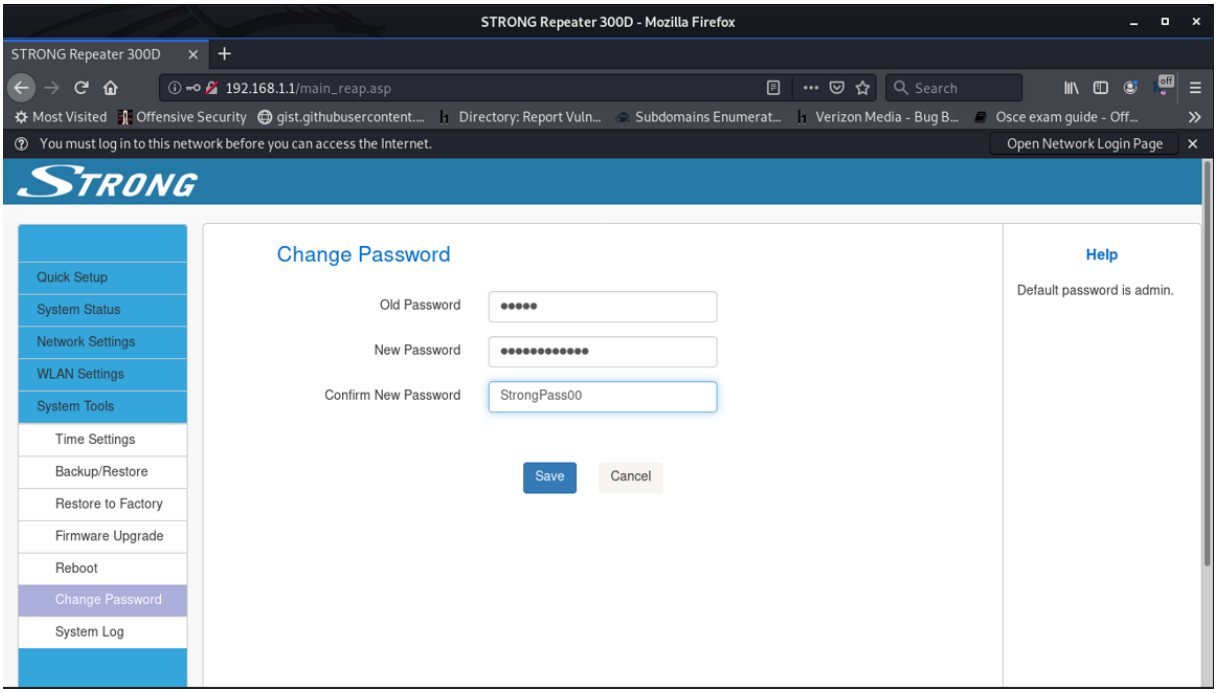
Strong 300D Wireless Router Information Disclosure Vulnerability

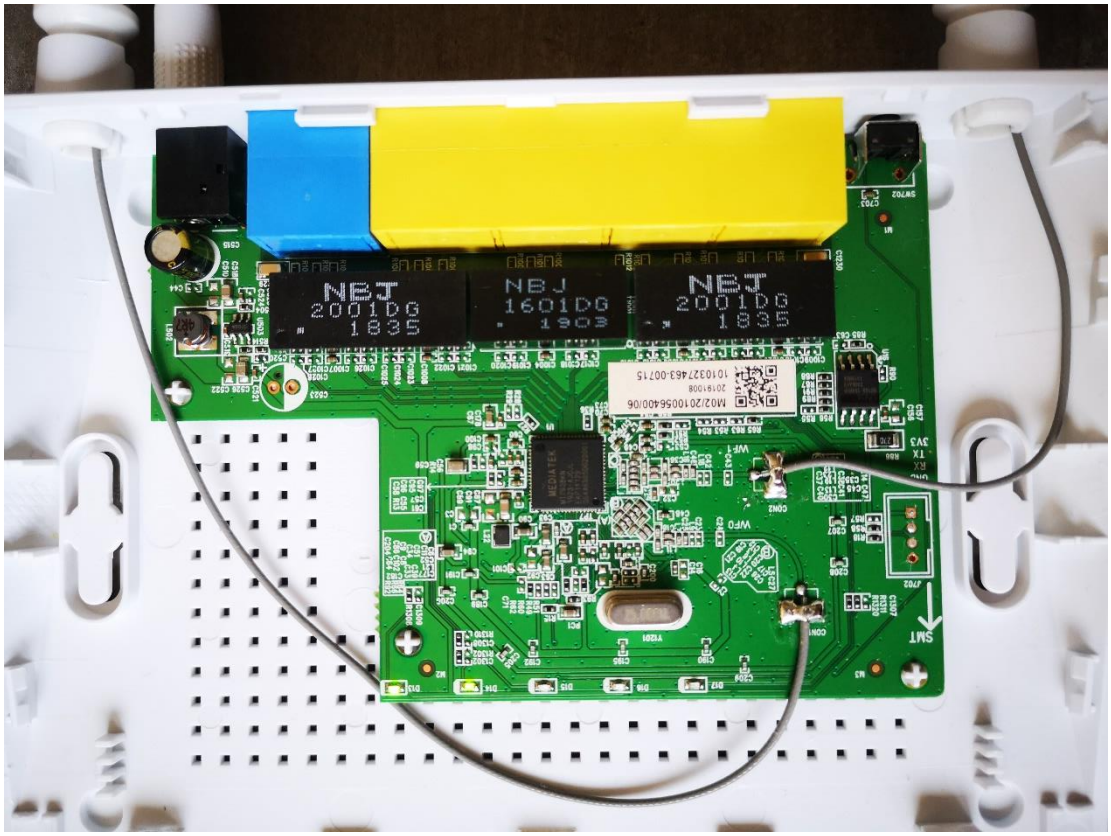
(Give me your admin password :D)

The Strong 300D is a simple wireless router for home use with basic features and a very simple web interface. As always, we have now begun our vulnerability research by examining the web interface. Aside from a couple of things, we didn't find anything interesting on the web interface. Injecting JavaScript and HTML code can cause some glitches, but based on our results so far, it cannot be exploited.

However, we noticed that the password for the web interface is limited to 12 characters and no special characters can be used. We used "StrongPass00" as the password.



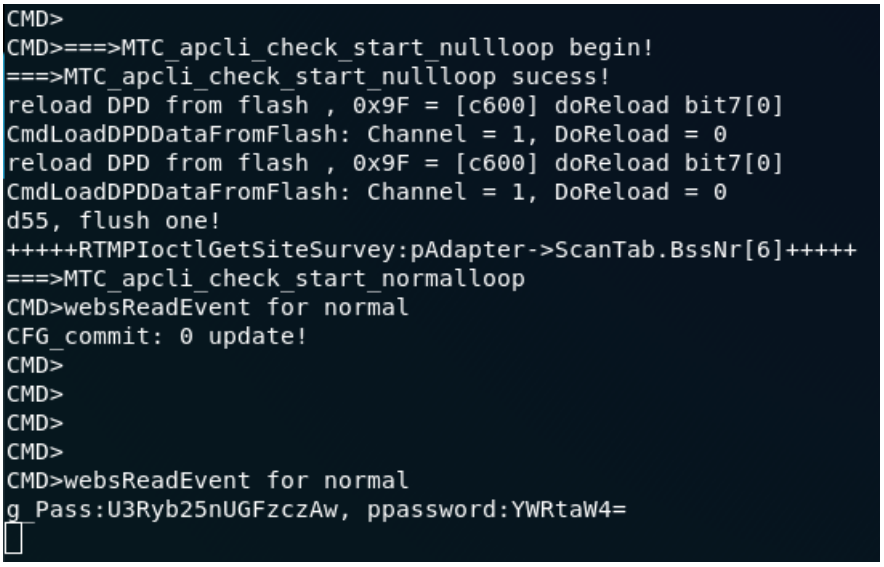
After disassembling the device, we were pleased to have the UART interface again.



We connected to the device through the UART interface and got a limited shell where we could only access certain information.

```
CMD>help
cfg         net         os

******argc=[1]******
******argv[0]=help******
******found=[0] help_mode=1******


CMD>net
NET>ls
show        br          eth         mon         ping        dhcpc       dhcpd
arp         pppoe       ntp         dns         ipnat       fw          route
timer       ifconfig    ated

******argc=[1]******
******argv[0]=ls******
******found=[0] help_mode=1******


NET>
```

Due to limited shell access, we have returned to the web user interface to examine the login a little more to see if we can bypass the login interface. It was then that we noticed a comparison of the values of the two variables seen on the debug console (UART interface) during login attempts. It's so much fun. The values of the two variables are the correct password for the web interface and the password we entered. Of course, the passwords are base64 encoded "for security". :D



after decrypting the Base64 encrypted password, I received the original admin login password. Thank you very much. :)