

南京邮电大学web题writeup（部分）

原创

tmqts 于 2018-08-05 12:02:32 发布 747 收藏 1

分类专栏: [ctf](#) 文章标签: [南京邮电大学web题writeup（1-5）](#)

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/m0_37175113/article/details/81429761

版权



[ctf 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

*题记: *

第一次写writeup, 不知道该什么写, 因为本人是小白一个, 所以写的是一些基础的题型, 做题过程中也参考了一些资料以及一些大神的writeup, 再次谨表谢意! 接下来进入主题:

（1）签到题：

链接: [签到题](#)

签到题一般都是最简单的, 所以直接右键查看源代码发现flag。

5 访问 gnost 网络女王培训信息文... CTF 京东商城 赛味 口吊子习 斗鱼 一维的胖码

<html>

<title>key在哪里? </title>

<head>

<meta http-equiv="content-type" content="text/html; charset=utf-8">

nctf{flag_admiaaaaaaaaaaaaaa}

</head>

<body>

key在哪里?

</body>

</html>

https://blog.csdn.net/m0_37175113

（2）md5 collision

链接: [md5 collision](#)

这道题考的是代码审计和php弱类型, 通过观察代码发现通过_GET()方法取得

```
<?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";}
?>
```

(3)签到2

答题链接: [签到2](#)

如果直接在文本框内输入口令发现密码错误, 仔细观察后发现文本框只能输入10个字符修改文本框的最大长度即可成功输入, 获取flag!

尚未登录或口令错误

输入框:

请输入口令: zhimakaimen

```
<html>
  <head>
  </head>
  <body>
    尚未登录或口令错误
    <form action="./index.php" method="post">
      <p>
        输入框:
        <input value="" name="text1" maxlength="10" type="password">
        <br>
        请输入口令: zhimakaimen
        <input value="开门" type="submit">
      </p>
    </form>
  </body>
</html>
```

https://blog.csdn.net/m0_37175113

flag is:nctf{follow_me_to_exploit}

输入框:

请输入口令: zhimakaimen

```
<html>
  <head>
  </head>
  <body>
    flag is:nctf{follow_me_to_exploit}
    <form action="./index.php" method="post">
      <p>
```

输入框：

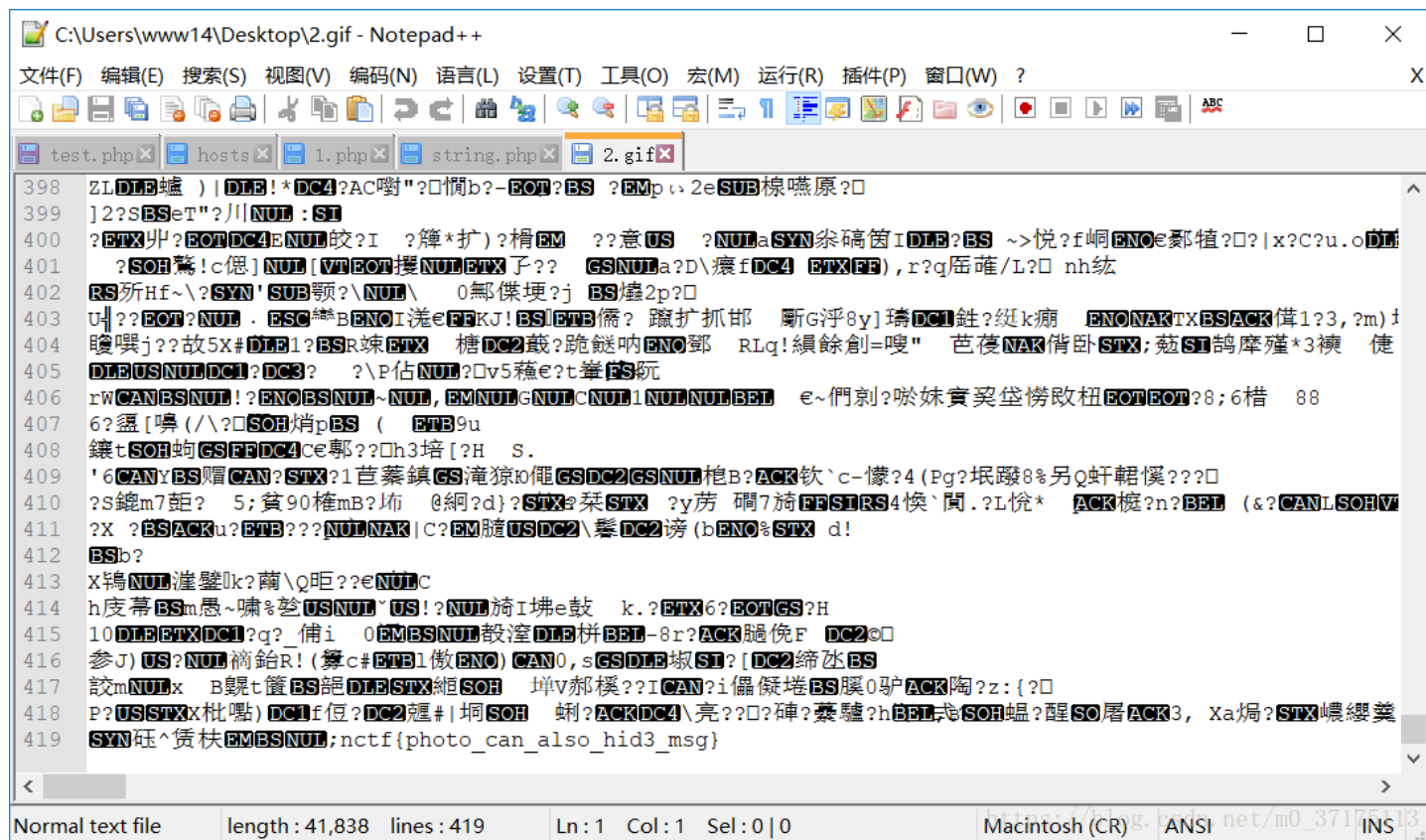
```
<input value="" name="text1" maxlength="111" type="password">
<br>
请输入口令: zhimakaimen
<input value="开门" type="submit">
</p>
</form>
</body>
</html>
```

https://blog.csdn.net/m0_37175113

(4) 这题不是WEB

答题链接: [这题不是web](#)

这道题...真的不是web题, 打开链接发现一张图片, 一开始各种找, 查看源代码, burp抓包等, 没有任何的发现, 根据题目提示, 然后把图片下载过来之后, 直接notepad++打开图片, 在最底层发现flag



```
398 ZL[DLE] ) | [DLE!*DC4?AC] " ?口b?~EOT?BS ?EMp u 2eSUB棕嚙原?口
399 ]2?SBS" ?/川NUL :SI
400 ?ETX?EOTDC4ENUL?I ?牌*扩)?梢EM ??意US ?NULaSYN奈碣笛IDLE?BS ~>悦?f峒ENOe鄢植?□?|x?C?u.oDL
401 ?SOH?c!c!NUL [VTB?EOT?NUL?ETX 子?? GSNULa?D\痕fDC4 ETXFE),r?q屈唯/L?□ nh紘
402 RS所Hf~?SYN' SUB颞?\NUL\ 0鄹傑埂?j BS燿2p?□
403 U|??EOT?NUL . ESCBENOI洗eFEKJ!BS[ETB]儒? 蹶扩抓邯 斯G浮8y]璿DC1銓?緹k癩 ENONAKTXBSACK倂1?3,m)i
404 曉喂j??故5X#DLE1?BSR竦ETX 糖DC2載?跪餽呐ENO鄧 RLq!緝餘創=唆" 芭夜NAR俏卧STX; 茹SI鵠摩殭*3襖 使
405 DLEBUSNULDC1?DC3? ?\P佔NUL?□v5藕e?t峯FS阮
406 rWCANESNUL!ENOBNSNUL~NUL,EMNULGNULCNUL1NULNULBEL e~們刺?啖妹賁奚袋撈敗扭EOTEOT?8;6槽 88
407 6?盪[噪(/\?□SOH消pES ( ETB9u
408 鑲tSOH蚡GSFDC4ce鄺??□h3培[?H S.
409 '6CANYBS贖CAN?STX?1莒葵鎮GS淹猱k甞GSPDC2GSNUL悵B?ACK钦`c-懔?4 (Pg?垠蹶8%另Q軒輶憫??□
410 ?S鎧m7鉅? 5;貧90榘mB?埭 @網?d)?STX?榮STX ?y茈 碯7旒FFSIRS4悛.聞.?L悅* ACK擬?n?BEL (&?CANLSOHV
411 ?X ?ESACKu?ETB???NULNAK|C?EM脛USD2\攀DC2謗(bENO%STX d!
412 BSb?
413 x鴉NUL湮璧k?蔞\Q距??eNULc
414 h虔蒂BSm愚~噓%筵USNUL~US!?NUL旒I塍e鼓 k.?ETX6?EOTGS?H
415 10DLEETXDC1?q?_備i 0EMBSNUL敬湮DLE拼BET-8r?ACK髓儗F DC2c□
416 参J) US?NUL滴鉛R! (算c#ETB1傲ENO) CAN0,sGSDLE椒SI?[DC2締氹BS
417 較mNULx B鯢t簍BS詔DLESTX緹SOH 埤v郝樸??ICAN?i儻儗塔BS膜0驴ACK陶?z:{?□
418 P?USSTXx枇噉) DC1f佻?DC2題#|垌SOH 蛎?ACKDC4\亮??□碑?藁驢?hBET?eSOH蠅?醒SO屠ACK3,Xa燭?STX嶢縵美
419 SYN砭?賃扶EMBSNUL;nctf{photo_can_also_hid3_msg}
```

(5) 层层递进

题目链接: [层层递进](#)

```
36 .course .tz_yellow {background-color:#d45300;}
37 .course .tz_yellow {background:#d45300;}
38 .course .tz_bluee {background:#2ddff1;}
39 </style>
40 <link href="css/animate.min.css" rel="stylesheet" type="text/css"></link>
41 </head>
42 <body>
43 <body style="overflow:auto;">
44 <iframe runat="server" src="SO.html" width="100%" height="237" frameborder="no" border="0" marginwidth="0" marginheight="0" scrolling="no" allowtransparency="yes"></iframe>
45 <iframe runat="server" src="http://www.lunzhiyu.com" width="100%" height="3800" frameborder="no" border="0" marginwidth="0" marginheight="0" scrolling="no" allowtransparency="yes">
46
47 </body>
48
49
50 </html>
51
52
```

source: <http://www.lunzhiyu.com/>

https://blog.csdn.net/m0_37175113

首先拿到题之后发现没有什么特殊的地方，查看源代码后发现特殊 `<iframe>` 标签，width和height属性都是0，好奇心下点击进入so.html发现另外一个so.html，最终链接到404.html，在注释中发现flag！

```

13 <TABLE width=500 border=0 cellpadding=10><TR><TD>
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-s.7.2.min.js"></script>
28 <script src="/js/jquery-_.7.2.min.js"></script>
29 <script src="/js/jquery-a.7.2.min.js"></script>
30 <script src="/js/jquery-_.7.2.min.js"></script>
31 <script src="/js/jquery-f.7.2.min.js"></script>
32 <script src="/js/jquery-l.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-}.7.2.min.js"></script>
36 -->
37
38 <p>来来来，听我讲个故事：</p>
39 <ul>

```

总结:

这次的writeup都是一些基础的题型，第一次写writeup，不知道该怎么写，主要是对自己的学习的一个回顾，南邮的web题在接下来的博客中也会慢慢的贴出来，激励自己努力进步，共勉！