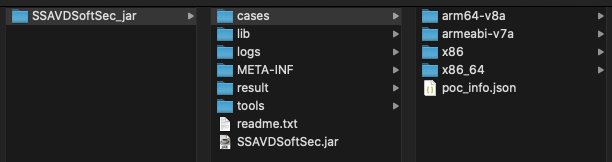
**车机检测系统新增poc流程**



如图，在工具目录下的cases文件夹中有四个文件夹和一个json文件。

四个文件夹名分别代表四种车机处理器芯片架构，编译好的poc按架构分别放入四个文件夹。如果某poc只有x86和x86-64架构，就只放入对应文件夹即可。

放置好poc文件，编辑cases/poc\_info.json文件，向其中写入poc具体信息。例如cve-2016-3940漏洞对应的poc信息如下：

**{**

**"cveId": "cve-2016-3940",**

**"type": "权限提升",**

**"description": "The Synaptics touchscreen ...",**

**"location": "Synaptics touch driver",**

**"CVSSV2Score": "9.3",**

**"pocName": "cve-2016-3940",**

**"isVulnerality": "Vulnerable:0;Not Vulnerable:1;error:-1;",**

**"testType": "Push"**

**}**

其中字段分别代表:

|  |  |
| --- | --- |
| cveId | 该poc对应的cve的漏洞编号 |
| type | 该poc对应的漏洞类型 |
| description | 该poc对应漏洞的描述 |
| location | 该poc对应漏洞的所处位置 |
| CVSSV2Score | 该poc对应漏洞的CVSSV2评分 |
| pocName | 编译好的poc文件名（四个文件夹中的文件名应一致） |
| isVulnerality | 漏洞触发状态对应的poc文件执行返回值 |
| testType | 检测方式（目前只有Push方式，表示将poc文件发送到测试机内部并执行） |

完成poc放置与poc信息添加后新规则添加流程结束。