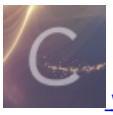
CG-CTF web题(部分)

原创

Rise ` 于 2019-05-11 13:12:43 发布 2016 收藏 19

分类专栏： web 文章标签： CTF

本文链接：https://blog.csdn.net/qq_43483333/article/details/90106813



南邮CTF练习题（http://ctf.nuptzj.cn/）

记录新手努力的每一时刻！

在学习CTF之前可以先了解一下它：

CTF入门简介：https://blog.csdn.net/Fly_hps/article/details/79783253， 然后从这个网站了解一下CTF web方面大概有哪些东西，看不懂没关系，就是知道一下以后要学什么https://ctf-wiki.github.io/ctf-wiki/web/introduction/ 。在这里推荐新手使用的工具：burp suite 和winhex。

可以找一下破解版的burp，方便使用。

好了下面进入正题：

1.签到题

这里采用的是360浏览器，打开题目地址，使用工具——查看源代码即可，这里也可以使用快捷键F12/CTRL+U。

```
<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>
```

Flag：nctf{flag_admiaanaaaaaaaaaaa}

2.md5 collision

分析代码：

要求

$md51 = md5('QNKCDZO');

$a= @$_GET['a'];

$md52= @md5($a);

if ($a != 'QNKCDZO' && $md51 == $md52) {

echo "nctf{**********}";md5加密，这里就多想一想，说明既要相等，又不能等于

md5(QNKCDZO,32) = 0e830400451993494058024219903391

在这里发现只要找到一个字符串在MD5加密后与其相等就可以，百度随便找一个即可，如

http://chinalover.sinaapp.com/web19/?a=240610708

页面出现flag：nctf{md5_collision_is_easy}

3.签到2
点击题目地址，发现以下情况

尚未登录或口令错误

输入框：
请输入口令：zhimakaimen 开门

输入zhimakaimen，发现口令错误，使用F12/CTRL+u进行查看，得出提示：输入框：

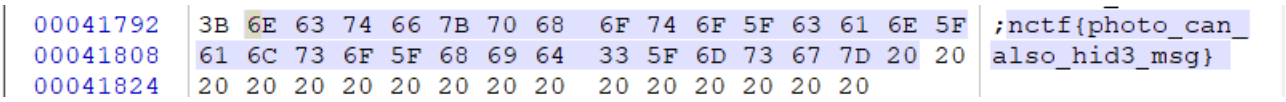
maxlength="10"，而zhimakaimen的长度大于10，所以在这里可以直接更改最大长度即可，输入口令：

flag is:nctf{follow_me_to_exploit}

输入框：
请输入口令：zhimakaimen 开门

Flag：nctf{follow_me_to_exploit}

4.这题不是WEB
打开题目地址，发现是一张gif的图，在这里就可以考虑一下使用工具：winhex。
将图片拖入winhex就会发现一些不太一样的地方，翻到最后一项ANSI ASCII 最后一处发现Flag。



flag：nctf{photo_can_also_hid3_msg}

5.层层递进

当时做这道题的时候，心里那个纠结呀，一直查找，更换，特别繁琐，不过这也许就是CTF的魅力所在了吧。

使用burpsuite抓包后，发现：

20	http://chinalover.sinaapp.com	GET	/web3/404.html			304	105	HTML	html

所以在其后缀加上404.html，即http://chinalover.sinaapp.com/web3/404.html，

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^)/~！

使用CTRL+u/F12查看：

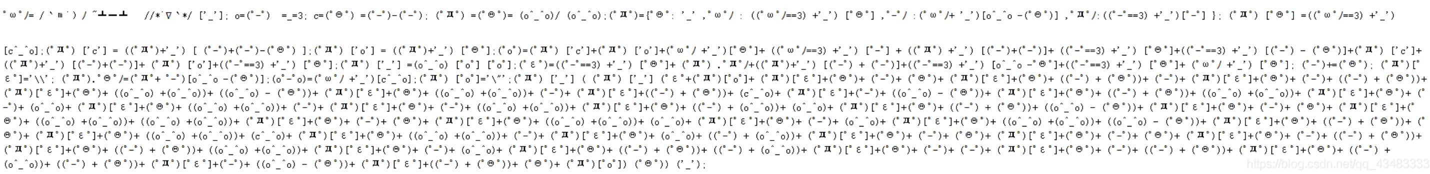
```
<!-- Placed at the end of the document so the pages load faster -->
<!--
<script src="./js/jquery-n.7.2.min.js"></script>
<script src="./js/jquery-c.7.2.min.js"></script>
<script src="./js/jquery-t.7.2.min.js"></script>
<script src="./js/jquery-f.7.2.min.js"></script>
<script src="./js/jquery-{.7.2.min.js"></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>
-->
```


到这里，是不是发现了些许不太一样的东西呢，咯咯咯，竖着读一下哦！

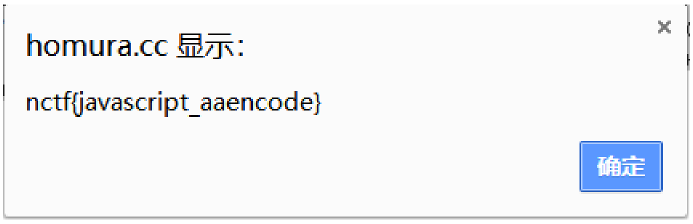
flag：nctf{this_is_a_fl4g}

6.AAencode

打开题目地址，发现是这样的：

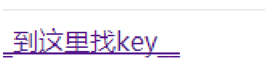


分析发现其实这是一段使用javascript编译的语句，在这里我们可以使用Chrome浏览器自带的工具直接解出，F12查看，将其复制到Console里，直接enter：



flag：nctf{javascript_aaencode}

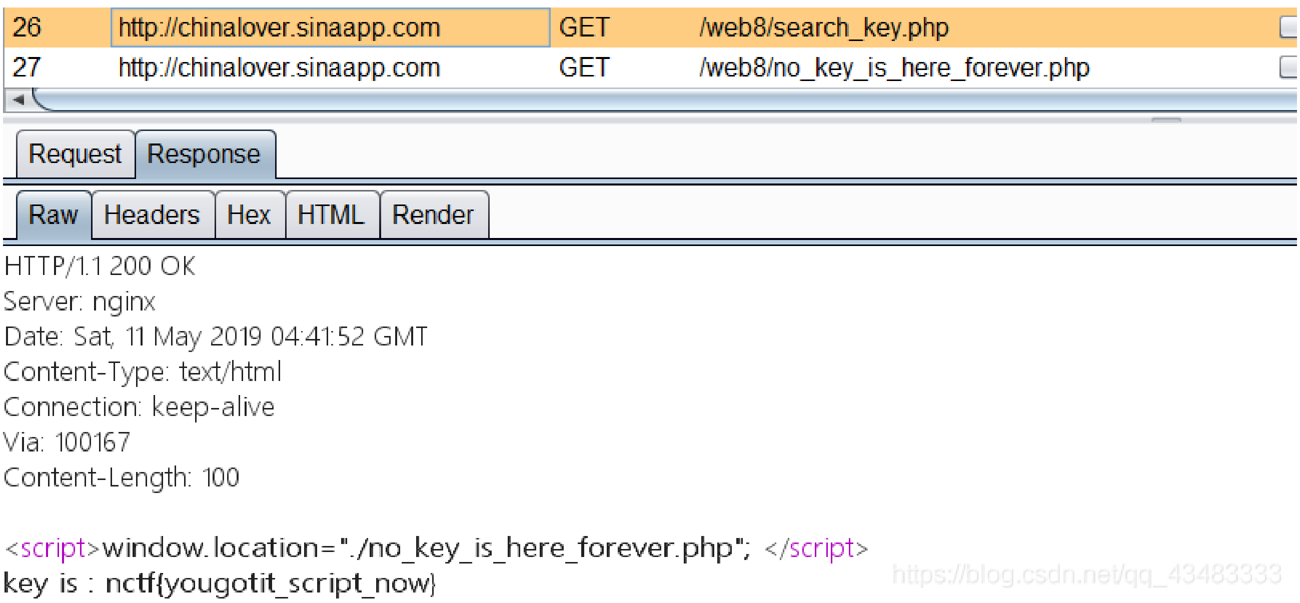
7.单身二十年



打开题目地址，弹出：

点击：

嗯哼，什么情况呢？这时我们可以思考以下使用burp抓包分析：



哈哈哈，喏，key is here.

flag：nctf{yougotit_script_now}

8.php decode

已经提示了：见到的一个类似编码的shell，请**解码**，所以网页搜索php在线运行，

```php
<?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+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA=="));
?>
```

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


flag：nctf{gzip_base64_hhhhhh}

9.文件包含

分析发现这个文件应该存在文件漏洞，则url后加入?file=php://filter/read=convert.base64-encode/resource=index.php。

（http://4.chinalover.sinaapp.com/web7/index.php?file=php://filter/read=convert.base64-encode/resource=index.php）

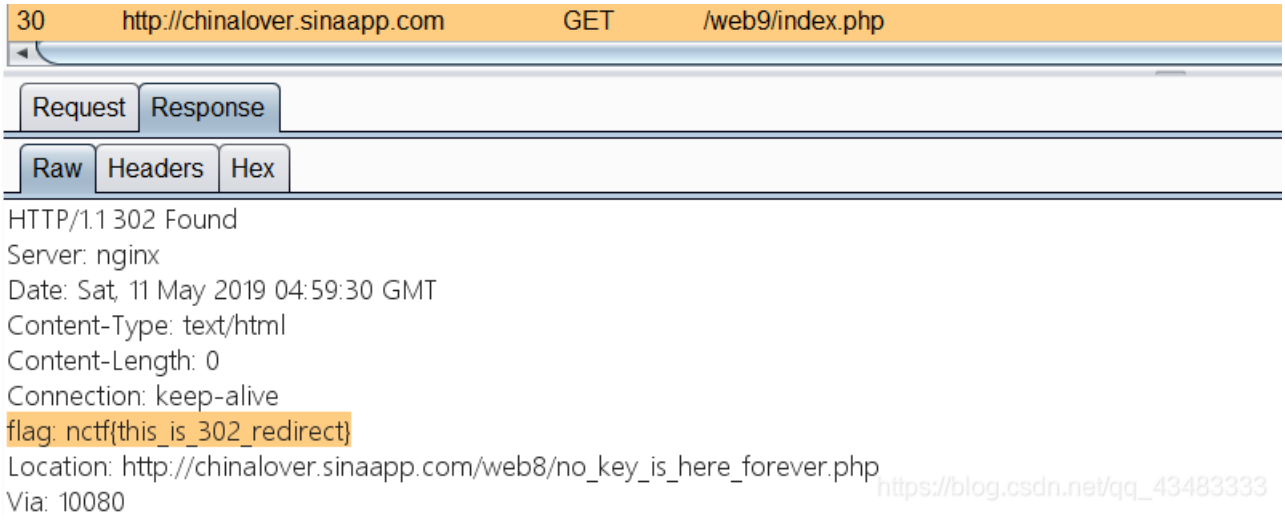
发现是一串base64加密的indexphp。这时百度base64在线解密即可：

<?php error_reporting(0); if(!$_GET[file]){echo ' click me? no';} $file=$_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} ?>

flag：nctf{edulcni_elif_lacol_si_siht}

10.单身一百年也没用

与单身20年解题思路相似，这里直接使用burp抓包分析：



flag:nctf{this_is_302_redirect}