南京邮电大学网络攻防平台——WriteUp(持续更新)

转载

weixin_30572613 于 2018-11-13 17:05:00 发布 51 收藏
文章标签： php 密码学
原文链接：http://www.cnblogs.com/Rasang/p/9953206.html

1.签到题

右键查看源代码直接获得flag

```
<html>
    <title>key在哪里？</title>
    <head>
        <meta http-equiv="content-type" content="text/html;charset=utf-8">
        <a style="display:none">nctf{flag_admiaanaaaaaaaaaaa}</a>
    </head>
    <body>
    key在哪里？
    </body>
</html>
```

2.MD5collision（MD5碰撞）

md5 collision

50

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";}
?>
```

传送门：题目地址

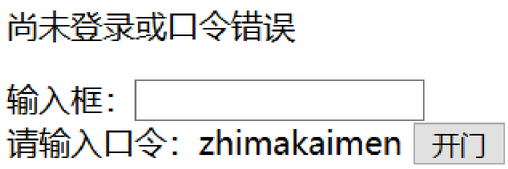
> 观察源码发现md51等于QNKCDZO通过MD5加密的结果，使用在线解密发现结果为***0e830400451993494058024219903391***，猜测这题考察的是php的弱类型，在php中，“===”和“==”是不一样的，“===”会先判断两种字符串的类型是否相等，再比较，而“==”会先将字符串类型转化成相同，再比较，所实际上md51等于0，所以只要传入一个加密后开头也是0e的就可以得到flag

```
nctf{md5_collision_is_easy}
```

php手册

> 当一个字符串欸当作一个数值来取值，其结果和类型如下:如果该字符串没有包含'.','e','E'并且其数值值在整形的范围之内该字符串被当作int来取值，其他所有情况下都被作为float来取值，***该字符串的开始部分决定了它的值，如果该字符串以合法的数值开始，则使用该数值，否则其值为0。***

3.签到题2



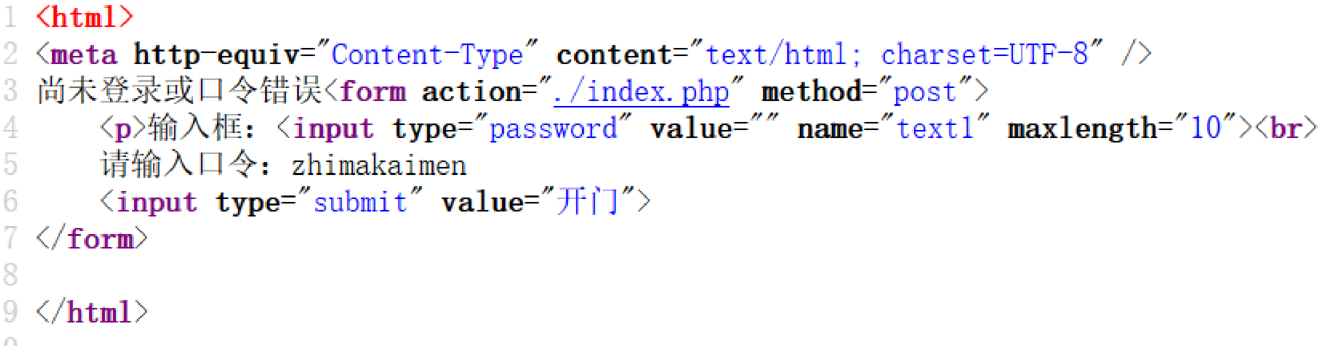
尚未登录或口令错误

输入框：

请输入口令：zhimakaimen

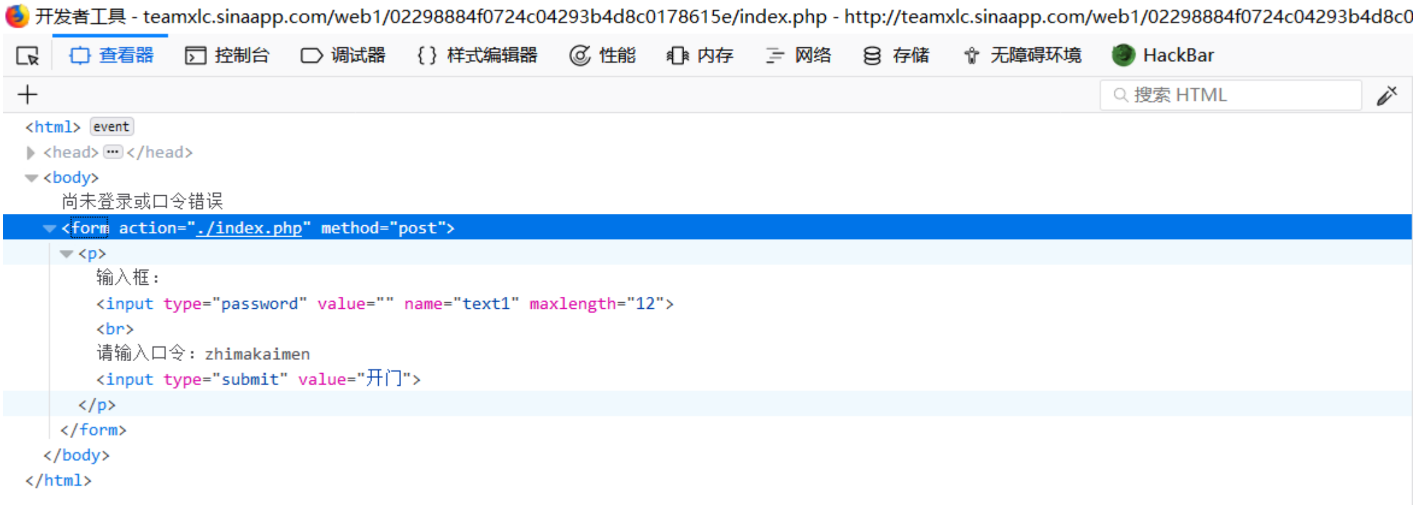
> 复制zhimakaimen发现不对，右击源代码查看发现maxlength被限制在了10,于是直接进入开发者工具，修改maxlength，再次输入密码，得到flag

---



```
<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>
```

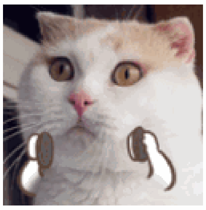


开发者工具 - teamxlc.sinaapp.com/web1/02298884f0724c04293b4d8c0178615e/index.php - http://teamxlc.sinaapp.com/web1/02298884f0724c04293b4d8c0

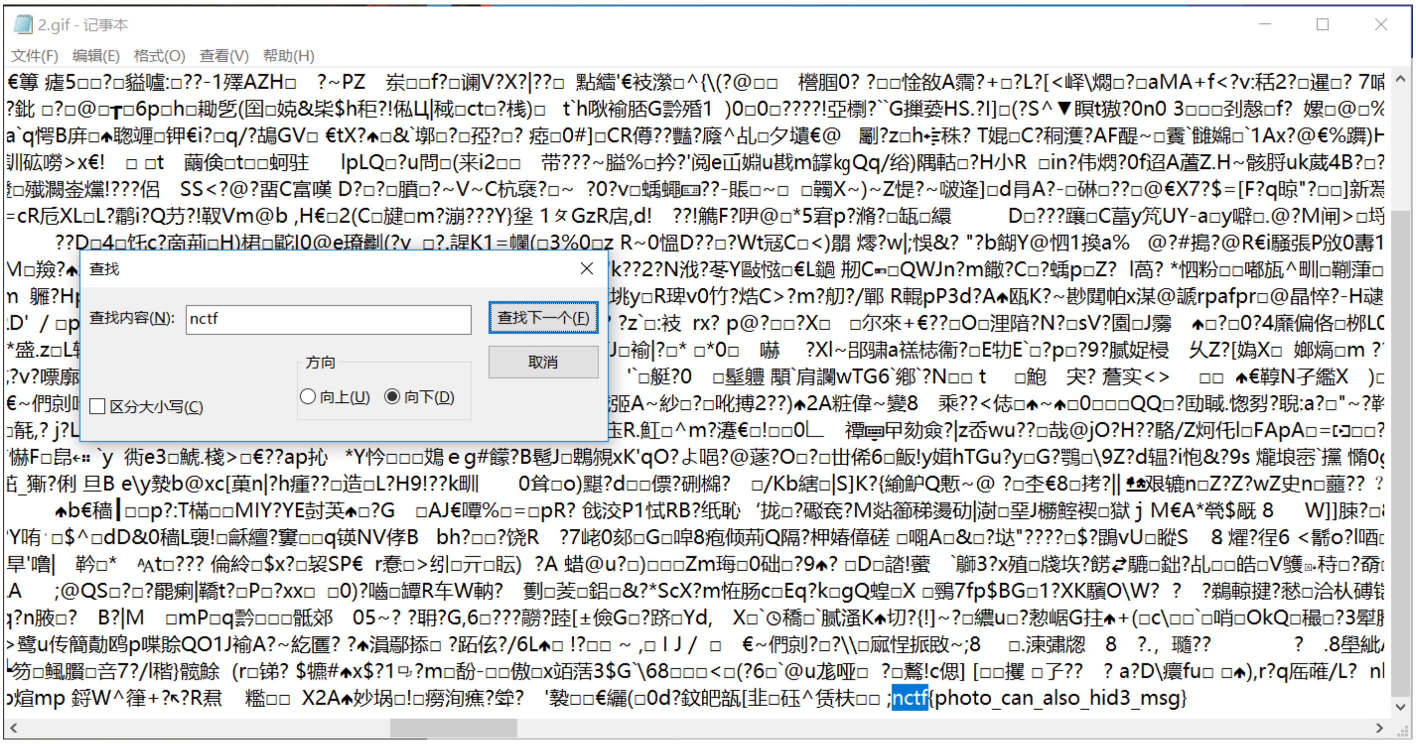
```
<html> event
  <head> … </head>
  <body>
    尚未登录或口令错误
    <form action="./index.php" method="post">
      <p>
        输入框：
        <input type="password" value="" name="text1" maxlength="12">
        <br>
        请输入口令：zhimakaimen
        <input type="submit" value="开门">
      </p>
    </form>
  </body>
</html>
```

4.这题不是WEB

进去看见这个

答案又是啥。。 

不是web，那就是杂项或者密码学呗，下载图片，记事本打开，查找nctf，得到flag



查找内容(N): nctf

☐ 区分大小写(C)

○ 向上(U) ● 向下(D)

nctf{photo_can_also_hid3_msg}

5.层层递进

Challenge

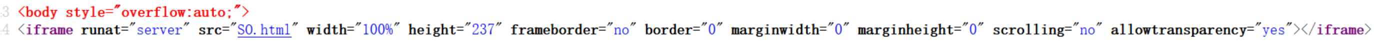
3975 Solves

层层递进

100

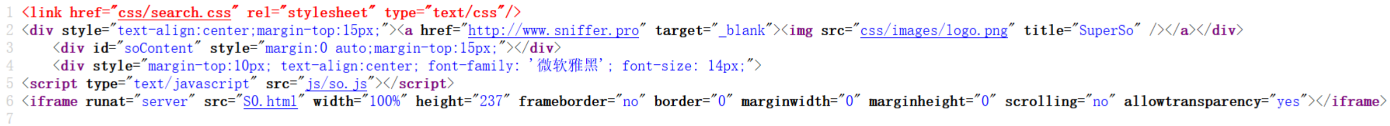
黑客叔叔p0tt1的题目
欢迎大家关注他的微博~
题目传送门:题目地址

> 老规矩，先查看源代码，发现一个奇怪的iframe



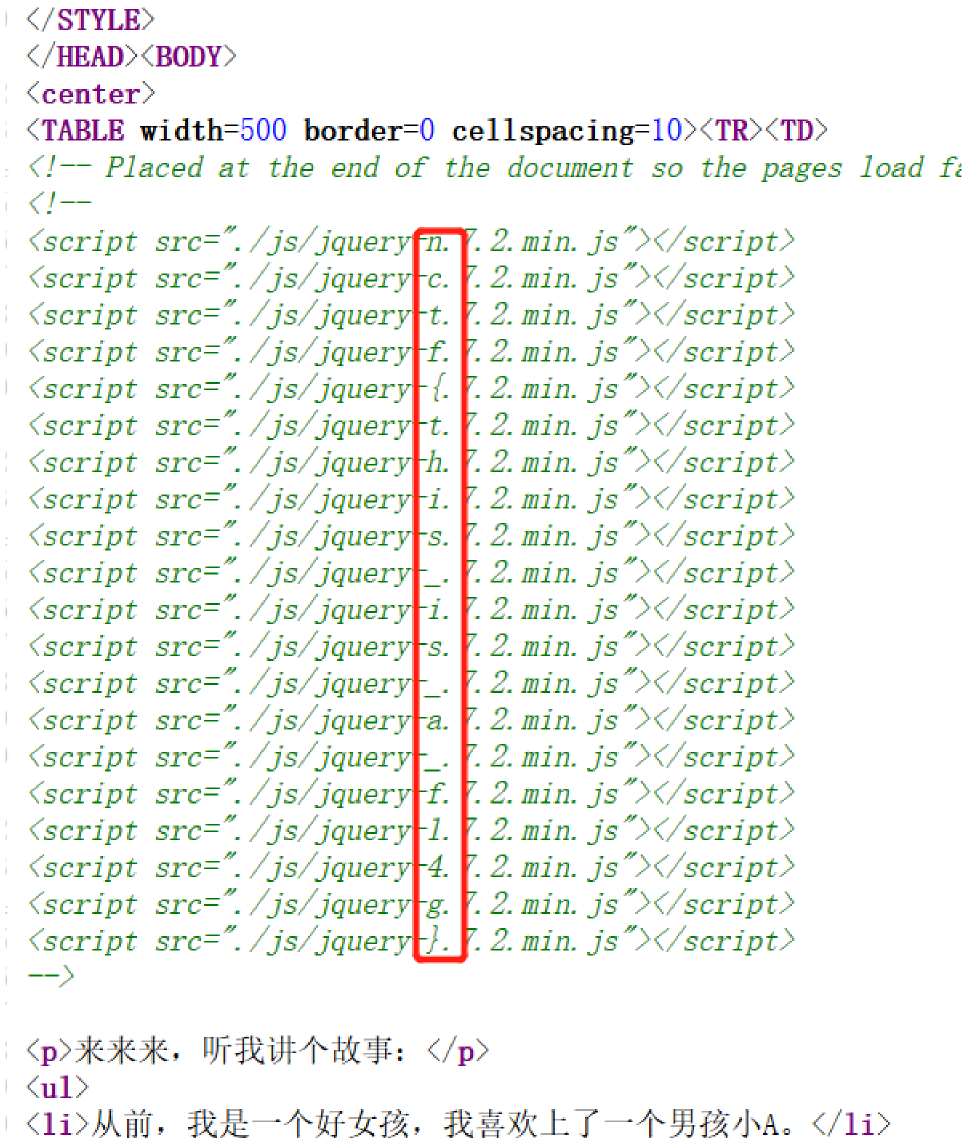
```html
<body style="overflow:auto;">
<iframe runat="server" src="SO.html" width="100%" height="237" frameborder="no" border="0" marginwidth="0" marginheight="0" scrolling="no" allowtransparency="yes"></iframe>
```

> 又发现了同样的SO.html，大概明白层层递进的意思了，继续进入下一个SO.html



```html
<link href="css/search.css" rel="stylesheet" type="text/css"/>
<div style="text-align:center;margin-top:15px;"><a href="http://www.sniffer.pro" target="_blank"><img src="css/images/logo.png" title="SuperSo" /></a></div>
    <div id="soContent" style="margin:0 auto;margin-top:15px;"></div>
    <div style="margin-top:10px; text-align:center; font-family: '微软雅黑'; font-size: 14px;">
<script type="text/javascript" src="js/so.js"></script>
<iframe runat="server" src="SO.html" width="100%" height="237" frameborder="no" border="0" marginwidth="0" marginheight="0" scrolling="no" allowtransparency="yes"></iframe>
```

> 最后在404.html发现了这个



```
</STYLE>
</HEAD><BODY>
<center>
<TABLE width=500 border=0 cellspacing=10><TR><TD>
<!-- Placed at the end of the document so the pages load fa
<!--
<script src="./js/jqueryn.7.2.min.js"></script>
<script src="./js/jqueryc.7.2.min.js"></script>
<script src="./js/jqueryt.7.2.min.js"></script>
<script src="./js/jqueryf.7.2.min.js"></script>
<script src="./js/jquery{.7.2.min.js"></script>
<script src="./js/jqueryt.7.2.min.js"></script>
<script src="./js/jqueryh.7.2.min.js"></script>
<script src="./js/jqueryi.7.2.min.js"></script>
<script src="./js/jquerys.7.2.min.js"></script>
<script src="./js/jquery_.7.2.min.js"></script>
<script src="./js/jqueryi.7.2.min.js"></script>
<script src="./js/jquerys.7.2.min.js"></script>
<script src="./js/jquery_.7.2.min.js"></script>
<script src="./js/jquerya.7.2.min.js"></script>
<script src="./js/jquery_.7.2.min.js"></script>
<script src="./js/jqueryf.7.2.min.js"></script>
<script src="./js/jqueryl.7.2.min.js"></script>
<script src="./js/jquery4.7.2.min.js"></script>
<script src="./js/jqueryg.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>
```

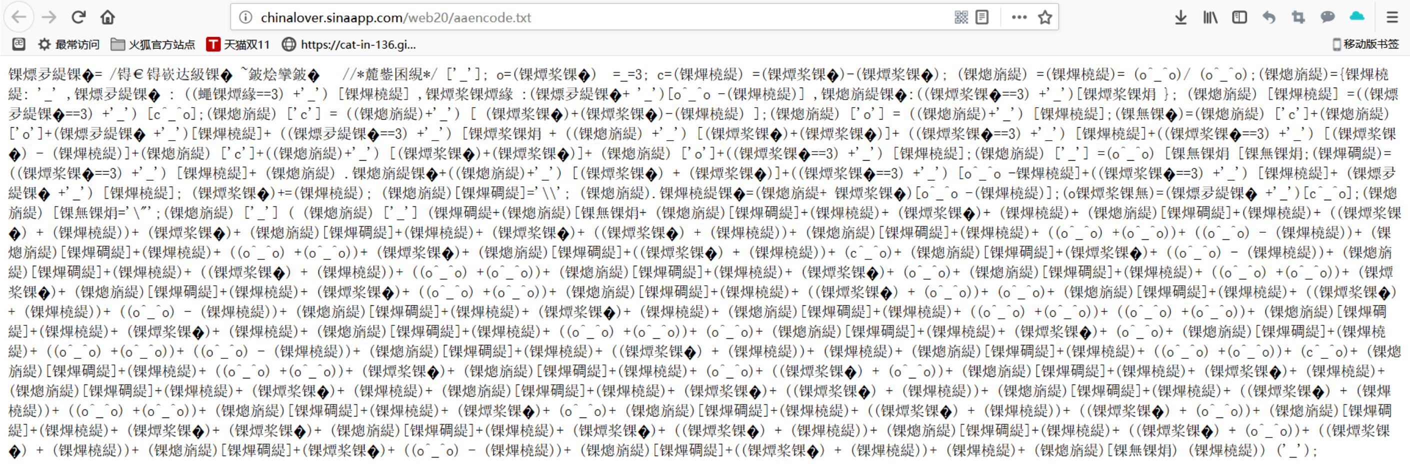
6.AAencode

AAencode

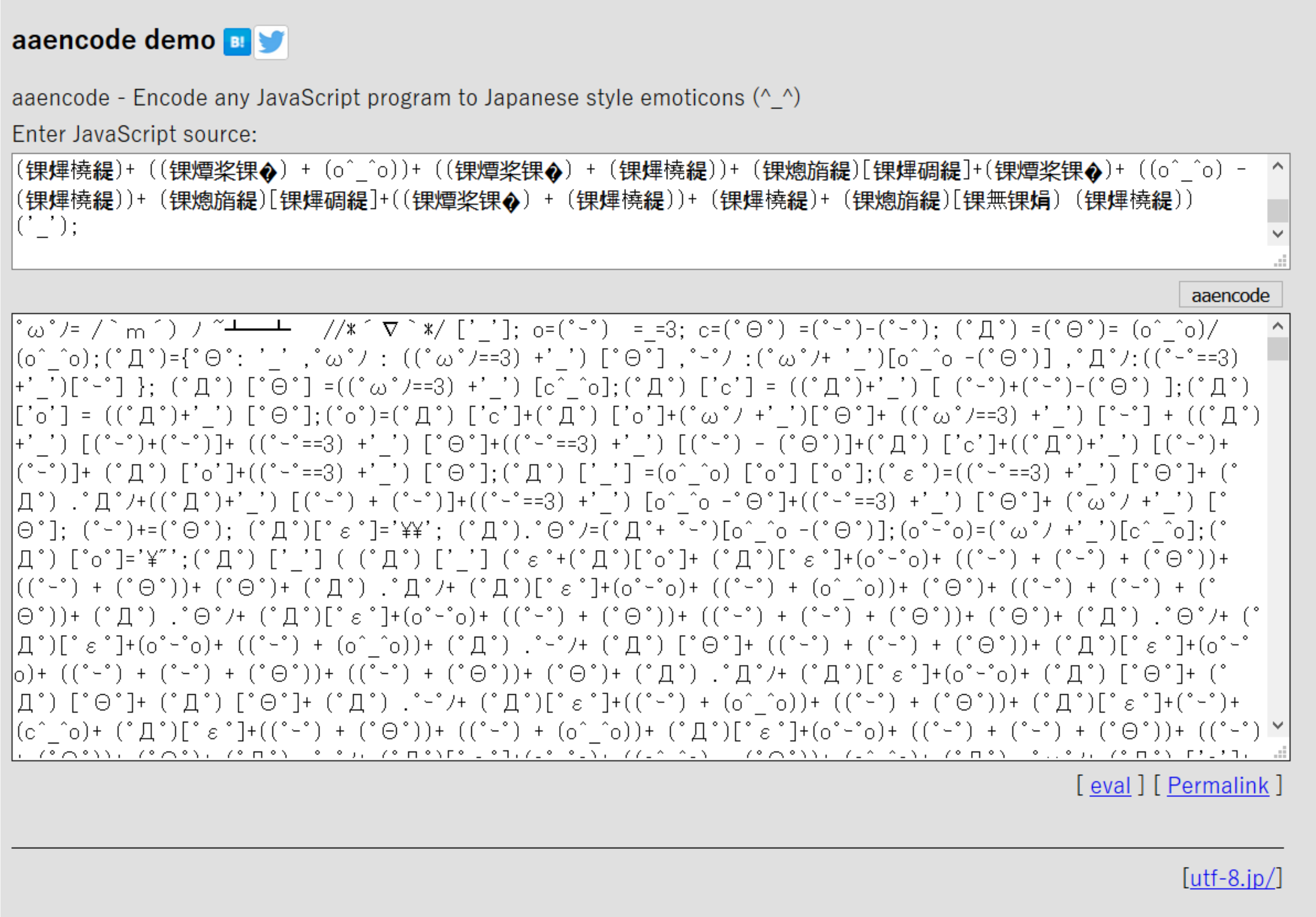
100

javascript aaencode

传送门：题目地址



猜测是什么解码题，百度题目提示，找到解码器，然而解出来还是表情符



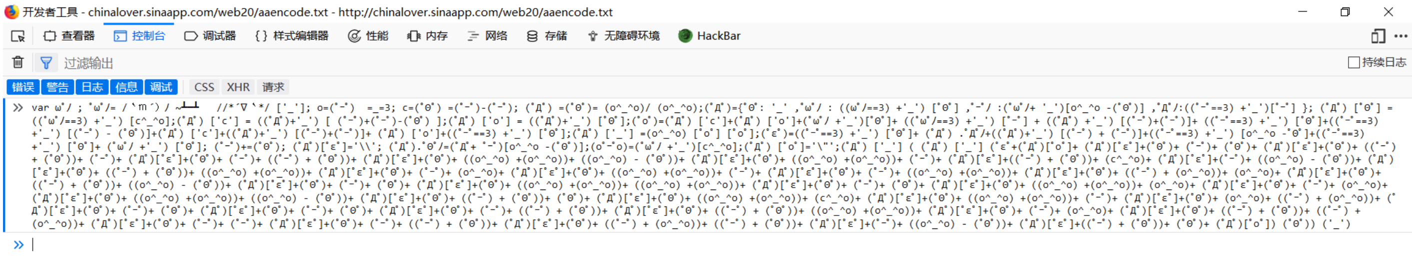
aaencode demo

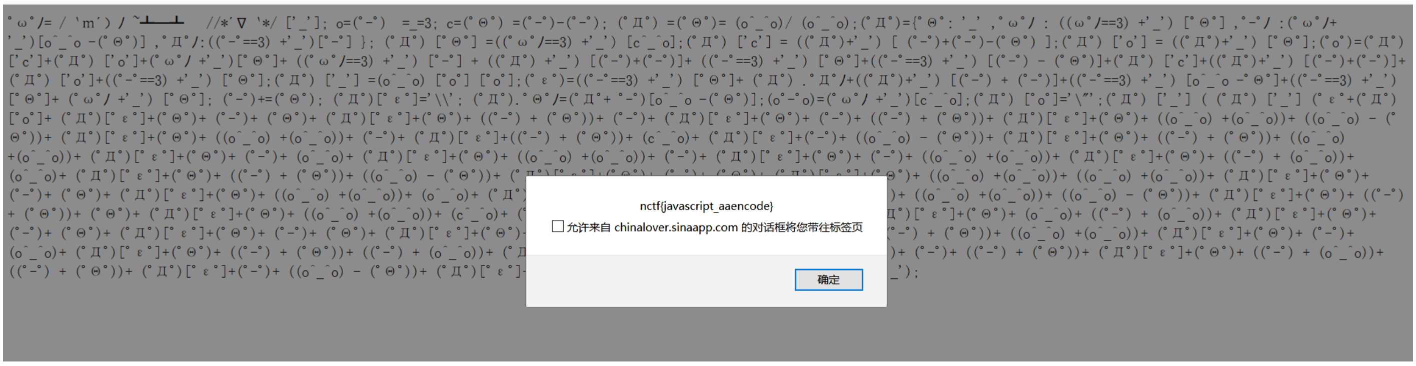
aaencode - Encode any JavaScript program to Japanese style emoticons (^_^)

Enter JavaScript source:

```
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]+(oﾟｰﾟo)+ ((ﾟｰﾟ) + (ﾟｰﾟ) + (ﾟΘﾟ))+
((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟΘﾟ)+ (ﾟДﾟ) .ﾟДﾟﾉ+ (ﾟДﾟ)[ﾟεﾟ]+(oﾟｰﾟo)+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟｰﾟ) + (ﾟ
Θﾟ))+ (ﾟДﾟ) .ﾟΘﾟﾉ+ (ﾟДﾟ)[ﾟεﾟ]+(oﾟｰﾟo)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ ((ﾟｰﾟ) + (ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟΘﾟ)+ (ﾟДﾟ) .ﾟΘﾟﾉ+ (ﾟ
Дﾟ)[ﾟεﾟ]+(oﾟｰﾟo)+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ) .ﾟｰﾟﾉ+ (ﾟДﾟ) [ﾟΘﾟ]+ ((ﾟｰﾟ) + (ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(oﾟｰﾟ
o)+ ((ﾟｰﾟ) + (ﾟｰﾟ) + (ﾟΘﾟ))+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟΘﾟ)+ (ﾟДﾟ) .ﾟДﾟﾉ+ (ﾟДﾟ)[ﾟεﾟ]+(oﾟｰﾟo)+ (ﾟДﾟ) [ﾟΘﾟ]+ (ﾟ
Дﾟ) [ﾟΘﾟ]+ (ﾟДﾟ) [ﾟΘﾟ]+ (ﾟДﾟ) .ﾟｰﾟﾉ+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (o^_^o))+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟｰﾟ)+
(c^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+((ﾟｰﾟ) + (ﾟΘﾟ))+ ((ﾟｰﾟ) + (o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(oﾟｰﾟo)+ ((ﾟｰﾟ) + (ﾟｰﾟ) + (ﾟΘﾟ))+ ((ﾟｰﾟ)
```

放到控制台里跑一遍，得到flag





nctf{javascript_aaencode}

☐ 允许来自 chinalover.sinaapp.com 的对话框将您带往标签页

转载于:https://www.cnblogs.com/Rasang/p/9953206.html