中科大HackerGame2018 web题目 writeup

原创

Smity(Liu) 于 2018-10-26 00:14:59 发布 2130 收藏 2
分类专栏： wp 文章标签： 中科大hackergame2018writeup

虽然很坑，但是总体来说这次还是做了很多有意思的web题，这里也只给出web题的答案

一：签到题

打开发现是要输入key值提交

签到题

本题的主要作用是向你展示获取 flag 的一般步骤：

1. 打开题目页面；（也就是本页面，你应该已经完成了）
2. 解题；（找到 flag）
3. 回到比赛平台提交 flag；
4. 完成！

是不是很简单！在本题中，你只要提交 hackergame2018 就可以得到 flag

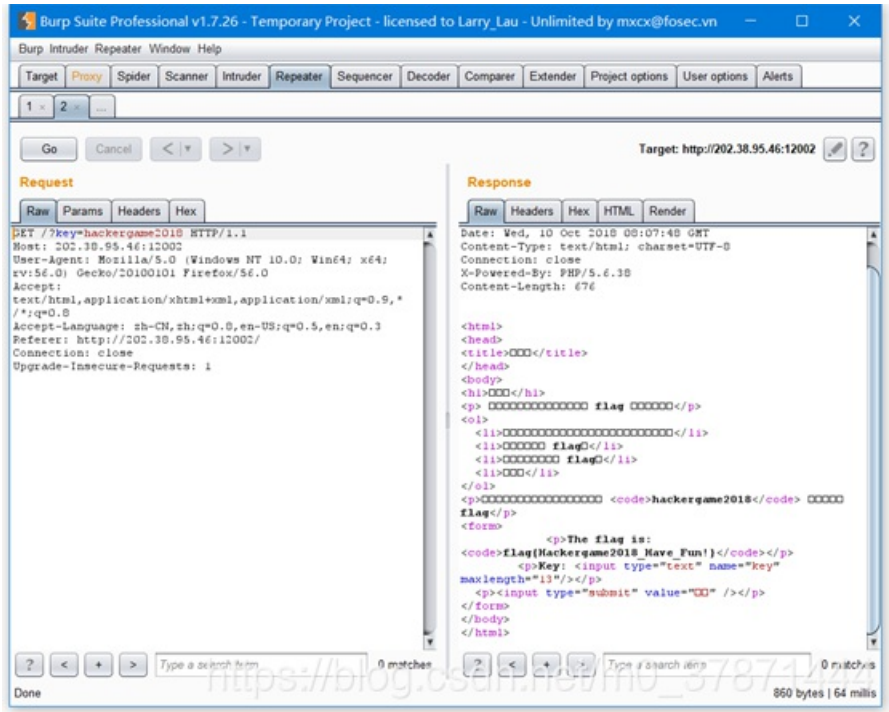
Key:

提交

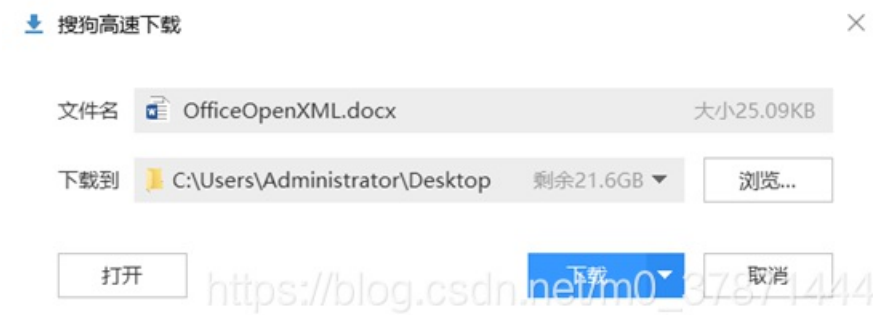

```
<html>
<head>
<title>签到题</title>
</head>
<body>
<h1>签到题</h1>
<p> 本题的主要作用是向你展示获取 flag 的一般步骤：</p>
<ol>
  <li>打开题目页面；（也就是本页面，你应该已经完成了）</li>
  <li>解题；（找到 flag）</li>
  <li>回到比赛平台提交 flag；</li>
  <li>完成！</li>
</ol>
<p>是不是很简单！在本题中，你只要提交 <code>hackergame2018</code> 就可以得到 flag</p>
<form>
    <p>Key: <input type="text" name="key" maxlength="13"/></p>
  <p><input type="submit" value="提交" /></p>
</form>
</body>
</html>
```


但是输入后发现限制了长度，只允许输入到hackergame201

打开burp，截包，改包，发送得到flag

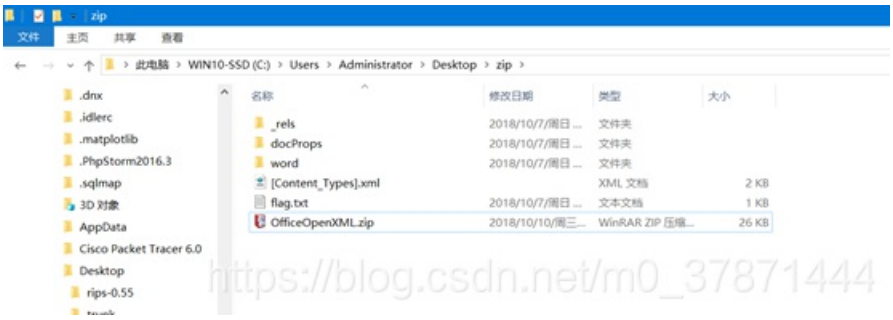


二：Word文档



打开题目链接发现是下载了一个officeopenXML.docx的文件

上网查阅发现这个是早期word推出的一种文件格式，其实可以改成zip格式并解压，修改后缀解压得到：



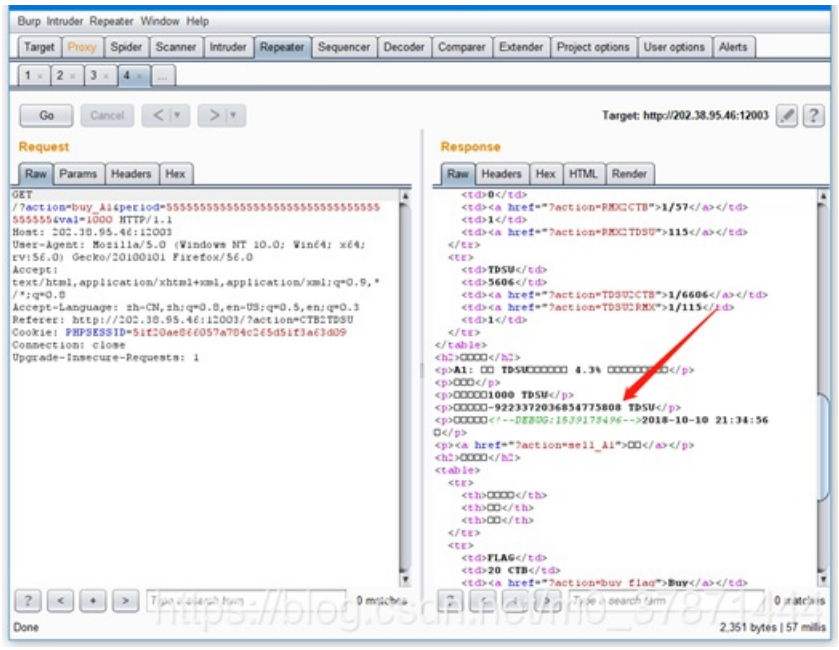
直接打开flag.txt就是答案了。

三：猫咪银行

以为是条件竞争，结果试了所有的按钮，都限制了访问频率，不是条件竞争的题目

唯一获取额外资源的地方，要求账号只有10分钟有效期，输入过量的时间试试

预计收益变成了负数，查看源代码



这里有脑洞，试了很久都没结果，后来才猜是利用了本地电脑时间做的一个十六进制加减法，写脚本跑

```php
<?php
$current_time = time();
echo $current_time;
$diff = 0xFFFFFFFF - $current_time;
echo $diff / 60;
?>
```

跑出来一个数字：153908197845931422
输进去得到：

理财产品

A1: 存入 TDSU，每分钟获得 4.3% 利息，最少一分钟。

已买入

买入份额：1000 TDSU

预计收益：6618052507375050752 TDSU

取出时间：-291924649100-07-30 21:05:04 后

取出

取出时间变成了负数，直接取出来就可以买了

四：黑曜石浏览器

唯一一道纯web题目，确实很坑

打开这个感觉是改UA，然后试了半天HEICORE都不对，是在没有办法，群里后来爆出来一个提示，真的有HEICORE这个浏览器，百度什么的都搜索不到，去谷歌上看发现实前不久刚刚建的一个网站，看起来是出题人故意为了题目设置的：www.heicore.com

访问后看到

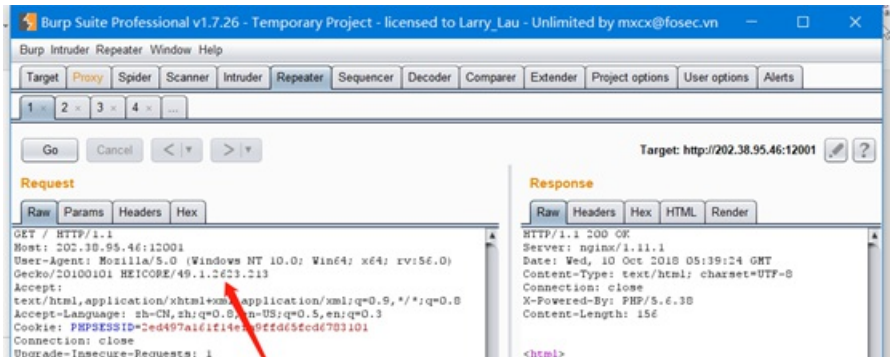
有下载的链接，但是需要登录，点击登录又需要先使用这个不存在的浏览器才可以，看来是死循环，想查看源码，发现没有办法查看

Curl之后发现了点：

看来其实网页是有一个exe的东西的，直接访问试试

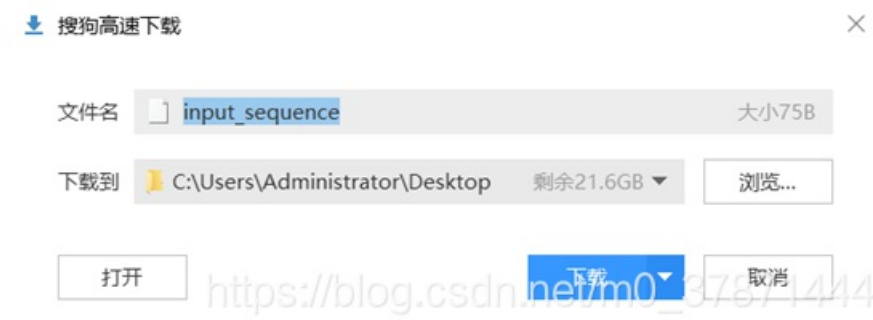
发现是一个假页面，直接F12保存那个exe发现是0字节，后来想想会不会是只想让我们知道这个49.1.2623.213这个版本号，拿到burp试着改ua

直接出来了flag



五：回到过去

题目告诉我们是ed编辑器的使用，搜索了一下发现ubuntu什么的都还有这个编辑器：



下载题目的文件打开：

```
q
ed
a
flag{
.
a
44a2b8
a3d9b2ESCc
c44039
f93345
}
.
2m3
2m5
2m1
2
s/4/t
q
q
```

题目告诉说是键盘记录，看着ed的命令走了一遍，有个点是esc c 的位置，那个是DEC VT终端的命令，不是ed的命令，就是返回到原来的命令行，和ed里面的“.”差不多，再加上个C就是替换最后一次的输入的位置，结果就是，显示如了44a2b8,再输入了a3d9b2，然后用c44039f93345替换了a3d9b2的位置，然后s/4/t将第一行的44a2b8的第一个4替换成t，就是flag了
走完以后的flag
flag{t4a2b8c44039f93345a3d9b2}

六：我是谁

第一关考察RFC2324愚人节彩蛋：
输入teapot直接就是flag了

Yes, I finally realized that I am a teapot!

This is my gift for you:

flag{i_canN0t_BReW_c0ffEE!}

Come to This Link, help me brew some tea, and you can get the 2nd FLAG!

第二关写脚本跑：
这里不能用python的request库，因为题目要求的请求方式为BREW，所以要么burp要么自己跑脚本，Content-Tyoe:message/teapot 是因为写message/cooffepot会报错，提示结合第一题flag，看到是i am not a coffepot，就换成了teapot。

```php
<?php
$socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
socket_connect($socket, "202.38.95.46", "12005");
$buffer = "BREW http://202.38.95.46:12005/the_super_great_hidden_url_for_brewing_tea/black_tea HTTP/1.0\r\n";
$buffer .= "Content-Type: message/teapot\r\n";
$buffer .= "\r\n\r\n";
socket_write($socket, $buffer);
sleep(1);
echo socket_read($socket, 2048);
socket_close($socket);
```