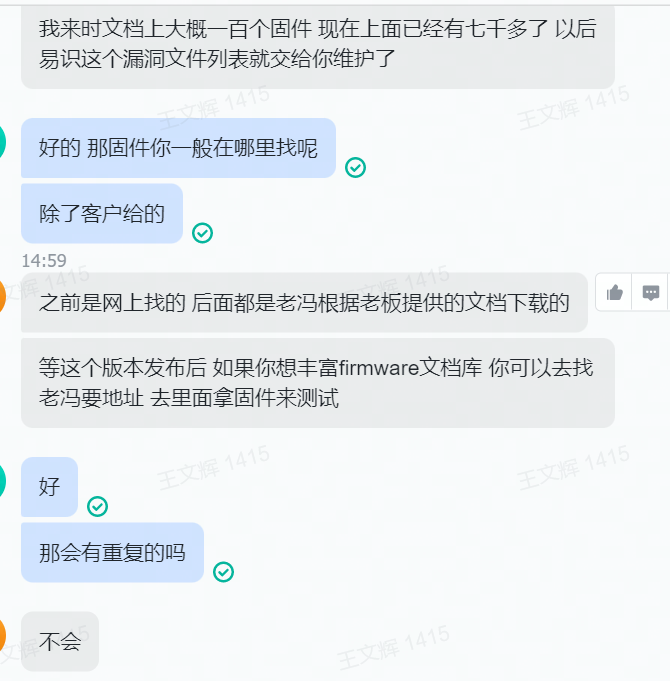
固件(Firmware)就是写入EPROM（可擦写可编程只读存储器）或EEPROM(电可擦可编程只读存储器)中的程序。

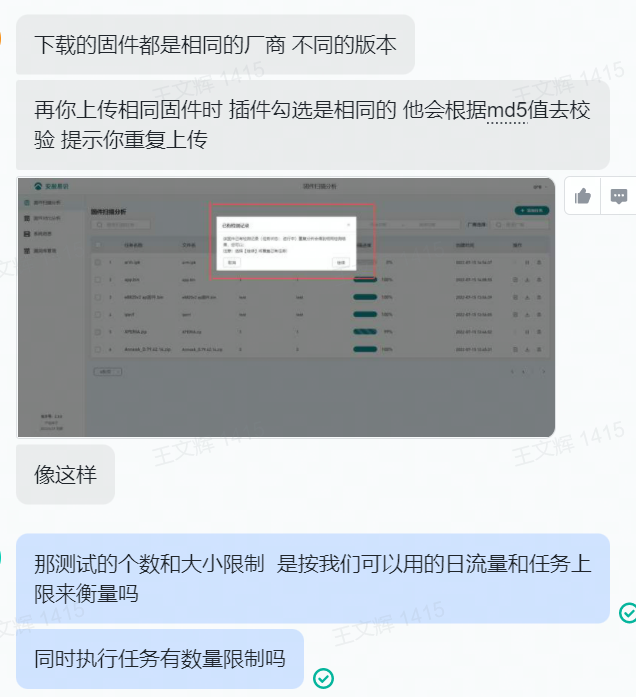
固件是指设备内部保存的设备“驱动程序”，通过固件，操作系统才能按照标准的设备驱动实现特定机器的运行动作，比如光驱、刻录机等都有内部固件。

固件是担任着一个系统最基础最底层工作的软件。而在硬件设备中，固件就是硬件设备的灵魂，因为一些硬件设备除了固件以外没有其它软件组成，因此固件也就决定着硬件设备的功能及性能。

CVE （Common Vulnerabilities & Exposures，通用漏洞披露）。 CVE 是国际著名的安全漏洞库，也是对已知漏洞和安全缺陷的标准化名称的列表，它是一个由企业界、政府界和学术界综合参与的国际性组织，采取一种非盈利的组织形式，其使命是为了能更加快速而有效地鉴别、发现和修复软件产品的安全漏洞。

维护固件文档库：





DEV development 开发

SIT System Integrate Test 系统整合测试（内测）

UAT User Acceptance Test 用户验收测试

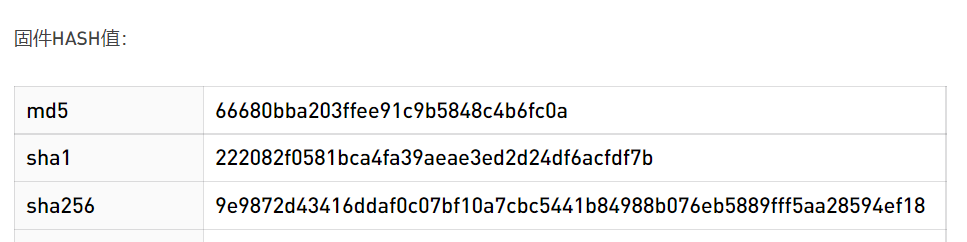
PET Performance Evaluation Test 性能评估测试（压测）

SIM simulation 仿真

PRD/PROD production 产品/正式/生产

测试重点：

md5值相当于id，是唯一的



**Docker命令：**

日志查看的重点：

docker logs -f [scheduler.yishi.anban.com](http://scheduler.yishi.anban.com" \t "_blank) 查看固件具体运行的一个状态

htop 命令 查看cpu的状态，内存使用情况和进程运行状态的

docker logs -f fe-file-type-ys --tail 100 动态查看file-type插件运动日志的后100行

docker logs -f fe-web-ys --tail 100 动态查看当前任务执行情况

docker logs -f fe-cwe-checker-ys --tail 100 查看cwe-checker插件运行情况

History 查看历史操作命令

docker ps -a 能看到当前所有容器的状态

**编辑禁用cwe的配置文件：**

docker exec -it fe-web-ys bash 进入容器

vim anafirm/settings.py 编辑配置文件

Exit 退出容器

docker restart fe-web-ys 重启服务

**编辑易识用户登录方式配置文件：(0为易识用户、1为管理平台用户)**

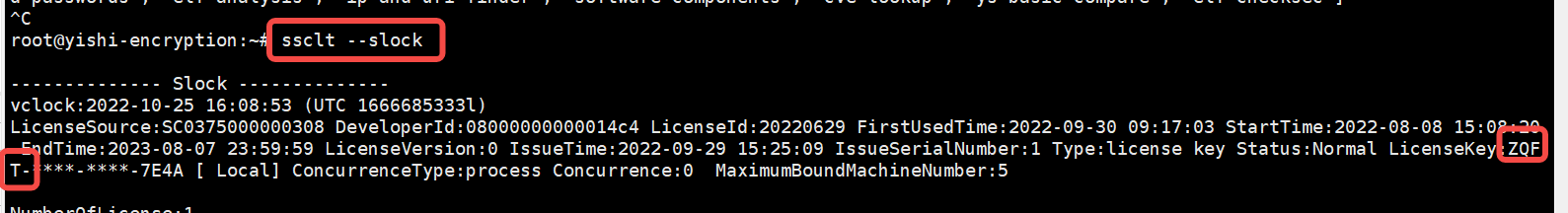
1. docker exec -it fe-web-ys bash # 进入容器
2. vim anafirm/config.yaml # 编辑内容
3. exit # 退出容器
4. 重启容器 docker restart fe-web-ys

**安装vim命令：**

apt-get update && apt-get install -y vim

**编辑授权码**

ssclt --slock 查看当前license信息，授权码前四位搜索



**命令绑定深思授权码：**

解绑

ssclt --online\_unbind\_license\_key --license\_key M73X-51YF-G2DM-UW1F

绑定

ssclt --online\_bind\_license\_key --license\_key DETV-TCDC-RTZ8-SS4A

刷新授权信息

ssclt --online\_refresh\_license --license\_key DETV-TCDC-RTZ8-SS4A

查看历史license命令

history | grep ssclt

**重启命令：**

# 1. 暂停调度器 docker stop [scheduler.yishi.anban.com](http://scheduler.yishi.anban.com" \t "_blank)

# 2.暂停插件 ./stop-plugin.sh

# 3.开启调度器 docker restart [scheduler.yishi.anban.com](http://scheduler.yishi.anban.com" \t "_blank)

# 4.开启插件 ./start-plugin.sh

**深思修改授权信息：**

登录---授权码许可---发布许可---搜索授权码---点进---点击编辑---数据区修改信息---复制授权码---易识在线授权即可

----cwe：0表示禁用，1表示可用

**配置是否复用之前文件数据**（复用相同文件的分析数据，但解包插件不会复用）：

1、docker exec -it [scheduler.yishi.anban.com](http://scheduler.yishi.anban.com" \t "_blank) bash

2、vim setting.py 112行

SAME\_CHECK = True

3、exit

4、重启调度器和插件

**数据库命令（清空已使用流量）：**

SELECT \* FROM public.ys\_limit\_info ORDER BY id ASC

INSERT INTO "public"."ys\_limit\_info" VALUES (1, '2022-10-12 12:38:12.241824', '2022-10-12 12:38:12.241824', 'f', E'MA==', E'MA==', E'MA==', E'MA==', NULL);

Unpacker 解包插件

old-unpacker 解包

file-type 文件类型------------------文件类型

file-hashes 文件哈希----------------------（MD5,sha）

Binwalk 签名分析-------------熵图

cpu-architecture cpu架构分析--------------------cpu架构

crypto-hints 加密算法分析-------------------加密算法

users-and-passwords 用户名和密码---------------敏感信息

elf-analysis elf分析--------------------ELF分析

ip-and-uri-finder ip和uri-----------------------敏感信息

software-components 软件组件-----------------------文件成分

cve-lookup cve漏洞

ys-basic-compare 基础对比

易识任务模块：

1/同时开启任务没有个数限制，但是日任务数量不超过1000个（后台自定义），且虽然前台任务显示全部执行中，实际后台是只执行6个任务；

2/系统信息-配额信息中，任意一项不满足则无法执行（年流量/补充能量/日流量/任务上限）；

3/任务执行和解包的文件个数相关，即使文件占用内存小，但文件数越多，时间越长；

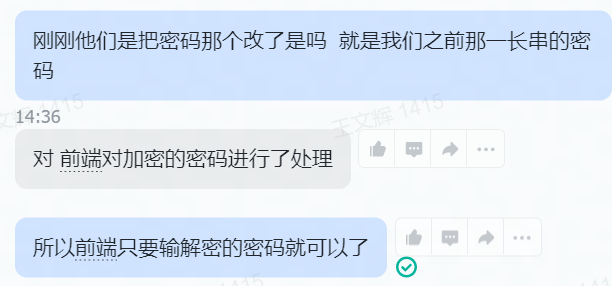
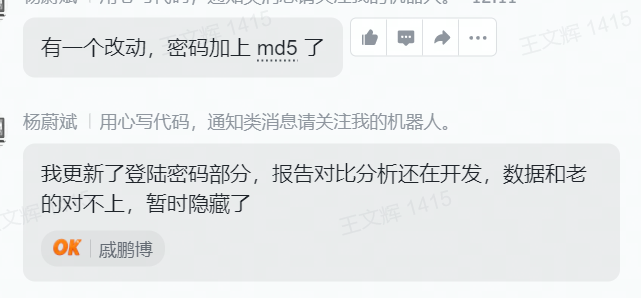
4/

易识漏洞库：



2.3待解决问题：  
1/ 2.0版本和2.3版本的解包方式变更，2.0比2.3解包出来的固件数量有问题；

2/ 2.0对比任务报告界面显示变更；

2.3密码更改（220719）：  


**Yara规则库扩充：**

**目的：**为了识别更多的CVE漏洞

**流程：**yara规则库是专门用于识别组件，根据组件名/版本/资格证通过cve去匹配是否含有对应的CVE漏洞；

**易识支持识别组件：**77种；

方式：

方式1：通过github开源的一些信息去查找；？

方式2：通过已知的cve去反推 ？

**漏洞得分：**

若存在cvss3则以cvss3评分为准，若不存在，则以cvss2评分为准；

**CVSS3**

9-10------------超危；  
7-8.9-----------高危；  
4-6.9-----------中危漏洞；  
0.1-3.9--------低危漏洞；

0/无得分-----未知漏洞；

**CVSS2**  
7-10------------高危；  
4-6.9-----------中危漏洞；  
0-3.9-----------低危漏洞；

**刷机包：**

1/安卓刷机包：组成文件

一个完整的安卓手机刷机包 根目录会有以下几个文件夹及文件：

data、 META-IN、 system、 boot.img 四个文件夹；

(data)是用户安装应用程序所在目录 ，(META-IN)是系统相关信息所在目录，一般定制一个刷机包修改系统版本信息都在这里面。

url地址 ======> conf文件下的server.ini

数据库地址 ======> conf文件下的sql.ini

生成测试报告 ======> 运行main.py

测试用例 ======> req\_case.case.yml

执行测试用例 ======> req\_case.test\_yaml.py

Archlinux操作系统：可以在里面下载安装包（里面是application/zstd格式的）

Fedora：下载安装包（里面是application/x-rpm格式的）

**记录：**

1. **日志记录：**插件异常记录（业务端通过接口查看调度器状态，非实时查看，若查看时正好有插件掉线，则会记录在日志当中，若未查询，则插件掉线情况不会记录在业务端日志中）；
2. 熵图插件多插件时，同时运行多个相同任务，会出现熵图缺失的情况；

Mongodb数据库查询命令：

{"plugin.software-components.summary.0":{$exists: true}} #查找有软件成分结果的数据

{"plugin.software-components.summary":{$in: ["OpenSSL "]}}# 查找软件成分结果中有OpenSSL的

linux查询语句：

du -h --max-depth=1 查看当前目录下文件夹大小