

BUUCTF Reverse reverse3 WriteUp

原创

[PlumpBoy](#)



于 2021-09-10 18:42:24 发布



307



收藏

分类专栏: [BUUCTF 逆向题解](#) 文章标签: [系统安全](#) [安全](#)

版权声明: 本文为博主原创文章, 遵循[CC 4.0 BY-SA](#)版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_45723661/article/details/120227888

版权



[BUUCTF 逆向题解 专栏收录该内容](#)

18 篇文章 1 订阅

订阅专栏

reverse3-WP

首先扔到IDA里面, 解析出主函数如下

```

int __cdecl main_0(int argc, const char **argv, const char **envp)
{
    int v3; // ebx
    int v4; // edi
    int v5; // esi
    int v6; // eax
    const char *v7; // eax
    size_t v8; // eax
    char v10; // [esp+0h] [ebp-188h]
    char v11; // [esp+0h] [ebp-188h]
    signed int j; // [esp+DCh] [ebp-ACh]
    int i; // [esp+E8h] [ebp-A0h]
    signed int v14; // [esp+E8h] [ebp-A0h]
    char Destination[108]; // [esp+F4h] [ebp-94h] BYREF
    char Str[28]; // [esp+160h] [ebp-28h] BYREF
    char v17[8]; // [esp+17Ch] [ebp-Ch] BYREF

//初始化为0
    for ( i = 0; i < 100; ++i )
    {
        if ( (unsigned int)i >= 0x64 )
            j____report_rangecheckfailure(v3, v4, v5);
        Destination[i] = 0;
    }

    sub_41132F("please enter the flag:", v10);
    sub_411375("%20s", (char)Str);
    v6 = j_strlen(Str);
    v7 = (const char *)sub_4110BE((int)Str, v6, (int)v17); //关键点

    strcpy(Destination, v7, 0x28u);
    v14 = j_strlen(Destination);

    for ( j = 0; j < v14; ++j )
        Destination[j] += j; //每个成员向后移动j位
    v8 = j_strlen(Destination);
    if ( !strcmp(Destination, Str2, v8) ) //与str2进行比较
        sub_41132F("right flag!\n", v11);
    else
        sub_41132F("wrong flag!\n", v11);
    return 0;
}

```

通过观察发现sub_4110BE是关键函数，转到函数查看

```

void * __cdecl sub_411AB0(char *a1, unsigned int a2, int *a3)
{
    int v4; // [esp+D4h] [ebp-38h]
    int v5; // [esp+D4h] [ebp-38h]
    int v6; // [esp+D4h] [ebp-38h]
    int v7; // [esp+D4h] [ebp-38h]
    int i; // [esp+E0h] [ebp-2Ch]
    unsigned int v9; // [esp+ECh] [ebp-20h]
    int v10; // [esp+ECh] [ebp-20h]
    int v11; // [esp+ECh] [ebp-20h]
    void *v12; // [esp+F8h] [ebp-14h]
    char *v13; // [esp+104h] [ebp-8h]

    if ( !a1 || !a2 )
        return 0;
    if ( !a3 )
        return 0;
    if ( a1 == v12 )
        *a3 = 1;
    if ( a1 == v13 )
        *a3 = 2;
    if ( a1 == v10 )
        *a3 = 3;
    if ( a1 == v9 )
        *a3 = 4;
    if ( a1 == v5 )
        *a3 = 5;
    if ( a1 == v6 )
        *a3 = 6;
    if ( a1 == v7 )
        *a3 = 7;
    if ( a1 == v4 )
        *a3 = 8;
    if ( a1 == v11 )
        *a3 = 9;
    if ( a1 == v12 )
        *a3 = 10;
    if ( a1 == v13 )
        *a3 = 11;
    if ( a1 == v9 )
        *a3 = 12;
    if ( a1 == v10 )
        *a3 = 13;
    if ( a1 == v5 )
        *a3 = 14;
    if ( a1 == v6 )
        *a3 = 15;
    if ( a1 == v7 )
        *a3 = 16;
    if ( a1 == v4 )
        *a3 = 17;
    if ( a1 == v11 )
        *a3 = 18;
    if ( a1 == v12 )
        *a3 = 19;
    if ( a1 == v13 )
        *a3 = 20;
    if ( a1 == v9 )
        *a3 = 21;
    if ( a1 == v10 )
        *a3 = 22;
    if ( a1 == v5 )
        *a3 = 23;
    if ( a1 == v6 )
        *a3 = 24;
    if ( a1 == v7 )
        *a3 = 25;
    if ( a1 == v4 )
        *a3 = 26;
    if ( a1 == v11 )
        *a3 = 27;
    if ( a1 == v12 )
        *a3 = 28;
    if ( a1 == v13 )
        *a3 = 29;
    if ( a1 == v9 )
        *a3 = 30;
    if ( a1 == v10 )
        *a3 = 31;
    if ( a1 == v5 )
        *a3 = 32;
    if ( a1 == v6 )
        *a3 = 33;
    if ( a1 == v7 )
        *a3 = 34;
    if ( a1 == v4 )
        *a3 = 35;
    if ( a1 == v11 )
        *a3 = 36;
    if ( a1 == v12 )
        *a3 = 37;
    if ( a1 == v13 )
        *a3 = 38;
    if ( a1 == v9 )
        *a3 = 39;
    if ( a1 == v10 )
        *a3 = 40;
    if ( a1 == v5 )
        *a3 = 41;
    if ( a1 == v6 )
        *a3 = 42;
    if ( a1 == v7 )
        *a3 = 43;
    if ( a1 == v4 )
        *a3 = 44;
    if ( a1 == v11 )
        *a3 = 45;
    if ( a1 == v12 )
        *a3 = 46;
    if ( a1 == v13 )
        *a3 = 47;
    if ( a1 == v9 )
        *a3 = 48;
    if ( a1 == v10 )
        *a3 = 49;
    if ( a1 == v5 )
        *a3 = 50;
    if ( a1 == v6 )
        *a3 = 51;
    if ( a1 == v7 )
        *a3 = 52;
    if ( a1 == v4 )
        *a3 = 53;
    if ( a1 == v11 )
        *a3 = 54;
    if ( a1 == v12 )
        *a3 = 55;
    if ( a1 == v13 )
        *a3 = 56;
    if ( a1 == v9 )
        *a3 = 57;
    if ( a1 == v10 )
        *a3 = 58;
    if ( a1 == v5 )
        *a3 = 59;
    if ( a1 == v6 )
        *a3 = 60;
    if ( a1 == v7 )
        *a3 = 61;
    if ( a1 == v4 )
        *a3 = 62;
    if ( a1 == v11 )
        *a3 = 63;
    if ( a1 == v12 )
        *a3 = 64;
    if ( a1 == v13 )
        *a3 = 65;
    if ( a1 == v9 )
        *a3 = 66;
    if ( a1 == v10 )
        *a3 = 67;
    if ( a1 == v5 )
        *a3 = 68;
    if ( a1 == v6 )
        *a3 = 69;
    if ( a1 == v7 )
        *a3 = 70;
    if ( a1 == v4 )
        *a3 = 71;
    if ( a1 == v11 )
        *a3 = 72;
    if ( a1 == v12 )
        *a3 = 73;
    if ( a1 == v13 )
        *a3 = 74;
    if ( a1 == v9 )
        *a3 = 75;
    if ( a1 == v10 )
        *a3 = 76;
    if ( a1 == v5 )
        *a3 = 77;
    if ( a1 == v6 )
        *a3 = 78;
    if ( a1 == v7 )
        *a3 = 79;
    if ( a1 == v4 )
        *a3 = 80;
    if ( a1 == v11 )
        *a3 = 81;
    if ( a1 == v12 )
        *a3 = 82;
    if ( a1 == v13 )
        *a3 = 83;
    if ( a1 == v9 )
        *a3 = 84;
    if ( a1 == v10 )
        *a3 = 85;
    if ( a1 == v5 )
        *a3 = 86;
    if ( a1 == v6 )
        *a3 = 87;
    if ( a1 == v7 )
        *a3 = 88;
    if ( a1 == v4 )
        *a3 = 89;
    if ( a1 == v11 )
        *a3 = 90;
    if ( a1 == v12 )
        *a3 = 91;
    if ( a1 == v13 )
        *a3 = 92;
    if ( a1 == v9 )
        *a3 = 93;
    if ( a1 == v10 )
        *a3 = 94;
    if ( a1 == v5 )
        *a3 = 95;
    if ( a1 == v6 )
        *a3 = 96;
    if ( a1 == v7 )
        *a3 = 97;
    if ( a1 == v4 )
        *a3 = 98;
    if ( a1 == v11 )
        *a3 = 99;
    if ( a1 == v12 )
        *a3 = 100;
    if ( a1 == v13 )
        *a3 = 101;
    if ( a1 == v9 )
        *a3 = 102;
    if ( a1 == v10 )
        *a3 = 103;
    if ( a1 == v5 )
        *a3 = 104;
    if ( a1 == v6 )
        *a3 = 105;
    if ( a1 == v7 )
        *a3 = 106;
    if ( a1 == v4 )
        *a3 = 107;
    if ( a1 == v11 )
        *a3 = 108;
    if ( a1 == v12 )
        *a3 = 109;
    if ( a1 == v13 )
        *a3 = 110;
    if ( a1 == v9 )
        *a3 = 111;
    if ( a1 == v10 )
        *a3 = 112;
    if ( a1 == v5 )
        *a3 = 113;
    if ( a1 == v6 )
        *a3 = 114;
    if ( a1 == v7 )
        *a3 = 115;
    if ( a1 == v4 )
        *a3 = 116;
    if ( a1 == v11 )
        *a3 = 117;
    if ( a1 == v12 )
        *a3 = 118;
    if ( a1 == v13 )
        *a3 = 119;
    if ( a1 == v9 )
        *a3 = 120;
    if ( a1 == v10 )
        *a3 = 121;
    if ( a1 == v5 )
        *a3 = 122;
    if ( a1 == v6 )
        *a3 = 123;
    if ( a1 == v7 )
        *a3 = 124;
    if ( a1 == v4 )
        *a3 = 125;
    if ( a1 == v11 )
        *a3 = 126;
    if ( a1 == v12 )
        *a3 = 127;
    if ( a1 == v13 )
        *a3 = 128;
    if ( a1 == v9 )
        *a3 = 129;
    if ( a1 == v10 )
        *a3 = 130;
    if ( a1 == v5 )
        *a3 = 131;
    if ( a1 == v6 )
        *a3 = 132;
    if ( a1 == v7 )
        *a3 = 133;
    if ( a1 == v4 )
        *a3 = 134;
    if ( a1 == v11 )
        *a3 = 135;
    if ( a1 == v12 )
        *a3 = 136;
    if ( a1 == v13 )
        *a3 = 137;
    if ( a1 == v9 )
        *a3 = 138;
    if ( a1 == v10 )
        *a3 = 139;
    if ( a1 == v5 )
        *a3 = 140;
    if ( a1 == v6 )
        *a3 = 141;
    if ( a1 == v7 )
        *a3 = 142;
    if ( a1 == v4 )
        *a3 = 143;
    if ( a1 == v11 )
        *a3 = 144;
    if ( a1 == v12 )
        *a3 = 145;
    if ( a1 == v13 )
        *a3 = 146;
    if ( a1 == v9 )
        *a3 = 147;
    if ( a1 == v10 )
        *a3 = 148;
    if ( a1 == v5 )
        *a3 = 149;
    if ( a1 == v6 )
        *a3 = 150;
    if ( a1 == v7 )
        *a3 = 151;
    if ( a1 == v4 )
        *a3 = 152;
    if ( a1 == v11 )
        *a3 = 153;
    if ( a1 == v12 )
        *a3 = 154;
    if ( a1 == v13 )
        *a3 = 155;
    if ( a1 == v9 )
        *a3 = 156;
    if ( a1 == v10 )
        *a3 = 157;
    if ( a1 == v5 )
        *a3 = 158;
    if ( a1 == v6 )
        *a3 = 159;
    if ( a1 == v7 )
        *a3 = 160;
    if ( a1 == v4 )
        *a3 = 161;
    if ( a1 == v11 )
        *a3 = 162;
    if ( a1 == v12 )
        *a3 = 163;
    if ( a1 == v13 )
        *a3 = 164;
    if ( a1 == v9 )
        *a3 = 165;
    if ( a1 == v10 )
        *a3 = 166;
    if ( a1 == v5 )
        *a3 = 167;
    if ( a1 == v6 )
        *a3 = 168;
    if ( a1 == v7 )
        *a3 = 169;
    if ( a1 == v4 )
        *a3 = 170;
    if ( a1 == v11 )
        *a3 = 171;
    if ( a1 == v12 )
        *a3 = 172;
    if ( a1 == v13 )
        *a3 = 173;
    if ( a1 == v9 )
        *a3 = 174;
    if ( a1 == v10 )
        *a3 = 175;
    if ( a1 == v5 )
        *a3 = 176;
    if ( a1 == v6 )
        *a3 = 177;
    if ( a1 == v7 )
        *a3 = 178;
    if ( a1 == v4 )
        *a3 = 179;
    if ( a1 == v11 )
        *a3 = 180;
    if ( a1 == v12 )
        *a3 = 181;
    if ( a1 == v13 )
        *a3 = 182;
    if ( a1 == v9 )
        *a3 = 183;
    if ( a1 == v10 )
        *a3 = 184;
    if ( a1 == v5 )
        *a3 = 185;
    if ( a1 == v6 )
        *a3 = 186;
    if ( a1 == v7 )
        *a3 = 187;
    if ( a1 == v4 )
        *a3 = 188;
    if ( a1 == v11 )
        *a3 = 189;
    if ( a1 == v12 )
        *a3 = 190;
    if ( a1 == v13 )
        *a3 = 191;
    if ( a1 == v9 )
        *a3 = 192;
    if ( a1 == v10 )
        *a3 = 193;
    if ( a1 == v5 )
        *a3 = 194;
    if ( a1 == v6 )
        *a3 = 195;
    if ( a1 == v7 )
        *a3 = 196;
    if ( a1 == v4 )
        *a3 = 197;
    if ( a1 == v11 )
        *a3 = 198;
    if ( a1 == v12 )
        *a3 = 199;
    if ( a1 == v13 )
        *a3 = 200;
    if ( a1 == v9 )
        *a3 = 201;
    if ( a1 == v10 )
        *a3 = 202;
    if ( a1 == v5 )
        *a3 = 203;
    if ( a1 == v6 )
        *a3 = 204;
    if ( a1 == v7 )
        *a3 = 205;
    if ( a1 == v4 )
        *a3 = 206;
    if ( a1 == v11 )
        *a3 = 207;
    if ( a1 == v12 )
        *a3 = 208;
    if ( a1 == v13 )
        *a3 = 209;
    if ( a1 == v9 )
        *a3 = 210;
    if ( a1 == v10 )
        *a3 = 211;
    if ( a1 == v5 )
        *a3 = 212;
    if ( a1 == v6 )
        *a3 = 213;
    if ( a1 == v7 )
        *a3 = 214;
    if ( a1 == v4 )
        *a3 = 215;
    if ( a1 == v11 )
        *a3 = 216;
    if ( a1 == v12 )
        *a3 = 217;
    if ( a1 == v13 )
        *a3 = 218;
    if ( a1 == v9 )
        *a3 = 219;
    if ( a1 == v10 )
        *a3 = 220;
    if ( a1 == v5 )
        *a3 = 221;
    if ( a1 == v6 )
        *a3 = 222;
    if ( a1 == v7 )
        *a3 = 223;
    if ( a1 == v4 )
        *a3 = 224;
    if ( a1 == v11 )
        *a3 = 225;
    if ( a1 == v12 )
        *a3 = 226;
    if ( a1 == v13 )
        *a3 = 227;
    if ( a1 == v9 )
        *a3 = 228;
    if ( a1 == v10 )
        *a3 = 229;
    if ( a1 == v5 )
        *a3 = 230;
    if ( a1 == v6 )
        *a3 = 231;
    if ( a1 == v7 )
        *a3 = 232;
    if ( a1 == v4 )
        *a3 = 233;
    if ( a1 == v11 )
        *a3 = 234;
    if ( a1 == v12 )
        *a3 = 235;
    if ( a1 == v13 )
        *a3 = 236;
    if ( a1 == v9 )
        *a3 = 237;
    if ( a1 == v10 )
        *a3 = 238;
    if ( a1 == v5 )
        *a3 = 239;
    if ( a1 == v6 )
        *a3 = 240;
    if ( a1 == v7 )
        *a3 = 241;
    if ( a1 == v4 )
        *a3 = 242;
    if ( a1 == v11 )
        *a3 = 243;
    if ( a1 == v12 )
        *a3 = 244;
    if ( a1 == v13 )
        *a3 = 245;
    if ( a1 == v9 )
        *a3 = 246;
    if ( a1 == v10 )
        *a3 = 247;
    if ( a1 == v5 )
        *a3 = 248;
    if ( a1 == v6 )
        *a3 = 249;
    if ( a1 == v7 )
        *a3 = 250;
    if ( a1 == v4 )
        *a3 = 251;
    if ( a1 == v11 )
        *a3 = 252;
    if ( a1 == v12 )
        *a3 = 253;
    if ( a1 == v13 )
        *a3 = 254;
    if ( a1 == v9 )
        *a3 = 255;
    if ( a1 == v10 )
        *a3 = 256;
    if ( a1 == v5 )
        *a3 = 257;
    if ( a1 == v6 )
        *a3 = 258;
    if ( a1 == v7 )
        *a3 = 259;
    if ( a1 == v4 )
        *a3 = 260;
    if ( a1 == v11 )
        *a3 = 261;
    if ( a1 == v12 )
        *a3 = 262;
    if ( a1 == v13 )
        *a3 = 263;
    if ( a1 == v9 )
        *a3 = 264;
    if ( a1 == v10 )
        *a3 = 265;
    if ( a1 == v5 )
        *a3 = 266;
    if ( a1 == v6 )
        *a3 = 267;
    if ( a1 == v7 )
        *a3 = 268;
    if ( a1 == v4 )
        *a3 = 269;
    if ( a1 == v11 )
        *a3 = 270;
    if ( a1 == v12 )
        *a3 = 271;
    if ( a1 == v13 )
        *a3 = 272;
    if ( a1 == v9 )
        *a3 = 273;
    if ( a1 == v10 )
        *a3 = 274;
    if ( a1 == v5 )
        *a3 = 275;
    if ( a1 == v6 )
        *a3 = 276;
    if ( a1 == v7 )
        *a3 = 277;
    if ( a1 == v4 )
        *a3 = 278;
    if ( a1 == v11 )
        *a3 = 279;
    if ( a1 == v12 )
        *a3 = 280;
    if ( a1 == v13 )
        *a3 = 281;
    if ( a1 == v9 )
        *a3 = 282;
    if ( a1 == v10 )
        *a3 = 283;
    if ( a1 == v5 )
        *a3 = 284;
    if ( a1 == v6 )
        *a3 = 285;
    if ( a1 == v7 )
        *a3 = 286;
    if ( a1 == v4 )
        *a3 = 287;
    if ( a1 == v11 )
        *a3 = 288;
    if ( a1 == v12 )
        *a3 = 289;
    if ( a1 == v13 )
        *a3 = 290;
    if ( a1 == v9 )
        *a3 = 291;
    if ( a1 == v10 )
        *a3 = 292;
    if ( a1 == v5 )
        *a3 = 293;
    if ( a1 == v6 )
        *a3 = 294;
    if ( a1 == v7 )
        *a3 = 295;
    if ( a1 == v4 )
        *a3 = 296;
    if ( a1 == v11 )
        *a3 = 297;
    if ( a1 == v12 )
        *a3 = 298;
    if ( a1 == v13 )
        *a3 = 299;
    if ( a1 == v9 )
        *a3 = 300;
    if ( a1 == v10 )
        *a3 = 301;
    if ( a1 == v5 )
        *a3 = 302;
    if ( a1 == v6 )
        *a3 = 303;
    if ( a1 == v7 )
        *a3 = 304;
    if ( a1 == v4 )
        *a3 = 305;
    if ( a1 == v11 )
        *a3 = 306;
    if ( a1 == v12 )
        *a3 = 307;
    if ( a1 == v13 )
        *a3 = 308;
    if ( a1 == v9 )
        *a3 = 309;
    if ( a1 == v10 )
        *a3 = 310;
    if ( a1 == v5 )
        *a3 = 311;
    if ( a1 == v6 )
        *a3 = 312;
    if ( a1 == v7 )
        *a3 = 313;
    if ( a1 == v4 )
        *a3 = 314;
    if ( a1 == v11 )
        *a3 = 315;
    if ( a1 == v12 )
        *a3 = 316;
    if ( a1 == v13 )
        *a3 = 317;
    if ( a1 == v9 )
        *a3 = 318;
    if ( a1 == v10 )
        *a3 = 319;
    if ( a1 == v5 )
        *a3 = 320;
    if ( a1 == v6 )
        *a3 = 321;
    if ( a1 == v7 )
        *a3 = 322;
    if ( a1 == v4 )
        *a3 = 323;
    if ( a1 == v11 )
        *a3 = 324;
    if ( a1 == v12 )
        *a3 = 325;
    if ( a1 == v13 )
        *a3 = 326;
    if ( a1 == v9 )
        *a3 = 327;
    if ( a1 == v10 )
        *a3 = 328;
    if ( a1 == v5 )
        *a3 = 329;
    if ( a1 == v6 )
        *a3 = 330;
    if ( a1 == v7 )
        *a3 = 331;
    if ( a1 == v4 )
        *a3 = 332;
    if ( a1 == v11 )
        *a3 = 333;
    if ( a1 == v12 )
        *a3 = 334;
    if ( a1 == v13 )
        *a3 = 335;
    if ( a1 == v9 )
        *a3 = 336;
    if ( a1 == v10 )
        *a3 = 337;
    if ( a1 == v5 )
        *a3 = 338;
    if ( a1 == v6 )
        *a3 = 339;
    if ( a1 == v7 )
        *a3 = 340;
    if ( a1 == v4 )
        *a3 = 341;
    if ( a1 == v11 )
        *a3 = 342;
    if ( a1 == v12 )
        *a3 = 343;
    if ( a1 == v13 )
        *a3 = 344;
    if ( a1 == v9 )
        *a3 = 345;
    if ( a1 == v10 )
        *a3 = 346;
    if ( a1 == v5 )
        *a3 = 347;
    if ( a1 == v6 )
        *a3 = 348;
    if ( a1 == v7 )
        *a3 = 349;
    if ( a1 == v4 )
        *a3 = 350;
    if ( a1 == v11 )
        *a3 = 351;
    if ( a1 == v12 )
        *a3 = 352;
    if ( a1 == v13 )
        *a3 = 353;
    if ( a1 == v9 )
        *a3 = 354;
    if ( a1 == v10 )
        *a3 = 355;
    if ( a1 == v5 )
        *a3 = 356;
    if ( a1 == v6 )
        *a3 = 357;
    if ( a1 == v7 )
        *a3 = 358;
    if ( a1 == v4 )
        *a3 = 359;
    if ( a1 == v11 )
        *a3 = 360;
    if ( a1 == v12 )
        *a3 = 361;
    if ( a1 == v13 )
        *a3 = 362;
    if ( a1 == v9 )
        *a3 = 363;
    if ( a1 == v10 )
        *a3 = 364;
    if ( a1 == v5 )
        *a3 = 365;
    if ( a1 == v6 )
        *a3 = 366;
    if ( a1 == v7 )
        *a3 = 367;
    if ( a1 == v4 )
        *a3 = 368;
    if ( a1 == v11 )
        *a3 = 369;
    if ( a1 == v12 )
        *a3 = 370;
    if ( a1 == v13 )
        *a3 = 371;
    if ( a1 == v9 )
        *a3 = 372;
    if ( a1 == v10 )
        *a3 = 373;
    if ( a1 == v5 )
        *a3 = 374;
    if ( a1 == v6 )
        *a3 = 375;
    if ( a1 == v7 )
        *a3 = 376;
    if ( a1 == v4 )
        *a3 = 377;
    if ( a1 == v11 )
        *a3 = 378;
    if ( a1 == v12 )
        *a3 = 379;
    if ( a1 == v13 )
        *a3 = 380;
    if ( a1 == v9 )
        *a3 = 381;
    if ( a1 == v10 )
        *a3 = 382;
    if ( a1 == v5 )
        *a3 = 383;
    if ( a1 == v6 )
        *a3 = 384;
    if ( a1 == v7 )
        *a3 = 385;
    if ( a1 == v4 )
        *a3 = 386;
    if ( a1 == v11 )
        *a3 = 387;
    if ( a1 == v12 )
        *a3 = 388;
    if ( a1 == v13 )
        *a3 = 389;
    if ( a1 == v9 )
        *a3 = 390;
    if ( a1 == v10 )
        *a3 = 391;
    if ( a1 == v5 )
        *a3 = 392;
    if ( a1 == v6 )
        *a3 = 393;
    if ( a1 == v7 )
        *a3 = 394;
    if ( a1 == v4 )
        *a3 = 395;
    if ( a1 == v11 )
        *a3 = 396;
    if ( a1 == v12 )
        *a3 = 397;
    if ( a1 == v13 )
        *a3 = 398;
    if ( a1 == v9 )
        *a3 = 399;
    if ( a1 == v10 )
        *a3 = 400;
    if ( a1 == v5 )
        *a3 = 401;
    if ( a1 == v6 )
        *a3 = 402;
    if ( a1 == v7 )
        *a3 = 403;
    if ( a1 == v4 )
        *a3 = 404;
    if ( a1 == v11 )
        *a3 = 405;
    if ( a1 == v12 )
        *a3 = 406;
    if ( a1 == v13 )
        *a3 = 407;
    if ( a1 == v9 )
        *a3 = 408;
    if ( a1 == v10 )
        *a3 = 409;
    if ( a1 == v5 )
        *a3 = 410;
    if ( a1 == v6 )
        *a3 = 411;
    if ( a1 == v7 )
        *a3 = 412;
    if ( a1 == v4 )
        *a3 = 413;
    if ( a1 == v11 )
        *a3 = 414;
    if ( a1 == v12 )
        *a3 = 415;
    if ( a1 == v13 )
        *a3 = 416;
    if ( a1 == v9 )
        *a3 = 417;
    if ( a1 == v10 )
        *a3 = 418;
    if ( a1 == v5 )
        *a3 = 419;
    if ( a1 == v6 )
        *a3 = 420;
    if ( a1 == v7 )
        *a3 = 421;
    if ( a1 == v4 )
        *a3 = 422;
    if ( a1 == v11 )
        *a3 = 423;
    if ( a1 == v12 )
        *a3 = 424;
    if ( a1 == v13 )
        *a3 = 425;
    if ( a1 == v9 )
        *a3 = 426;
    if ( a1 == v10 )
        *a3 = 427;
    if ( a1 == v5 )
        *a3 = 428;
    if ( a1 == v6 )
        *a3 = 429;
    if ( a1 == v7 )
        *a3 = 430;
    if ( a1 == v4 )
        *a3 = 431;
    if ( a1 == v11 )
        *a3 = 432;
    if ( a1 == v12 )
        *a3 = 433;
    if ( a1 == v13 )
        *a3 = 434;
    if ( a1 == v9 )
        *a3 = 435;
    if ( a1 == v10 )
        *a3 = 436;
    if ( a1 == v5 )
        *a3 = 437;
    if ( a1 == v6 )
        *a3 = 438;
    if ( a1 == v7 )
        *a3 = 439;
    if ( a1 == v4 )
        *a3 = 440;
    if ( a1 == v11 )
        *a3 = 441;
    if ( a1 == v12 )
        *a3 = 442;
    if ( a1 == v13 )
        *a3 = 443;
    if ( a1 == v9 )
        *a3 = 444;
    if ( a1 == v10 )
        *a3 = 445;
    if ( a1 == v5 )
        *a3 = 446;
    if ( a1 == v6 )
        *a3 = 447;
    if ( a1 == v7 )
        *a3 = 448;
    if ( a1 == v4 )
        *a3 = 449;
    if ( a1 == v11 )
        *a3 = 450;
    if ( a1 == v12 )
        *a3 = 451;
    if ( a1 == v13 )
        *a3 = 452;
    if ( a1 == v9 )
        *a3 = 453;
    if ( a1 == v10 )
        *a3 = 454;
    if ( a1 == v5 )
        *a3 = 455;
    if ( a1 == v6 )
        *a3 = 456;
    if ( a1 == v7 )
        *a3 = 457;
    if ( a1 == v4 )
        *a3 = 458;
    if ( a1 == v11 )
        *a3 = 459;
    if ( a1 == v12 )
        *a3 = 460;
    if ( a1 == v13 )
        *a3 = 461;
    if ( a1 == v9 )
        *a3 = 462;
    if ( a1 == v10 )
        *a3 = 463;
    if ( a1 == v5 )
        *a3 = 464;
    if ( a1 == v6 )
        *a3 = 465;
    if ( a1 == v7 )
        *a3 = 466;
    if ( a1 == v4 )
        *a3 = 467;
    if ( a1 == v11 )
        *a3 = 468;
    if ( a1 == v12 )
        *a3 = 469;
    if ( a1 == v13 )
        *a3 = 470;
    if ( a1 == v9 )
        *a3 = 471;
    if ( a1 == v10 )
        *a3 = 472;
    if ( a1 == v5 )
        *a3 = 473;
    if ( a1 == v6 )
        *a3 = 474;
    if ( a1 == v7 )
        *a3 = 475;
    if ( a1 == v4 )
        *a3 = 476;
    if ( a1 == v11 )
        *a3 = 477;
    if ( a1 == v12 )
        *a3 = 478;
    if ( a1 == v13 )
        *a3 = 479;
    if ( a1 == v9 )
        *a3 = 480;
    if ( a1 == v10 )
        *a3 = 481;
    if ( a1 == v5 )
        *a3 = 482;
    if ( a1 == v6 )
        *a3 = 483;
    if ( a1 == v7 )
        *a3 = 484;
    if ( a1 == v4 )
        *a3 = 485;
    if ( a1 == v11 )
        *a3 = 486;
    if ( a1 == v12 )
        *a3 = 487;
    if ( a1 == v13 )
        *a3 = 488;
    if ( a1 == v9 )
        *a3 = 489;
    if ( a1 == v10 )
        *a3 = 490;
    if ( a1 == v5 )
        *a3 = 491;
    if ( a1 == v6 )
        *a3 = 492;
    if ( a1 == v7 )
        *a3 = 493;
    if ( a1 == v4 )
        *a3 = 494;
    if ( a1 == v11 )
        *a3 = 495;
    if ( a1 == v12 )
        *a3 = 496;
    if ( a1 == v13 )
        *a3 = 497;
    if ( a1 == v9 )
        *a3 = 498;
    if ( a1 == v10 )
        *a3 = 499;
    if ( a1 == v5 )
        *a3 = 500;
    if ( a1 == v6 )
        *a3 = 501;
    if ( a1 == v7 )
        *a3 = 502;
    if ( a1 == v4 )
        *a3 = 503;
    if ( a1 == v11 )
        *a3 = 504;
    if ( a1 == v12 )
        *a3 = 505;
    if ( a1 == v13 )
        *a3 = 506;
    if ( a1 == v9 )
        *a3 = 507;
    if ( a1 == v10 )
        *a3 = 508;
    if ( a1 == v5 )
        *a3 = 509;
    if ( a1 == v6 )
        *a3 = 510;
    if ( a1 == v7 )
        *a3 = 511;
    if ( a1 == v4 )
        *a3 = 512;
    if ( a1 == v11 )
        *a3 = 513;
    if ( a1 == v12 )
        *a3 = 514;
    if ( a1 == v13 )
        *a3 = 515;
    if ( a1 == v9 )
        *a3 = 516;
    if ( a1 == v10 )
        *a3 = 517;
    if ( a1 == v5 )
        *a3 = 518;
    if ( a1 == v6 )
        *a3 = 519;
    if ( a1 == v7 )
        *a3 = 520;
    if ( a1 == v4 )
        *a3 = 521;
    if ( a1 == v11 )
        *a3 = 522;
    if ( a1 == v12 )
        *a3 = 523;
    if ( a1 == v13 )
        *a3 = 524;
    if ( a1 == v9 )
        *a3 = 525;
    if ( a1 == v10 )
        *a3 = 526;
    if ( a1 == v5 )
        *a3 = 527;
    if ( a1 == v6 )
        *a3 = 528;
    if ( a1 == v7 )
        *a3 = 529;
    if ( a1 == v4 )
        *a3 = 530;
    if ( a1 == v11 )
        *a3 = 531;
    if ( a1 == v12 )
        *a3 = 532;
    if ( a1 == v13 )
        *a3 = 533;
    if ( a1 == v9 )
        *a3 = 534;
    if ( a1 == v10 )
        *a3 =
```

```

    return v,
v9 = a2 / 3;
if ( (int)(a2 / 3) % 3 )
    ++v9;
v10 = 4 * v9;
*a3 = v10;
v12 = malloc(v10 + 1);
if ( !v12 )
    return 0;
j_memset(v12, 0, v10 + 1);
v13 = a1;
v11 = a2;
v4 = 0;
while ( v11 > 0 )
{
    byte_41A144[2] = 0;
    byte_41A144[1] = 0;
    byte_41A144[0] = 0;
    for ( i = 0; i < 3 && v11 >= 1; ++i )
    {
        byte_41A144[i] = *v13;
        --v11;
        ++v13;
    }
    if ( !i )
        break;
    switch ( i )
    {
        case 1:
            *((_BYTE *)v12 + v4) = aAbcdefghijklmn[(int)(unsigned __int8)byte_41A144[0] >> 2];
            v5 = v4 + 1;
            *((_BYTE *)v12 + v5) = aAbcdefghijklmn[((byte_41A144[1] & 0xF0) >> 4) | (16 * (byte_41A144[0] & 3))];
            *((_BYTE *)v12 + ++v5) = aAbcdefghijklmn[64];
            *((_BYTE *)v12 + ++v5) = aAbcdefghijklmn[64];
            v4 = v5 + 1;
            break;
        case 2:
            *((_BYTE *)v12 + v4) = aAbcdefghijklmn[(int)(unsigned __int8)byte_41A144[0] >> 2];
            v6 = v4 + 1;
            *((_BYTE *)v12 + v6) = aAbcdefghijklmn[((byte_41A144[1] & 0xF0) >> 4) | (16 * (byte_41A144[0] & 3))];
            *((_BYTE *)v12 + ++v6) = aAbcdefghijklmn[((byte_41A144[2] & 0xC0) >> 6) | (4 * (byte_41A144[1] & 0xF))];
            *((_BYTE *)v12 + ++v6) = aAbcdefghijklmn[64];
            v4 = v6 + 1;
            break;
        case 3:
            *((_BYTE *)v12 + v4) = aAbcdefghijklmn[(int)(unsigned __int8)byte_41A144[0] >> 2];
            v7 = v4 + 1;
            *((_BYTE *)v12 + v7) = aAbcdefghijklmn[((byte_41A144[1] & 0xF0) >> 4) | (16 * (byte_41A144[0] & 3))];
            *((_BYTE *)v12 + ++v7) = aAbcdefghijklmn[((byte_41A144[2] & 0xC0) >> 6) | (4 * (byte_41A144[1] & 0xF))];
            *((_BYTE *)v12 + ++v7) = aAbcdefghijklmn[byte_41A144[2] & 0x3F];
            v4 = v7 + 1;
            break;
    }
}

```

通过观察发现，此处非常像base64加密，查看aAbcdefghijklmn处发现，

```

db     0
db     0
mn db 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/='
; DATA XREF: .text:004117E8↑o
; .text:00411827↑o ...
db 0

```

确定是base64加密，再查看str2的值发现是 `e3nifIH9b_C@n@dH`

写出解密脚本

```

import base64
s = "e3nifIH9b_C@n@dH"
x = ""
for i in range(0, len(s)):
    x += chr(ord(s[i])-i)

print(base64.b64decode(x))

```

其中`ord`函数是将一个字符的ASCII值返回，`chr`函数是将0~255内的整数转换为对应的ASCII字符，这俩是配对函数。

得出最终flag `flag{i_10ve_you}`

注：base64加密原理

base64是以每3个字节为一组，共24位，再以6位为一个单位组成新的数据。对于不足3字节的处理：
1.不足三字节后面填充0；
2.对于编码前的数据产生的6位，如果为0，则索引到的字符为'A'；因不足3字节而填充的0，用 '=' 来替代。

base64编码表是64个可见字符集。

十进制数值	编码字符	十进制数值	编码字符	十进制数值	编码字符	十进制数值	编码字符
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	http://blog.sdn...	63	@PlumpBoy

如何分辨出base64加密：

1.base64加密过后的密文后面可能会存在=

2.通过查看字母表来确定

3.代码中含有0xF、0x3F、0x3等符号