

Vulnerability Research

TP-LINK TL-WR1043ND v2

Researcher: Uriel Kosayev

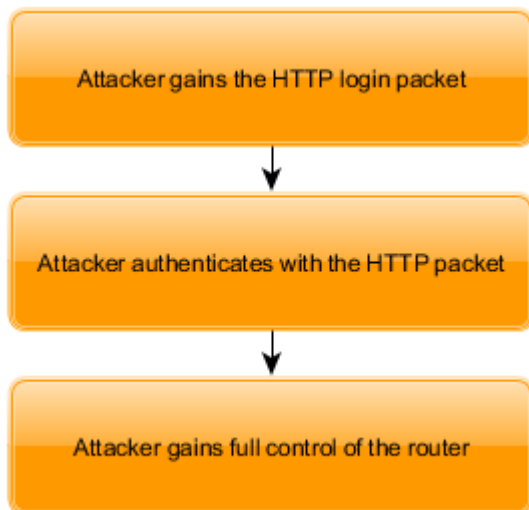
Email: urielsh4@gmail.com

PoC Video: <https://www.youtube.com/watch?v=G1vaxlxNylk>

General Explanation

The following vulnerability that can give the attacker/adversary a full access to the router's web management interface and thus manipulating it's settings.

Attack Kill Chain

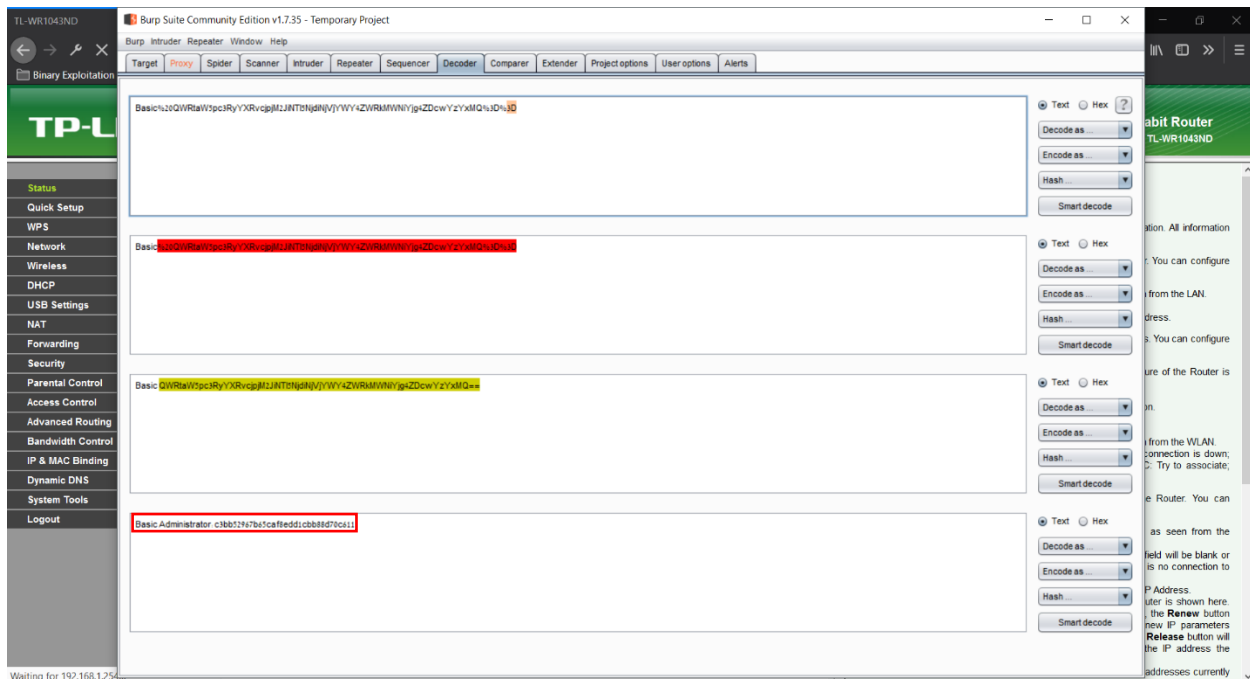


Findings

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 or some other methods:

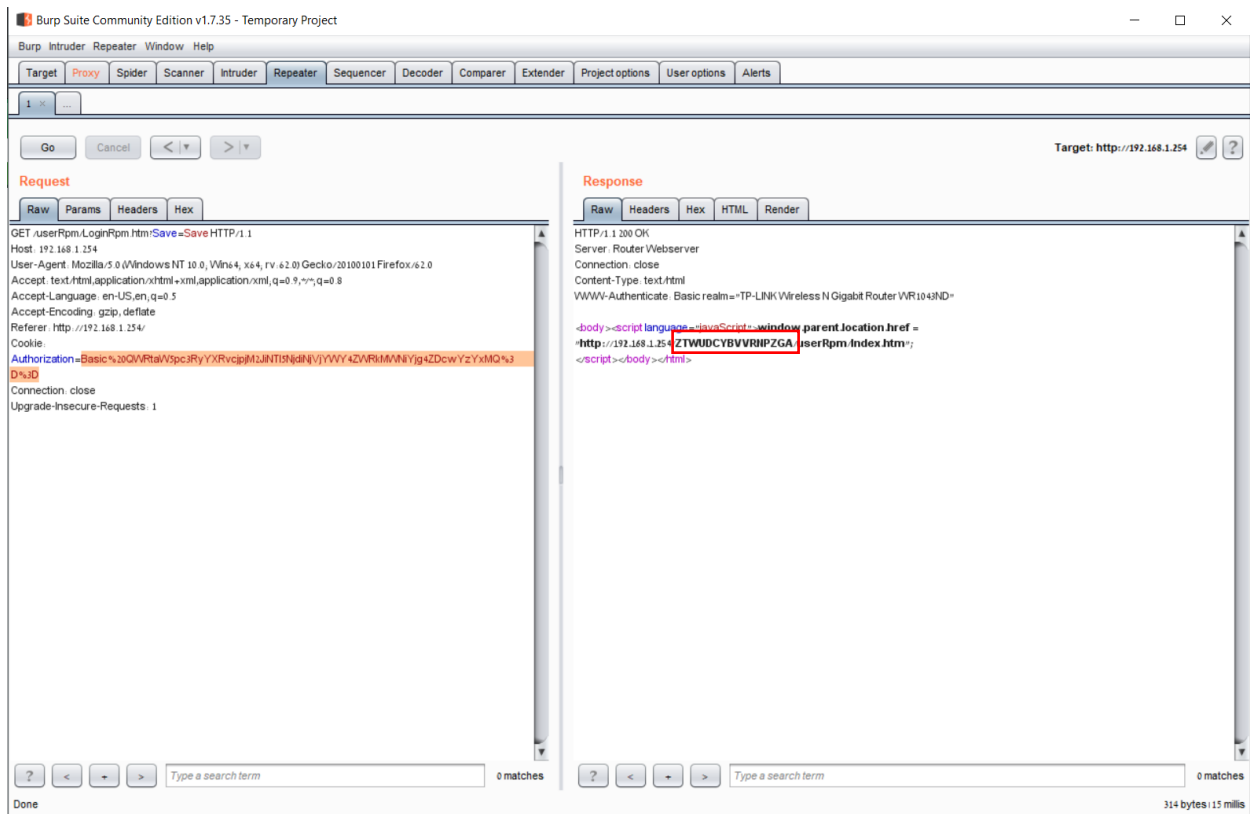
HTTP packet with the “Authorization” credentials cookie

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

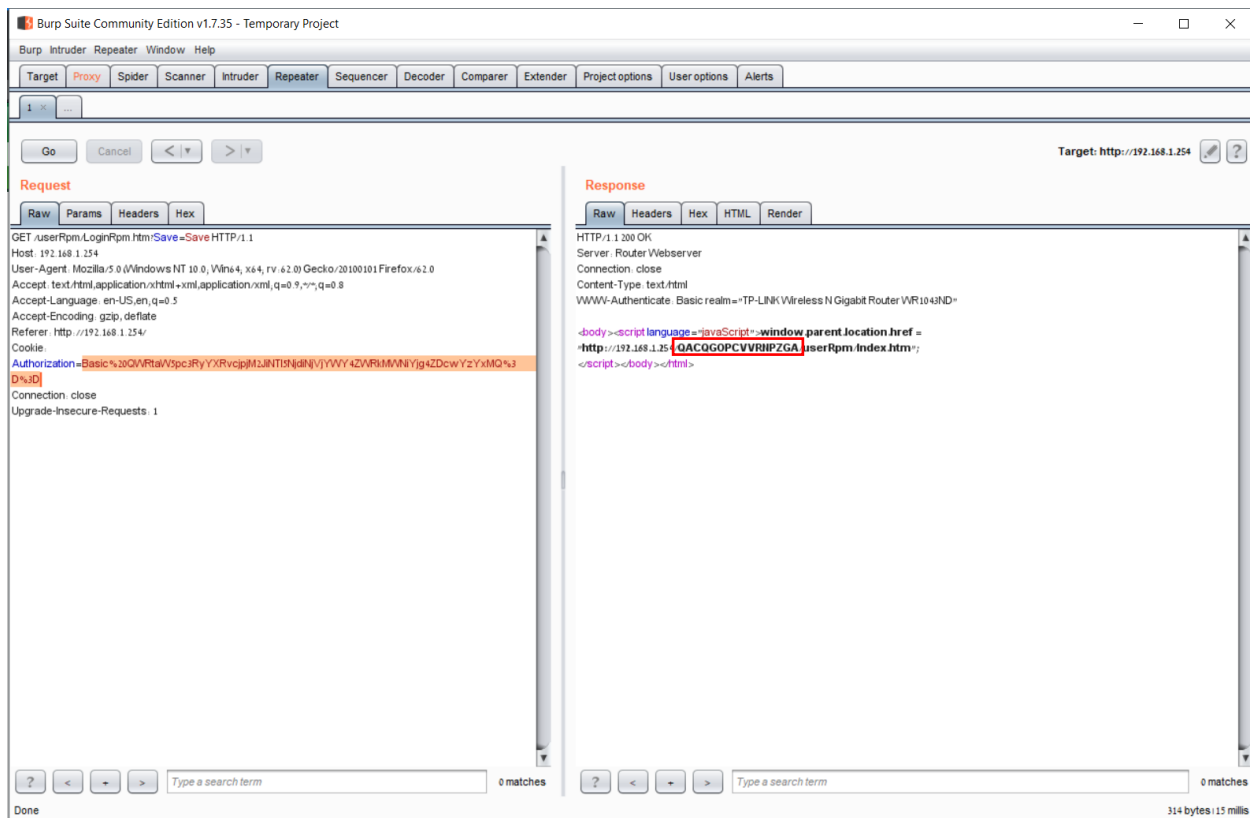


Decode of the “Authorization” cookie

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 screenshot shows the TP-Link web interface for a 300M Wireless N Gigabit Router (Model No. TL-WR1043ND). The left sidebar contains navigation links: Status, Quick Setup, WPS, Network, Wireless, DHCP, USB Settings, NAT, Forwarding, Security, Parental Control, Access Control, Advanced Routing, Bandwidth Control, IP & MAC Binding, Dynamic DNS, System Tools, and Logout. The main content area is divided into sections: Wireless, WAN, and Traffic Statistics. The Wireless section shows the following settings: Wireless Radio: Disable, Name (SSID): CaliberXSRV (highlighted with a red box), Mode: 11bgn mixed, Channel Width: Automatic, Channel: 1, MAC Address: 30-B5-C2-88-66-0A, and WDS Status: Disable. The WAN section shows: MAC Address: 30-B5-C2-88-66-0B, IP Address: 0.0.0.0 (Dynamic IP), Subnet Mask: 0.0.0.0, Default Gateway: 0.0.0.0, and DNS Server: 1.1.1.1, 1.0.0.1. A red message indicates 'WAN port is unplugged!'. The Traffic Statistics section shows a table with columns for Bytes, Received, and Sent, all currently at 0.

The SSID before manipulation

This screenshot shows the same TP-Link web interface as the previous one, but with the SSID changed to 'MalFuzzer' (highlighted with a red box). A Windows command prompt window is overlaid on the right side of the interface, displaying the following text: 'Enter your TP-Link router IP: 192.168.2.250', 'Press 1 to check if your TP-Link router is vulnerable: 1', 'Vulnerable!', 'Press 2 if you want to change the router's SSID or any other key to quit: 2', 'New name: MalFuzzer', 'Changed to: MalFuzzer', and 'E:\Vuln_Research\TP_Link-Router\PoC code>'. The rest of the interface remains the same, with the WAN port still unplugged and traffic statistics at 0.

The SSID after manipulation

Censys report

The report show that not a small amount of this device model around the globe are vulnerable:



TP-Link's answer:



Security <security@tp-link.com>
to me ▾

Hello Uriel,

Sorry for this trouble anyway.

This model is released and sold for many years, and we think for now many customers have changed to the new generation models, such as 11ac products. And the code/development for this model is old, different from our new routers. Thus I'm afraid we cannot develop new FW on it.

...

No problem, I understand.

Ok, thank you.

No worries, thanks for the update.

Received CVE numbers

CVE-2019-6971

CVE-2019-6972

Conclusion

1. This version of TP-LINK router is vulnerable to authentication bypass attacks.
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.