FREEBUF | FIT

智能硬件安全测试的常用方法

HackPanda 青藤云安全·安全研究员

目录

固件获取、解包、分析

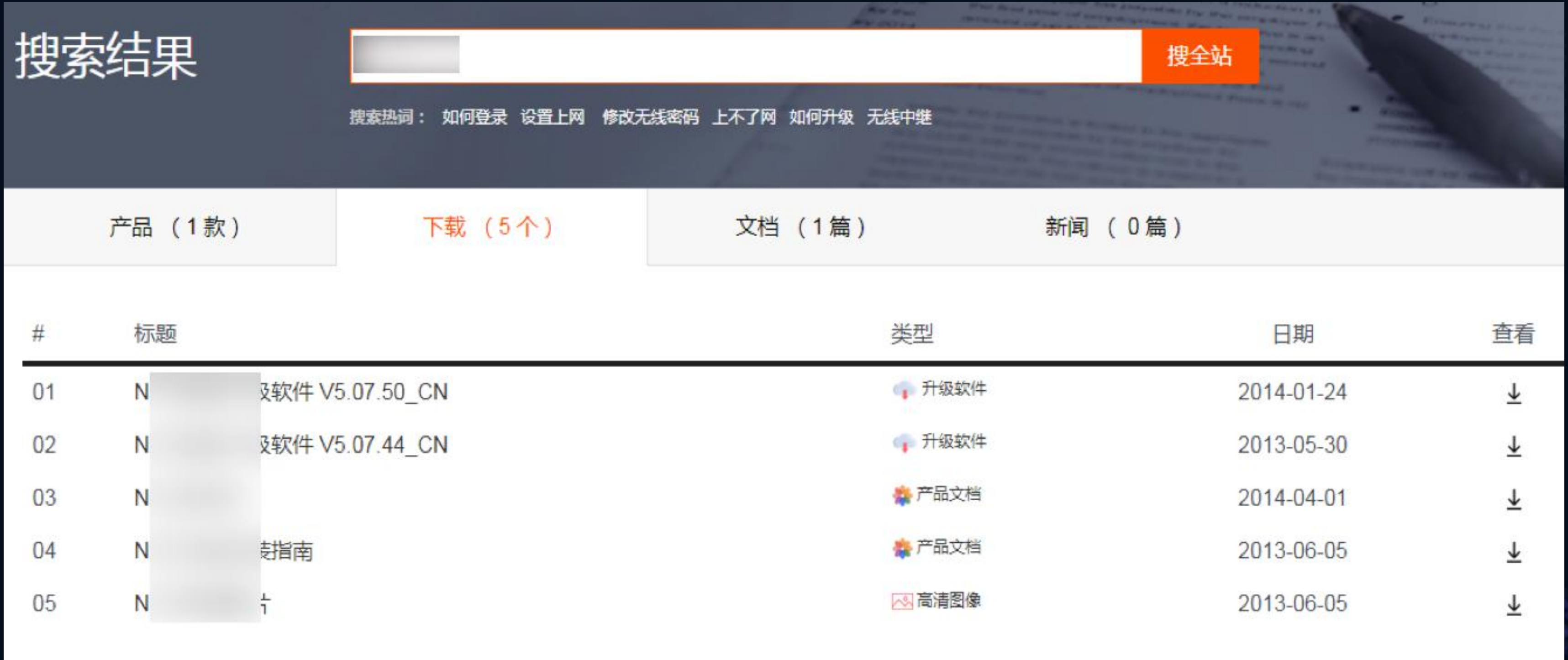
Web接口

App

固件获取

1. 通过官方网站下载
2. 通过网络抓包获取
3. 通过编程器提取
4. ……

官方网站下载



搜索结果

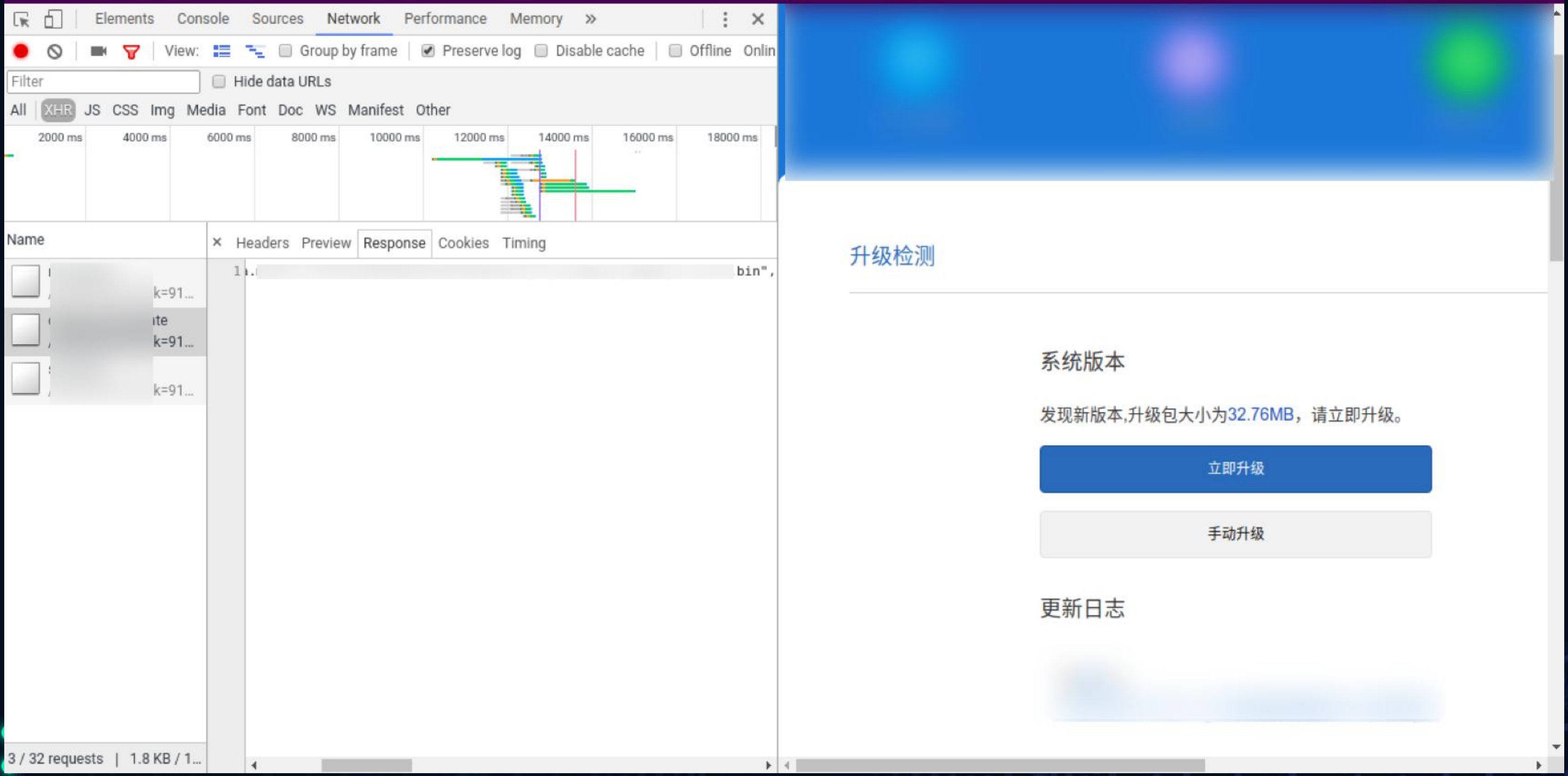
[redacted] 搜全站

搜索热词： 如何登录 设置上网 修改无线密码 上不了网 如何升级 无线中继

产品 （1款） | 下载 （5个） | 文档 （1篇） | 新闻 （0篇）

#	标题	类型	日期	查看
01	N[redacted]级软件 V5.07.50_CN	升级软件	2014-01-24	⤓
02	N[redacted]级软件 V5.07.44_CN	升级软件	2013-05-30	⤓
03	N[redacted]	产品文档	2014-04-01	⤓
04	N[redacted]指南	产品文档	2013-06-05	⤓
05	N[redacted]片	高清图像	2013-06-05	⤓

网络抓包获取



```
1 ı.(                                   bin",
```

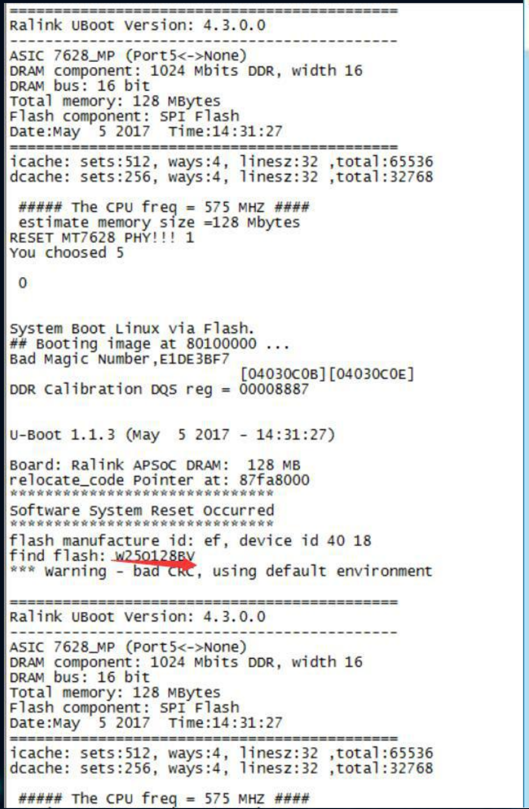
升级检测

系统版本

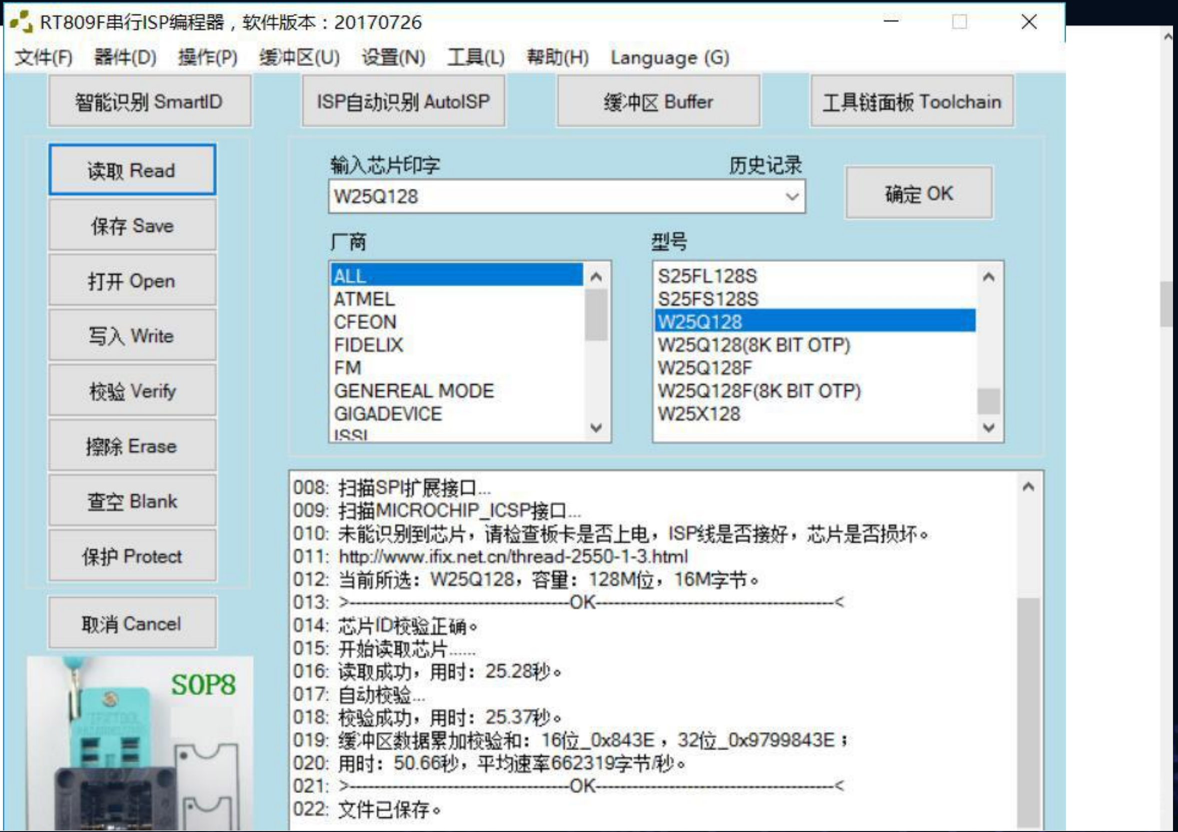
发现新版本,升级包大小为32.76MB，请立即升级。

更新日志

编程器提取



```
============================================
Ralink UBoot Version: 4.3.0.0
--------------------------------------------
ASIC 7628_MP (Port5<->None)
DRAM component: 1024 Mbits DDR, width 16
DRAM bus: 16 bit
Total memory: 128 MBytes
Flash component: SPI Flash
Date:May  5 2017  Time:14:31:27
============================================
icache: sets:512, ways:4, linesz:32 ,total:65536
dcache: sets:256, ways:4, linesz:32 ,total:32768

 ##### The CPU freq = 575 MHZ ####
 estimate memory size =128 Mbytes
RESET MT7628 PHY!!!!! 1
You choosed 5

 0


System Boot Linux via Flash.
## Booting image at 80100000 ...
Bad Magic Number,E1DE3BF7
                                 [04030C0B][04030C0E]
DDR Calibration DQS reg = 00008887


U-Boot 1.1.3 (May  5 2017 - 14:31:27)

Board: Ralink APSoC DRAM:  128 MB
relocate_code Pointer at: 87fa8000
******************************
Software System Reset Occurred
******************************
flash manufacture id: ef, device id 40 18
find flash: W25Q128BV
*** Warning - bad CRC, using default environment

============================================
Ralink UBoot Version: 4.3.0.0
--------------------------------------------
ASIC 7628_MP (Port5<->None)
DRAM component: 1024 Mbits DDR, width 16
DRAM bus: 16 bit
Total memory: 128 MBytes
Flash component: SPI Flash
Date:May  5 2017  Time:14:31:27
============================================
icache: sets:512, ways:4, linesz:32 ,total:65536
dcache: sets:256, ways:4, linesz:32 ,total:32768

 ##### The CPU freq = 575 MHZ ####
```



输入芯片印字: W25Q128

历史记录

厂商: ALL, ATMEL, CFEON, FIDELIX, FM, GENEREAL MODE, GIGADEVICE, ISSI

型号: S25FL128S, S25FS128S, W25Q128, W25Q128(8K BIT OTP), W25Q128F, W25Q128F(8K BIT OTP), W25X128

```
008: 扫描SPI扩展接口...
009: 扫描MICROCHIP_ICSP接口...
010: 未能识别到芯片，请检查板卡是否上电，ISP线是否接好，芯片是否损坏。
011: http://www.ifix.net.cn/thread-2550-1-3.html
012: 当前所选：W25Q128，容量：128M位，16M字节。
013: >----------------------------OK----------------------------<
014: 芯片ID校验正确。
015: 开始读取芯片......
016: 读取成功，用时：25.28秒。
017: 自动校验...
018: 校验成功，用时：25.37秒。
019: 缓冲区数据累加校验和：16位_0x843E，32位_0x9799843E；
020: 用时：50.66秒，平均速率662319字节/秒。
021: >----------------------------OK----------------------------<
022: 文件已保存。
```

固件信息提取-binwalk

1.下载地址:

https://github.com/ReFirmLabs/binwalk/archive/master.zip

2. 安装方法:

debian系列:

```
sudo apt-get install python-lzma binwalk
```

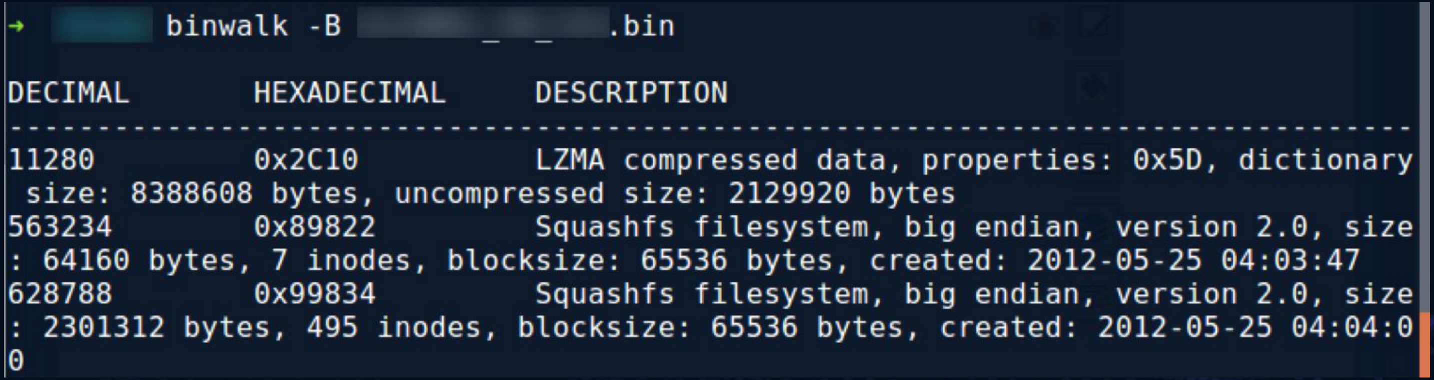
其它linux:

```
unzip master.zip && cd binwalk-master && python setup.py install
```

固件信息提取-binwalk

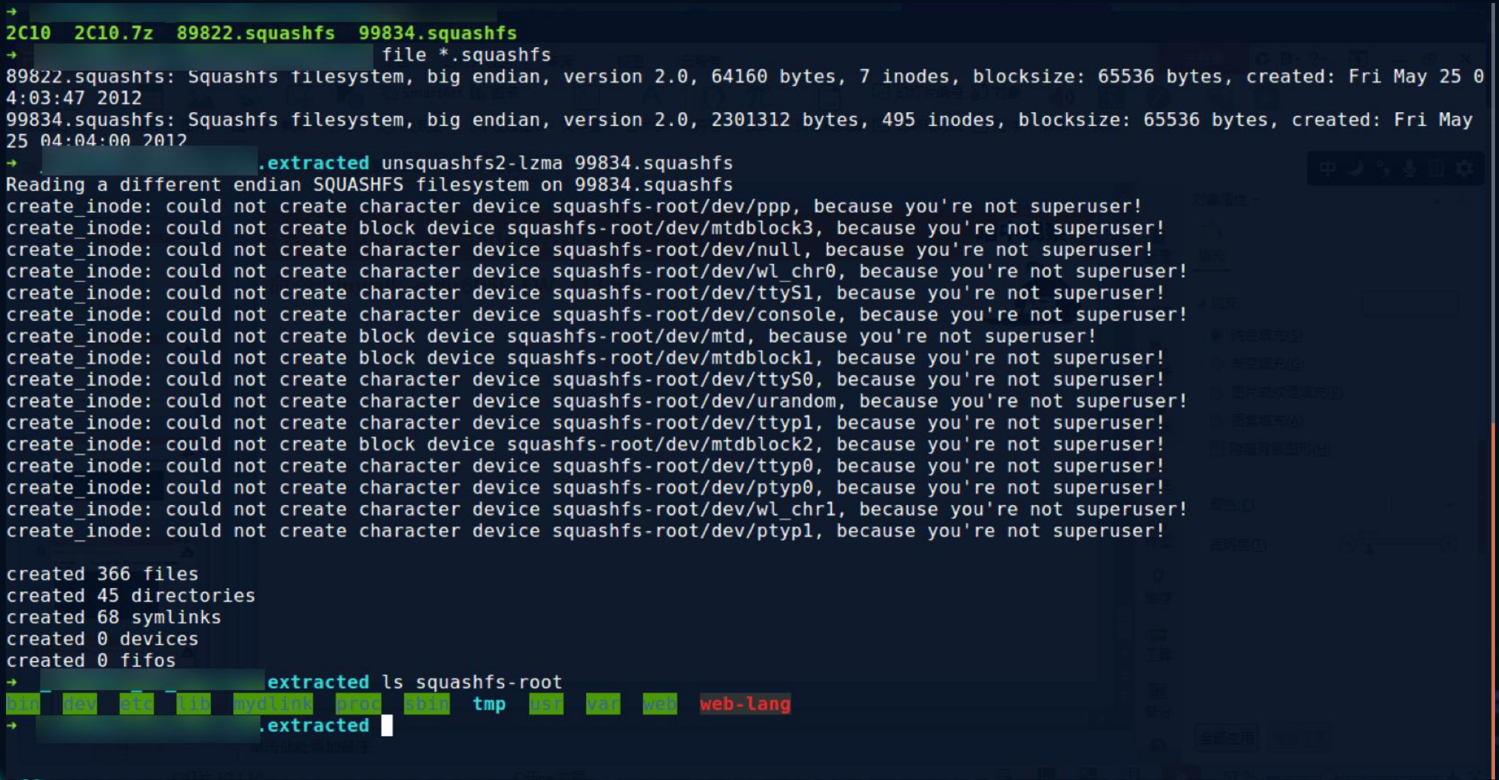
命令:binwalk -B xxx.bin

-B, --signature   Scan target file(s) for common file signatures



```
➜  [redacted] binwalk -B [redacted].bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
11280         0x2C10          LZMA compressed data, properties: 0x5D, dictionary
 size: 8388608 bytes, uncompressed size: 2129920 bytes
563234        0x89822         Squashfs filesystem, big endian, version 2.0, size
: 64160 bytes, 7 inodes, blocksize: 65536 bytes, created: 2012-05-25 04:03:47
628788        0x99834         Squashfs filesystem, big endian, version 2.0, size
: 2301312 bytes, 495 inodes, blocksize: 65536 bytes, created: 2012-05-25 04:04:0
0
```

固件解包



```
→ [redacted]
2C10  2C10.7z  89822.squashfs  99834.squashfs
→ [redacted] file *.squashfs
89822.squashfs: Squashfs filesystem, big endian, version 2.0, 64160 bytes, 7 inodes, blocksize: 65536 bytes, created: Fri May 25 0
4:03:47 2012
99834.squashfs: Squashfs filesystem, big endian, version 2.0, 2301312 bytes, 495 inodes, blocksize: 65536 bytes, created: Fri May
25 04:04:00 2012
→ [redacted].extracted unsquashfs2-lzma 99834.squashfs
Reading a different endian SQUASHFS filesystem on 99834.squashfs
create_inode: could not create character device squashfs-root/dev/ppp, because you're not superuser!
create_inode: could not create block device squashfs-root/dev/mtdblock3, because you're not superuser!
create_inode: could not create character device squashfs-root/dev/null, because you're not superuser!
create_inode: could not create character device squashfs-root/dev/wl_chr0, because you're not superuser!
create_inode: could not create character device squashfs-root/dev/ttyS1, because you're not superuser!
create_inode: could not create character device squashfs-root/dev/console, because you're not superuser!
create_inode: could not create block device squashfs-root/dev/mtd, because you're not superuser!
create_inode: could not create block device squashfs-root/dev/mtdblock1, because you're not superuser!
create_inode: could not create character device squashfs-root/dev/ttyS0, because you're not superuser!
create_inode: could not create character device squashfs-root/dev/urandom, because you're not superuser!
create_inode: could not create character device squashfs-root/dev/ttyp1, because you're not superuser!
create_inode: could not create block device squashfs-root/dev/mtdblock2, because you're not superuser!
create_inode: could not create character device squashfs-root/dev/ttyp0, because you're not superuser!
create_inode: could not create character device squashfs-root/dev/ptyp0, because you're not superuser!
create_inode: could not create character device squashfs-root/dev/wl_chr1, because you're not superuser!
create_inode: could not create character device squashfs-root/dev/ptyp1, because you're not superuser!

created 366 files
created 45 directories
created 68 symlinks
created 0 devices
created 0 fifos
→ [redacted]extracted ls squashfs-root
bin  dev  etc  lib  mydlink  proc  sbin  tmp  usr  var  web  web-lang
→ [redacted].extracted
```

固件分析

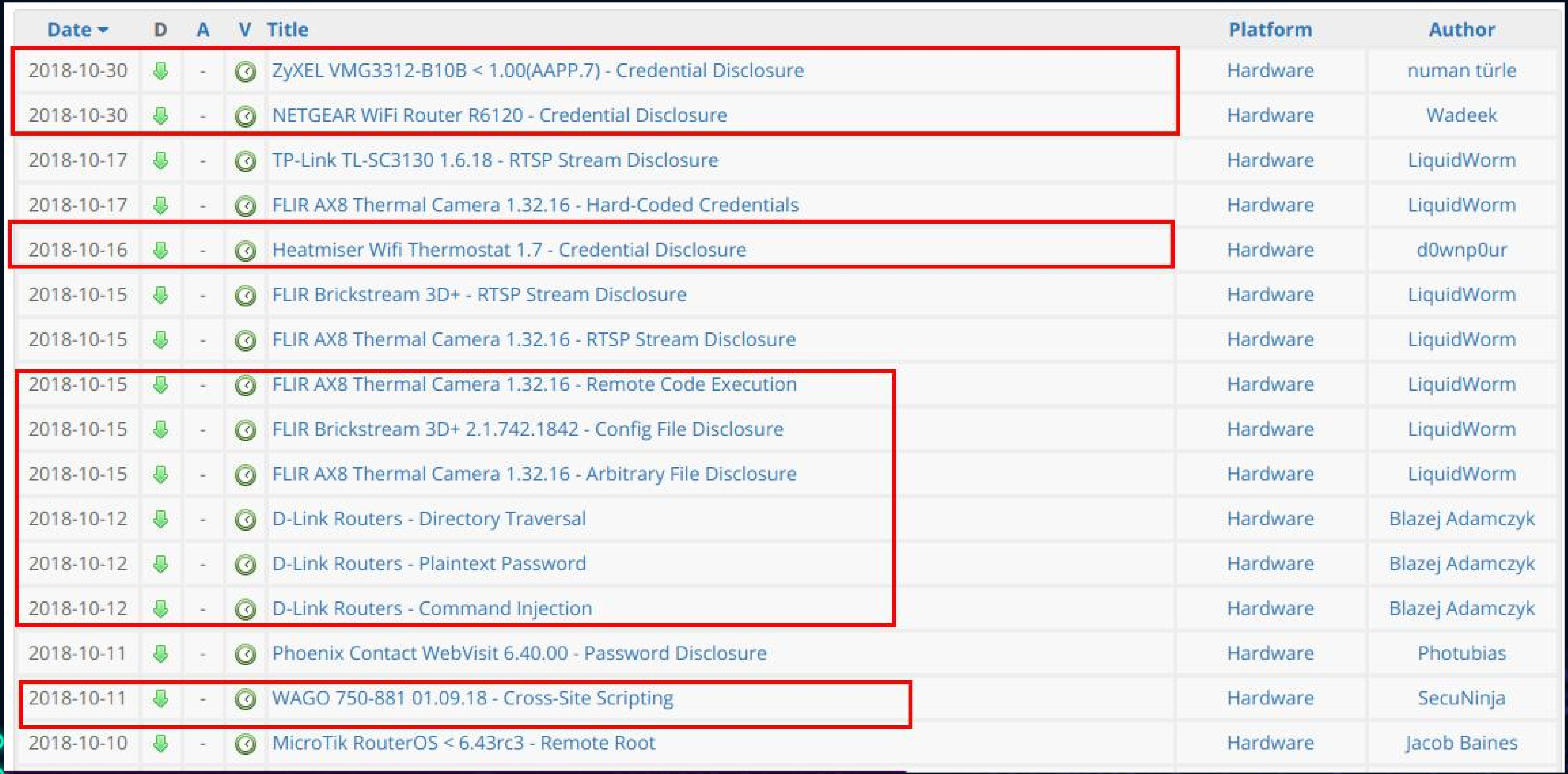
分析其中可被访问应用程序、服务

分析路由器的web服务进程、配置、业务代码

分析认证相关的文件

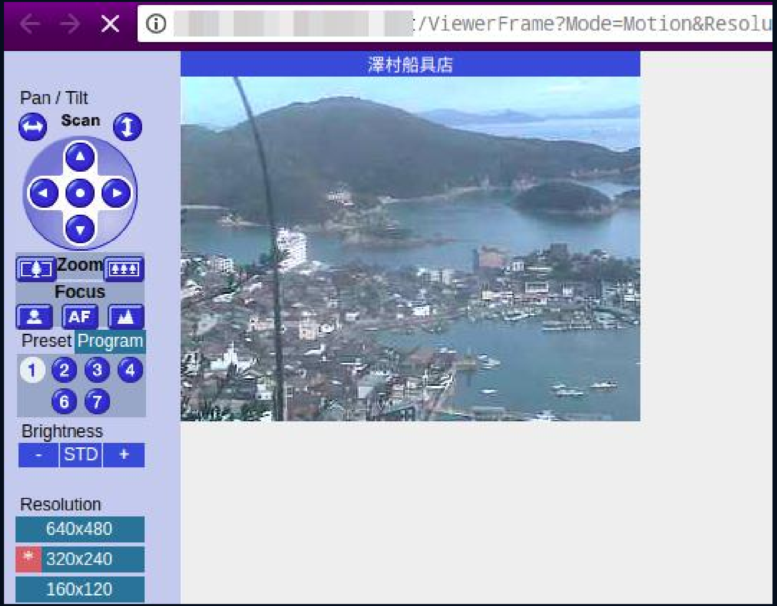
分析工厂模式

Web接口

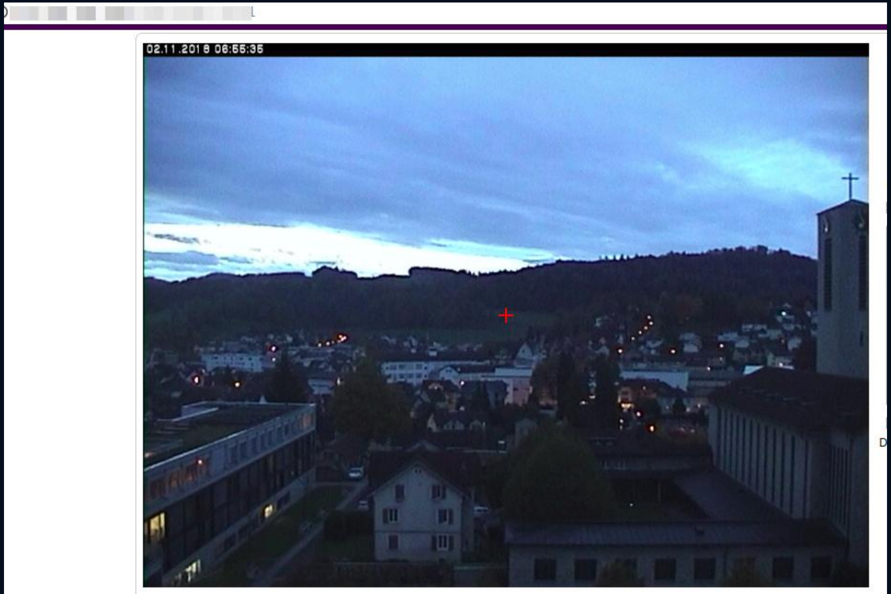


Date ▾	D	A	V	Title	Platform	Author
2018-10-30	⬇	-	✓	ZyXEL VMG3312-B10B < 1.00(AAPP.7) - Credential Disclosure	Hardware	numan türle
2018-10-30	⬇	-	✓	NETGEAR WiFi Router R6120 - Credential Disclosure	Hardware	Wadeek
2018-10-17	⬇	-	✓	TP-Link TL-SC3130 1.6.18 - RTSP Stream Disclosure	Hardware	LiquidWorm
2018-10-17	⬇	-	✓	FLIR AX8 Thermal Camera 1.32.16 - Hard-Coded Credentials	Hardware	LiquidWorm
2018-10-16	⬇	-	✓	Heatmiser Wifi Thermostat 1.7 - Credential Disclosure	Hardware	d0wnp0ur
2018-10-15	⬇	-	✓	FLIR Brickstream 3D+ - RTSP Stream Disclosure	Hardware	LiquidWorm
2018-10-15	⬇	-	✓	FLIR AX8 Thermal Camera 1.32.16 - RTSP Stream Disclosure	Hardware	LiquidWorm
2018-10-15	⬇	-	✓	FLIR AX8 Thermal Camera 1.32.16 - Remote Code Execution	Hardware	LiquidWorm
2018-10-15	⬇	-	✓	FLIR Brickstream 3D+ 2.1.742.1842 - Config File Disclosure	Hardware	LiquidWorm
2018-10-15	⬇	-	✓	FLIR AX8 Thermal Camera 1.32.16 - Arbitrary File Disclosure	Hardware	LiquidWorm
2018-10-12	⬇	-	✓	D-Link Routers - Directory Traversal	Hardware	Blazej Adamczyk
2018-10-12	⬇	-	✓	D-Link Routers - Plaintext Password	Hardware	Blazej Adamczyk
2018-10-12	⬇	-	✓	D-Link Routers - Command Injection	Hardware	Blazej Adamczyk
2018-10-11	⬇	-	✓	Phoenix Contact WebVisit 6.40.00 - Password Disclosure	Hardware	Photubias
2018-10-11	⬇	-	✓	WAGO 750-881 01.09.18 - Cross-Site Scripting	Hardware	SecuNinja
2018-10-10	⬇	-	✓	MicroTik RouterOS < 6.43rc3 - Remote Root	Hardware	Jacob Baines

Web接口-未授权访问

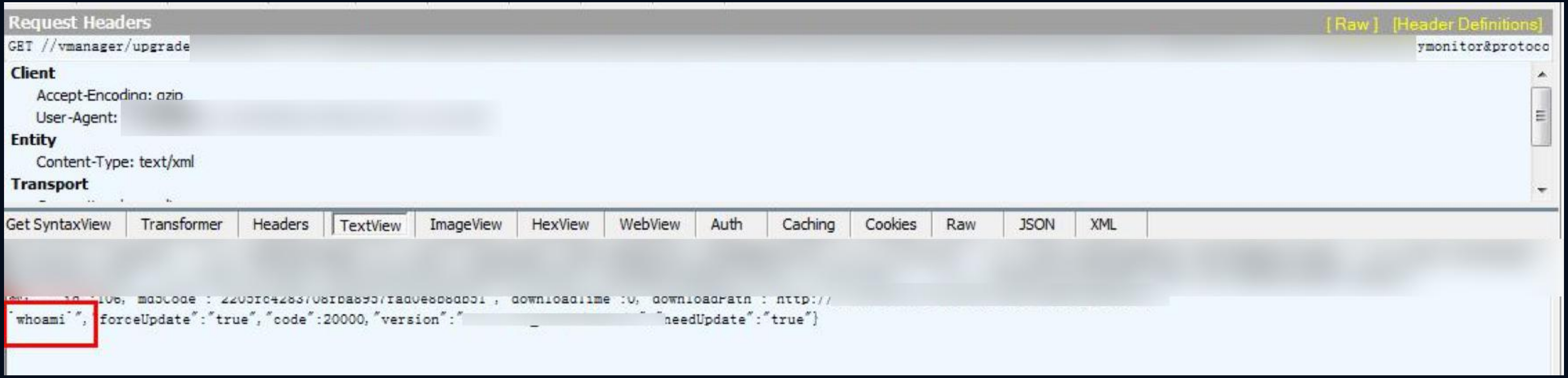


[redacted]/ViewerFrame?Mode=Motion&Resolu



[redacted]

Web接口-RCE



```
GET //vmanager/upgrade[redacted]ymonitor&protoco
```

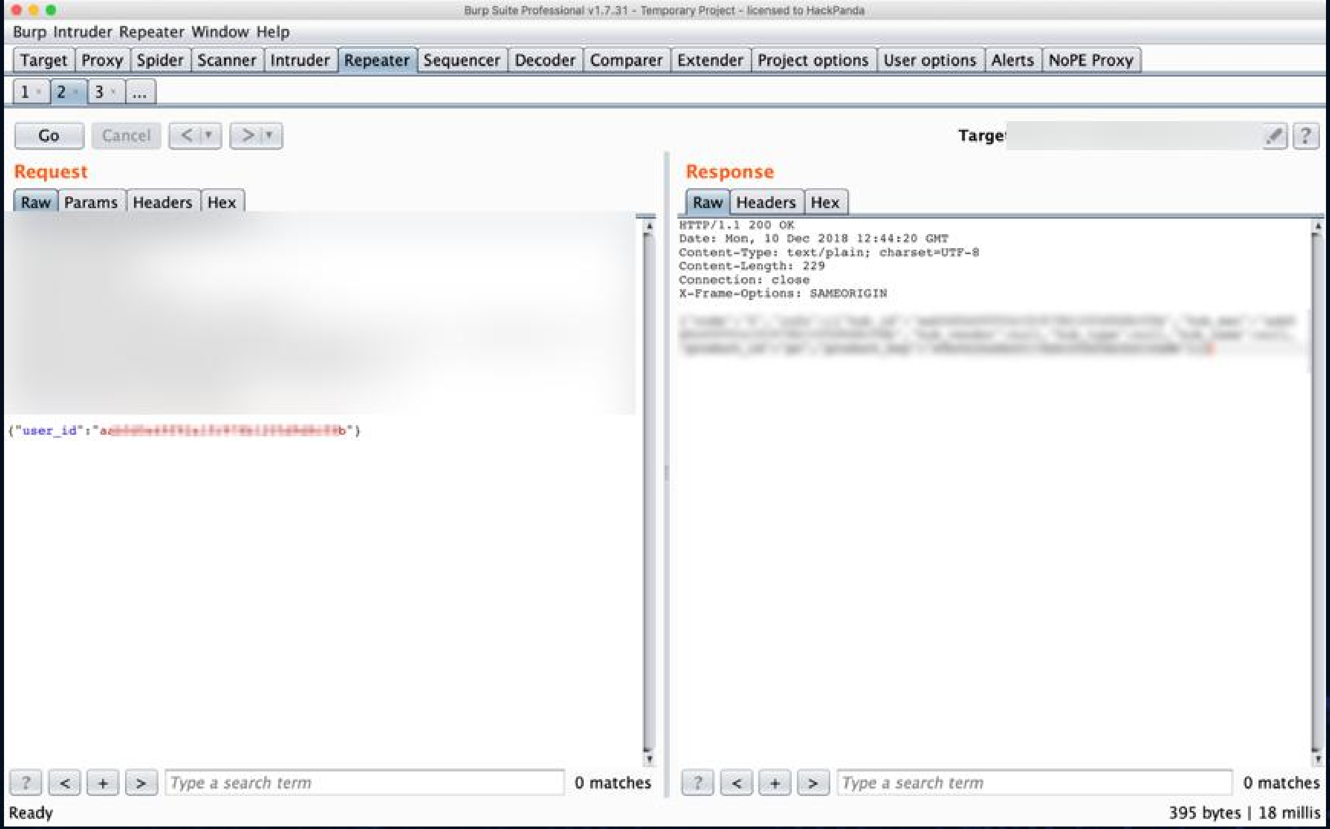
Client
- Accept-Encoding: gzip
- User-Agent: [redacted]

Entity
- Content-Type: text/xml

Transport

```
[redacted]
"id":106, "md5Code":"2205fc4283708fba8957fad0e8b8db51", "downloadTime":0, "downloadPath":"http://[redacted]
`whoami`", "forceUpdate":"true","code":20000,"version":"[redacted]","needUpdate":"true"}
```

Web接口-平行越权


Burp Suite Professional v1.7.31 - Temporary Project - licensed to HackPanda
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts NoPE Proxy
1 2 3 ...
Go Cancel < > Target
Request
Raw Params Headers Hex
Response
Raw Headers Hex
? < + > Type a search term 0 matches
Ready
? < + > Type a search term 0 matches
395 bytes | 18 millis

Request:

[redacted]

```
{"user_id":"a[redacted]b"}
```

Response:

```
HTTP/1.1 200 OK
Date: Mon, 10 Dec 2018 12:44:20 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 229
Connection: close
X-Frame-Options: SAMEORIGIN

[redacted]
```

APP

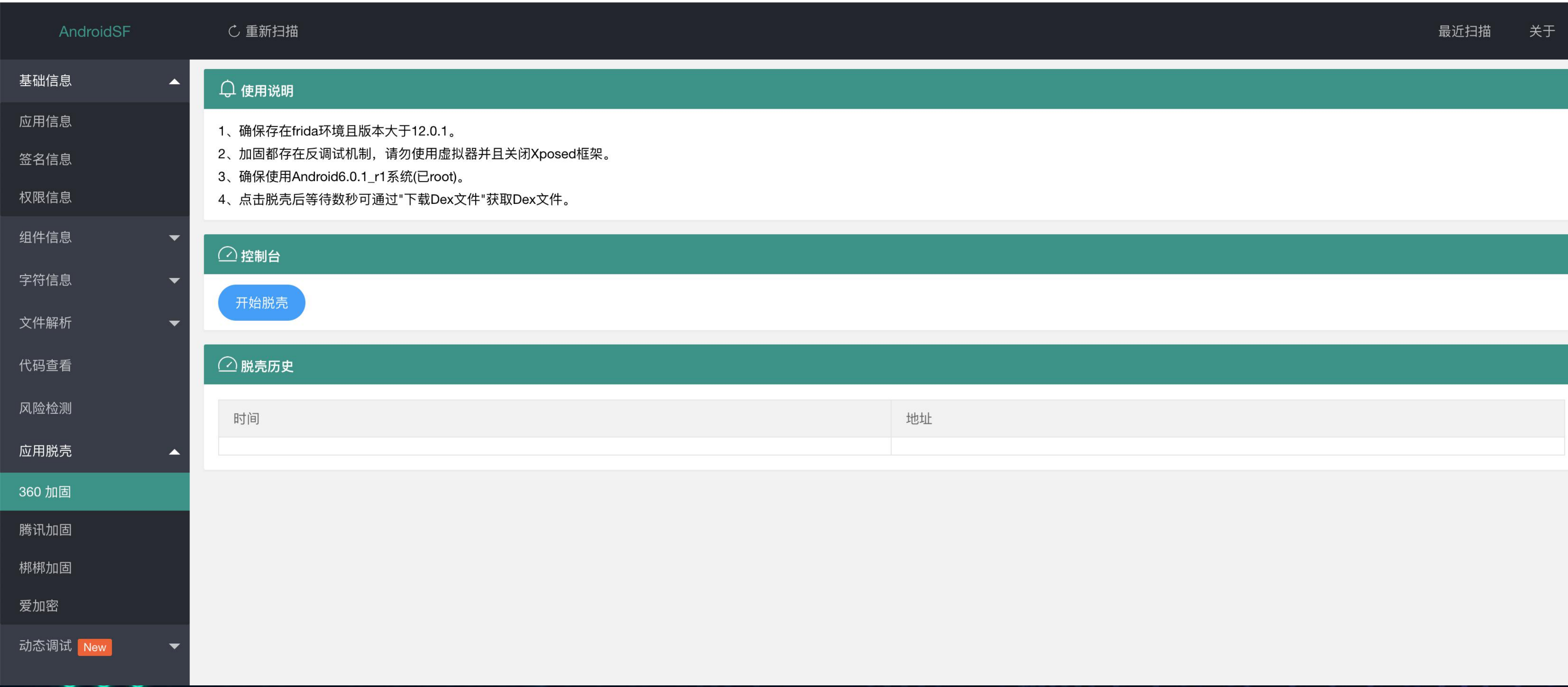
大多数的IoT设备都允许通过手机端进行控制

分析App代码了解其如何控制IoT设备

少不了脱壳、混淆、加密

关注通用的第三方库

APP-自动化脱壳



使用说明

1、确保存在frida环境且版本大于12.0.1。

2、加固都存在反调试机制，请勿使用虚拟器并且关闭Xposed框架。

3、确保使用Android6.0.1_r1系统(已root)。

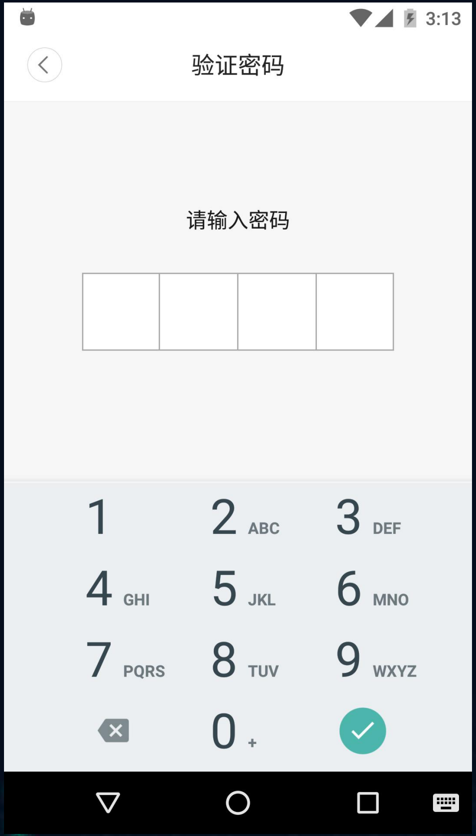
4、点击脱壳后等待数秒可通过"下载Dex文件"获取Dex文件。

控制台

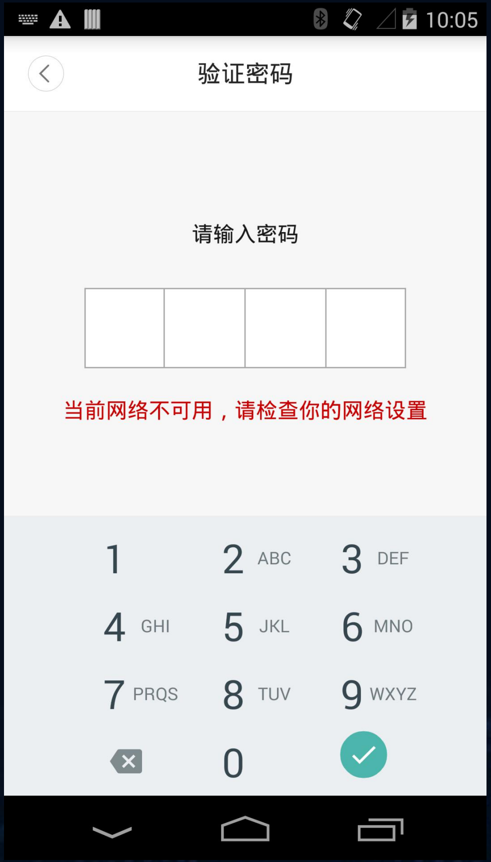
脱壳历史

时间	地址

APP

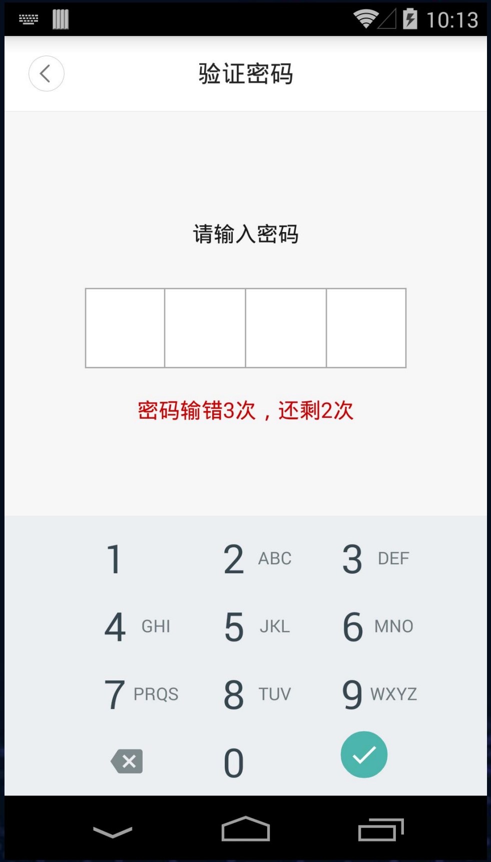


请输入密码



请输入密码

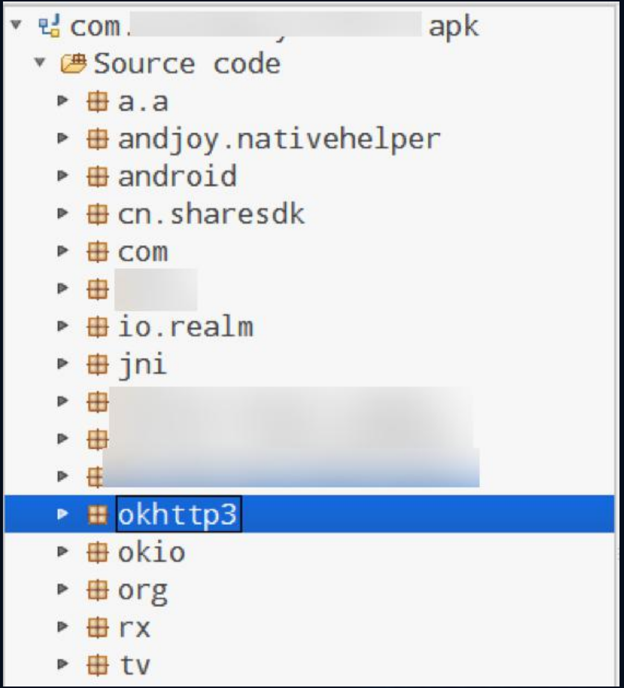
当前网络不可用，请检查你的网络设置



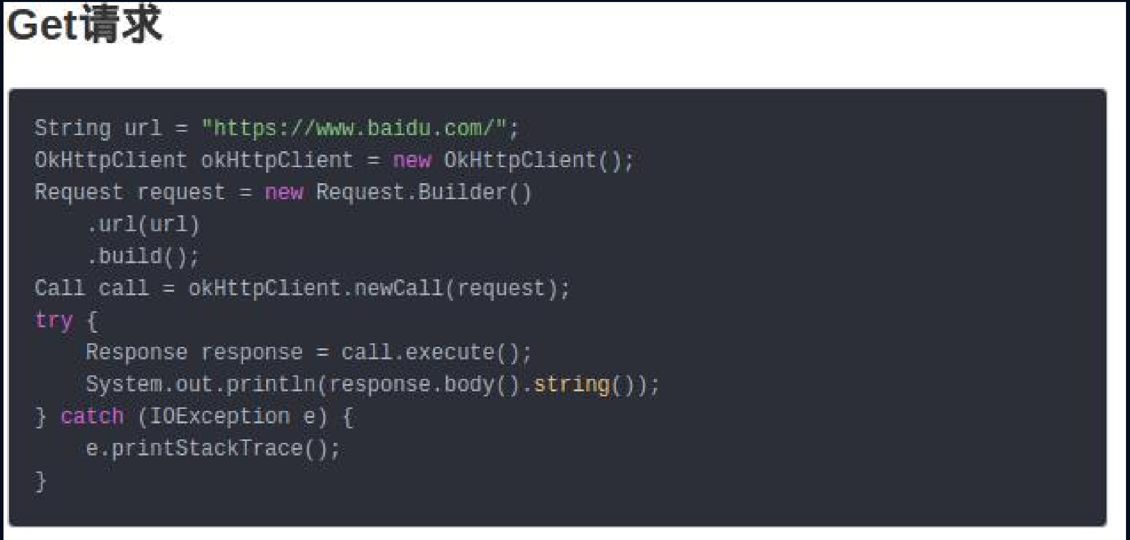
请输入密码

密码输错3次，还剩2次

APP



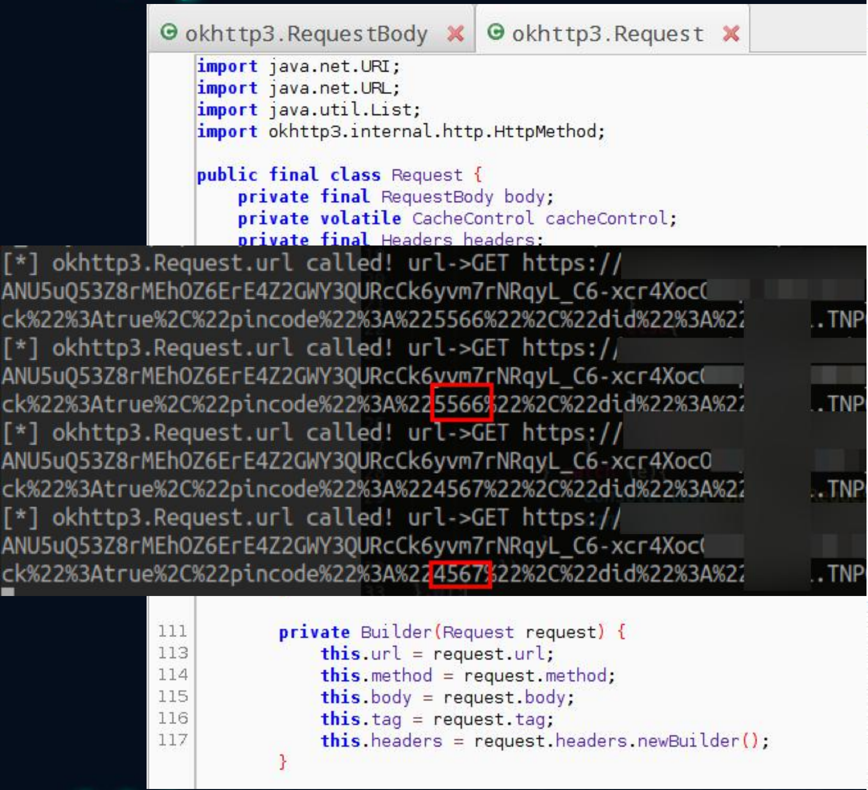
- com.[redacted]apk
  - Source code
    - a.a
    - andjoy.nativehelper
    - android
    - cn.sharesdk
    - com
    - [redacted]
    - io.realm
    - jni
    - [redacted]
    - okhttp3
    - okio
    - org
    - rx
    - tv



Get请求

```
String url = "https://www.baidu.com/";
OkHttpClient okHttpClient = new OkHttpClient();
Request request = new Request.Builder()
    .url(url)
    .build();
Call call = okHttpClient.newCall(request);
try {
    Response response = call.execute();
    System.out.println(response.body().string());
} catch (IOException e) {
    e.printStackTrace();
}
```

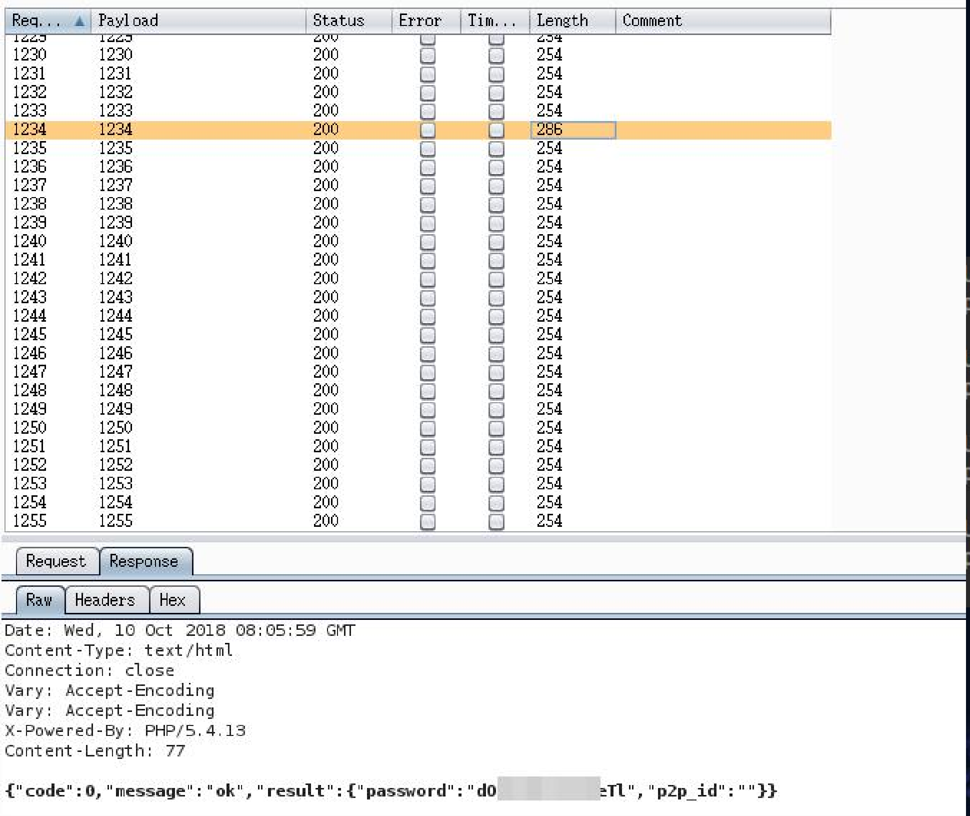
APP



```java
import java.net.URI;
import java.net.URL;
import java.util.List;
import okhttp3.internal.http.HttpMethod;

public final class Request {
    private final RequestBody body;
    private volatile CacheControl cacheControl;
    private final Headers headers;
```

```
[*] okhttp3.Request.url called! url->GET https:// [redacted] UUxY4d
ANU5uQ53Z8rMEhOZ6ErE4Z2GWY3QURcCk6yvm7rNRqyL_C6-xcr4XocC [redacted] pinChe
ck%22%3Atrue%2C%22pincode%22%3A%225566%22%2C%22did%22%3A%22 [redacted] ..TNP
[*] okhttp3.Request.url called! url->GET https:// [redacted] UUxY4d
ANU5uQ53Z8rMEhOZ6ErE4Z2GWY3QURcCk6yvm7rNRqyL_C6-xcr4XocC [redacted] pinChe
ck%22%3Atrue%2C%22pincode%22%3A%225566%22%2C%22did%22%3A%22 [redacted] ..TNP
[*] okhttp3.Request.url called! url->GET https:// [redacted] UUxY4d
ANU5uQ53Z8rMEhOZ6ErE4Z2GWY3QURcCk6yvm7rNRqyL_C6-xcr4XocO [redacted] pinChe
ck%22%3Atrue%2C%22pincode%22%3A%224567%22%2C%22did%22%3A%22 [redacted] ..TNP
[*] okhttp3.Request.url called! url->GET https:// [redacted] UUxY4d
ANU5uQ53Z8rMEhOZ6ErE4Z2GWY3QURcCk6yvm7rNRqyL_C6-xcr4XocC [redacted] pinChe
ck%22%3Atrue%2C%22pincode%22%3A%224567%22%2C%22did%22%3A%22 [redacted] ..TNP
```

```java
        private Builder(Request request) {
            this.url = request.url;
            this.method = request.method;
            this.body = request.body;
            this.tag = request.tag;
            this.headers = request.headers.newBuilder();
        }
```



Req... ▲	Payload	Status	Error	Tim...	Length	Comment
1229	1229	200	□	□	254	
1230	1230	200	□	□	254	
1231	1231	200	□	□	254	
1232	1232	200	□	□	254	
1233	1233	200	□	□	254	
1234	1234	200	□	□	286	
1235	1235	200	□	□	254	
1236	1236	200	□	□	254	
1237	1237	200	□	□	254	
1238	1238	200	□	□	254	
1239	1239	200	□	□	254	
1240	1240	200	□	□	254	
1241	1241	200	□	□	254	
1242	1242	200	□	□	254	
1243	1243	200	□	□	254	
1244	1244	200	□	□	254	
1245	1245	200	□	□	254	
1246	1246	200	□	□	254	
1247	1247	200	□	□	254	
1248	1248	200	□	□	254	
1249	1249	200	□	□	254	
1250	1250	200	□	□	254	
1251	1251	200	□	□	254	
1252	1252	200	□	□	254	
1253	1253	200	□	□	254	
1254	1254	200	□	□	254	
1255	1255	200	□	□	254	

```
Date: Wed, 10 Oct 2018 08:05:59 GMT
Content-Type: text/html
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.13
Content-Length: 77

{"code":0,"message":"ok","result":{"password":"d0[redacted]eTl","p2p_id":""}}
```

APP

1. Hook不同的方法了解APP与IoT设备交互时所进行的操作
2. Logcat
3. 数据交换格式相关的类和方法，比如JSON、XML格式相关

Q&A

🐼👤

斐济

扫一扫上面的二维码图案，加我微信

FREEBUF | FIT

THANKS