南邮CTF平台writeup：Web(一)

原创

All__Blue 于 2017-11-04 14:09:02 发布 3983 收藏 4

分类专栏： Web Writeup 文章标签： web ctf

本文链接：https://blog.csdn.net/All__Blue/article/details/78443244


Web 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏


Writeup

1 篇文章 0 订阅

订阅专栏

签到题

查看网页源代码即可

```
<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>
```


md5 collision

```
$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";}
```

PHP漏洞题

源码的意思是要求两个变量不相等但是他们的MD5值要相等，这是不可能的。这里用的是PHP在比较哈希值时会将0e开头的哈希值都解释为0的缺陷(和编程语言的科学计数法有关)，也就是说只要让GET传参的值的MD5以0e开头就行了

补个相关的链接：

http://www.cnblogs.com/Primzahl/p/6018158.html

payload:http://chinalover.sinaapp.com/web19/?a=s878926199a

```
nctf{md5_collision_is_easy}
```


签到2

```
"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
     "
```

可以看到源码里限制了最大输入长度位10位，但口令为11位。

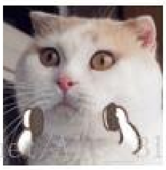
有两个方法：一个是改当前网页的源码，一个是拦截数据包改口令。

这里用简便点的第一个方法

```
"输入框："
<input type="password" value="" name="text1" maxlength="11">
```

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

这题不是WEB

答案又是啥。。 

这题还真不是web…..是一道隐写

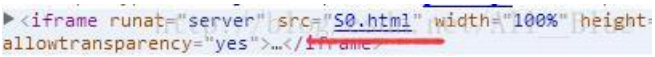
下载图片以文本形式打开，在末尾有flag

```
BELH×??□NAKX>ETX帄酈任霿cEOX編BS
;nctf{photo_can_also_hid3_msg}
```

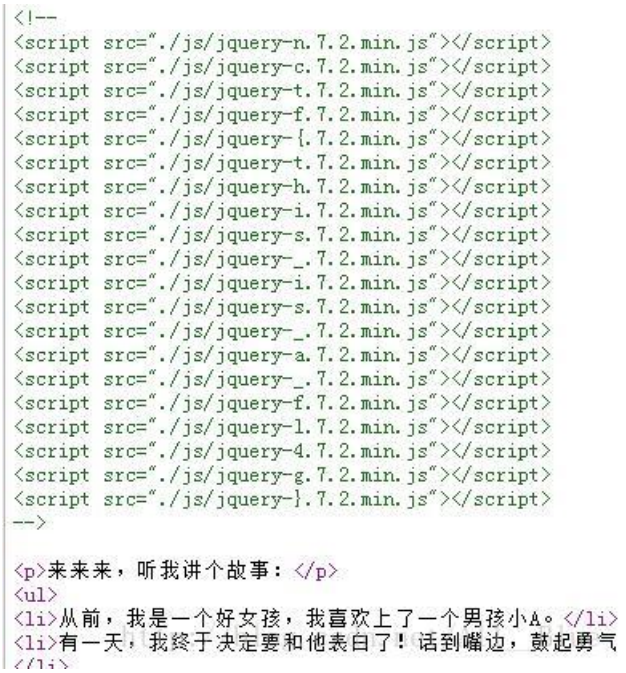
层层递进

源码里看见一个奇怪的链接

去这个网页后源码里又有个奇怪的链接，细心点发现和上次是不一样的，上次是SO.html，这是是S0.html



这样点了几个链接后，来到了最终的链接：
http://chinalover.sinaapp.com/web3/404.html
源码里有一段奇怪的注释

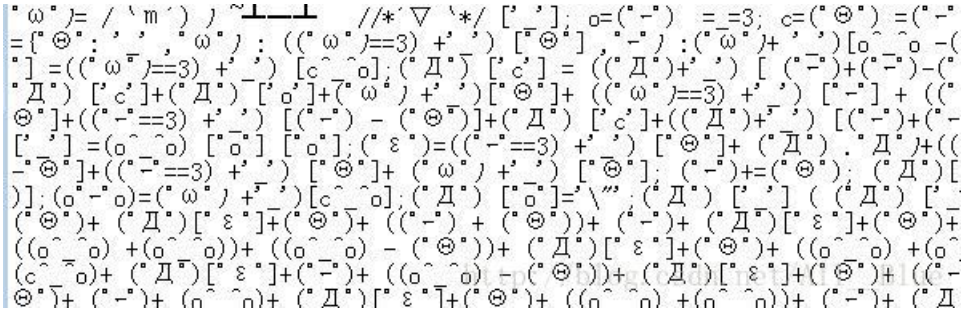


仔细看一下就能发现竖着的flag

AAencode

aaencode就是JS颜文字代码，本质上还是代码，可以运行
点开链接发现是混着AAencode代码和乱码的一堆字符串

有乱码猜测是编码方式的问题，下载这个txt文档
用UTF-8打开就能得到原本的aaencode

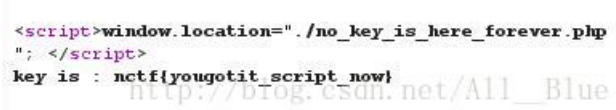


本来是要对代码进行改动，补充完整一个颜文字的，今天发现出题人把题目改简单了
现在直接扔进控制台运行即可

单身二十年

源码里让到这里找flag

但是点开后会被迅速地重定向到另一个页面，我没有像题目名那样单身二十年，所以我手速不过关→_→，还是上burpsuite吧



php decode

考察对PHP和shell的理解

```
<?php function CLsI($ZzvSWE) { $ZzvSWE = gzinflate(base64_decode($ZzvSWE)); for ($i = 0; $i < strlen($Z
```

eval()函数会执行括号里面的语句，这种代码在现实中一般是某个黑客上传的一句话马，但在这里eval里面肯定就是flag了，找个在线代码执行的网站，复制粘贴代码，将eval改成echo即可

```
phpinfo();\r
flag:nctf{gzip_base64_hhhhhh}
sandbox> exited with status 0
```


文件包含

文件包含是CTF里一种常见的漏洞
这里有个介绍文件包含的链接:http://www.freebuf.com/articles/4843.html
打开题目链接后可以看到这个链接
http://4.chinalover.sinaapp.com/web7/index.php?file=show.php
可以看到file=....，是典型的文件包含的样式
payload:http://4.chinalover.sinaapp.com/web7/index.php?file=php://filter/read=convert.base64-encode/resource=index.php
可以得到index.php的源代码的base64加密形式
解码即可得到flag

```
            echo "Oh no!";
            exit();
        }
        include($file);
//flag:nctf{edulcni_elif_lacol_si_siht}

?>
```


单身一百年也没用

考察HTTP头，flag被放在了response的头里，用burpsuite的repeater去访问即可

```
HTTP/1.1 302 Found
Server: sae
Date: Sat, 04 Nov 2017 05:38:10 GMT
Content-Type: text/html
Content-Length: 0
Connection: close
flag: nctf{this_is_302_redirect}
Location:
http://chinalover.sinaapp.com/web8/no_key_is_here_for
ever.php
Via: 1529
```


Download~!

在源码里可以看到下载链接很奇怪，是base64加密的

```
<p>为了让大家更轻松的比赛，为大家准备了两首歌让大家下载</p>
<p>
  <a href="download.php?url=eGluZ3hpbmdkaWFuZGVuZy5tcDM=" target="_blank">星星点灯</a>
</p>
<p>
  <a href="download.php?url=YnV4aWFuZ3poYW5nZGEubXAz" target="_blank">不想长大</a>
</p>
<div class="cleaner"> </div>
```


把星星点灯的下载链接base64解密后发现是和其相对应的

```
eGluZ3hpbmdkaWFuZGVuZy5tcDM=
```

```
结果：（字符数统计：20）
xingxingdiandeng.mp3
```


那猜测这里是一个任意文件下载的漏洞，flag会在什么文件里？
尝试下载flag.php：
http://way.nuptzj.cn/web6/download.php?url=ZmxhZy5waHA=

```
?Access Forbidden!
```


禁止连接，看来出题者不想就这么让我直接拿到flag
试了几个都不对，最后试到download.php：
http://way.nuptzj.cn/web6/download.php?url=ZG93bmxvYWQucGhw
给出了源码

```
<?php error_reporting(0); include("hereiskey.php"); $url=base64_decode($_GET[url]); if( $url=="hereiske
```

可以看到flag应该在hereiskey.php里，下载后得到flag

```
hereiskey.php - 记事本
文件(F)  编辑(E)  格式(O)  查看(V)  帮助(H)
?<?php
//flag:nctf{download_any_file_666}
?>
```


COOKIE

COOKIE就是甜饼的意思~

TIP: 0==not

题目给出了提示0==not

打开链接没有多的信息，那就是要拦数据包改cookie了

```
(KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36
Referer: http://chinalover.sinaapp.com/web10/index.php
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: td_cookie=1844[illegible] Login=0;
td_cookie=1[illegible]9
Connection: close
```


cookie里有个不正常的login=0，结合提示那就改为1了

```
1; WOW64) AppleWebKit/537.36
02 Safari/537.36
/web10/index.php


; Login=1;
```

flag:nctf{cookie_is_different_from_session}

总共是前12道题的writeup