

南京邮电大学网络攻防平台——WriteUp(持续更新)

转载

[dbwuawuug822801895](#) 于 2018-11-13 17:05:00 发布 117 收藏 1

文章标签: [php](#) [密码学](#)

原文链接: <http://www.cnblogs.com/Rasang/p/9953206.html>

版权

1.签到题

右键查看源代码直接获得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_admiaaaaaaaaaaaaaa}</a>
6   </head>
7   <body>
8     key在哪里?
9   </body>
10 </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";}
?>
```

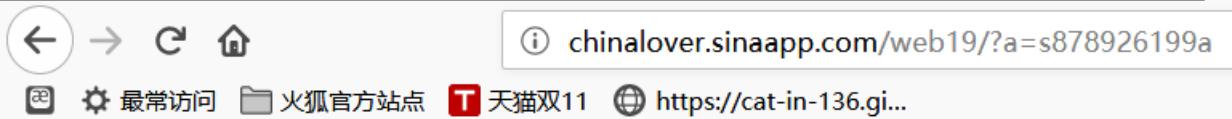
传送门: 题目地址

Key

SUBMIT

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

1 <html>
2 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
3 尚未登录或口令错误<form action="./index.php" method="post">
4 <p>输入框: <input type="password" value="" name="text1" maxlength="10">

5 请输入口令: zhimakaimen
6 <input type="submit" value="开门">
7 </form>
8
9 </html>
^

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

查看器 控制台 调试器 {} 样式编辑器 性能 内存 网络 存储 无障碍环境 HackBar

+

Q 搜索 HTML

<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">

请输入口令: zhimakaimen

<input type="submit" value="开门">

</p>

</form>

</body>

</html>

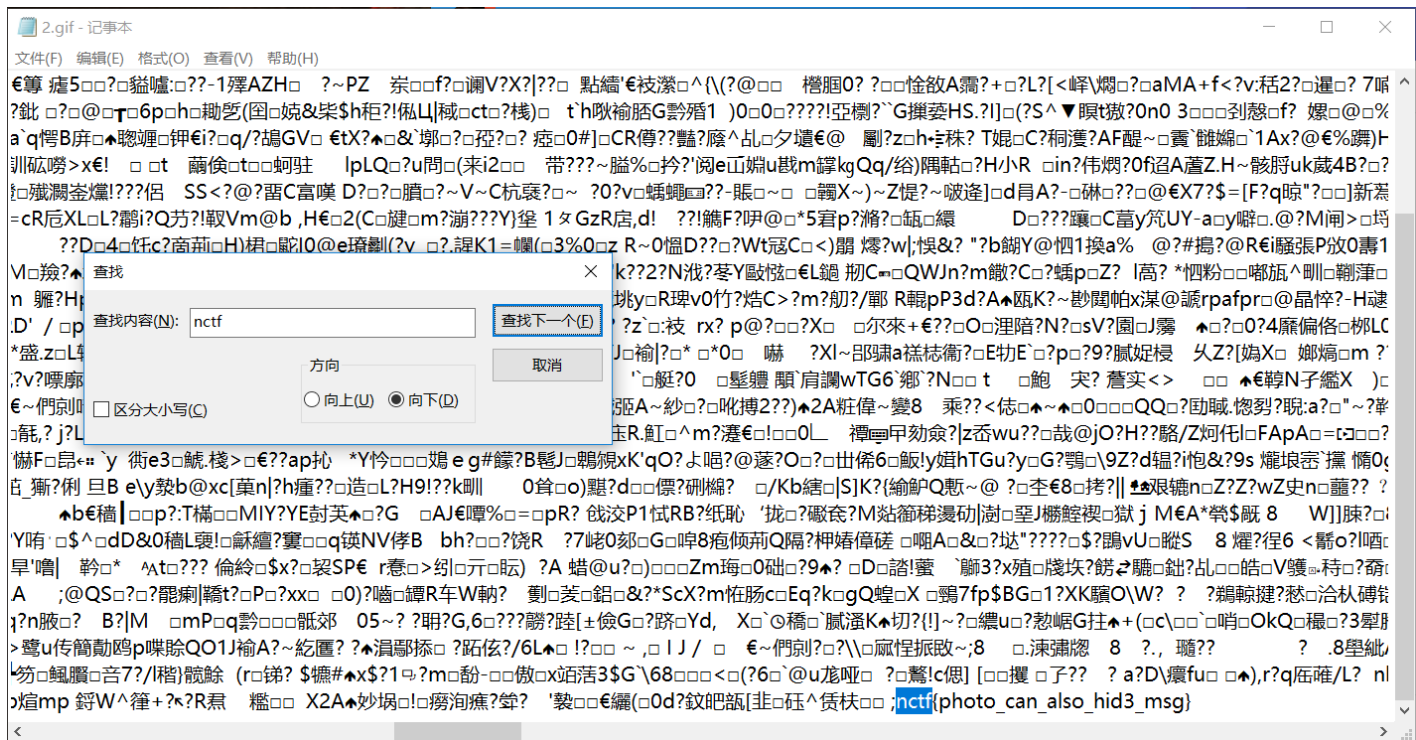
4.这题不是WEB

进去看见这个



答案又是啥。。

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



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

Key

SUBMIT

老规矩，先查看源代码，发现一个奇怪的iframe

```
3 <body style="overflow:auto;">
4 <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

```
1 <link href="css/search.css" rel="stylesheet" type="text/css"/>
2 <div style="text-align:center;margin-top:15px;"><a href="http://www.sniffer.pro" target="_blank"></a></div>
3 <div id="soContent" style="margin:0 auto;margin-top:15px;"></div>
4 <div style="margin-top:10px;text-align:center;font-family:'微软雅黑';font-size:14px;">
5 <script type="text/javascript" src="js/so.js"></script>
6 <iframe runat="server" src="SO.html" width="100%" height="237" frameborder="no" border="0" marginwidth="0" marginheight="0" scrolling="no" allowtransparency="yes"></iframe>
7
```

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 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-l.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>

```

6.AAencode

Challenge

2905 Solves

×

AAencode

100

javascript aaencode

传送门：题目地址

Key

SUBMIT



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:

[illegible]

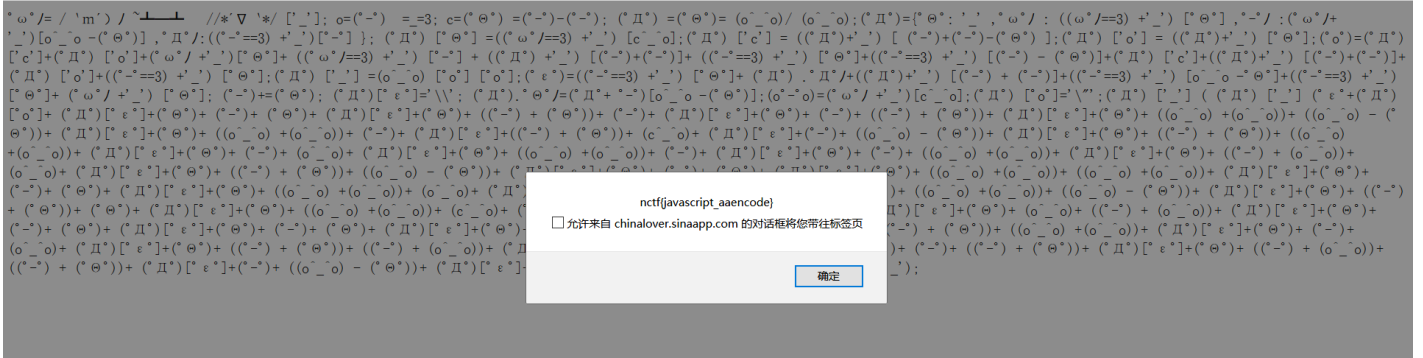
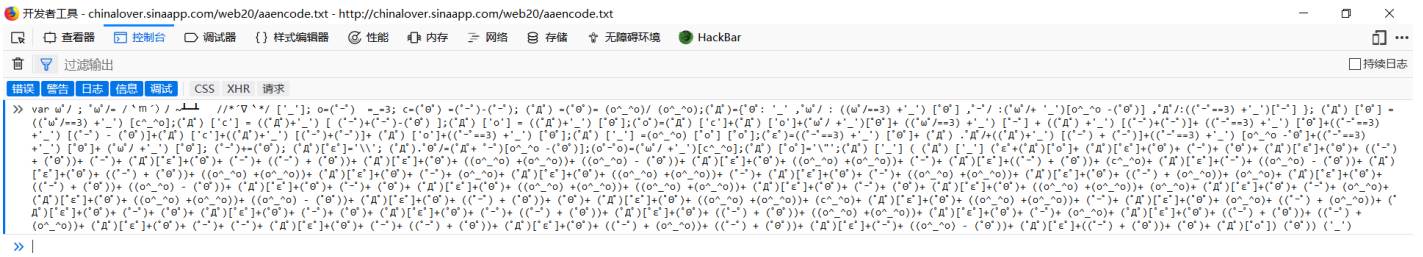
aaencode

$\omega^{\circ}/= / \wedge m^{\circ}) / \sim \underline{\text{L}} \quad // \text{X}^{\circ} \nabla^{\circ} \text{X}^{\circ} / [\text{'_'}]; \text{o}=(^{\circ}) \quad =_{\text{3}}; \text{c}=(^{\circ}\Theta^{\circ})=(^{\circ}\text{^-})-(^{\circ}\text{^-}); (^{\circ}\text{D}^{\circ})=(^{\circ}\Theta^{\circ})=(\text{o}^{\circ}\text{^-}\text{o}^{\circ})/$
 $(\text{o}^{\circ}\text{^-}\text{o}^{\circ}); (^{\circ}\text{D}^{\circ})=\{^{\circ}\Theta^{\circ}: \text{'_'} , \omega^{\circ}/: ((\omega^{\circ}/=_{\text{3}}) + \text{'_'}) [^{\circ}\Theta^{\circ}], \text{'_'}/:(\omega^{\circ}/+ \text{'_'})[\text{o}^{\circ}\text{^-}\text{o}^{\circ}-(^{\circ}\Theta^{\circ})], \text{'D}^{\circ}/:((^{\circ}\text{^-}=_{\text{3}})$
 $+ \text{'_'})[^{\circ}\text{^-}] \}$; $(^{\circ}\text{D}^{\circ}) [^{\circ}\Theta^{\circ}] = ((\omega^{\circ}/=_{\text{3}}) + \text{'_'}) [\text{c}^{\circ}\text{^-}\text{o}^{\circ}]; (^{\circ}\text{D}^{\circ}) [\text{'c'}] = ((^{\circ}\text{D}^{\circ}) + \text{'_'}) [(^{\circ}\text{^-}) + (^{\circ}\text{^-}) - (^{\circ}\Theta^{\circ})]; (^{\circ}\text{D}^{\circ})$
 $[\text{'o'}] = ((^{\circ}\text{D}^{\circ}) + \text{'_'}) [^{\circ}\Theta^{\circ}]; (\text{o}^{\circ}) = (^{\circ}\text{D}^{\circ}) [\text{'c'}] + (^{\circ}\text{D}^{\circ}) [\text{'o'}] + (\omega^{\circ}/ + \text{'_'}) [^{\circ}\Theta^{\circ}] + ((\omega^{\circ}/=_{\text{3}}) + \text{'_'}) [^{\circ}\text{^-}] + ((^{\circ}\text{D}^{\circ})$
 $+ \text{'_'}) [(^{\circ}\text{^-}) + (^{\circ}\text{^-})] + ((^{\circ}\text{^-}=_{\text{3}}) + \text{'_'}) [^{\circ}\Theta^{\circ}] + ((^{\circ}\text{^-}=_{\text{3}}) + \text{'_'}) [(^{\circ}\text{^-}) - (^{\circ}\Theta^{\circ})] + (^{\circ}\text{D}^{\circ}) [\text{'c'}] + ((^{\circ}\text{D}^{\circ}) + \text{'_'}) [(^{\circ}\text{^-}) +$
 $(^{\circ}\text{^-})] + (^{\circ}\text{D}^{\circ}) [\text{'o'}] + ((^{\circ}\text{^-}=_{\text{3}}) + \text{'_'}) [^{\circ}\Theta^{\circ}]; (^{\circ}\text{D}^{\circ}) [\text{'_'}] = (\text{o}^{\circ}\text{^-}\text{o}^{\circ}) [\text{'o'}] [\text{'o'}]; (^{\circ}\varepsilon^{\circ}) = ((^{\circ}\text{^-}=_{\text{3}}) + \text{'_'}) [^{\circ}\Theta^{\circ}] + (^{\circ}\text{D}^{\circ})$
 $\text{'D}^{\circ}/ + ((^{\circ}\text{D}^{\circ}) + \text{'_'}) [(^{\circ}\text{^-}) + (^{\circ}\text{^-})] + ((^{\circ}\text{^-}=_{\text{3}}) + \text{'_'}) [\text{o}^{\circ}\text{^-}\text{o}^{\circ}-(^{\circ}\Theta^{\circ})] + ((^{\circ}\text{^-}=_{\text{3}}) + \text{'_'}) [^{\circ}\Theta^{\circ}] + (\omega^{\circ}/ + \text{'_'}) [^{\circ}\Theta^{\circ}];$
 $(^{\circ}\text{^-}) + (^{\circ}\Theta^{\circ}); (^{\circ}\text{D}^{\circ}) [\varepsilon^{\circ}] = \text{'\text{X}\text{X}'}; (^{\circ}\text{D}^{\circ}) \text{'\text{O}^{\circ}}/ = (^{\circ}\text{D}^{\circ} + ^{\circ}\text{^-}) [\text{o}^{\circ}\text{^-}\text{o}^{\circ}-(^{\circ}\Theta^{\circ})]; (\text{o}^{\circ}\text{^-}\text{o}^{\circ}) = (\omega^{\circ}/ + \text{'_'}) [\text{c}^{\circ}\text{^-}\text{o}^{\circ}]; (^{\circ}\text{D}^{\circ})$
 $[\text{'o'}] = \text{'\text{X}\text{X}'}; (^{\circ}\text{D}^{\circ}) [\text{'_'}] ((^{\circ}\text{D}^{\circ}) [\text{'_'}] (^{\circ}\varepsilon^{\circ} + (^{\circ}\text{D}^{\circ}) [\text{'o'}] + (^{\circ}\text{D}^{\circ}) [\varepsilon^{\circ}] + (\text{o}^{\circ}\text{^-}\text{o}^{\circ}) + ((^{\circ}\text{^-}) + (^{\circ}\text{^-}) + (^{\circ}\Theta^{\circ})) +$
 $((^{\circ}\text{^-}) + (^{\circ}\Theta^{\circ})) + (^{\circ}\Theta^{\circ}) + (^{\circ}\text{D}^{\circ}) \text{'D}^{\circ}/ + (^{\circ}\text{D}^{\circ}) [\varepsilon^{\circ}] + (\text{o}^{\circ}\text{^-}\text{o}^{\circ}) + ((^{\circ}\text{^-}) + (\text{o}^{\circ}\text{^-}\text{o}^{\circ})) + (^{\circ}\Theta^{\circ}) + ((^{\circ}\text{^-}) + (^{\circ}\text{^-}) + (^{\circ}\Theta^{\circ})) +$
 $(^{\circ}\text{D}^{\circ}) \text{'\text{O}^{\circ}}/ + (^{\circ}\text{D}^{\circ}) [\varepsilon^{\circ}] + (\text{o}^{\circ}\text{^-}\text{o}^{\circ}) + ((^{\circ}\text{^-}) + (^{\circ}\Theta^{\circ})) + ((^{\circ}\text{^-}) + (^{\circ}\text{^-}) + (^{\circ}\Theta^{\circ})) + (^{\circ}\Theta^{\circ}) + (^{\circ}\text{D}^{\circ}) \text{'\text{O}^{\circ}}/ + (^{\circ}\text{D}^{\circ}) [\varepsilon^{\circ}] + (\text{o}^{\circ}\text{^-}\text{o}^{\circ}) +$
 $((^{\circ}\text{^-}) + (^{\circ}\text{^-}) + (^{\circ}\Theta^{\circ})) + ((^{\circ}\text{^-}) + (^{\circ}\Theta^{\circ})) + (^{\circ}\Theta^{\circ}) + (^{\circ}\text{D}^{\circ}) \text{'D}^{\circ}/ + (^{\circ}\text{D}^{\circ}) [\varepsilon^{\circ}] + (\text{o}^{\circ}\text{^-}\text{o}^{\circ}) + (^{\circ}\text{D}^{\circ}) [^{\circ}\Theta^{\circ}] + (^{\circ}\text{D}^{\circ}) [^{\circ}\Theta^{\circ}] +$
 $(^{\circ}\text{D}^{\circ}) [^{\circ}\Theta^{\circ}] + (^{\circ}\text{D}^{\circ}) \text{'_'}/ + (^{\circ}\text{D}^{\circ}) [\varepsilon^{\circ}] + ((^{\circ}\text{^-}) + (\text{o}^{\circ}\text{^-}\text{o}^{\circ})) + ((^{\circ}\text{^-}) + (^{\circ}\Theta^{\circ})) + (^{\circ}\text{D}^{\circ}) [\varepsilon^{\circ}] + (^{\circ}\text{^-}) +$
 $(\text{c}^{\circ}\text{^-}\text{o}^{\circ}) + (^{\circ}\text{D}^{\circ}) [\varepsilon^{\circ}] + ((^{\circ}\text{^-}) + (^{\circ}\Theta^{\circ})) + ((^{\circ}\text{^-}) + (\text{o}^{\circ}\text{^-}\text{o}^{\circ})) + (^{\circ}\text{D}^{\circ}) [\varepsilon^{\circ}] + (\text{o}^{\circ}\text{^-}\text{o}^{\circ}) + ((^{\circ}\text{^-}) + (^{\circ}\text{^-}) + (^{\circ}\Theta^{\circ})) + ((^{\circ}\text{^-})$

[[eval](#)] [[Permalink](#)]

[utf-8.jp/]

放到控制台里跑一遍，得到flag



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