强网杯青少年赛部分writeup

原创

CSDNzr97 于 2020-09-18 20:02:38 发布 246 收藏

分类专栏： CTF-writeup 文章标签： 安全

本文链接：https://blog.csdn.net/CSDNzr97/article/details/108672094

简单算法

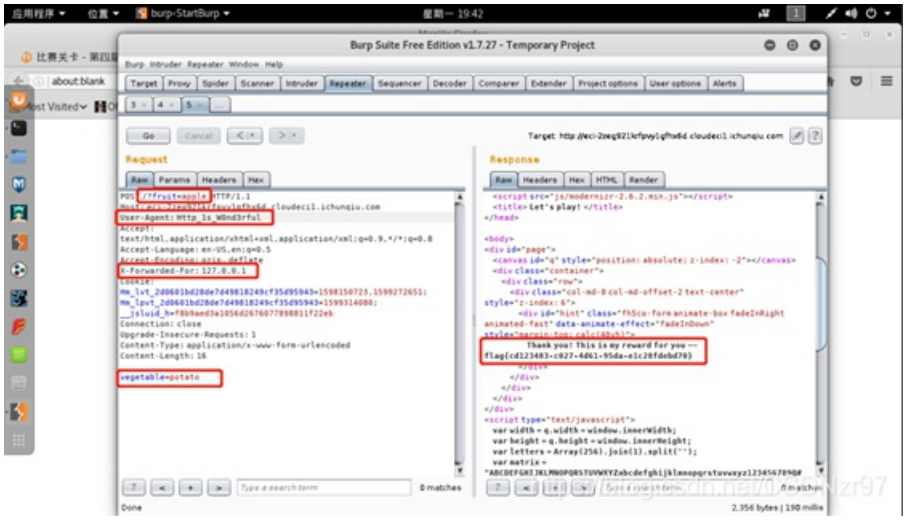
```
flag=""
def encode(a):
    s=[]
    k=0
    for i in a:
        k=k+1
        s.append((ord(i)^86)+k)
    return s

print encode(flag)
#[49, 60, 58, 53, 50, 107, 117, 63, 57, 107, 63, 109, 66, 137, 65, 119, 118, 128, 142, 118, 117, 118, 123, 147, 77, 126, 130, 124, 152, 80, 127, 134, 83, 87, 134, 87, 147, 148, 142, 95, 93, 85]
```

题目给出一个python文件，可以看到最后注释那里是加密后的flag
这种加密题先分析算法然后直接写python脚本逆回去

运行跑出flag

easy_http

题目给出网页链接，访问后页面提示传递一个GET参数（水果=苹果），然后直接url后面加上/?fruit=apple，访问后提示传递一个POST参数（蔬菜=土豆）。因为POST参数只能抓包添加。
访问eci-2zeg921krfpvy1gfhx6d.cloudeci1.ichunqiu.com/?fruit=apple
Burp抓包拦截首先将GET数据包改为POST数据包，然后在路径后加上?fruit=apple，实现同时传递GET参数和POST参数。
然后访问后提示需要由本地提交，因为我们是Burp抓包不是本地提交。想到http请求头中X-Forwarded-For字段代表源地址，所以添加这个字段，值为本地127.0.0.1。再次访问后发现页面提示需要有一个身份标识：Http_1s_W0nd3rful，通过尝试得出替换UA的值为：Http_1s_W0nd3rful。再次访问得到flag



easy_php

题目给了网址，访问发现是php代码审计，发现需要绕过三级验证，最后才能得到flag。
第一级绕过：

```
if( ($_GET['a1'] == $_GET['a2']) || (md5($_GET['a1']) != md5($_GET['a2'])) ){
die("No");
}
```

绕过思路php弱类型：a1[]=1a2[]=2（php里的MD5()函数在给数组加密的时候会返回null，实现绕过）
第二级绕过：

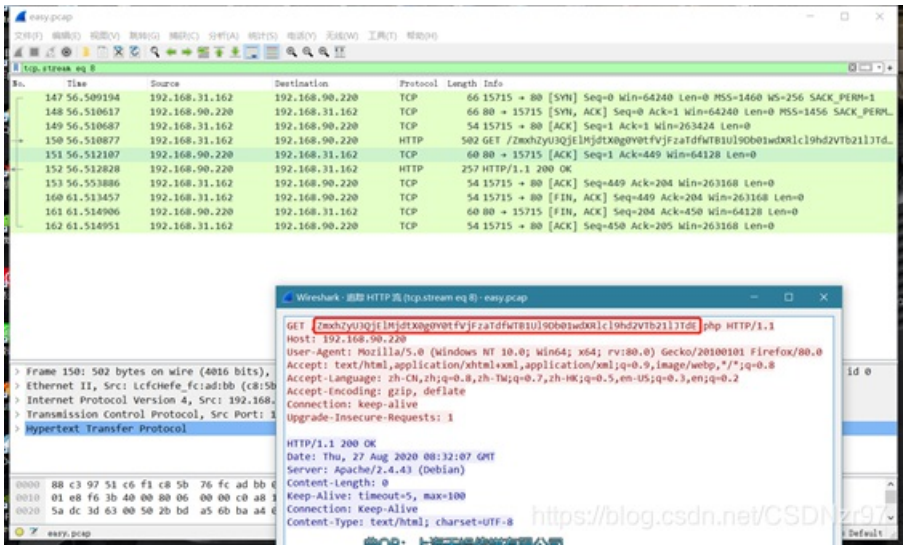
```
if( ($_GET['b1'] === $_GET['b2']) || (md5($_GET['b1']) !== md5($_GET['b2'])) ){
die("NoNo");
}
```

绕过思路php弱类型：b1[]=2&b2[]=3
第三级绕过：

```
if( strlen($_GET['time'])>4 || $_GET['time']<time() || is_array($_GET['time'])){
die("NoNoNo");
}
```

绕过思路：函数time()返回的是很大的数值，传入的time参数必须小于5位数，并且要大于time()函数的返回值，并且不能为数组。所以利用科学计数法传入一个很大的数值实现绕过。
time=9e12
最终payload：
http://eci-2ze57ktwcm7rytwozj99.cloudeci1.ichunqiu.com/?a1[]=1&a2[]=2& b1[]=2&b2[]=3& time=9e12
得到flag

easy_pcap



题目下载下来是数据包，分析数据包直接http追踪流，在第八个的时候看到一个类似base64加密的文件名。
解密后得到flag%7B1%27m_H4cK_V1si7_Y0uR_CoMputer_aweSome%7D
在进行url解码得到flag：flag{1'm_H4cK_V1si7_Y0uR_CoMputer_aweSome}

easy_Crypto

Crypto3_1.txt 内容 ﾟωﾟノ=/ｍ)ノ~┻━┻ //*´∇｀*/['_'];o=…这种是 aaencode 加密
解密网址:https://www.qtool.net/decode

所有 | 开发工具 | 站长工具 | 多媒体 | 生活查询 | 技巧分享

jjencode与aaencode解密

```
alert("You will use the number 5.");
```

解密后得到数字5
crypto3_2.png是猪圈密码
http://www.metools.info/code/c90.html网站解密后得到

摩斯密码翻译器

加密的内容：

解密的内容：

fpyitlythnsiaropiosengcgasstrgre

回退 清空

fpyitlyth__nsiaropiosengcgasstrg{r_e}

题目提示说是栅栏密码，从Crypto3_1.txt得到栏数为5，去http://www.atoolbox.net/Tool.php?Id=777解密得到flag

flag{cryptography_is_so_insteresting}

moss

打开文件得到一串摩斯密码,拿去解密得到 F L A G %u7b M O S S I S V E R Y F 4 N T Y %u7d ，

发现里面需要%u7b 和%u7d根据flag格式换成{ },提交后发现flag不对，看到题目写的是小写的流水滴滴答，

去https://www.iamwawa.cn/daxiaoxie.html转换为小写

得到flag：flag{mossisveryf4nty}