Vulnerability Research

TP-LINK TL-WR1043ND v2

Researcher: Uriel Kosayev

Email: urielsh4@gmail.com

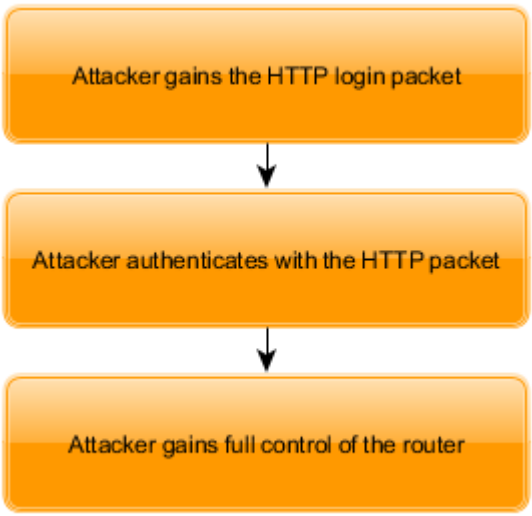
Country: Israel

Date: 01/10/19

General Explanation

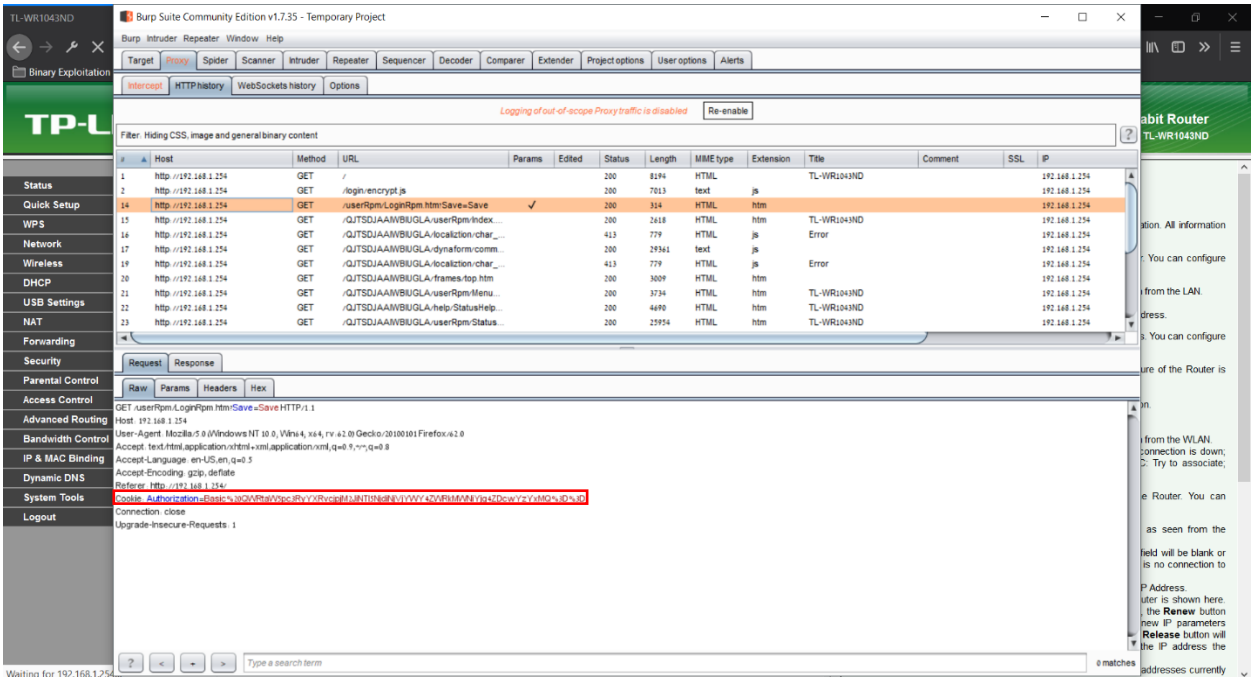
I found the following vulnerability that can give the attacker/adversary a full access to the router's web management interface.

Attack Kill Chain



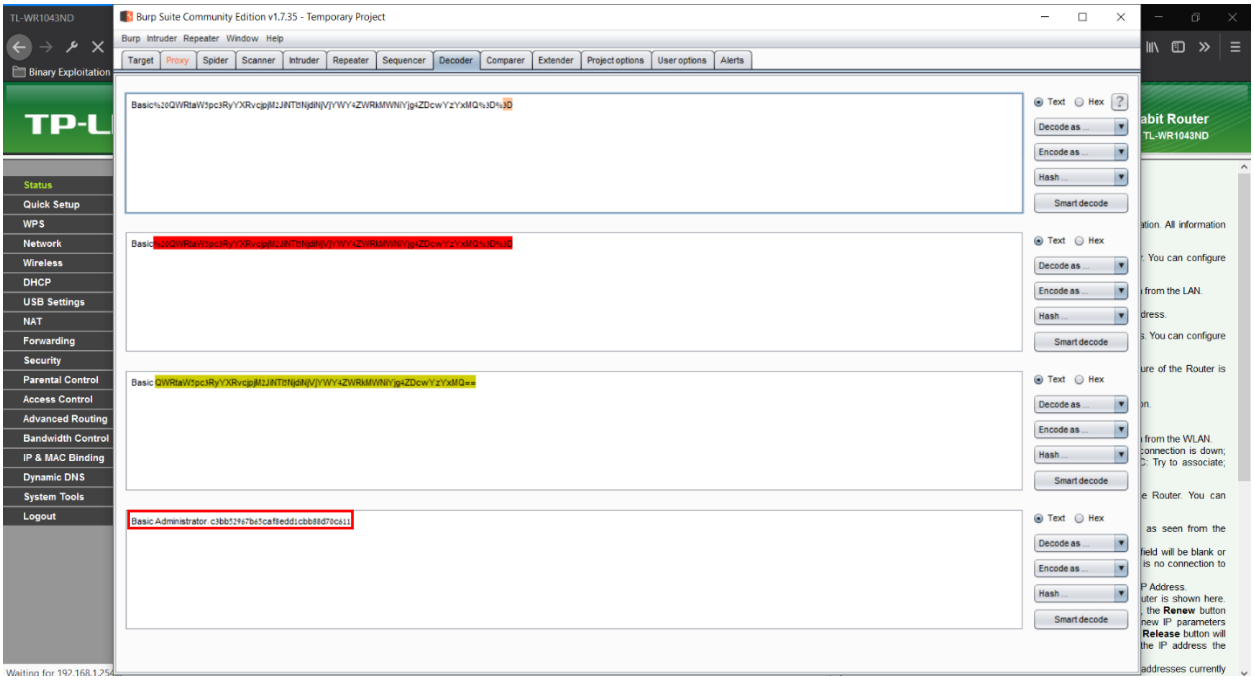
Findings

1. The attacker gains the HTTP login packet with the “Authorization” cookie that contains the login credentials by a Man-in-the-Middle attack, Social Engineering attack or some other method:



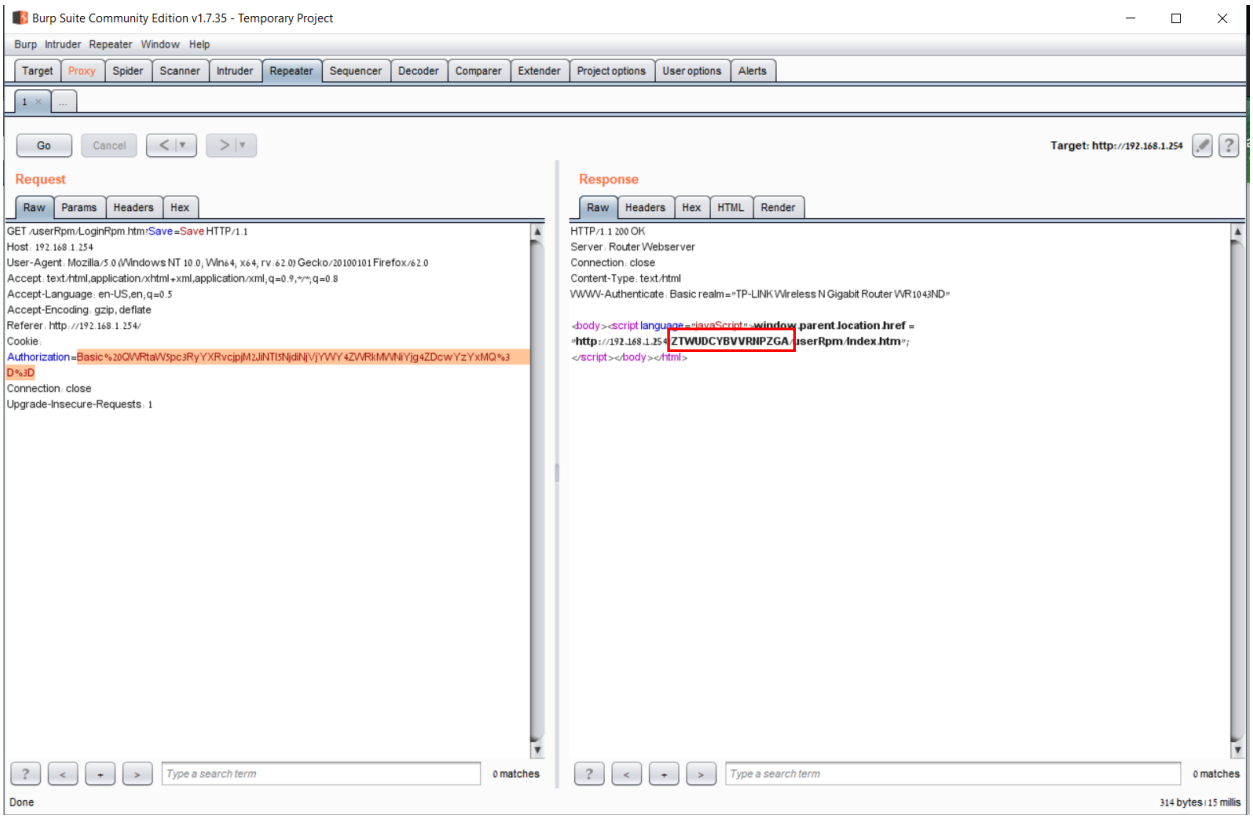
HTTP packet with the “Authorization” credentials cookie

2. The “Authorization” credentials can be easily decoded because the mechanism is implemented with weak encoding mechanisms (URL-Encoded and base64):

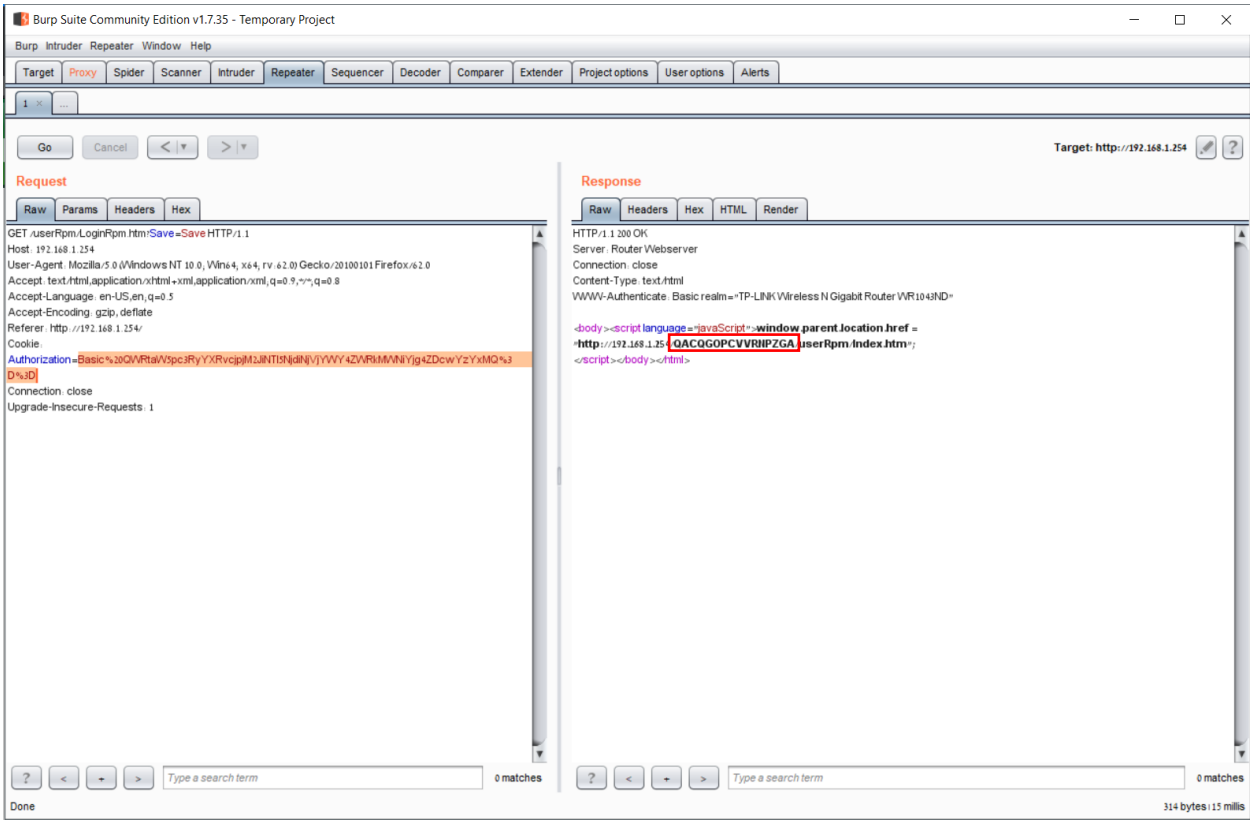


Decode of the “Authorization” cookie

3. An adversary/attacker can “generate” unlimited authentication tokens by passing the HTTP packet with the login credentials (followed by the “Authorization” credentials cookie):



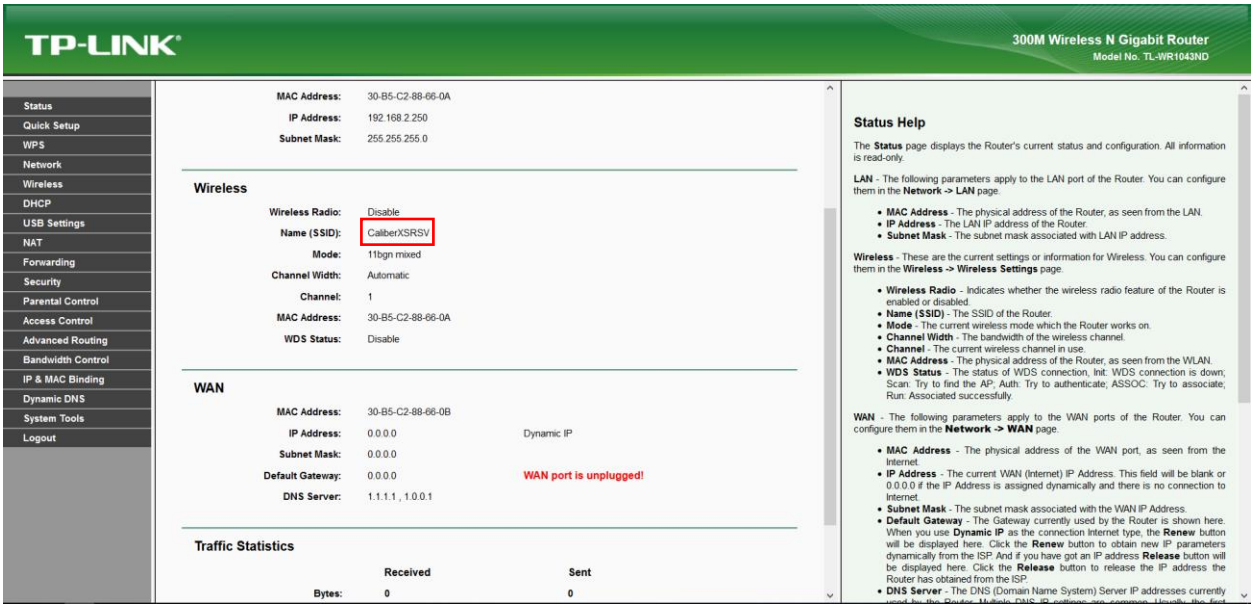
1st Token generated



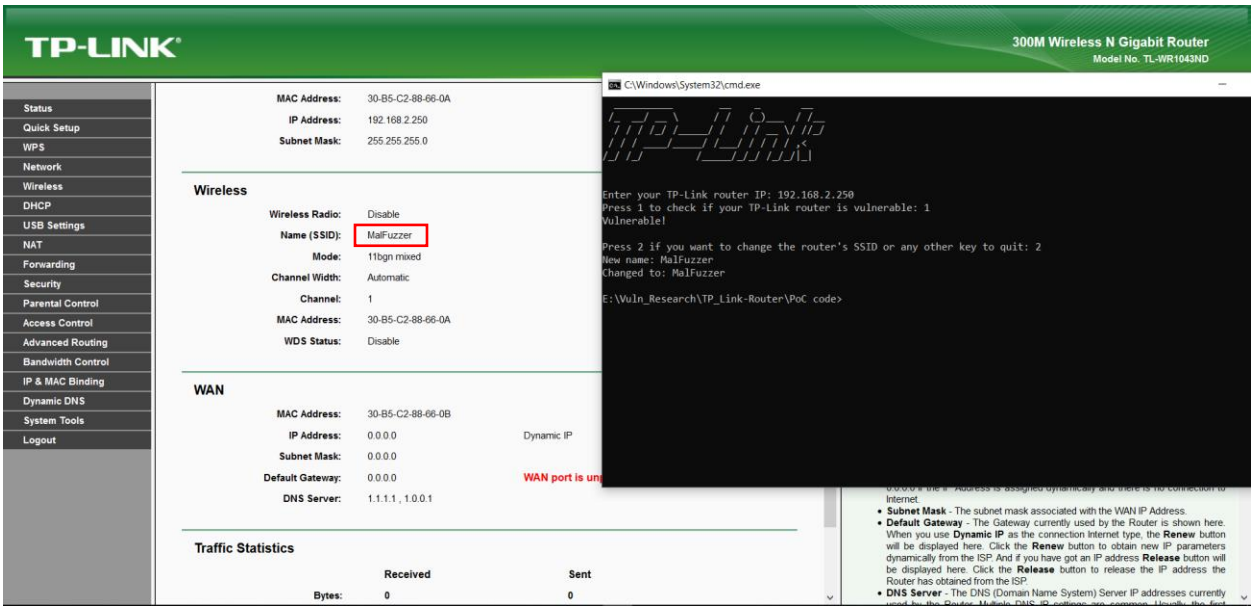
2nd Token generated

Attack example

After the attacker gained the HTTP login packet with the credentials cookie, he can do anything on the vulnerable device. For example, The attacker can change configurations, add a new user for backdoor purposes, disable/enable features and more. In this example, I will introduce the ability of manipulating the SSID name of the wireless AP (Access Point):



The SSID before manipulation



The SSID after manipulation

Conclusion

1. This version of TP-LINK router is vulnerable to “Auth bypass using cookie” and “Insecure Credentials” vulnerabilities.

2. The attacker does not have to “crack” the credentials, he can “pass” the login packet and gain full control.

3. The user authentication mechanism is very weak by utilizing encoding types such as URL-Encoding and base64.

4. After the decode procedure, the username is easily obtained because it’s not encrypted or hashed (clear-text).

5. After the decode procedure, it seems that the password is hashed with an MD5 hash algorithm that can be recovered by a brute-force, wordlist or Rainbow-Table attacks.