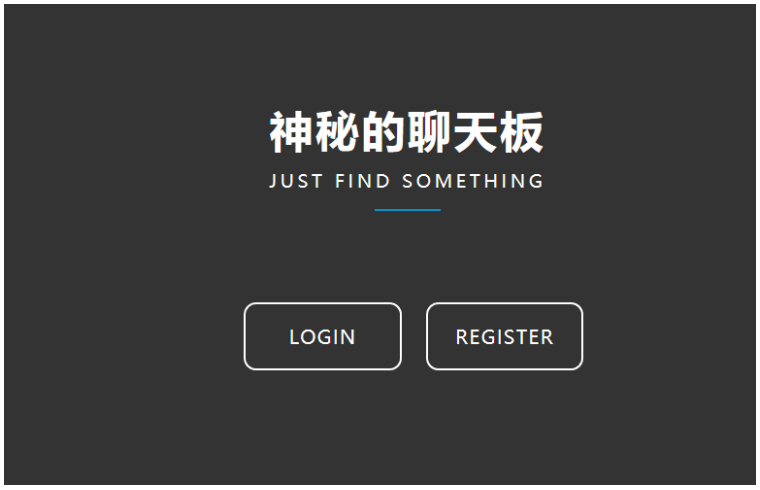
HTCF2017 writeup

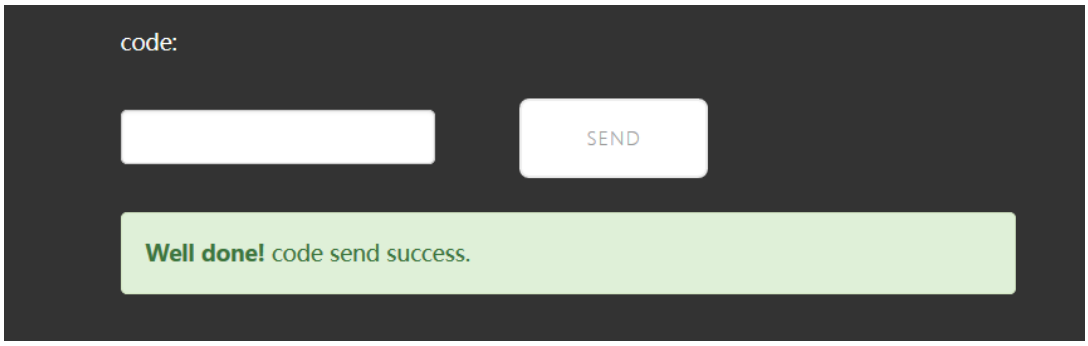
PENTEST

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。

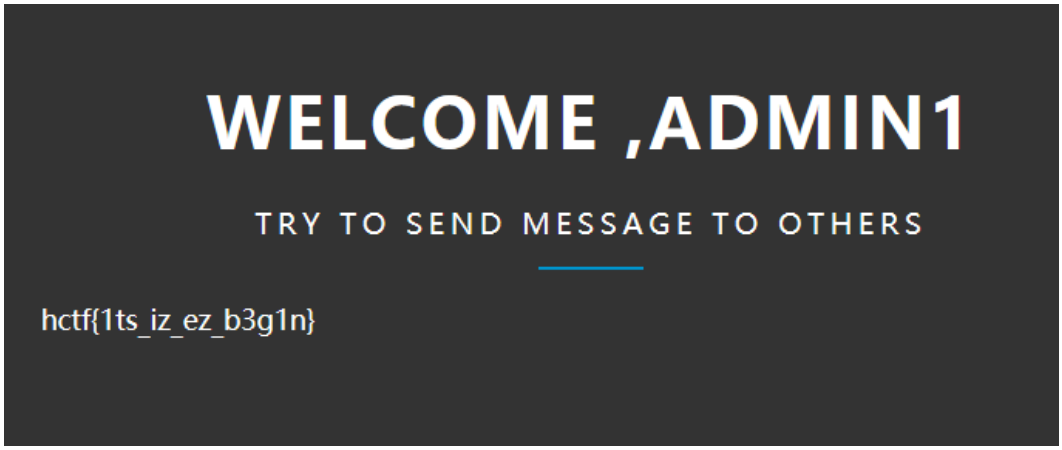


一开始天真地以为真的会发到我的手机上（因为注册的时候填了手机号）然而并没有 - -

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>
```

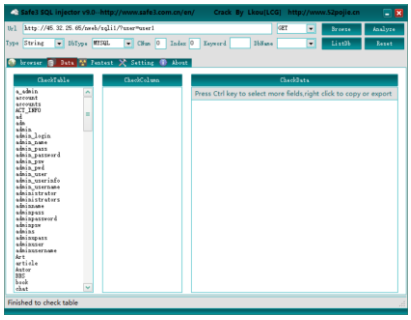
这里面有个 value=xxxxxx，直觉告诉我这个值就是 code。
然后直觉竟然是对的。Bingo。



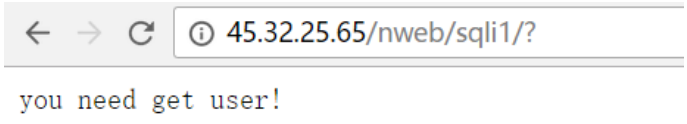
WEB

从 0 开始之 SQLI 之 2

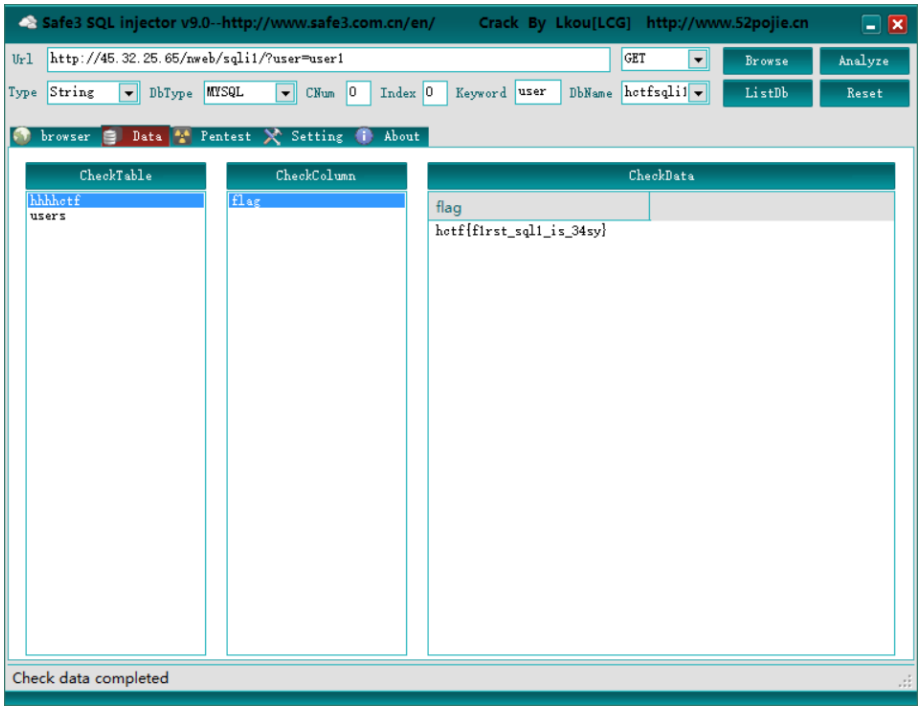
题目 ID： 65
题目描述： http://45.32.25.65/nweb/sqli1/?user=user1
一开始直接用工具 Safe3，发现出来好多表，但感觉不太对，因为看了几个列里的数据都是空的。



然后在页面上试了试，发现了关键字。



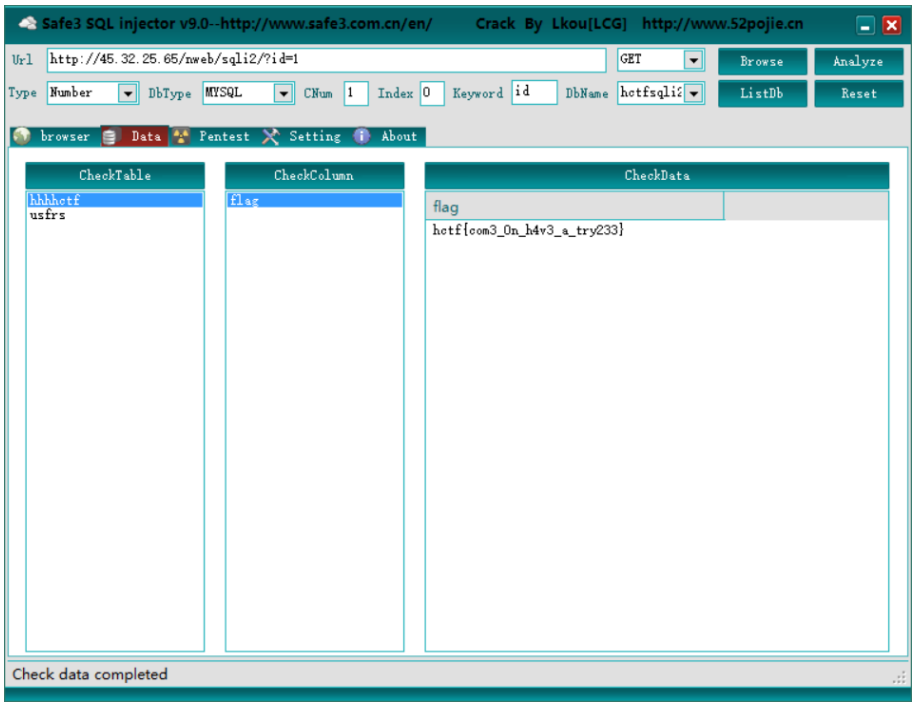
然后就把关键字输进去再次分析。就发现进入了一个叫 hctfsqli1 的库。
flag 就出来了。



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

同上题，找到关键字 id，工具分析。



Ryan
2017/2/6