【F2C】NCTF 南邮攻防平台 Write Up

原创

KANITAN___ 于 2019-11-19 15:11:19 发布 268 收藏 1
分类专栏： 攻防 文章标签： writeup

说在前面

大部分参考：NCTF 南京邮电大学网络攻防训练平台 WriteUp

做题网址：CG-CTF
(里面时不时出现某同学的名字实在好出戏啊！)

里面只有web。解答比较全，不过我有几题没写出来，以后做出来了会更新。另外也有非web题。
刚接触CTF，很多东西不懂，只是为了做个笔记，比较适合新入门的小萌新看，有一些工具入门的介绍，还有总结出的解题思路，在dalao们面前肯定是班门弄斧了，有什么错误或者指导意见，请务必在评论区写出来，一定虚心学习！
比较喜欢碎碎念，不要介意~

做题环境

操作系统：Win10 64x
浏览器：firefox
查看器：sublime text，文本文档
工具 ：·burpsuite 用于抓取数据包分析
·winhex 16进制分析工具
·firefox hackbar插件

#正题

web

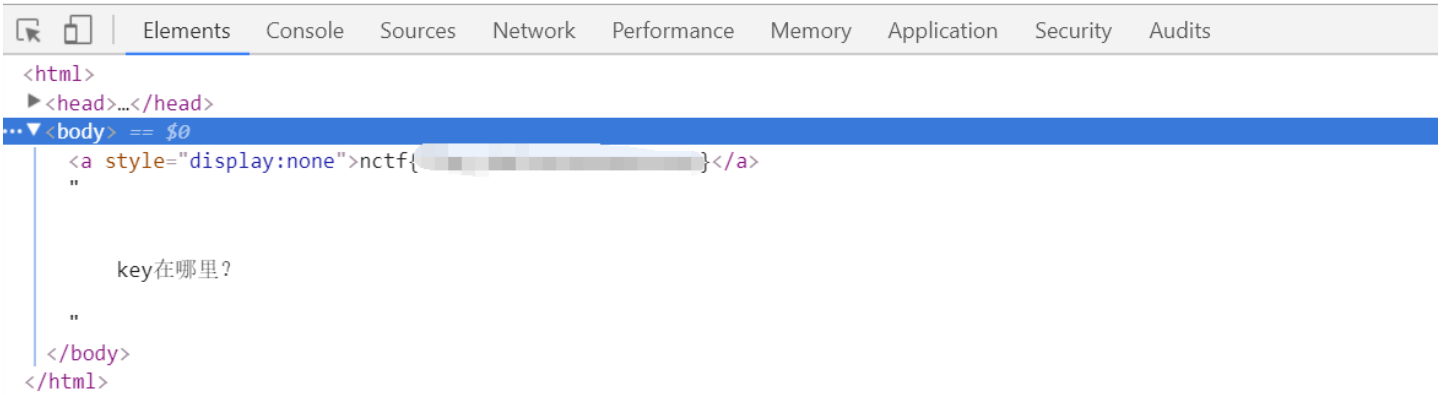
签到题

这题一定是最简单的

~~你说简单就简单？~~

第一次接触实在摸不着头脑，结果只需要戳一下F12查看网页源代码就能看到。好嘛，上来就是套路

key在哪里？



md5 collision

来看源代码，顺手加点注释

```
$md51 = md5('QNKCDZO');       #md5加密
$a = @$_GET['a'];         #GET的值传给a
$md52 = @md5($a);         #对a进行md5加密
if(isset($a)){         #如果a的值不为空
if ($a != 'QNKCDZO' && $md51 == $md52) { #判断是否相同
 echo "nctf{*****************}";
} else {
    echo "false!!!";
}}
else{echo "please input a";}
```

~~这段代码还蛮重要的，后面有好几题都是差不多的结构，又套路子？~~

显然不可能是让我们真去搞碰撞，然后就去百度了一下这个QNKCDZO这个字符串，没想到.....

```
PHP在处理哈希字符串时，会利用”!=”或”==”来对哈希值进行比较，它把每一个以”0E”开头的哈希值都解释为0，所以如果两个不同的密码经过哈希以后，其哈希值都是以”0E”开头的，那么PHP将会认为他们相同，都是0。
```

也就是说，只要0E开头的就行了，百度一下，人家一下子给列了好几十条，随便找一条就对了，比如找了xxxxxxxx
然后用get方式传入参数，只要在url后面加一个`?a=xxxxxxxx`就可以了
顺道也说一下，用post方式传递参数是一样的，至于post和get的差别这里就不讲了，http的知识~
也就是说在地址栏输入`http://chinalover.sinaapp.com/web19/?a=xxxxxxxx`

签到题2

签到题1的套路，上来先戳一戳F12
~~说真的上面一题要是题目没给代码，上来也是先戳F12，看透.jpg~~
关键在这里

```
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">
```

看到maxlength突然警觉，数了数果然是，zhimakaimen有11个字
直接把10改成11及以上，就成功开门啦~

这题不是web

~~既然不是web放在隔壁不好吗？？？~~
戳进去就一张gif，又不是web……
只好又跑去看题解，原来是道图片隐写
于是把gif改成txt格式，用文本文档查看末尾获得flag
花了几分钟查了查图片隐写，原来不同文件类型的图片都有特定的结束字段，图片查看器一般只读到结束字段为止，那么在末尾藏信息就是一种很简单便捷的方式了

层层递进

~~打个ctf还相亲，居然觉得挺浪漫~~
点进链接实在不知所措……戳戳F12呗，也没发现什么
可是又发现了什么，切换到**网络**，刷新一下页面，发现有一个404.html，点进去一看

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！

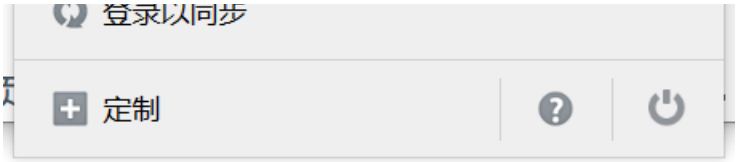
谢谢你给出的一份支持！哇哈哈\(^o^)/~！

~~怪不得单身二十年（笑脸）~~
查看网页源代码，一首藏尾诗 0110 0110 0110 。flag get

AAencode

题目提示太明显了，百度一下aaencode，有很多说明，js转换可以用sublime自带的package实现
但是！这题我卡了一天！你问我为什么？

谁能告诉我这堆中文怎么解？：）去问隔壁的dalao并获得两个直男专属笑脸表情后
知道了是编码的问题，就开始百度怎么转成UTF-8。结果chrome不！支！持！编码转换得，拜拜了您嘞。火速换成firefox，点击选项窗口（就是设置所在的那个）右键添加更多项目，里面有个文字编码，改成UTF-8就可以。sublime text/notepad++也支持编码转换

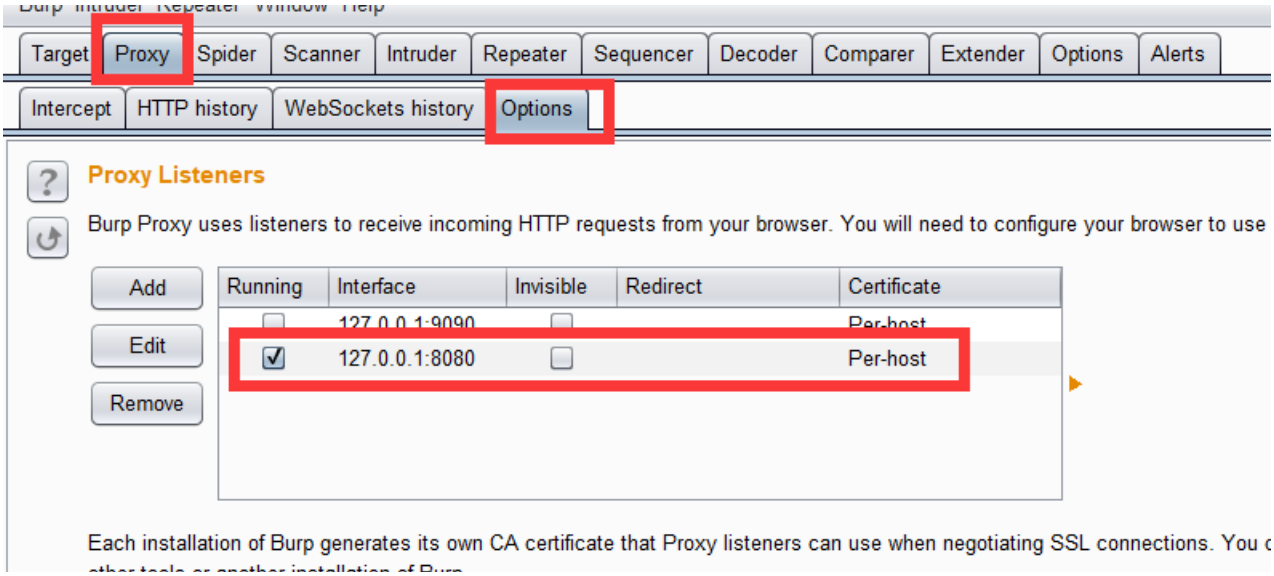


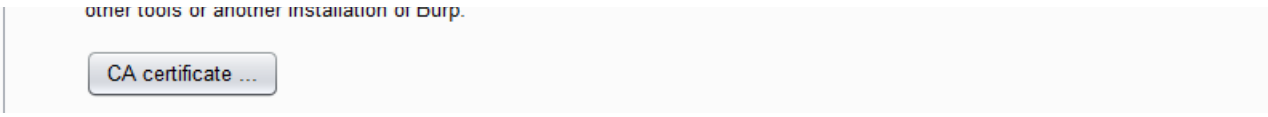
终于看到了可爱的颜文字，转成js之后进入题目页面，戳F12，切换到**命令行**窗口，把整个js放进去运行就得到flag了

单身二十年

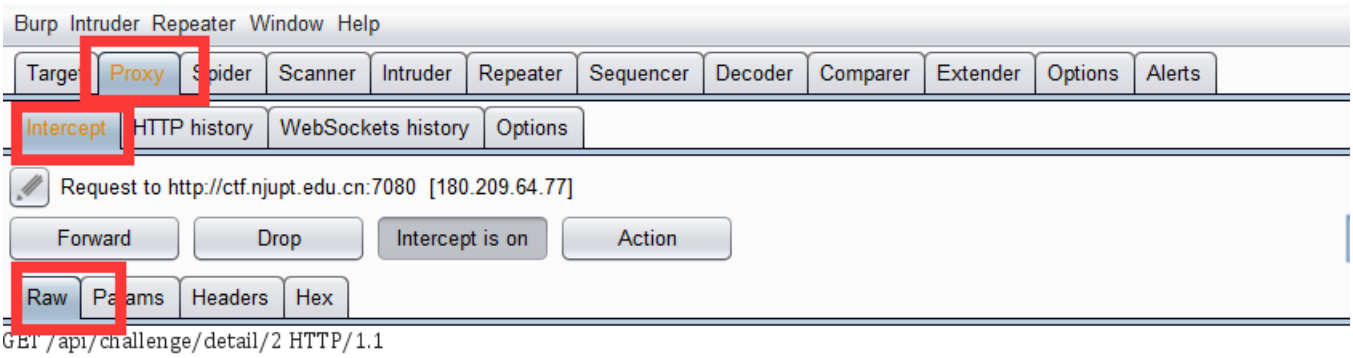
这题可以靠技术也可以靠手速！ 老夫单身二十年，自然靠的是手速！
看题目完全不知道在说啥，两个页面都戳了F12也没用，好吧再去看看dalao的题解
原来要抓包！是时候掏出burpsuite了。官网有free版本的，下载后是一个jar包，直接双击就能打开，不分操作系统
在使用之前先改一下代理，打开firefox的设置

通常burpsuite的配置不用改了，如果改过的可以看这里

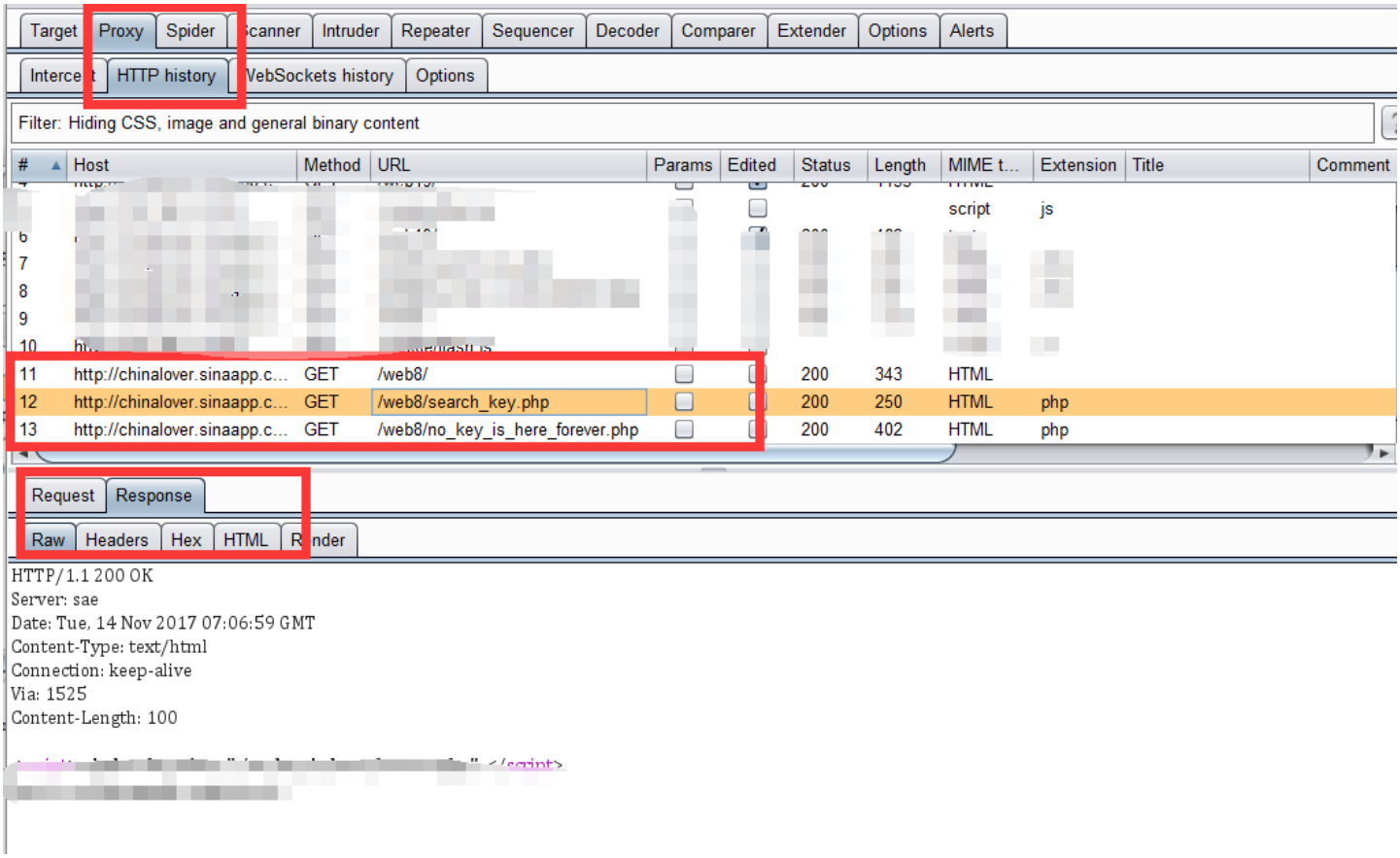




好了，开始抓包吧



刚才打开的界面刷新一下，burpsuite里就会出现抓到的数据包了。点击页面上的链接会发现无法跳转，在burpsuite上戳forward按钮，将截断的数据包重新发出去，就会跳到下一个页面了，没跳过去就多戳几下



……原来这就是需要多戳几下的理由，明明只有两个界面中间多出来的那个是啥玩意儿？
点开看数据包，查看数据包的response message，原来flag就在里面了

但是我不服输！不单身也必须有手速？！
所以来来回回看了好几遍
好吧，中间的确飞速闪过一个路径为search_key.php的url。
……
下一题

php decode

看看源码。本人不会php，所以碰到函数基本上网查

```
<?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;

}
eval(CLsI("+7DnQGFmYVZ+eoGmlg0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA=="));
?>
```