**DWR 2000M 5G (CPE) Multiple Security Vulnerability**



**09-Feb-2024**

|  |  |
| --- | --- |
| **Submitted By** |  |
| **Vinod Kumar Shrimalii (mrnmap)**  **Nayab Keshodwala (NK)** |  |

**NAME OF AFFECTED PRODUCT(S) AND VERSION(S)]**

**Model:** DLink DWR 2000M 5G CPEWith Wifi 6 Ax1800

**Version:** DWR-2000M\_1.34ME

**Date: 09 Feb-2024**

**Description**

The new DWR-2000M 5G customer premise equipment (CPE) serves as a powerful networking focal point for homes and offices. The DWR-2000M CPE integrates LTE Advanced standard, which combines with leading-edge 5G to dramatically elevate connection speeds. Wi-Fi 6 innovation provides users with simultaneous and seamless access to voice, data and video content. Additional product specifications include

1. **Bypassing Weak Brute Force Protection Mechanism HIGH**

During the testing of the Dlink DWR 2000M router, a weakness was identified in its brute force protection mechanism. The router is designed to impose a temporary block on unauthorized login attempts after three unsuccessful tries, with a five-minute cooldown period. However, further investigation revealed that this protection was easily bypassed by exploiting a flaw in the implementation.

**Recommendation**

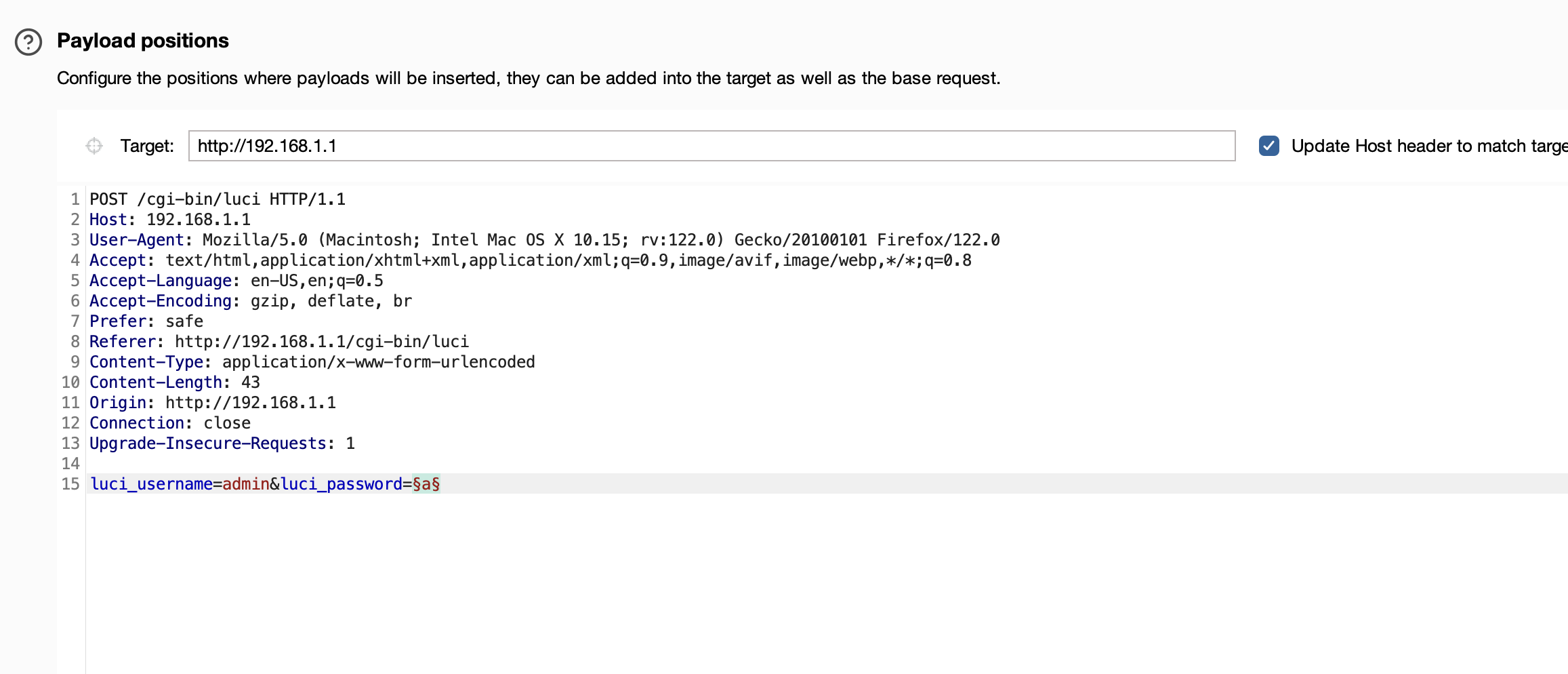
* Strengthen the brute force protection mechanism to impose more robust restrictions on repeated login attempts. Consider implementing progressive delays or CAPTCHA challenges to deter automated attacks.
* Implement server-side validation to enforce the temporary block on login attempts at the backend, rather than relying solely on client-side restrictions. This ensures that the block cannot be bypassed by manipulating client-side elements
* Apply rate limiting and account lockout policies to prevent excessive login attempts within a specified timeframe. Temporarily lockout accounts that exceed the allowed number of failed login attempts to thwart brute force attacks effectively.
* Ensure that firmware updates are regularly released to patch security vulnerabilities and improve the overall security posture of the router. Encourage users to install updates promptly to mitigate potential risks.

**Bypassing Weak Brute Force Protection Mechanism -POC**

* User Block After 3 unsuccessful attempts to CPE admin panel for 5 minutes

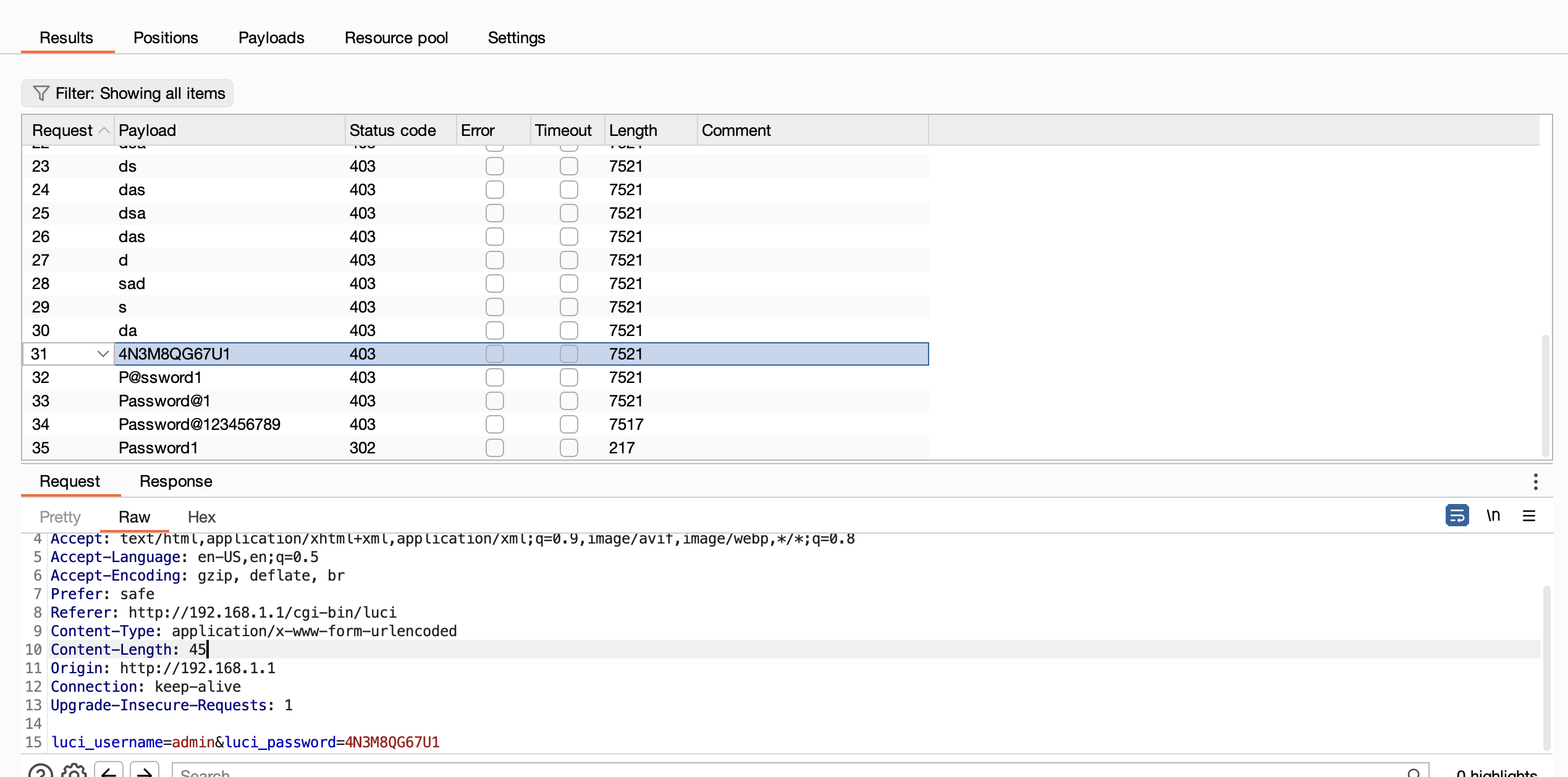


* Capturing user request for brute force attack and preparing for attack

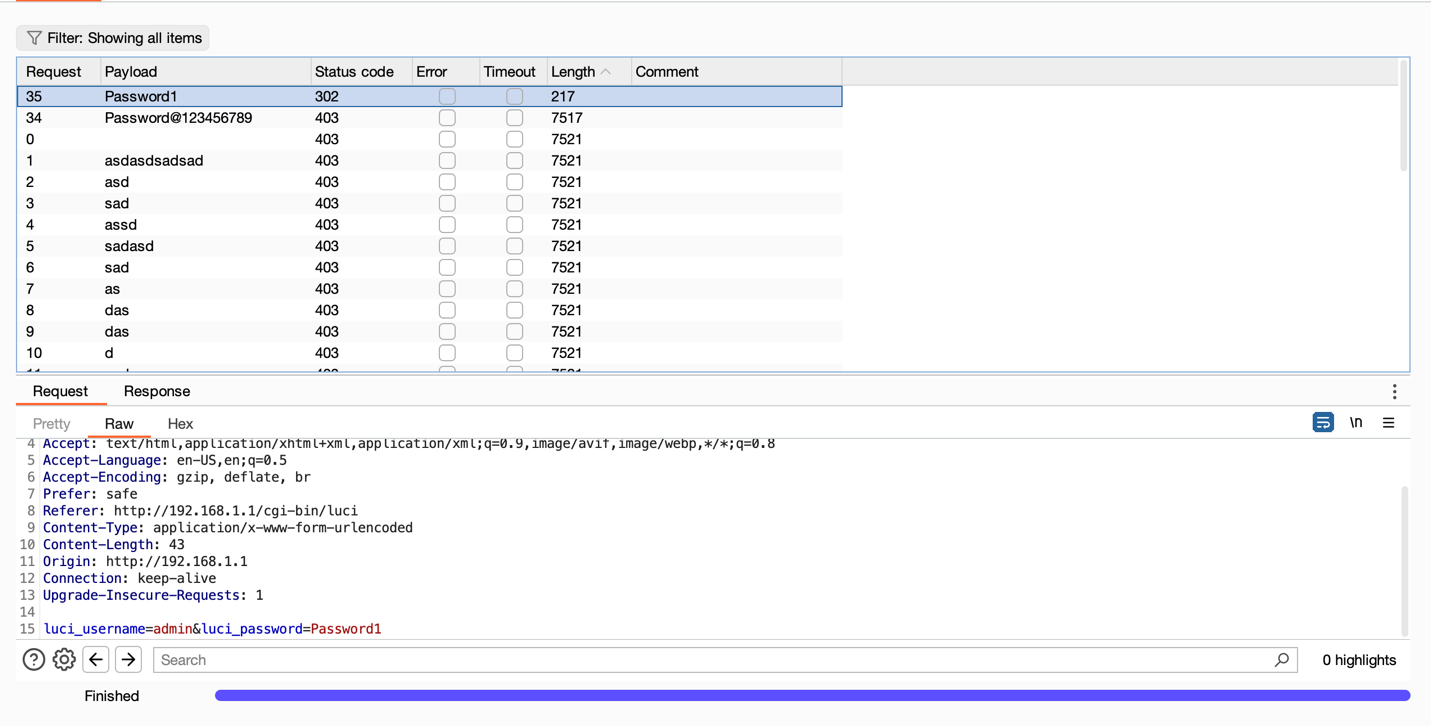


In this test we user 50-word dictionary

* Launching brute force attack



* Finding correct username and password and not getting block by CPE



* Using this password attack can login into system after time is over.