (e.g. by using an XSS attack) then the cookie will be accessible and it can be transmitted to another site. In case of a session cookie, this could lead to session hijacking.
 - Recommendation
 - Set the HttpOnly flag for `all` cookies on the website

XSS vulnerabilities

- Through manual testing we detected a stored XSS vulnerability on the device registration form
 - Risk

- Stored XSS allows the user to write a script and store it in the applications database to be run everytime a user opens a specific page
- Recommendation
 - Sanitize and urlencode all inputs from forms to prevent users from embedding script tags in the forms