buuctf——简单注册器

原创

re3sry 于 2021-05-28 20:34:29 发布 75 收藏

1，得到apk文件。

丢到APkIDA中发现啥也不是，什么也没看出来。又把他丢到JEB中查看代码

```
if(v2 == 1) {
    char[] v5 = "dd2940c04462b4dd7c450528835cca15".toCharArray();
    v5[v9] = ((char)(v5[v9] + v5[3] - 50));
    v5[4] = ((char)(v5[v9] + v5[5] - 0x30));
    v5[30] = ((char)(v5[v11] + v5[9] - 0x30));
    v5[14] = ((char)(v5[27] + v5[28] - 97));
    int v4;
    for(v4 = 0; v4 < 16; ++v4) {
        char v0 = v5[0x1F - v4];
        v5[0x1F - v4] = v5[v4];
        v5[v4] = v0;
    }

    this.val$textview.setText("flag{" + String.valueOf(v5) + "}");
}
else {
    this.val$textview.setText("输入注册码错误");
}
```


2.分析代码，一下就找到了关键，简单看一下，很简单，就是计算，上脚本

```
v5=["d","d","2","9","4","0","c","0","4","4","6","2","b","4","d","d","7","c","4","5","0","5","2","8","8","3","5","c","c","a","1","5"]
v5[2]=chr(ord(v5[2])+ord(v5[3])-50)
v5[4] =chr(ord(v5[2])+ord(v5[5])-48)
v5[30] =chr(ord(v5[31])+ord(v5[9])-48)
v5[14] =chr(ord(v5[27])+ord(v5[28])-97)
for i in range(16):
    v=v5[31-i]
    v5[31-i]=v5[i]
    v5[i]=v
flag=''.join(v5)
print('flag{'+flag+'}')
```


3.get flag

flag{59acc538825054c7de4b26440c0999dd}