Web题目

原创

耀光少年 于 2020-01-10 15:21:07 发布 1209 收藏 5

分类专栏： CGCTF

本文链接：https://blog.csdn.net/qq_44766557/article/details/103925148

签到题

题目地址

这道题就是入门题，很简单

打开之后就是

---

key在哪里?

然后就是F12大法

```
body> == $0
<a style="display:none">nctf{flag_admiaanaaaaaaaaaa}</a>
"

    key在哪里?
"
```

得到flag。

php decode

打开之后给的是一个php代码片段

php decode

Web 25pt

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+eoGmlgOfd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA=="));
?>
```


看完之后应该是一个base64加密和解密
可以把这个那个eval改为echo，然后把代码输入解释器中，得到flag。

```
<?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+eoGmlgOfd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA=="));
?>
```

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


对于这种gzinflate(base64_decode($ZzvSWE))，是常见的压缩编码和解码代码方法。

签到2

题目地址

打开之后是这样的页面

> 尚未登录或口令错误
>
> 输入框：
> 请输入口令：zhimakaimen 开门

开始还是常见的f12大法，这道题应该是按照他给的口令输入，但是输入进去发现不能输入完毕，应该是长度被限制了，改一下长度就行。

> 尚未登录或口令错误
>
> 输入框：
> 请输入口令：zhimakaimen 开门

改成20输进去，开门

> flag is:nctf{follow_me_to_exploit}
>
> 输入框：
> 请输入口令：zhimakaimen 开门

得到flag。

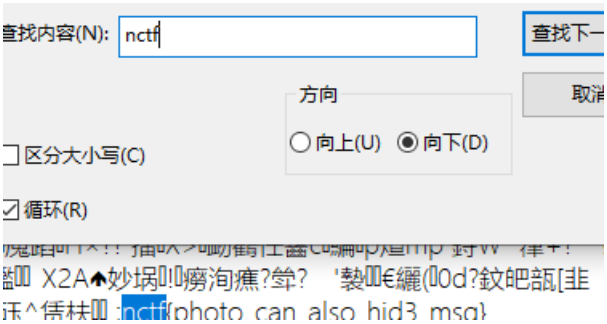
也是很简单的。

这题不是WEB

题目地址

这道题还是有点坑的。开始试了f12，还用burpsuite抓包看了看，但还是没有。最后看了一下网上的writeup，发现是那个图片的问题。

另存为之后，查找nctf得到flag。



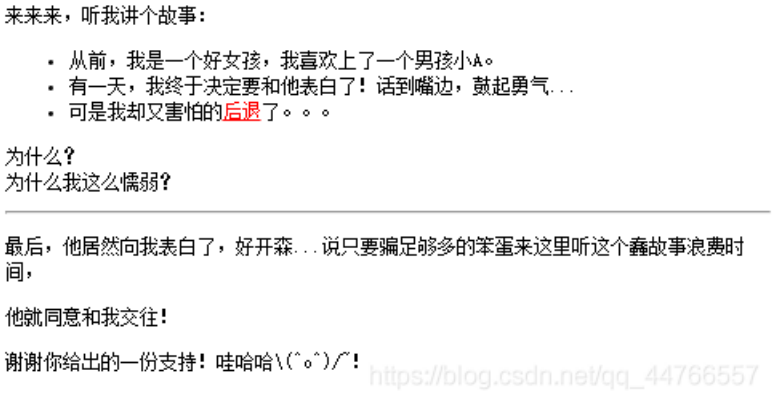
层层递进

题目地址

这算是第一个看起来比较麻烦的一个题了，因为打开网页之后没有丝毫的思路。按f12也不知道找啥，出来一堆代码。没办法，看一下别人做的吧。

看完之后也是真的对应题目的名字，层层递进，一层一层向里进。下面为解题思路。

一切还需从f12大法开始，打开网页按f12，里面有一个很陌生的标签，iframe。看过简介也还是有点头蒙，反正就是这里就对了。
可以发现有两个iframe标签，其中src属性，第二个比较正常，第一个就比较反常，然后把它复制下来，去搜索。
这样就到了第一层，同样的找iframe标签，去搜索，到第二层，继续这样找下去。最后找到404.html这个网页，得到这样的一个页面。


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^)/~！

里面有个后退，是红色的，点完的确后退了，返现这是假的。还是f12，会发现里面有js代码，然后顺着看下来，就得到flag。

```
<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>
```

这道题感觉好像是进入了web的大门，没有想的那么简单了，以后就得多想想看看了。

单身二十年

题目地址
这道题友好了许多。
打开网页是

_到这里找key__

这样，是一个链接，打开只有换到另一个页面

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

就只有这么多东西，按f12也是没有什么，这时候就要请出web神器了，burpsuite，进行抓包，按照题目意思，感觉是要不断刷新，然后一直刷新，刷了半天一直木得反应，好吧，有点天真。进入下个页面抓包，然后运行，结果，哈哈哈，得到flag。

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

我感觉中间应该是很快跳转到下个页面了，这时候抓包就很重要了。
此题结束。

md5 collision

题目地址
题目给的是php代码

```
$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";}
```


看完之后知道是md5的碰撞，因为以前做过，传入一个参数让两个md5之后的开头为0e就行。实际是php弱类型的了解。
php关于==号是这样处理的，如果一边是整型，另一边也需要是整型。
举一个反面的例子
1e1和1e2
1e1 == 1e2 这个结果是对是错？
这里
1e1=1*10^1=10
1e2=1*10^2=100
所以1e1 == 1e2这是false，但是
100 == 1e2 这是true，为什么1e2先转为整型，是100
注意，对于e是指幂次。而其他26字符并不具有此能力。

文件包含

题目地址

以前做过类似的，但老是忘，这次稍微总结一下。

借用别人的整理的吧

文件包含总结

这道题通过

php://filter协议读取index文件

> payload:http://4.chinalover.sinaapp.com/web7/index.php?file=php://filter/read=convert.base64-encode/resource=./index.php
> 解码之后得到源码

```
<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($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
  echo "Oh no!";
  exit();
 }
 include($file);
//flag:nctf{edulcni_elif_lacol_si_siht}

?>
</html>
```

得到flag

AAencode

[题目地址](#)

打开之后是这样的乱码，

是js编码，之后找到了charset这个插件，把编码格式变成了utf-8，

```
ﾟωﾟﾉ= /｀ｍ´）ﾉ ~┻━┻   //*´∇｀*/ ['_']; o=(ﾟｰﾟ)  =_=3; c=(ﾟΘﾟ) =(ﾟｰﾟ)-(ﾟｰﾟ); (ﾟДﾟ) =(ﾟΘﾟ)= (o^_^o)/ (o^_^o);(ﾟДﾟ)={ﾟΘﾟ: '_' ,ﾟωﾟﾉ : ((ﾟωﾟﾉ==3) +'_') [ﾟΘﾟ] ,ﾟｰﾟﾉ :(ﾟωﾟﾉ+ '_')[o^_^o -(ﾟΘﾟ)] ,ﾟДﾟﾉ:((ﾟｰﾟ==3) +'_')[ﾟｰﾟ] }; (ﾟДﾟ) [ﾟΘﾟ] =((ﾟωﾟﾉ==3) +'_') [c^_^o];(ﾟДﾟ) ['c'] = ((ﾟДﾟ)+'_') [ (ﾟｰﾟ)+(ﾟｰﾟ)-(ﾟΘﾟ) ];(ﾟДﾟ) ['o'] = ((ﾟДﾟ)+'_') [ﾟΘﾟ];(ﾟoﾟ)=(ﾟДﾟ) ['c']+(ﾟДﾟ) ['o']+(ﾟωﾟﾉ +'_')[ﾟΘﾟ]+ ((ﾟωﾟﾉ==3) +'_') [ﾟｰﾟ] + ((ﾟДﾟ) +'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ ((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [(ﾟｰﾟ) - (ﾟΘﾟ)]+(ﾟДﾟ) ['c']+((ﾟДﾟ)+'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ (ﾟДﾟ) ['o']+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ];(ﾟДﾟ) ['_'] =(o^_^o) [ﾟoﾟ] [ﾟoﾟ];(ﾟεﾟ)=((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟДﾟ) .ﾟДﾟﾉ+((ﾟДﾟ)+'_') [(ﾟｰﾟ) + (ﾟｰﾟ)]+((ﾟｰﾟ==3) +'_') [o^_^o -ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟωﾟﾉ +'_') [ﾟΘﾟ]; (ﾟｰﾟ)+=(ﾟΘﾟ); (ﾟДﾟ)[ﾟεﾟ]='\\'; (ﾟДﾟ).ﾟΘﾟﾉ=(ﾟДﾟ+ ﾟｰﾟ)[o^_^o -(ﾟΘﾟ)];(oﾟｰﾟo)=(ﾟωﾟﾉ +'_')[c^_^o];(ﾟДﾟ) [ﾟoﾟ]='\"';(ﾟДﾟ) ['_'] ( (ﾟДﾟ) ['_'] (ﾟεﾟ+(ﾟДﾟ)[ﾟoﾟ]+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ ((o^_^o) +(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (o^_^o))+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ ((o^_^o) +(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (o^_^o)+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ ((o^_^o) +(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (ﾟｰﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (o^_^o))+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+ ((o^_^o) - (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟΘﾟ)+ (ﾟДﾟ)[ﾟoﾟ]) (ﾟΘﾟ)) ('_');
```

然后复制到控制台回车就出来了。

单身一百年也没用

[题目地址](#)

这道题和那个单身二十年的一样，很奇怪，不知道为啥出一样的。但还是按照那个方法，抓包就行。

Download!

这个打不开网页目前没有思路。找了一下writeup，发现这个题应该是炸了，没法写。

COOKIE

[题目地址](#)

这道题真的是有点怎么说，知道怎么做，但不知道具体怎么实施。

这道题很明显就是让改rookie的，但是用burpsuite我好像就是改不了，找了好多方法，最后发现很简单，之间在抓包那里改就行，把rookie改为1，flag就出来了。

此题结束。

MYSQL

[题目地址](#)

进去后是

> Do you know robots.txt?
> [百度百科](#)

点百度百科就直接进到robots协议了，明显不太对，之后在链接后面加了robots.txt
进入下面这个页面，上面的不知道是什么乱码了，下面是PHP代码。

```
鍒□ぉ寮€濂冿紝flag涓嶅湪杩欙紝杩欓噷鏈夊嵆欢鎶勭敓闅旇緟鍔熺畝浜嗚紵
鍦－TF姣旇禌涓□紝杩欓噷鏈夊嵆欢寰€寰€瀛樺湪鐫€鍏堜ず淇℃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]);
  }
}
```

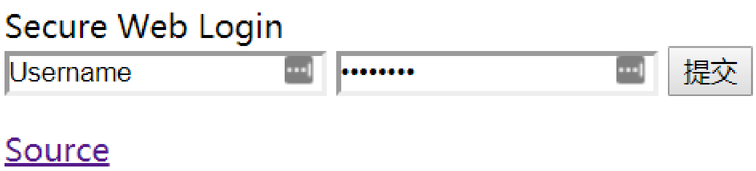
看完应该是让传参的。传一个id的值，就是常见的get传参。然后就是==号问题了。intval函数就是相当于取整了。看完writeup之后，知道就是绕过了，输入浮点数就行，类似于1024.1
最后得到flag。
此题结束。

GBK injection

这是一道没有见过的题目，所以看了看writeup。
通常来说，一个gbk编码的汉字通常占用两个字节，一个utf-8编码汉字，占用三个字节，

SQL注入1

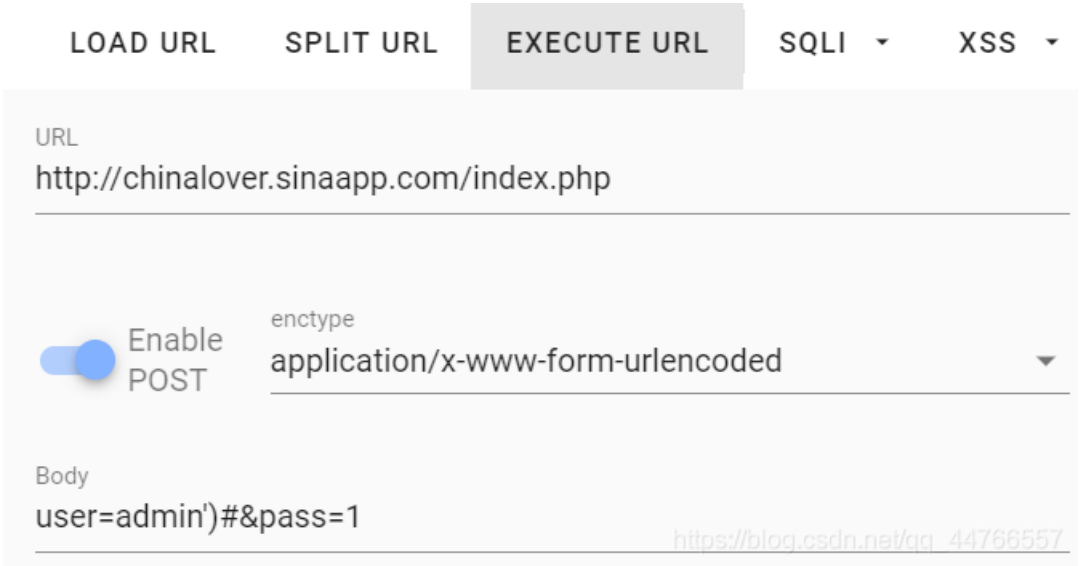
题目地址
打开是这样一个页面，这可能是这sql方面的常见画面，我猜。这算是第一道sql 注入题了。看了看网上的题解，感觉看了几天的sql注入还是有点用的，知道是什么意思。



打开source网页

```
<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>
```

是这样的代码，trim()是**移除字符串两侧的空白字符或其他预定义字符**，然后分析一下，这个应该是只看user的，经过加入注释操作后，得到flag。



/x00

题目地址

打开之后题目是这样

```
  if (isset ($_GET['nctf'])) {  //检测nctf变量是否设置并且不为NULL
      if (@ereg ("^[1-9]+$", $_GET['nctf']) === FALSE)  //ereg(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,否则返回false)，搜索nctf变量匹配的正则，这里的正则是首字母必须匹配到[1-9]，即1-9，+表示匹配前面的表达式1次或多次，就是后面可以匹配[1-9]1次或多次。这里if需要true===False，才能执行下面的elseif语句。注：=== 全等（完全相同） $x === $y 如果 $x 等于 $y，且它们类型相同，则返回 true。
          echo '必须输入数字才行';
      else if (strpos ($_GET['nctf'], '#biubiubiu') !== FALSE)  //strops函数，查找#biubiubiu第一次在nctf变量中出现的位置，存在则返回true，不存在则返回false，这里需要if(true!==False)，才能执行die()函数，输出flag，因此，需要nctf变量中包含#biubiubiu。注：!== 不全等（完全不同） $x !== $y 如果 $x 不等于 $y，或它们类型不相同，则返回 true。
          die('Flag: '.$flag);
      else
          echo '骚年，继续努力吧啊~';
  }
```

是提交表单问题

- @ereg("[1]+”,_GET[‘nctf’]) === FALSE)

^ 这个是匹配输入字符串的开始位置
[标记一个中括号表达式的开始。
[1-9] 表示输入1-9的数字
+ 表示匹配前面的子表达式一次或多次
$ 匹配输入字符串的结尾位置
合起来就是**nctf中的内容必须是数字形式**

- strops（$_GET[‘nctf’],’#biubiubiu’) !== FALSE

strpos() 函数查找字符串在另一字符串中第一次出现的位置.。
所以这句话表达的就是**nctf中必须有#biubiubiu这个字符串**

绕过

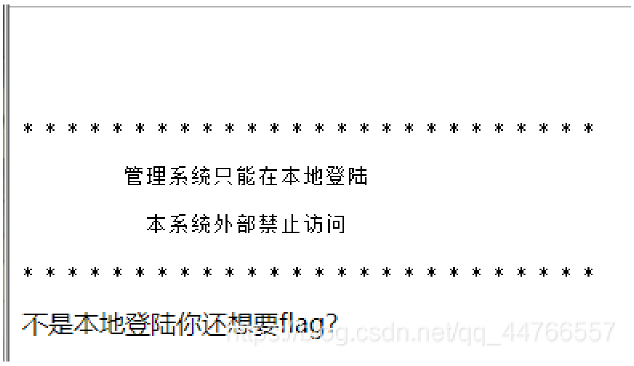
方法一： 这时候就要想如何绕过@ereg函数

> @ereg()函数存在NULL截断漏洞，导致正则过滤被绕过，所以可以用%00来截断正则匹配。

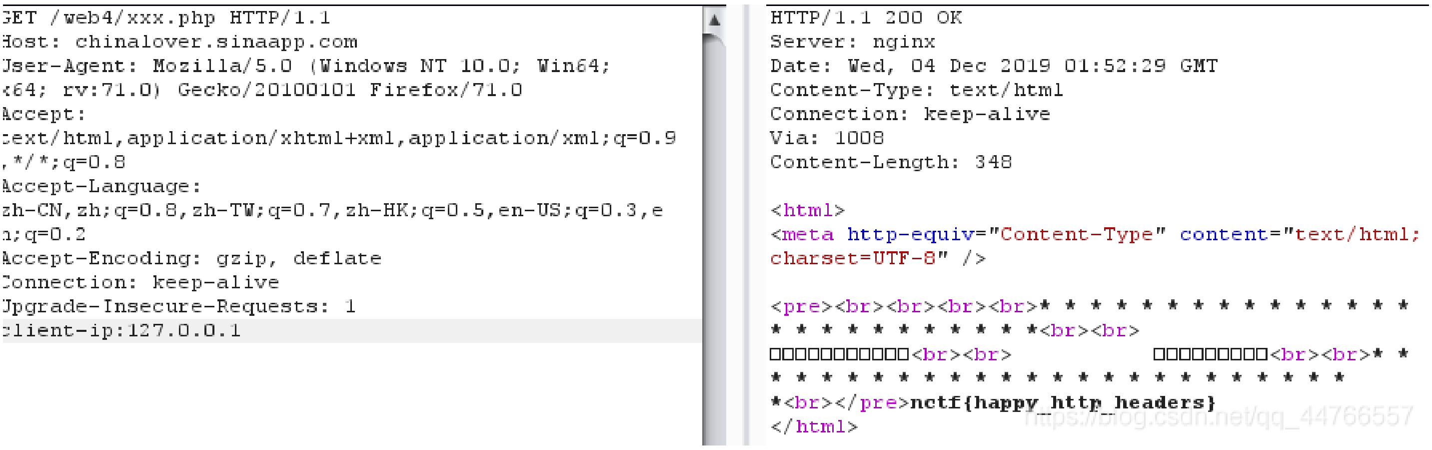
所以可以设置payload：nctf=123%00#biubiubiu，但是输进去却失败。
经过找资料后，知道url中的#后面的字符都会被浏览器结束为位置标识符。这些字符都不会发送到服务器端，需要对#进行url编码
nctf=123%00%23biubiubiu，这样就行了。
方法二： 使用数组形式绕过，payload：nctf[]=123,传入之后ereg是返回NULL，=判断NULL和FALSE，是不相等的。可以进入第二个判断，strpos处理数组时，也是返回NULL，注意这里时！，NULL！==FALSE，条件成立，拿到flag。

伪装者

[题目地址]
打开页面是这样



看完应该是要以本地地址登录才行。用Burpsuite抓包，改ip地址，需要x-forwarded-for或client-ip



得出flag。

Header

这个网页进去错误，可能是网站炸了。

Bypass again

[题目地址]
这道题是php的弱类型。

```
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.';
```

考查的是MD5碰撞，当两个变量的md5值为0ed+类型时，==会认为两边的值都为0，即可满足条件。符合条件的值如下：
md5（‘240610708’) == md5('QNKCDZO')，payload：a=240610708&b=QNKCDZO，提交得到flag。

变量覆盖

[题目地址]
找到代码

```
<?php
include("secret.php");
?>
<html>
  <head>
    <title>The Ducks</title>
    <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-1q8mTJOASx8j1Au+a5WDVnPi2lkFfwwEAa8hDDdjZlpLegxhjVME1fgjWPGmkzs7" crossorigin="anonymous">
    <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.6/js/bootstrap.min.js" integrity="sha384-0mSbJDEHialfmuBBQP6A4Qrprq5OVfW37PRR3j5ELqxss1yVqOtnepnHVP9aJ7xS" crossorigin="anonymous"></script>
  </head>
  <body>
    <div class="container">
      <div class="jumbotron">
        <center>
          <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 } ?>
          <form action="." method="POST">
            <div class="row">
              <div class="col-md-6 col-md-offset-3">
                <div class="row">
                  <div class="col-md-9">
                    <input type="password" class="form-control" name="pass" placeholder="Password" />
                  </div>
                  <div class="col-md-3">
                    <input type="submit" class="btn btn-primary" value="Submit" />
                  </div>
                </div>
              </div>
            </div>
          </form>
        </center>
      </div>
      <p>
        <center>
          source at <a href="source.php" target="_blank">/source.php</a>
        </center>
      </p>
    </div>
  </body>
</html>
```

其中$_SERVER[]函数为
$_SERVER[‘REQUEST_METHOD’] #访问页面时的请求方法。例如：“GET”、“HEAD”，“POST”，“PUT”。

这道题考察的主要是extract（）覆盖漏洞

1.extract()函数介绍

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。

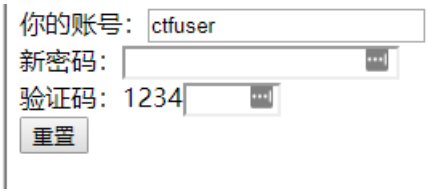
该函数返回成功设置的变量数目。

2.语法

extract(array,extract_rules,prefix)

密码重置

题目地址



这道题应该是有两个小问题。一个是把密码改一下，任意的都行，然后是设置账号，题目给提示是设置admin的密码，所以账号为admin。但是却改不了，这时看一下url栏吗，后面有一串base64编码，解出来是给的账号的base64码，改为admin的base64，然后改密码

最后得出flag。

pass check

题目地址

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

这道题是strcmp函数问题。
这个函数是用于比较字符串的函数

int strcmp (string $str1 , string $str2)
参数 str1第一个字符串。str2第二个字符串。
如果 str1 小于 str2 返回 < 0；
如果 str1 大于 str2 返回 > 0；
如果两者相等，返回 0。

对于这段代码，我们可以利用它的漏洞绕过
只要$_POST['password']是一个数组或者一个object即可

password[]=1.1
即可使得上述代码绕过

1-9 □□