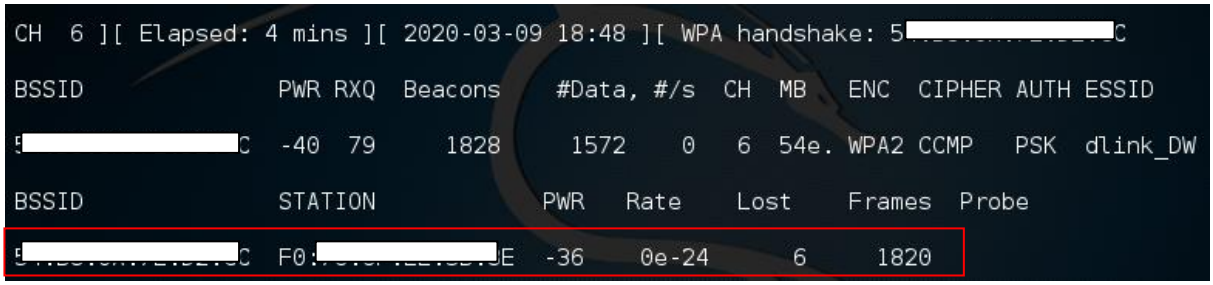
Security vulnerability scenerio:

Step 1: Remote access point password cracking

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

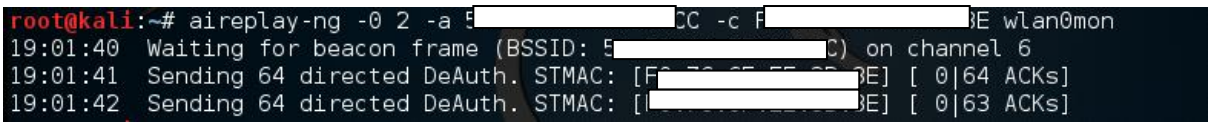
Step 2:

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



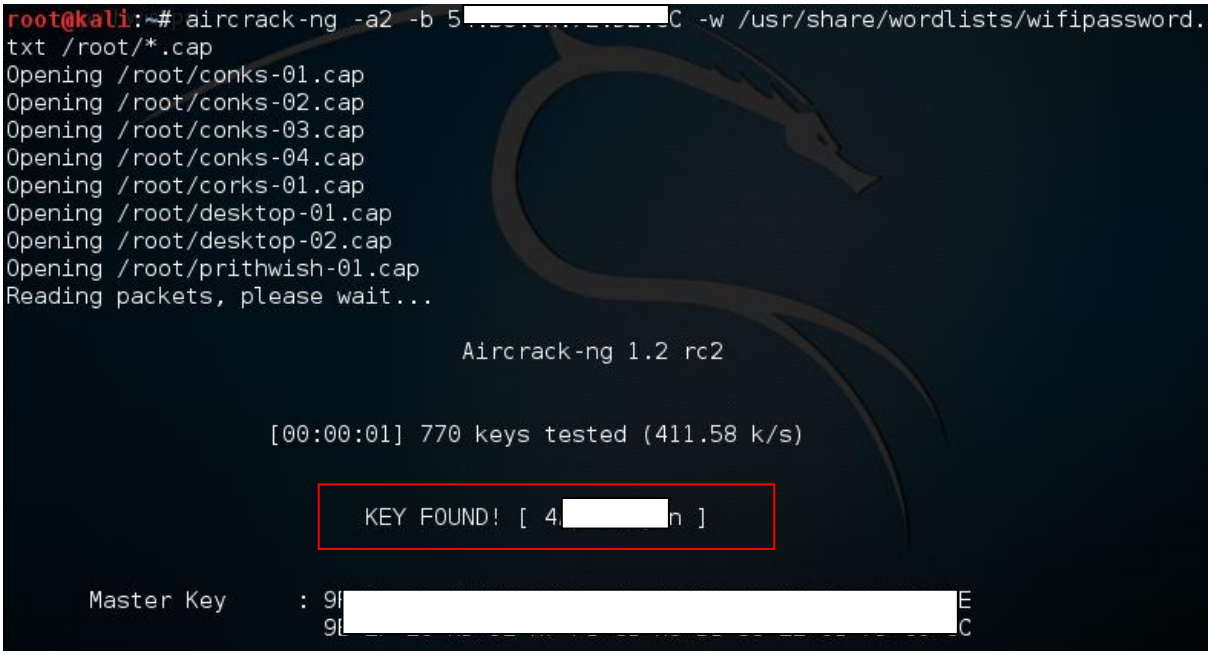
Step 3:

Sending the de-auth tokens



Step 4:

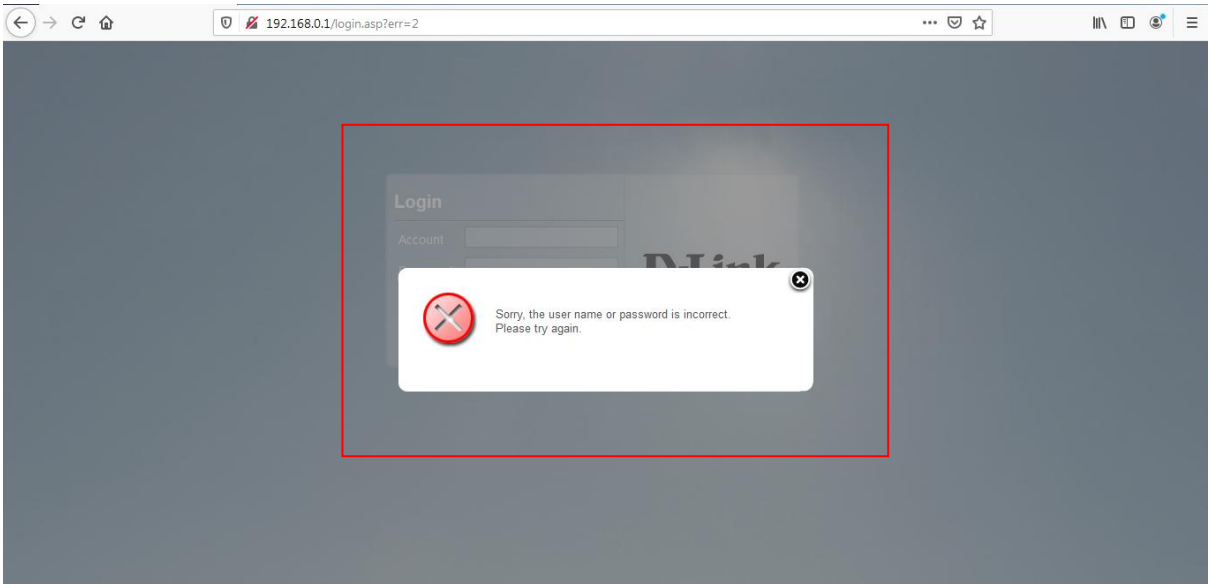
Cracking the password using .cap file and set of wordlist.



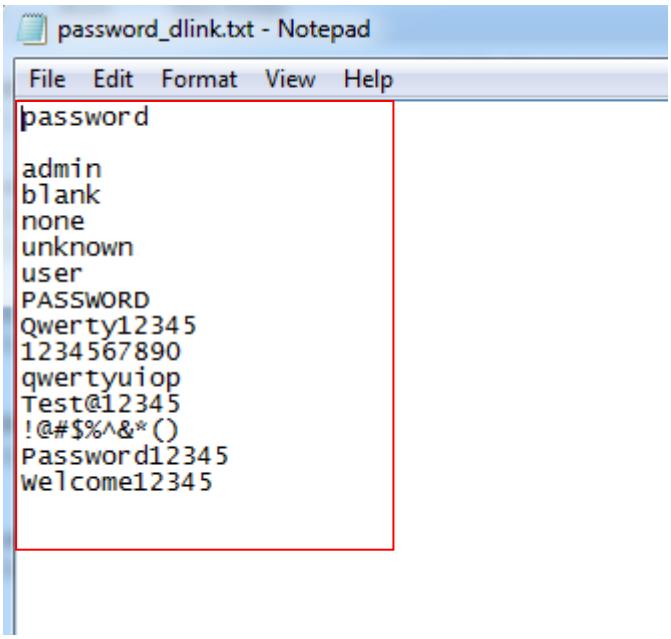
Step 5:

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

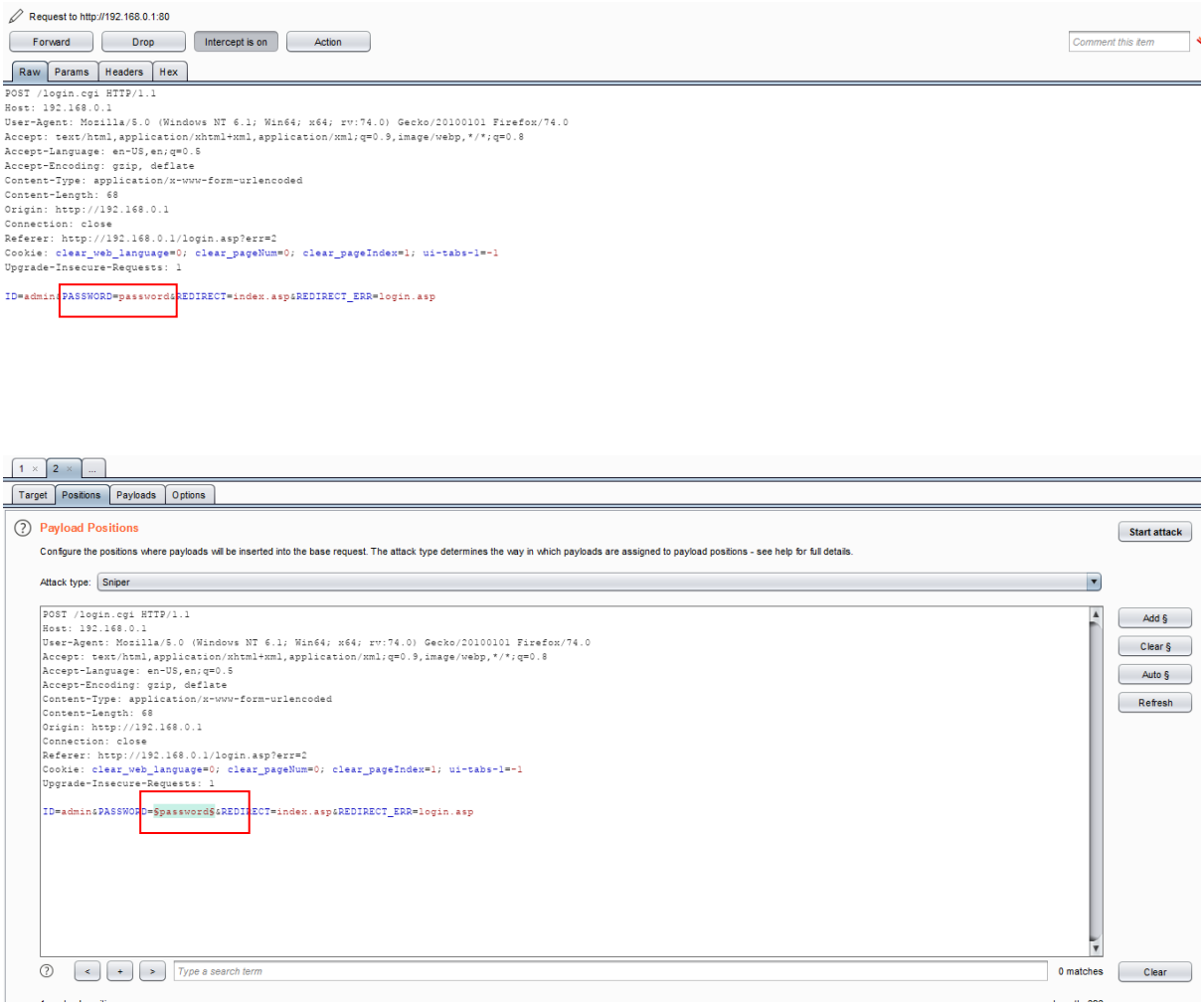
Since the password is unknown to the attacker so the management console interface is throwing errors



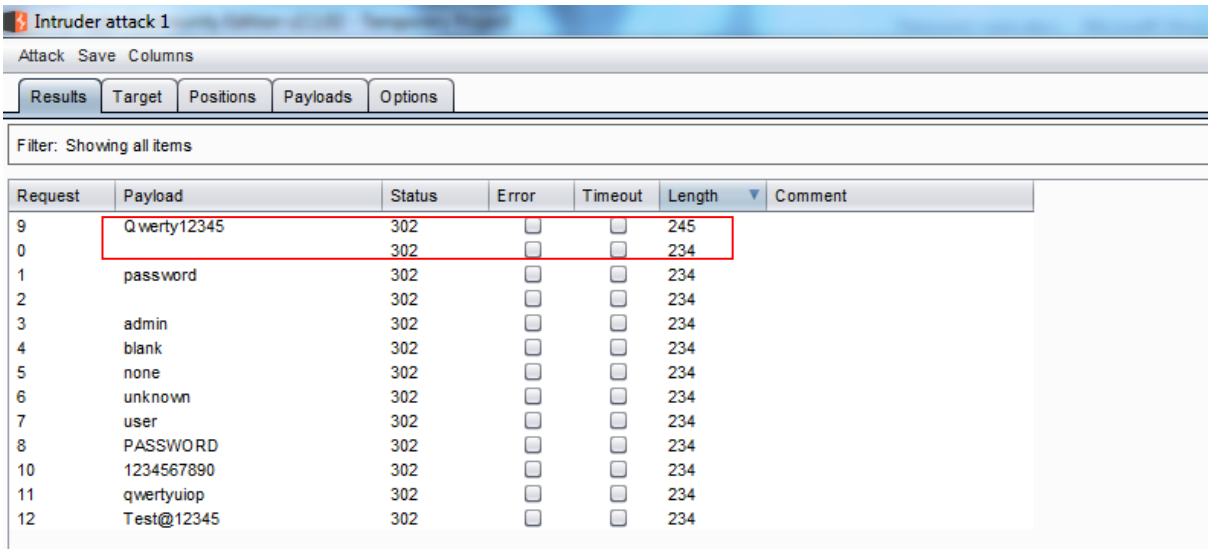
Step 6: Using internet, gathered possible default password and predictable passwords that are configured by manufacturer or set by access point owners.



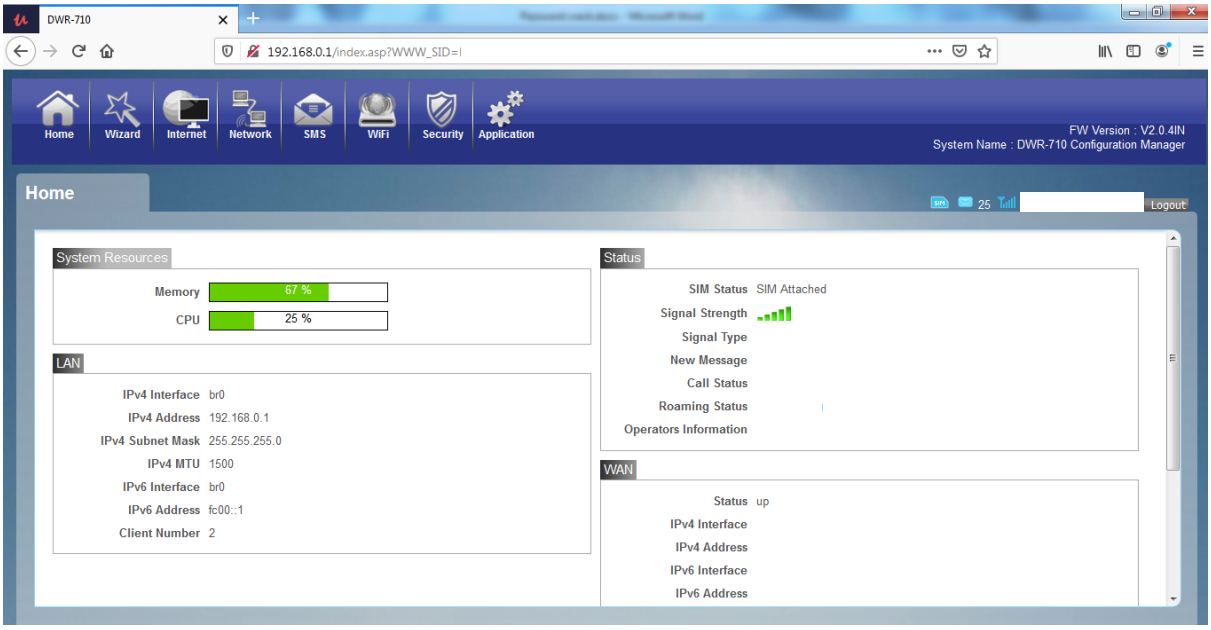
Step 7: Performing bruteforcing in login request



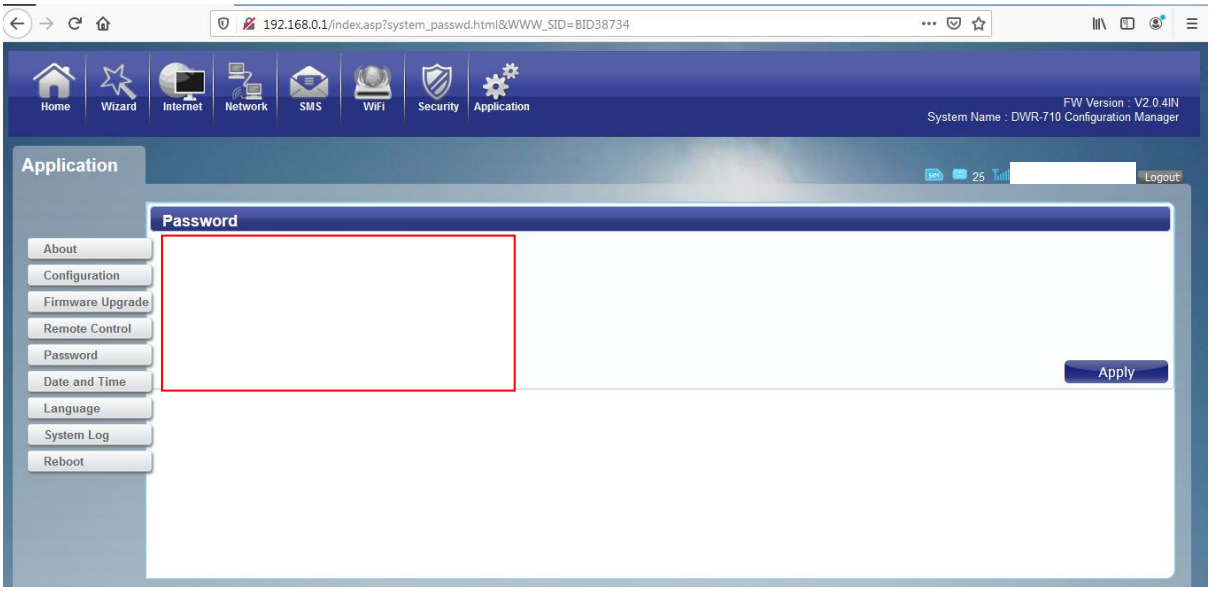
Step 8: It was identified from the response length that Qwerty12345 can be a possible password because the length of the response is 245 and for others it 234



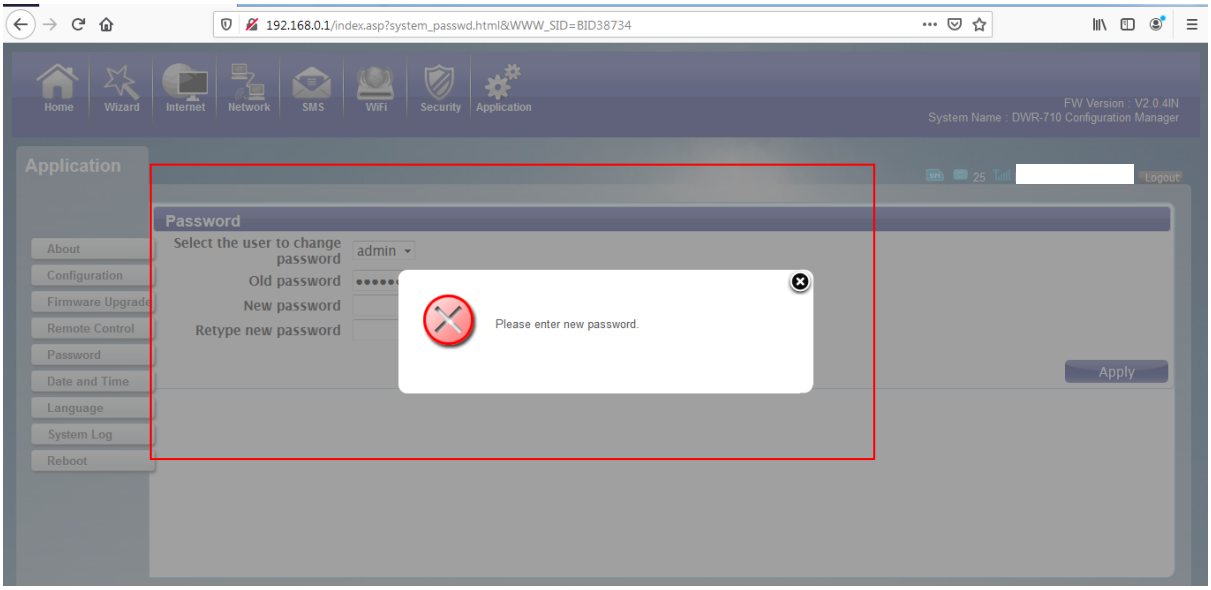
Step 9: Trying to login with Username:admin and password:Qwerty12345



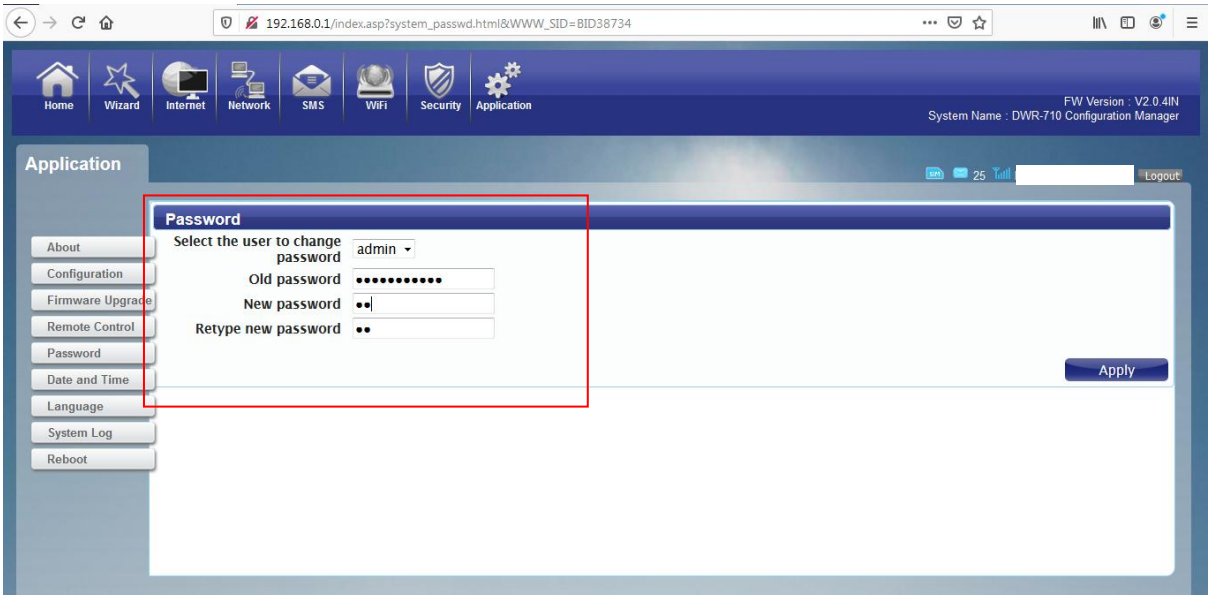
Step10: Now configuring the password for managment console to nothing i.e. empty so that any person connected to the access point and easily login to the management console and change the desired configuration



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

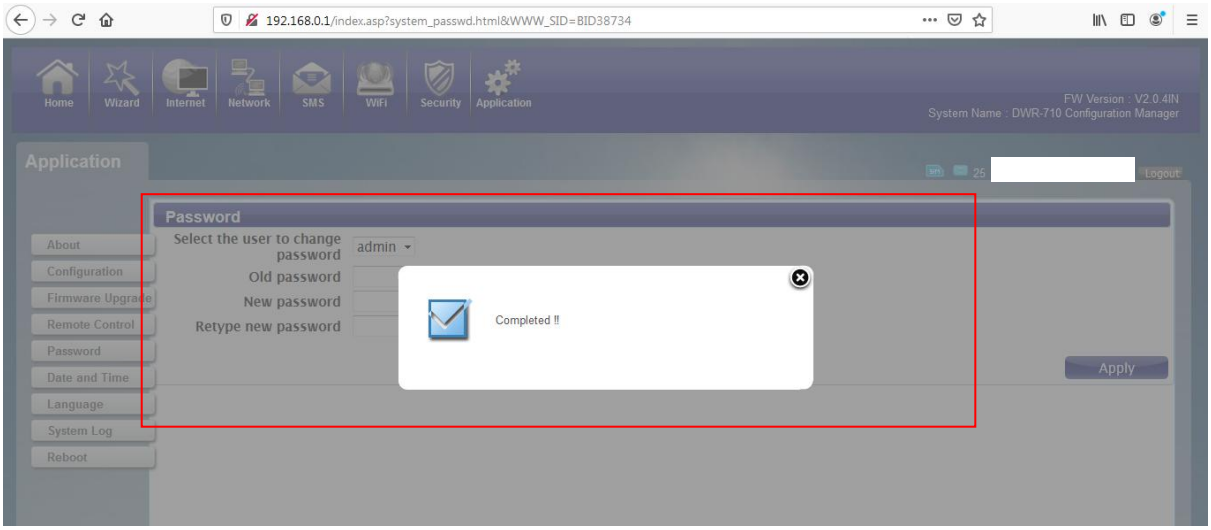


Since only client side validation is implemented, so we will try to set the new password field to nothing or blank using burp suite tool. For UI end we are entering new password as 12 to satisfy client side validation.



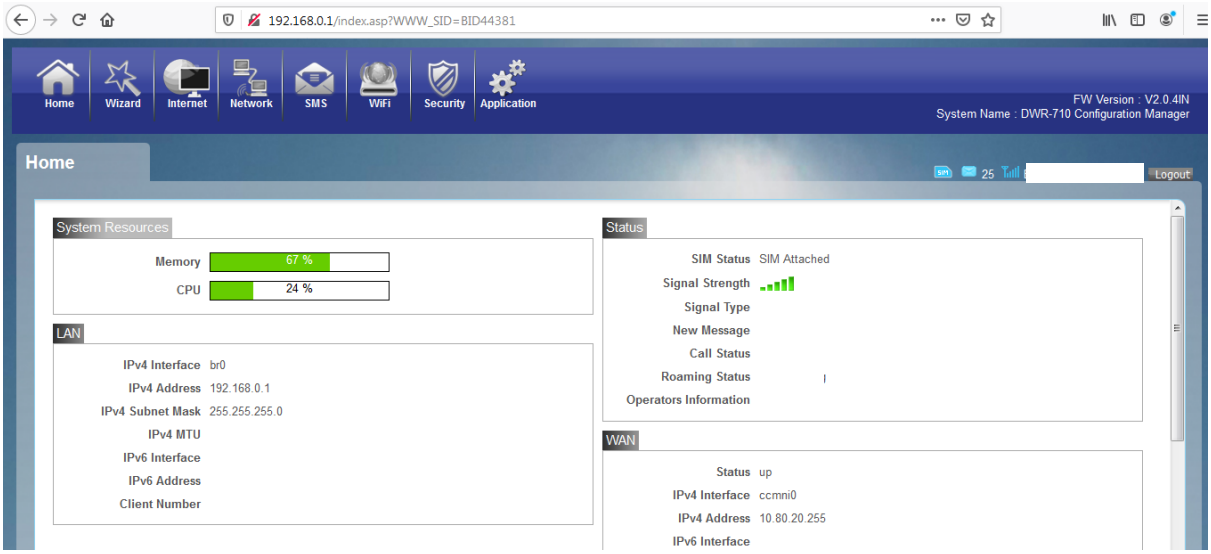
Setting the new password to blank

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



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 the home access points where generally management console is not well securely configured.