

Vulnerability Research

TP-LINK TL-WR1043ND v2

Researcher: Uriel Kosayev

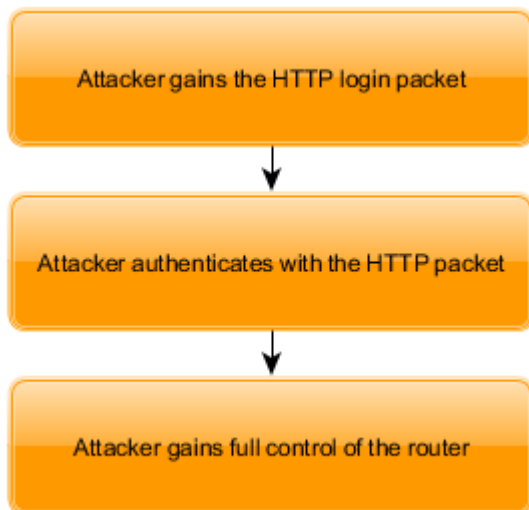
Email: urielsh4@gmail.com

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:

The screenshot displays the Burp Suite Community Edition v1.7.35 interface. The main pane shows a list of intercepted HTTP requests. The selected request is a GET request to `/userRpm/LoginRpm.htm?Save=Save` with a status of 200. The 'Cookie' header is highlighted in red, showing the value `Authorization=Basic: 802VRH8V0pcaRvYvRcepfUj8HT08Gf4UjVWY4ZQRMWMMVp4ZDoxZrZrLMDwIDwD`. The interface includes a sidebar with various tools like Target, Spider, Scanner, and a main pane showing the packet details and raw data.

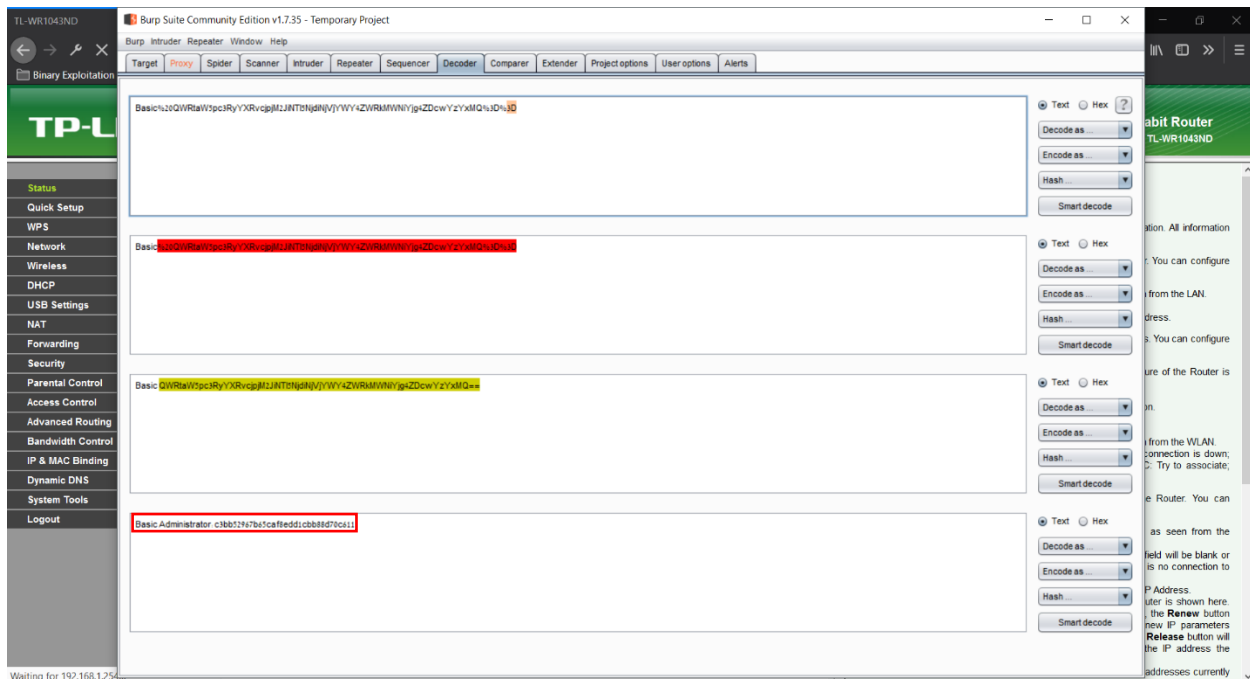
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
1	http://192.168.1.254	GET	/			200	8194	HTML		TL-WR1043ND			192.168.1.254
2	http://192.168.1.254	GET	/login-encrypt.js			200	7013	text	js				192.168.1.254
14	http://192.168.1.254	GET	/userRpm/LoginRpm.htm?Save=Save		✓	200	314	HTML	htm				192.168.1.254
15	http://192.168.1.254	GET	/QJTSQJAAWBUGLA-userRpm/index...			200	2618	HTML	htm	TL-WR1043ND			192.168.1.254
16	http://192.168.1.254	GET	/QJTSQJAAWBUGLA-localization/char...			200	29361	text	js	Error			192.168.1.254
17	http://192.168.1.254	GET	/QJTSQJAAWBUGLA-localization/char...			200	29361	text	js	Error			192.168.1.254
18	http://192.168.1.254	GET	/QJTSQJAAWBUGLA-localization/char...			200	3009	HTML	htm				192.168.1.254
19	http://192.168.1.254	GET	/QJTSQJAAWBUGLA-frames-top.htm			200	3734	HTML	htm	TL-WR1043ND			192.168.1.254
20	http://192.168.1.254	GET	/QJTSQJAAWBUGLA-userRpm/Menu...			200	4490	HTML	htm	TL-WR1043ND			192.168.1.254
21	http://192.168.1.254	GET	/QJTSQJAAWBUGLA-help/Status/help...			200	25954	HTML	htm	TL-WR1043ND			192.168.1.254
22	http://192.168.1.254	GET	/QJTSQJAAWBUGLA-userRpm/Status...			200	25954	HTML	htm	TL-WR1043ND			192.168.1.254

Raw data view shows the following headers:

```
Host: 192.168.1.254
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:42.0) Gecko/20100101 Firefox/42.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.254/
Cookie: Authorization=Basic: 802VRH8V0pcaRvYvRcepfUj8HT08Gf4UjVWY4ZQRMWMMVp4ZDoxZrZrLMDwIDwD
Connection: close
Upgrade-Insecure-Requests: 1
```

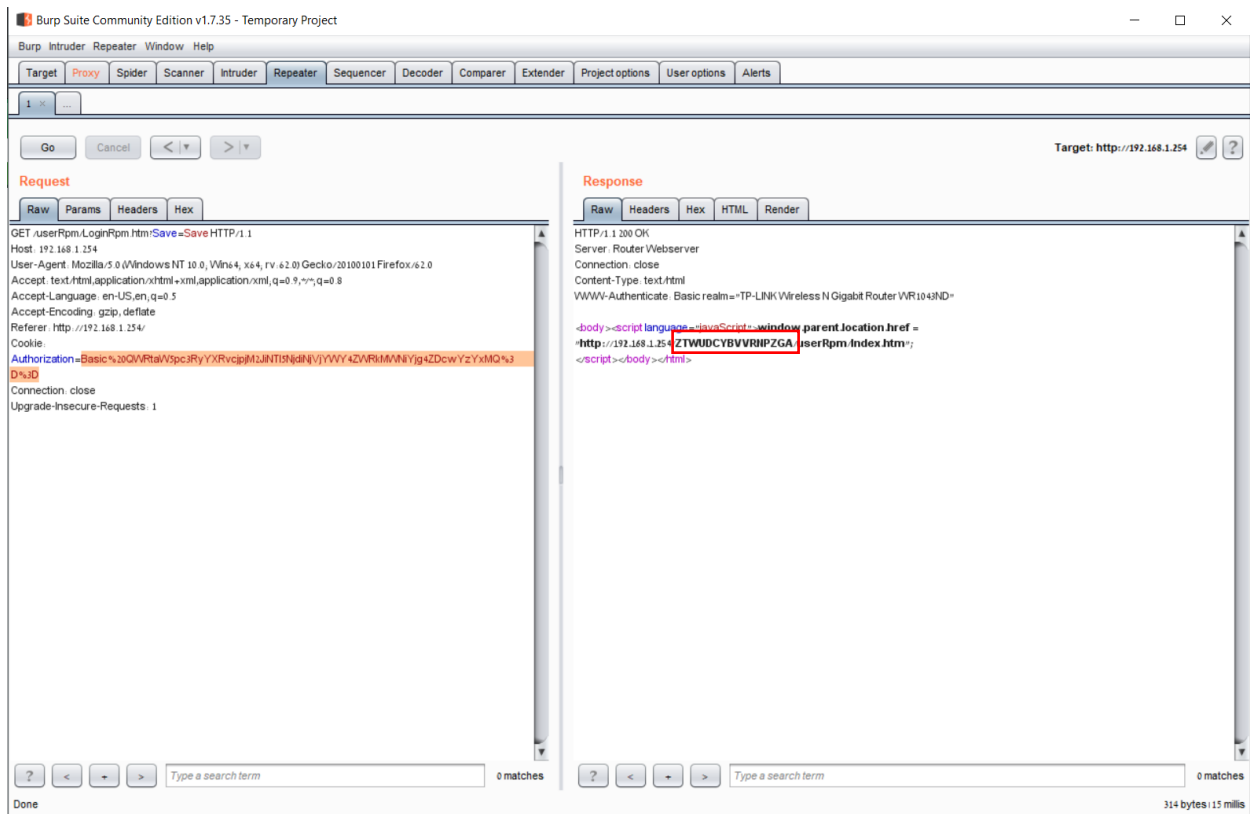
HTTP packet with the “Authorization” credentials cookie

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

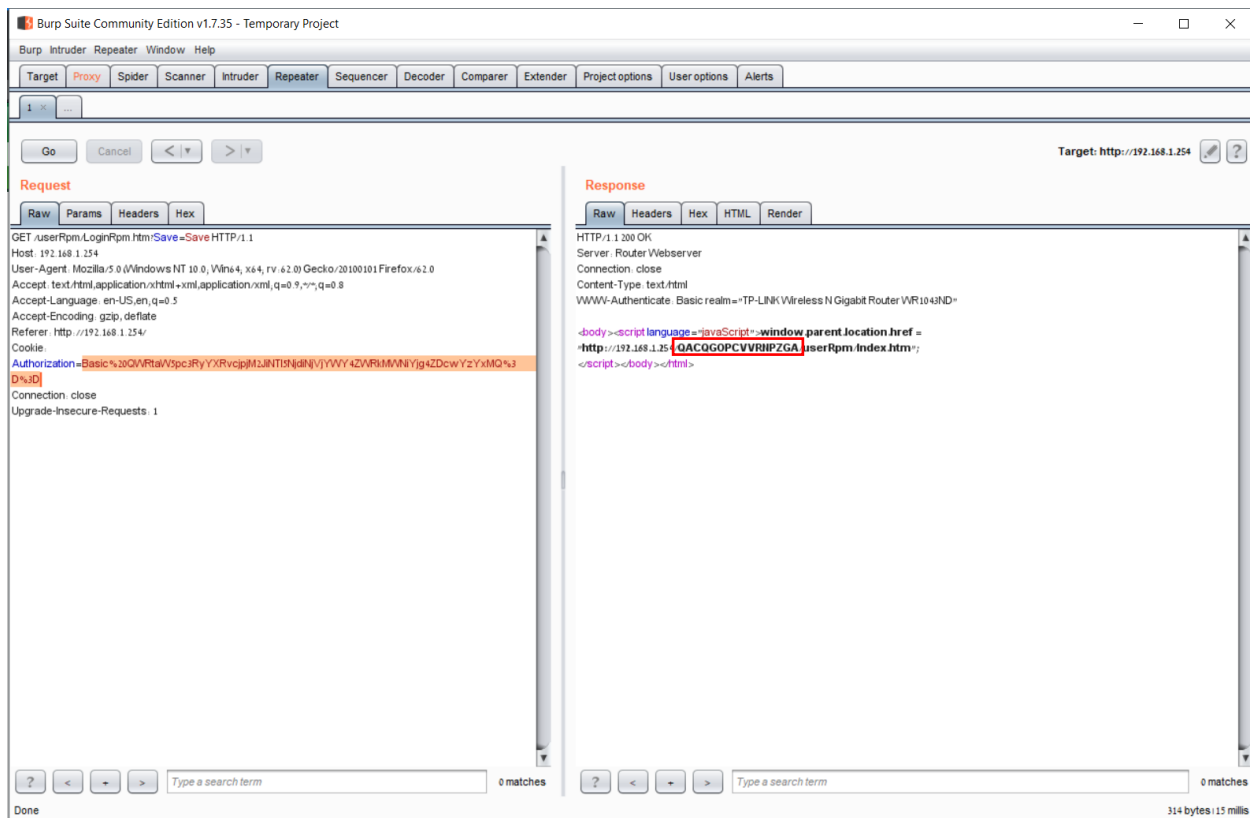


Decode of the “Authorization” cookie

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 300M Wireless N Gigabit Router web interface. 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 'WAN port is unplugged!' is displayed. The Traffic Statistics section shows a table with columns for Bytes, Received, and Sent, all currently at 0.

The SSID before manipulation

The screenshot shows the TP-Link 300M Wireless N Gigabit Router web interface, similar to the previous one, but with the SSID changed to 'MalFuzzer' (highlighted with a red box). A terminal window titled 'C:\Windows\System32\cmd.exe' is overlaid on the right side of the interface. The terminal output shows the following commands and responses: '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, including the Wireless and WAN settings, remains the same as in the previous screenshot.

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/develop for this model is old, different from our new routers. Thus I'm afraid we can not develop new FW on it.

...

No problem, I understand.

Ok, thank you.

No worries, thanks for the update.

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.