



easy_re

📅 2021-09-05 | 📁 Challenge , 2021 , 第七届全国工控系统信息安全攻防竞赛 , 二类

Challenge | 2021 | 第七届全国工控系统信息安全攻防竞赛 | 二类 | easy_re

[点击此处](#)获得更好的阅读体验

WriteUp来源

来自 毕方安全实验室 战队及 bad_cat 战队

题目描述

根据附件得出flag

提示信息

无

题目考点

- 逆向
- 换表base64

解题思路

下载附件，拖入IDA

```

3  sub_455D73(&unk_52E00A);
0  v7 = 0;
2  sub_455EA9("Usage: xxx.exe -e flag");
3  sub_455EA9("Usage: xxx.exe -x flag");
4  if ( a1 == 3 )
5  {
6      v7 = sub_455EA4(*(_DWORD *)(a2 + 8));
7      if ( !sub_453249("-e", *(_DWORD *)(a2 + 4)) )
8      {
9          sub_453AA0("%s\n", v7);
0 LABEL_14:
1      sub_454D56(v7);
2      LODWORD(v2) = 0;
3      goto LABEL_15;
4  }
5  if ( sub_453249("-x", *(_DWORD *)(a2 + 4)) )
6  {
7      sub_455EA9("error2!");
8      goto LABEL_14;
9  }
0  v6 = 0;
1  sub_454DBA(&v6, "ct.txt", "r");
2  if ( v6 )
3  {
4      sub_45407C(&v5, 255, v6);
5      if ( sub_453249(v7, &v5) )
6          sub_455EA9("No! The flag is wrong!");
7      else
8          sub_453AA0("Yes! The real flag is %s\n", *(_DWORD *)(a2 + 8));
9      goto LABEL_14;
0  }
1  sub_453CB7("File ct.txt opening failed");
2  LODWORD(v2) = 1;
3  }
4  else
5  {
6      sub_455EA9("error1!");
7      LODWORD(v2) = -1;
8  }
0 LABEL_15:
0  v3 = v2;
1  sub_454AC7(&savedregs, &dword_45AA04);

```



发现主要在 455EA4 处理数据，算法是 base64

```

int v3; // [esp+E0h] [ebp-2Ch]
int v4; // [esp+ECh] [ebp-20h]
int v5; // [esp+F8h] [ebp-14h]
int v6; // [esp+104h] [ebp-8h]

sub_455D73(&unk_52E003);
sub_4538ED();
sub_455A17();
v5 = sub_456138(a1);
if ( v5 % 3 )
    v6 = 4 * (v5 / 3) + 4;
else
    v6 = 4 * (v5 / 3);
v4 = sub_453357((v6 + 1) | -__CFADD__(v6, 1));
*(_BYTE *)(v6 + v4) = 0;
v3 = 0;
v2 = 0;
while ( v3 < v6 - 2 )
{
    *(_BYTE *)(v3 + v4) = *(_BYTE *)(&word_52AF44 + (((signed int)*(unsigned __int8 *) (v2 + a1) >> 2)));
    *(_BYTE *)(v3 + v4 + 1) = *(_BYTE *)(&word_52AF44
        + (((signed int)*(unsigned __int8 *) (v2 + a1 + 1) >> 4) | 16
        * (_BYTE *) (v2 + a1) & 3)));
    *(_BYTE *)(v3 + v4 + 2) = *(_BYTE *)(&word_52AF44
        + (((signed int)*(unsigned __int8 *) (v2 + a1 + 2) >> 6) | 4
        * (_BYTE *) (v2 + a1 + 1) & 0xF)));
    *(_BYTE *)(v3 + v4 + 3) = *(_BYTE *)(&word_52AF44 + (*(_BYTE *) (v2 + a1 + 2) & 0x3F));
    v2 += 3;
    v3 += 4;
}
if ( v5 % 3 == 1 )
{
    *(_BYTE *) (v3 + v4 - 2) = 61;
    *(_BYTE *) (v3 + v4 - 1) = 61;
}
else if ( v5 % 3 == 2 )
{
    *(_BYTE *) (v3 + v4 - 1) = 61;
}
return v4;
}

```

00007580 sub_45A180:1 (45A180)



CTFHub

进一步得出是换了码表的base64，继续跟踪得到码表



1 /+9876543210PUNSLQJOHMFKDIBGZEXCVATYRWjohmfkdibgzexcvatyrwpunslq

使用新的码表解密即为flag

Last build: A day ago

Recipe	Input
<div style="background-color: #e0f2f1; padding: 5px; margin-bottom: 5px;"> From Base64 <div style="float: right;">⏏ ⏸</div> </div> <div style="background-color: #e0f2f1; padding: 5px; margin-bottom: 5px;"> Alphabet /+9876543210PUNSLQJOHMFKDIBGZEXCVATYRWjohmfkdibgzexcva... </div> <div style="background-color: #e0f2f1; padding: 5px;"> <input checked="" type="checkbox"/> Remove non-alphabet chars </div>	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px; margin-bottom: 5px;"> OHA0LaDtQMqNORAF07iJMcVyOMR= </div> <div style="background-color: #f5f5f5; padding: 5px; margin-bottom: 5px;"> Output </div> <div style="border: 1px solid #ccc; padding: 5px;"> MHKCV6ETNNHVLKRW87MY </div>

CTFHub

```

Usage: xxx.exe -e flag
Usage: xxx.exe -x flag
Yes! The real flag is MHKCV6ETNNHVLKRW87MY

```

Flag



```
1  flag{MHKCV6ETNNHVLKRW87MY}
```

本文作者：CTFHub

本文链接：<https://writeup.ctfhub.com/Challenge/2021/第七届全国工控系统信息安全攻防竞赛/二类/38oPFjZ2ZeyDXvHHb8bTJX.html>

版权声明： 本博客所有文章除特别声明外，均采用 [©BY-NC-SA](#) 许可协议。转载请注明出处！

[# Challenge](#) [# 2021](#) [# 第七届全国工控系统信息安全攻防竞赛](#) [# 二类](#)

[← base64](#)

[Web2 →](#)

© 2019 – 2022 CTFHub

由 [Hexo](#) & [NexT.Gemini](#) 强力驱动