

baby_baby_rev-en

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    int i; // [rsp+Ch] [rbp-74h]
    char s; // [rsp+10h] [rbp-70h] BYREF
    char v6; // [rsp+11h] [rbp-6Fh]
    char v7; // [rsp+12h] [rbp-6Eh]
    char v8; // [rsp+13h] [rbp-6Dh]
    char v9; // [rsp+14h] [rbp-6Ch]
    char v10; // [rsp+15h] [rbp-6Bh]
    char v11; // [rsp+16h] [rbp-6Ah]
    char v12; // [rsp+17h] [rbp-69h]
    char v13; // [rsp+18h] [rbp-68h]
    char v14; // [rsp+19h] [rbp-67h]
    char v15; // [rsp+1Ah] [rbp-66h]
    char v16; // [rsp+1Bh] [rbp-65h]
    char v17; // [rsp+1Ch] [rbp-64h]
    char v18; // [rsp+1Dh] [rbp-63h]
    char v19; // [rsp+1Eh] [rbp-62h]
    char v20; // [rsp+1Fh] [rbp-61h]
    char v21; // [rsp+20h] [rbp-60h]
    char v22; // [rsp+21h] [rbp-5Fh]
    char v23; // [rsp+22h] [rbp-5Eh]
    char v24; // [rsp+23h] [rbp-5Dh]
    char v25; // [rsp+24h] [rbp-5Ch]
    char v26; // [rsp+25h] [rbp-5Bh]
    char v27; // [rsp+26h] [rbp-5Ah]
    char v28; // [rsp+27h] [rbp-59h]
    char v29; // [rsp+28h] [rbp-58h]
    char v30; // [rsp+29h] [rbp-57h]
    char v31; // [rsp+2Ah] [rbp-56h]
    char v32; // [rsp+2Bh] [rbp-55h]
    char v33; // [rsp+2Ch] [rbp-54h]
    char v34; // [rsp+2Dh] [rbp-53h]
    char v35; // [rsp+2Eh] [rbp-52h]
    char v36; // [rsp+2Fh] [rbp-51h]
    unsigned __int64 v37; // [rsp+78h] [rbp-8h]

    v37 = __readfsqword(0x28u);
    setvbuf(stdin, 0LL, 2, 0LL);
    setvbuf(_bss_start, 0LL, 2, 0LL);
    puts("Welcome to SuperTexEdit!\n");
    puts("To begin using SuperTexEdit, please enter your registration code.");
    printf("Code: ");
    __isoc99_scanf("%99s", &s);
    if ( strlen(&s) == 32 )
    {
        s -= 'i';
        v6 = v6 - 'r' + 1;
        v7 = v7 - 'i' + 2;
        v8 = v8 - 's' + 3;
        v9 = v9 - 'c' + 4;
        v10 = v10 - 116 + 5;
        v11 = v11 - 102 + 6;
        v12 = v12 - 123 + 7;
        v13 = v13 - 109 + 8;
        v14 = v14 - 105 + 9;
        v15 = v15 - 99 + 10;
        v16 = v16 - 114 + 11;
        v17 = v17 - 111 + 12;
        v18 = v18 - 115 + 13;
        v19 = v19 - 111 + 14;
        v20 = v20 - 102 + 15;
        v21 = v21 - 116 + 16;
        v22 = v22 - 95 + 17;
        v23 = v23 - 119 + 18;
        v24 = v24 - 111 + 19;
        v25 = v25 - 114 + 20;
        v26 = v26 - 100 + 21;
        v27 = v27 - 95 + 22;
        v28 = v28 - 97 + 23;
        v29 = v29 - 116 + 24;
        v30 = v30 - 95 + 25;
        v31 = v31 - 104 + 26;
        v32 = v32 - 111 + 27;
        v33 = v33 - 109 + 28;
        v34 = v34 - 101 + 29;
        v35 = v35 - 58 + 30;
        v36 = v36 - 125 + 31;
        for ( i = 0; ; ++i )
        {
```

```

    if ( i > 31 )
    {
        puts("Key Valid!");
        puts("SuperTexEdit booting up...");
        abort();
    }
    if ( i != *(&s + i) )
        break;
}
puts("Invalid code!");
return 1;
}

```

If v37 is ignored as canary, char-type data is declared from s.

In the stack structure, this is shown in chars[31].

```

for ( i = 0; ; ++i )
{
    if ( i > 31 )
    {
        puts("Key Valid!");
        puts("SuperTexEdit booting up...");
        abort();
    }
    if ( i != *(&s + i) )
        break;
}

```

In the code above, s[i] == i are passed. Therefore, if you calculate as follows, you will get results.

```

datas = [105, 114, 105, 115, 99, 116, 102, 123, 109, 105, 99 , 114, 111, 115, 111, 102, 116, 95 , 119, 111, 114, 100, 95 , 97 , 116, 9
res = [chr(x) for x in datas]
flag = ''.join(res)

print(flag)

```

```
flag: irisctf{microsoft_word_at_home:}
```