

# EasyRe-wp

出题人：DOUBL3SEV3N

学校：大理大学

考点:代码理解能力，逆向思维能力

下载附件之后载入 ida64，f5 反编译，查看 main 函数

```
_main();
    strcpy(v4, "]P_ISRF^PCY[I_YWERYC");
    memset(v5, 0, sizeof(v5));
    v6 = 0;
    v7 = 0;
    puts("please input your strings:");
    gets(Str);
    v10 = strlen(Str);
    while ( Str[i] )
    {
        for ( i = 0; i < v10; ++i )
            v8[i] = Str[i] ^ 0x11;
    }
    for ( i = 0; i < v10; ++i )
    {
        if ( v8[i] == 66 || v8[i] == 88 )
            v8[i] = -101 - v8[i];
    }
    for ( i = v10 - 1; i >= 0; --i )
        v8[v10 - i - 1] = v8[i];
    i = 0;
    if ( v10 > 0 )
    {
        if ( v8[i] == v4[i] )
            printf("yes!!!");
        else
            printf("no!!!");
    }
    return 0;
}
```

主函数逻辑是，由用户输入一个字符串，然后将字符串每一个字符与 0x11 异或。异或完了之后检测字符串中是否有字母 B 和字母 X 因为（66 是 B，88 是 X）如果有就执行 155-66 或者 155-88，

实际上这里的目也就是字符替换

```
break,  
if ( v6[i] == 66 || v6[i] == 88 )  
    v6[i] = 155 - v6[i];  
,
```

接着往下，就是倒序经过变换后的字符串。

```
for ( i = v10 - 1; i >= 0; --i )  
    v8[v10 - i - 1] = v8[i];  
.
```

接着到了比较这里：

```
if ( v10 > 0 )  
{  
    if ( v8[i] == v4[i] )  
        printf("yes!!!");  
    else  
        printf("no!!!");  
}
```

显然，是比较 v8 和 v4 两个数组的数据是否完全相同，如果相同那么输出判断 yes，反之判断 no。而 v4 的数据已经给了，v8 又是 flag 经过变化后得到的密文，那么显然密文就是 v4 的数据，也就是：

```
strcpy(v4, "]P_ISRF^PCY[I_YWERYC");
```

那么得到密文之后，解题过程就应该和算法反过来，先把这个字符串逆序，然后字符替换，然后与 0x11 异或，最后输出得到 flag。


解题脚本如下：

```

#include <stdio.h>
#include <string.h>
#include <ctype.h>
int main()
{
    char String[99];
    int i;
    char s1[99],s2[99];
    printf("please input your strings:\n");
    gets(String);
    int n=strlen(String);
    for(i=n-1;i>=0;i--) //逆序字符串
        s1[n-i-1]=String[i];

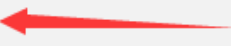
    for(i=0;i<strlen(s1);i++){
        if(s1[i] == 'Y' || s1[i]== 'C') //字符替换，因为题目替换的是 B
和 x，155-66 是 89，155-88 是 67.所以这里换成 y 和 c 把 B 和 x 换回来
            s1[i]=0x9b-s1[i];
    }
    for(i=0;i<strlen(s1);i++)
        s2[i]=s1[i]^0x11; //异或运算。
    for(i=0;i<strlen(s2);i++)
        printf("%c",s2[i]); //输出 flag
    return 0;
}

```

 选择 C:\Users\86198\Desktop\challenge\isctf2023出题人\EasyRe\解题.exe

please input your strings:

]P\_ISR\F^PCY[I\_YWERYC

ISCTFSNXJSIAOWMCBXNAL 

Process exited after 4.893 seconds with return value 0

得到 flag

ISCTF{SNXJSIAOWMCBXNAL}