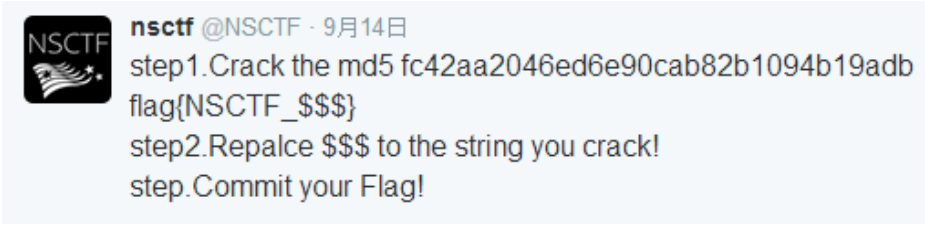
Misc100 Twitter

还在上微博吗?换个口味吧，试试twitter吧
关注我们的twitter，有惊喜
一般人我不告诉他

这个，去 Twitter 上搜索 NSCTF，可以看到：



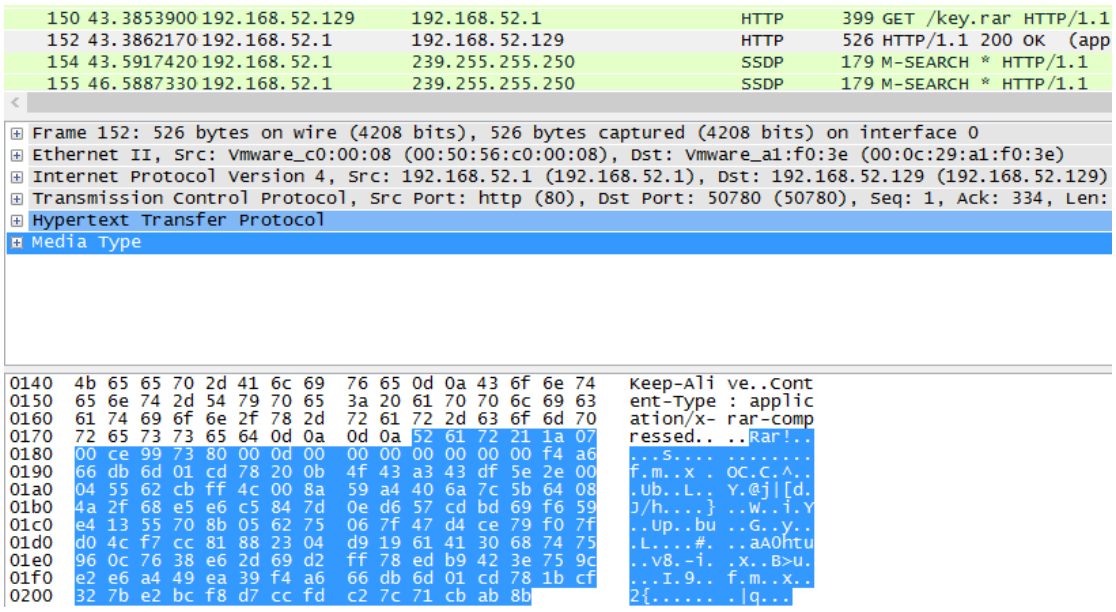
然后解 md5 得到 flag：
NSCTF_nsfocus666

Misc250 WireShark

小绿在学习了wireshark后，在局域网内抓到了室友下载的小东东0.0
你能帮小绿找到吗？

sniffer.pcapng

先过滤 HTTP 包，可以得到 key.rar。



然后翻到了一个 html 文件，dump 出来是这样的：

KEY

密码是nsfocus+5位数字

key

然后就是暴力破解了……最后得到的 flag：

NCTF_R4r_Cr4ck

Misc400 小绿的女神

小绿女神的生日是2月8日，小绿想给她的卡里冲到208元，你能帮他吗？

刷卡机器地址为：

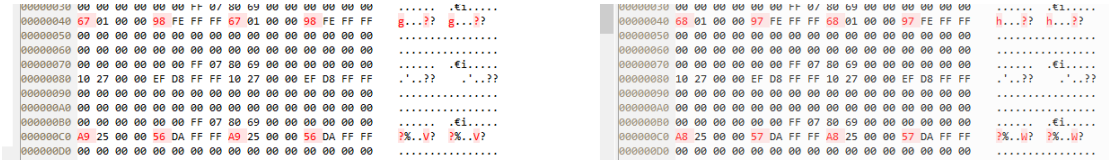
http://www.nsctf.net:8002/fa81bb665474f11c025b5355582af315/misc/

tips:

查询余额时为208即可

card

这里首先把原始的卡刷一下，对比下不同的字节：



可以看到在 0x40 和 0xc0 那两行有改变，可以发现 0xc0-0xc3 表示当前卡的余额，然后 0xc4-0xc7 是 0xFFFFFFFF 减去余额。而 0x40-0x43 处是 0x80-0x83 减去卡的余额。

这里构造 208 的时候需要注意，中间那一行的总数要改成 300，最开始是 100。然后依次构造第一行和第三行的数据，可以得到：

本题 flag：NSCTF_RfID_Cr4ck

Web100 Be careful

粗心的小绿

http://www.nsctf.net:8002/fa81bb665474f11c025b5355582af315/web/01

这个 web 目录下存在 index.php，然后抓包发现 flag：

```
<html><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>NSCTF</title>
</head>
<body alink="#007000" background="../images/dot.gif" bgcolor="#000000" link="gold" text="#008000"
vlink="#00c000">
<center>
<br><br>
<center>
<h1>□□□□□□□</h1>
<script>
window.location.href="index.html";
</script>
</center>
<br>
<br>
<br>
<!--flag:{NSCTF_1E72F25BA71580D7D7DDBD25ACF4A8F3}-->
</html>
```

Flag：NSCTF_1E72F25BA71580D7D7DDBD25ACF4A8F3

Web100 Where are you come from

你是谁

从哪来

到哪去

http://www.nsctf.net:8002/fa81bb665474f11c025b5355582af315/web/02/

这题也是……从题目提示肯定考点在 HTTP 头，需要把 X-Forwarded-For 改成题目的 ip，把 Referer 改成官网，不能有子目录，这样就得到了 base64 的 Flag：

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.152 Safari/537.36
Referer: http://www.nsctf.net/
X-Forwarded-For: 101.200.73.168
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: session=97793663-b877-4701-a17a-114edf4c7bfa
```

Response

Raw Headers Hex HTML Render

```
Content-Type: text/html

<html><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>NSCTF</title>
</head>
<body alink="#007000" background="../images/dot.gif" bgcolor="#000000" link="gold" text="#008000" vlink="#00c000">
<center>Wm14aFp6cDdUbE5EVkVaZk5EZzRZamRoTW1SalkyUXdNbUUzTXpReE5qVmpNemxpWVRRMU1UZGtZbU45</center>
</html>
```

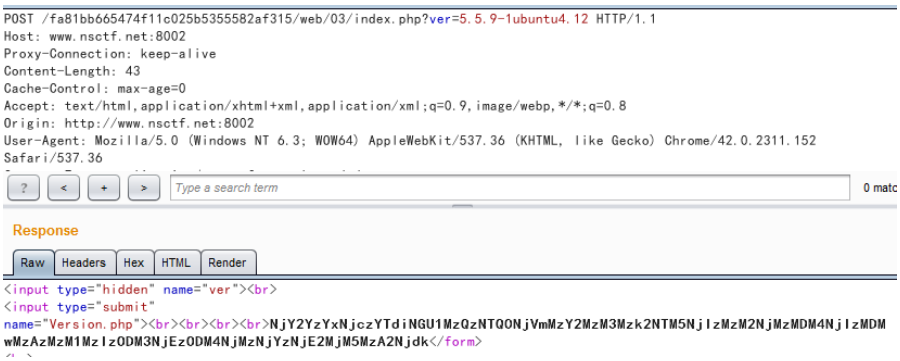
本题 Flag：NSCTF_488b7a2dccd02a734165c39ba4517dbc

Web100 Version

http://www.nsctf.net:8002/fa81bb665474f11c025b5355582af315/web/03/

官方给了提示是填写 PHP 的版本号，并且不要使用 POST 方法，所以正确的方法是把 ver

变量用 GET 方法传过去：

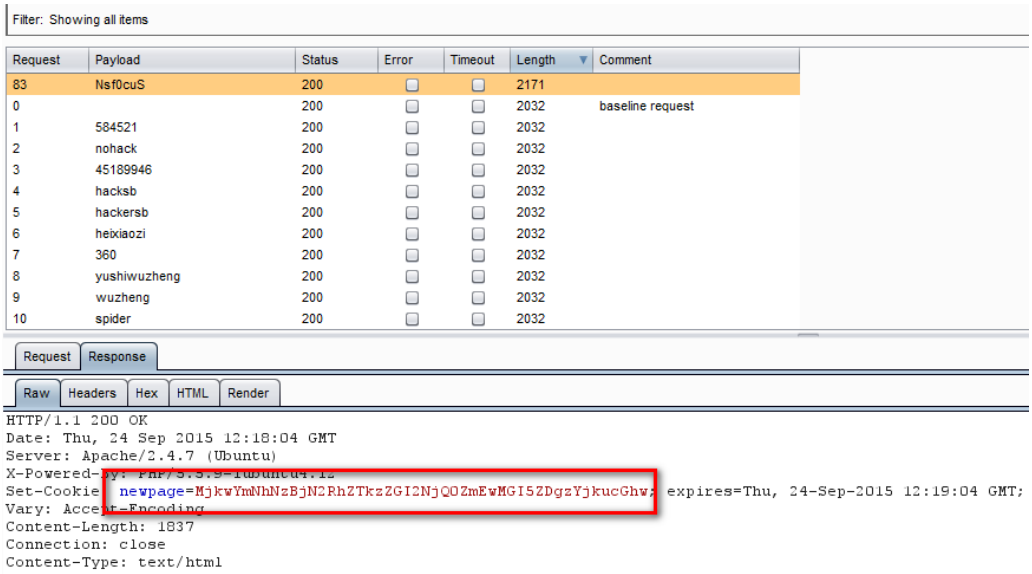


Base64、hex2char 解密后得到本题 flag：NSCTF_6c79e9b36c08b00035287a88c6cab90f

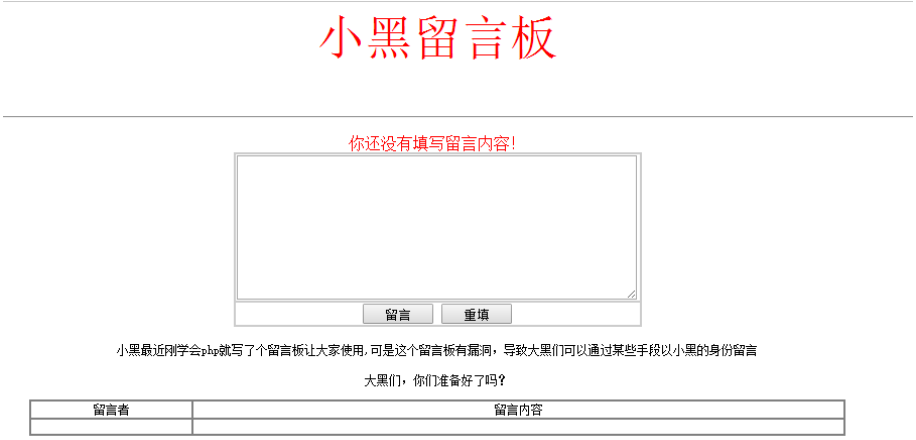
Web150 Brute force

http://www.nsctf.net:8002/fa81bb665474f11c025b5355582af315/web/04/

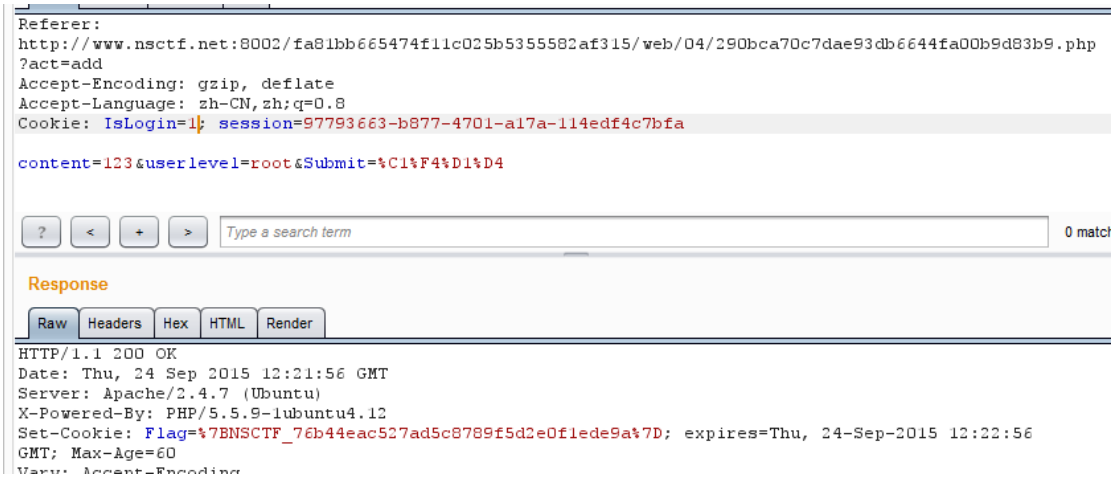
右键源代码拿到提示 password.txt，然后开始爆破：



解密之后，进到万恶的留言板：



留言抓包，发现 cookie 里面有个 Islogin 变量，POST 数据有个 userlevel 变量，需要分别修改为 1 和 root（为啥是 root 不是 admin，我并不知道……）



然后得到本题目的 flag：NSCTF_76b44eac527ad5c8789f5d2e0f1ede9a

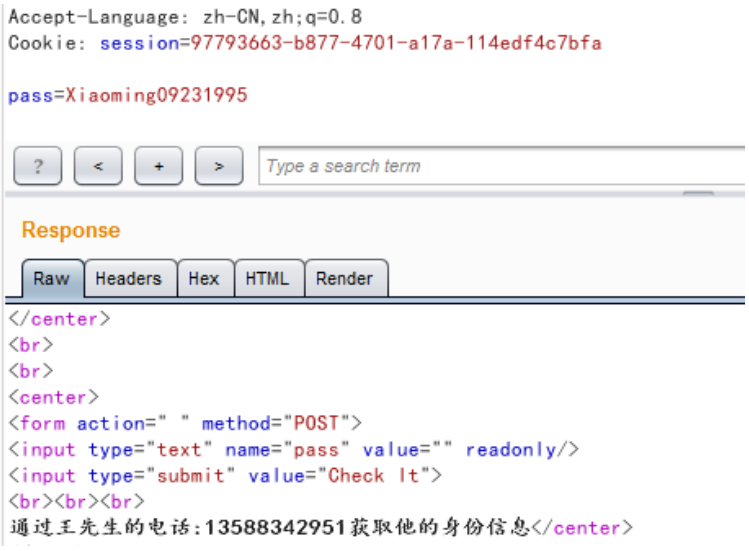
Web150 social engeer

http://www.nsctf.net:8002/fa81bb665474f11c025b5355582af315/web/07/

这题首先需要根据主办方的提示（生日和姓名），生成对应的字典，这里写了个脚本：

```
name = ['xiaoming', 'Xiaoming', 'XiaoMing', 'xiaoMing', 'Xming', 'XMing', 'xMing
birth = ['1995', '09', '9', '23', '199509', '9509', '19959', '959', '19950923',

f = open('dir_s.txt', 'w')

for n in name:
    for b in birth:
        for b2 in birth:
            f.write(b2+n+b+'\n')
            f.write(b2+b+n+'\n')
            f.write(n+b2+b+'\n')
```

爆破得到密码为：Xiaoming09231995



然后搜索之前泄露的某酒店会员数据社工库，可以得到王先生的个人信息：

```
王伟,,,ID,341125198312248 75X,M,19831224,-,,F,,,,,,,,,13588342951,,,,,,,,,,0,20
13-1-14 9:30:18,20050105
```

再次提交身份证号码作为密钥，得到 Flag：

本题 Flag：NSCTF_3ad65730a8f203a5ab861169e9547f6

Web200 Javascript

http://www.nsctf.net:8002/fa81bb665474f11c025b5355582af315/web/06/

小绿不懂javascript，你能帮助他吗？

右键查看源代码，然后点进去 check.js，把混淆之后的 js 代码进行解密：

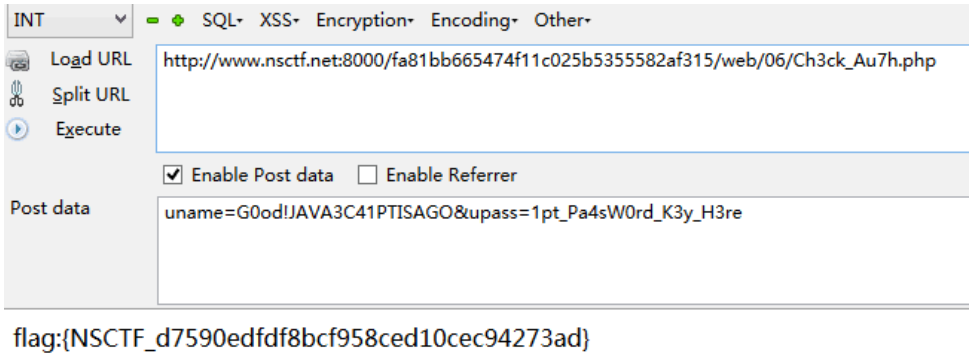
http://tool.chinaz.com/js.aspx?qq-pf-to=pcqq.c2c

之后得到可以看的源码：

```
var strKey1 = "JaVa3C41ptIsAGo0DStAff";
var strKey2 = "CaNUknOWThIsK3y";
var strKey3 = String.fromCharCode(71, 48, 111, 100, 33);
if (uname == (strKey3 + (((strKey1.toLowerCase()).substring(0, strKey1.indexOf("0")) + strKey2.substring(2, 6)).toUpperCase()).substring(0, 15))) {
    var strKey4 = 'Java_Scr1pt_Pa4sW0rd_K3y_H3re';
    if (upass == (strKey4.substring(strKey4.indexOf('1', 5), strKey4.length - strKey4.indexOf('_') + 5))) {
        alert('Login Success!');
        document.getElementById('key').innerHTML = unescape("%3Cfont%20color%3D%22%23000%22%3Ea2V5X0NoM2NrXy50eHQ=%3C/font%3E");
    } else {
        alert('Password Error!');
    }
} else {
    alert('Login Failed!');
}
```

解 url 编码和 base64 得到：key_Ch3ck_.txt，提示使用 Ch3ck_Au7h.php。

用 firebug 解出对应的 username 和 password，然后登录：



flag:{NSCTF_d7590edfdf8bcf958ced10cec94273ad}

得到 Flag：NSCTF_d7590edfdf8bcf958ced10cec94273ad

Web200 lFI

http://www.nsctf.net:8001/fa81bb665474f11c025b5355582af315/web/08/

根据标题可知，考察点是 PHP 本地文件包含漏洞，参考：

https://www.baidu.com/link?url=AHeX86n3AFmTq5u92IsEId8O2tsMPmRg7XlpOml_35hz-5yYKkwqEC1EuUJy9AlH&wd=&eqid=f1c90a5100020470000000035603ba7b

填入 php://filter/read=convert.base64-encode/resource=index.php ，可以读到 base64 之后的 index.php 文件：

```
77u/PGh0bWw+PGhlYWQ+PG1ldGEgaHR0cC1lcXVpdj0iQ29udGVudC1UeXBlIiBjb250ZW50PSJ0ZXh0L2h0bWw7IGNoYXJzZXQ9dX
RmLTgiPg0KPHRpdGxlPkxGSTwvdGl0bGU+DQo8L2hlYWQ+DQo8Ym9keSBhbGluaz0iIzAwNzAwMCIgYmFja2dyb3VuZD0iLi4vaW1h
Z2VzL2RvdC5naWYiIGJnY29sb3I9IiMwMDAwMDAiIGxpbms9ImdvbGQiIHRleHQ9IiMwMDgwMDAiIHZsaW5rPSIjMDBjMDAwIj4NCj
xicj4NCjxicj4NCjxicj4NCjxjZW50ZXI+DQo8aGVhZD48aDE+6L+Z6YeM5LuA5LmI6Y095rKh5pyJfjwvaDE+PC9oZWFkPjxicj4N
Cjxicj4NCjxicj48YnI+DQo8Zm9ybSBtZXRob2Q9InBvc3QiIGFjdGlvbj0iIyI+DQogPGlucHV0IHR5cGU9InRleHQiIG5hbWU9Im
ZpbGUiIHZhbHVlPSIiLz4NCiA8aW5wdXQgdHlwZT0ic3VibWl0IiBuYW1lPSJzdWJtaXQiIHZhbHVlPSLmj5DkuqQiLz4NCjwvZm9y
WydmaWxlJ10pKXsNCg0KICAJJGZpbGUgPSAkX1BPU1RbJ2ZpbGUnXTsNCg0KICAJJG1ldGhvZCA9IGV4cGxvZGUoIj0iLCAkZmlsZS
k7DQoNCiAgCWlmKCAoJG1ldGhvZFswXSA9PSAic3Ghw0i8vZmlsdGVyL3JlYWQiKSAmJiAoJG1ldGhvZFsyXSA9PSAiaW5kZXguc Ghw
IikgKXsNCiAgCQlpbmNsdWRlKCRmaWxlKTsNCiAgICAgICAgZXhpdCgp0w0KICAgIH1lbHNlew0KICAgIAlleGl0KCdlcnJvciBmaW
xlIG9yIGVycm9yIG1ldGhvZCcp0w0KICAgIH0NCiAgfQ0KfQ0KLy9mbGFn0nt0UONURl85YmFjN2E2ZTI40WJm0DllZTAwNjFiZDBh
YmRl+
```

解密之后得到 Flag：

NSCTF_9bac7a6e289bf89ee0061bd0abdef0ab

Web200 Decode

按照 php 代码，将密文先进行 rot13 一下解密，再倒叙，再 base64。然后对字符循环减 1、再倒叙可以得到 flag：

NSCTF_b73d5adfb819c64603d7237fa0d52977

Web200 Decode

http://www.nsctf.net:8000/fa81bb665474f11c025b5355582af315/web/09/

据说小绿经常喜欢在Linux下做开发工作。

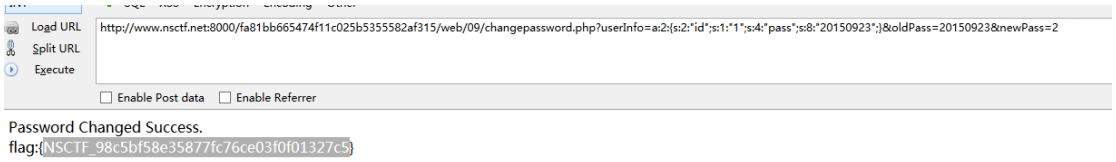
访问.index.php.swp 可以看到部分源码：

```
$userInfo = @unserialize($_REQUEST['userInfo']);

$query = 'SELECT * FROM users WHERE id = \''.clear($userInfo['id']).'\' AND password = \''.clear($userInfo['pass']).'\';';

$result = mysql_query($query);
if(!$result || mysql_num_rows($result) < 1){
        die('Invalid password!');
}

$row = mysql_fetch_assoc($result);
foreach($row as $key => $value){
        $userInfo[$key] = $value;
}

$oldPass = @$_REQUEST['oldPass'];
$newPass = @$_REQUEST['newPass'];
if($oldPass == $userInfo['password']){
        $userInfo['password'] = $newPass;
        $query = 'UPDATE users SET pass = \''.clear($newPass).'\' WHERE id = \''.clear($userInfo['id']).'\';';
        mysql_query($query);
        echo 'Password Changed Success.<br>';
}
else{
        echo 'Invalid old password entered.';
}
```

然后 id 和 pass 是在 index.php 的返回包中抓到的：

```
HTTP/1.1 200 OK
Date: Fri, 25 Sep 2015 11:13:06 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.12
Set-Cookie: pass=ZDI4ZGY3NDE3OWNjMzFmYjEyMjRhMDMyZTQyOWQOMGY%3D; expires=Fri, 25-Sep-2015 11:14:06 GMT; Max-Age=60
Set-Cookie: id=3; expires=Fri, 25-Sep-2015 11:14:06 GMT; Max-Age=60
Vary: Accept-Encoding
Content-Length: 387
Content-Type: text/html

<html><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
```

解得 pass=20150923，这里有个坑，id 需要改成 1，才能过第一个判断点。另一个坑点是 POST 过去是没用的，最后构造数据：



本题 Flag：NSCTF_98c5bf58e35877fc76ce03f0f01327c5

Web200 Variable cover

http://www.nsctf.net:8000/fa81bb665474f11c025b5355582af315/web/10/

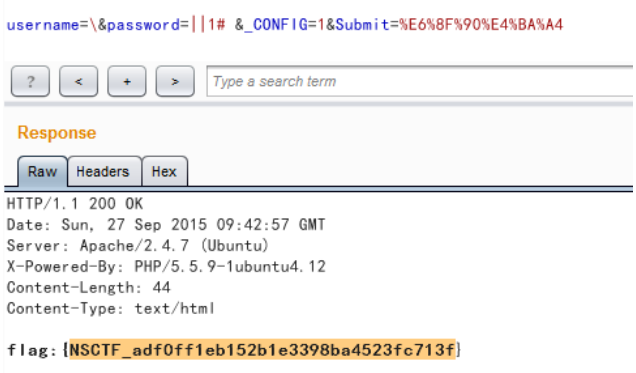
小绿总是偷懒，就是因为这一点，Boss不给他涨工资。

根据主办方的提示，体面是在暗示 index.php.文件，看到变量覆盖源码：

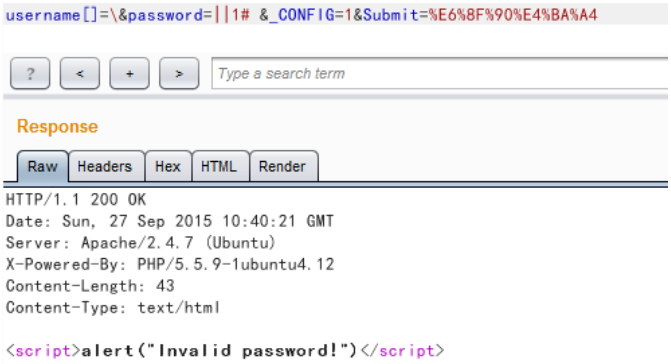
```
$_CONFIG['Security']=true;

foreach(array('_GET','_POST','_REQUEST','_COOKIE') as $method){
     foreach($$method as $key=>$value){
          unset($$key);
     }
}

function clear($string){
  //构橱嗽构团护镊芥暄锅
}

$username = isset($_REQUEST['username']) ? clear($_REQUEST['username']) : die('Please enter in a username.');
$password = isset($_REQUEST['password']) ? clear($_REQUEST['password']) : die('Please enter in a password.');

if($_CONFIG['Security']){
     $username=preg_replace('#[^a-z0-9_-]#i','',$username);
     $password=preg_replace('#[^a-z0-9_-]#i','',$password);

}

if (is_array($username)){
  foreach ($username as $key => $value) {
    $username[$key] = $value;
  }
}

$query='SELECT * FROM users WHERE user=\''.$username[0].'\' AND password=\''.$password.'\';';

$result=mysql_query($query);

if($result && mysql_num_rows($result) > 1){
  echo('Success ! ');
  exit();
}
```

首先需要绕过的是一个正则，由$_CONFIG[‘Security’]控制，在对其赋值之后，有一段 unset 语句，所以只需要在传参的时候，传入_CONFIG，就可以 unset 掉全局变量$_CONFIG 数组，使得正则无效。

然后就是绕过 clean 函数，要想查询记录数>1，就必须截断单引号，最后尝试得到的正确姿势：



而如果是以 username[0]传入就会过滤：



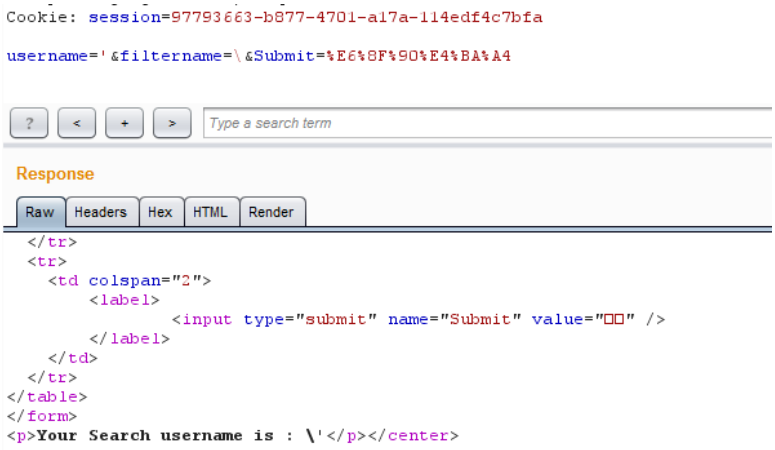
所以得到最终 flag：NSCTF_adf0ff1eb152b1e3398ba4523fc713f

Web350 SQLI

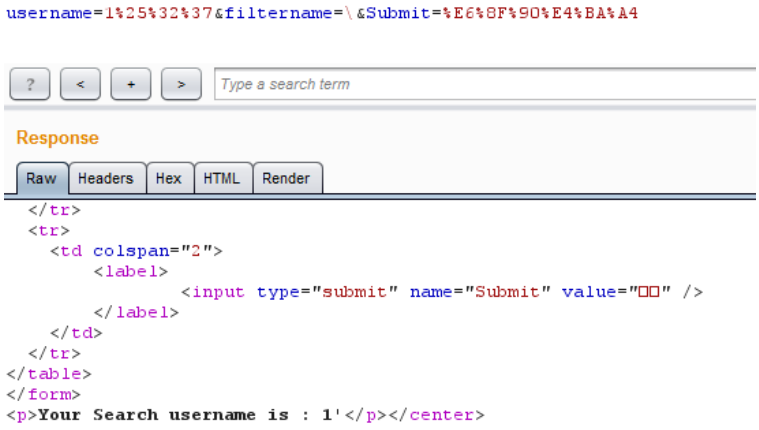
http://www.nsctf.net:8000/fa81bb665474f11c025b5355582af315/web/12/

这个题目可以控制的 POST 参数有两个：username 和 filtername，刚开始一直没理解第二个参数是干嘛的。

直接给 username 传个’会被反斜线：

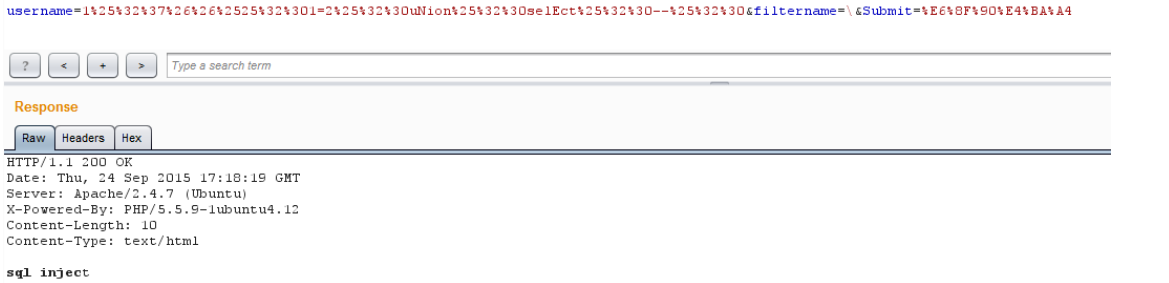


然后偶然中发现，用 URL 两次编码就可以绕过了：

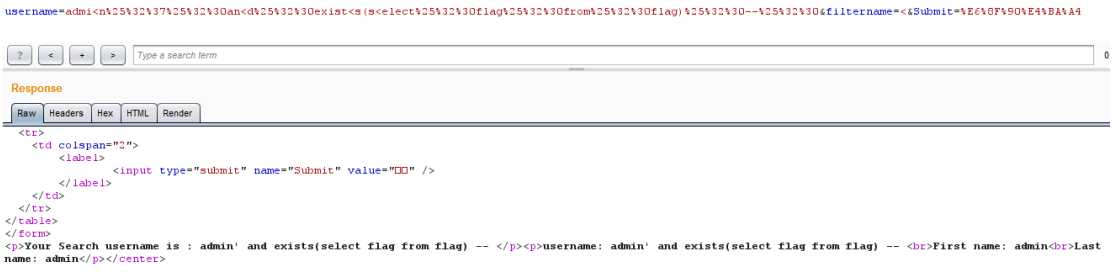


然后先构造一个可以出数据的 payload：

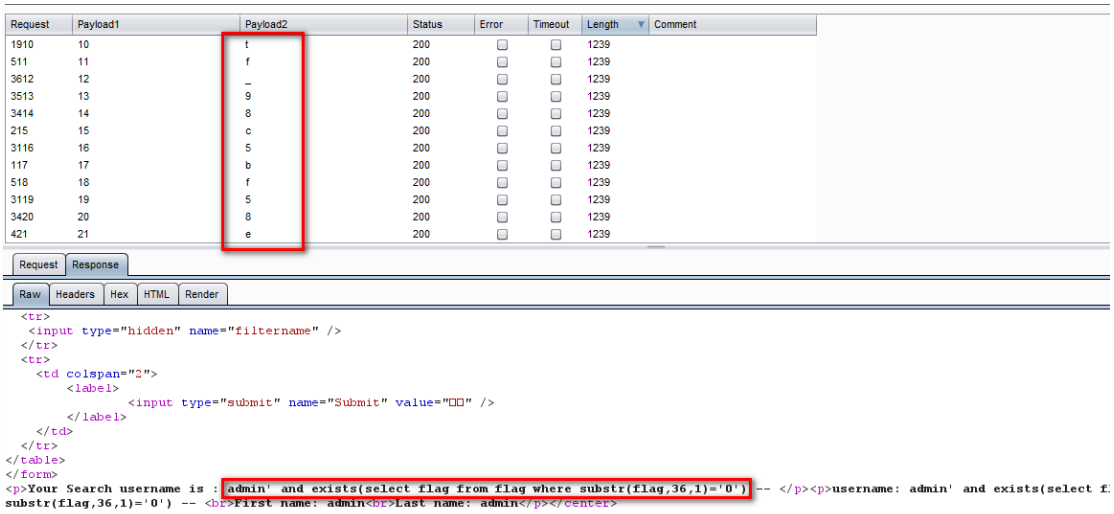
然后尝试注入的时候就被拦截了 = =：



郁闷中翻了翻宫老师写的 SSCTF 题解，提到了<>被过滤后绕过对关键字的过滤，于是明白第二个参数是帮助绕 WAF 的……



猜到表名和列名后，用 BOOL 型盲注 payload，利用 burpsuite 跑一下：



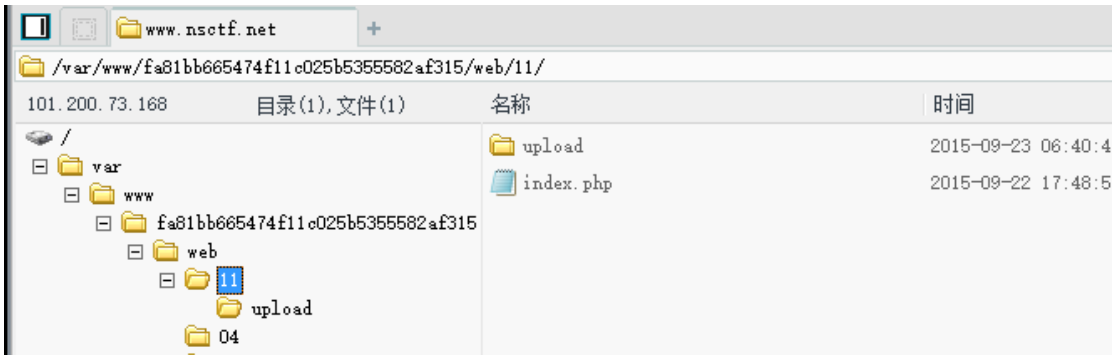
最后跑出来 Flag：nsctf_98c5bf58e35877fc76ce03f0f01327c5

（比较蠢的是，最开始没发现 flag 表，把 user 表内容整个拖了一遍，QAQ……以及后来发现貌似可以 Union 注入……）

Web400 File Upload

http://www.nsctf.net:8001/fa81bb665474f11c025b5355582af315/web/11/

上传.php，发现被重命名，这里先是对 ph*形式进行了 fuzz，写入<?php phpinfo()?>，发现为 pht 的时候，竟然解析了，于是：



然后就这样拿到了 flag：NSCTF_8f0fc74ddf786103ed56d20af3bf2697

后来上交了 shell 之后，题目略微有了修改，重新 fuzz，发现传.php5 的时候，会出现：

好吧，开两个脚本，一个写 php5 一个访问，果然得到了想要的：

```
HTTP/1.1 200 OK
Date: Thu, 24 Sep 2015 12:50:12 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.12
Content-Length: 45
Connection: close
Content-Type: text/html

flag:{NSCTF_8f0fc74ddf786103ed56d20af3bf2697}
```

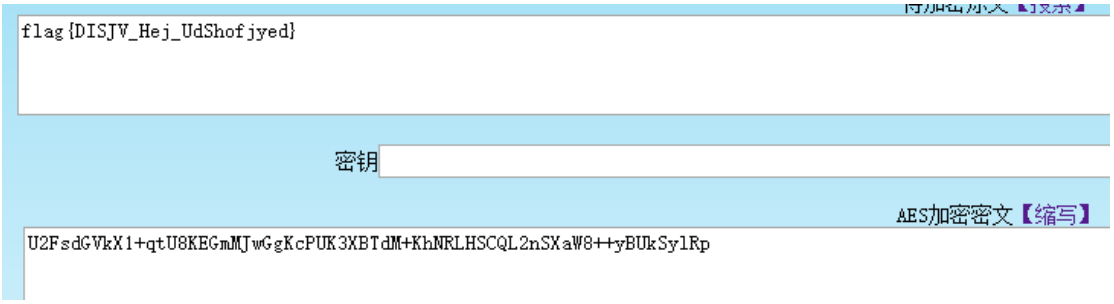
当然也可以 getshell 啦，不过题目后来迁移了……没什么用了……

Crypto50 神奇的字符串

小绿在学习了抓包技术后，在局域网中抓到了这样一串神秘的字符串：
U2FsdGVkX1+qtU8KEGmMJwGgKcPUK3XBTdM+KhNRLHSCQL2nSXaW8++yBUkSylRp
请帮帮小绿

搜索在线 AES 解密：

http://www.idgui.com/AES/?|m||m|U2FsdGVkX1+qtU8KEGmMJwGgKcPUK3XBTdM+KhNRLHSCQL2nSXaW8++yBUkSylRp



看来还需要进行移位：

得到最后的 Flag：

NSCTF_Rot_EnCryption

Crypto100 神奇的图片

小绿从网上找到一张神奇的图片
据说图片中有好东西
你能找到它吗？

oddpic.jpg

文件尾巴被加了一张图片，foremost 提取出来就有 flag 了：

falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

呃，貌似发现了什么……

本题 Flag：NSCTF_e6532a34928a3d1dadd0b049d5a3cc57

Crypto200 神秘的图片+10086

小绿在黑进一台服务器后，在root文件夹下找到了一张图片，据说图片中有root的密码您能帮他找到吗？

newnewnew.jpg

呃，stegsolve 看出一个二维码：

Dump 下来写脚本发色一下，扫到 F lag：

本题 Flag：NSCTF_Qr_C0De

本次线上赛，给我带来最大收获的题目是逆向第四题 python 字节码的逆向和分析，花一下午把没有接触过的事情弄懂是一件很有成就感的事情。