[CTF]No.0007 [强网杯] phone number

原创

林毅洋 于 2019-05-14 03:24:24 发布 715 收藏
分类专栏： CTF每日一题 CTF 文章标签： ctf每日一题 ctf

本文链接：https://blog.csdn.net/kajweb/article/details/77971526

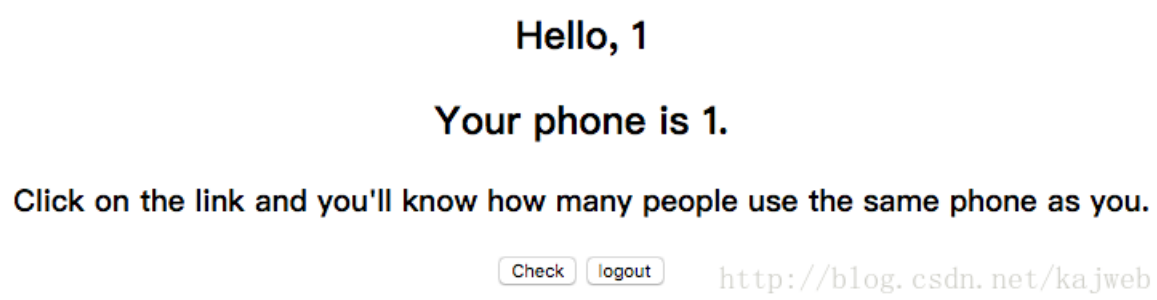

CTF每日一题 同时被 2 个专栏收录
9 篇文章 0 订阅
订阅专栏

CTF
13 篇文章 0 订阅
订阅专栏
#[CTF]No.0007 [强网杯] phone number
Phone number is a good thing.

CTF每日一题汇总

来源：强网杯-第二届-WEB
类别：16进制绕过 sql注入
来源：https://gdqwb2017.ichunqiu.com/competition/index
用到工具：无

##尝试
进入地址，首先alert一个please login！接着跳转到首页
正常注册一个电话号码和用户名都为1的账号，登陆后跳转到



点击check返回There only 1 people use the same phone as you

由此可以考虑二次注入。

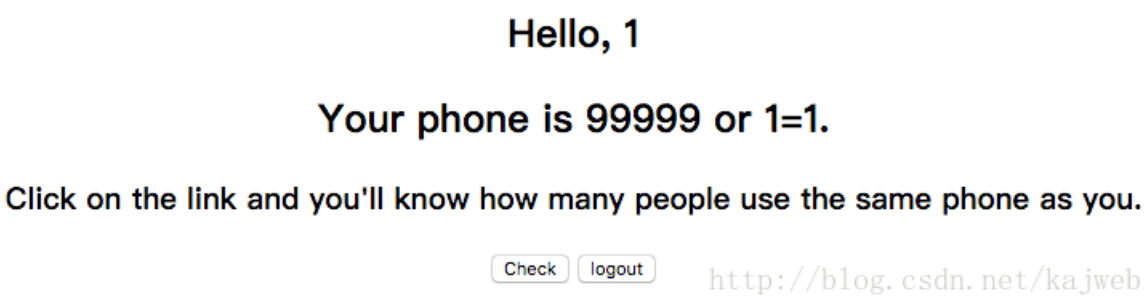
推出登录，重新进入注册页面。

##猜测
可以猜测，查询手机号码数量的语句为：

```
$sql = select count(*) from `user_phone` where phone = {$phone};
```

构造`SELECT count(*) FROM `user_phone` where phone=99999 or 1=1`

直接请求`99999 or 1=1`发现提示只能输入数字，然后这时候对字符串进行hex编码得到`0x39393939206f7220313d31`。提交，注册成功。



点击check返回`There only 3 people use the same phone as you`
这里对意思是数据库共有3条数据，而不是99999号码有3条数据。