Day 28: Brute Force OTP Attack on Quantower (Sniper Mode)

Date: July 21, 2025

Topics Covered :

- Brute Force Attack using Burp Suite Professional
- Configuring and executing an attack in Sniper Mode
- Bypassing OTP verification on Quantower (simulated)

Attack Overview :

A Brute Force OTP Attack targets the OTP (One-Time Password) mechanism by submitting a large number of OTP values in sequence, attempting to discover the valid one. This method exploits weak or improperly secured OTP verification endpoints.

- Tool Used: Burp Suite Professional
- Attack Method: Intruder Module — Sniper Mode

Steps Performed :

1. Captured the OTP Request
   Intercepted the OTP verification request using Burp Suite's proxy after submitting the form on Quantower's registration page.
2. Sent the Request to Intruder
   Right-clicked on the captured request and sent it to the Intruder module.
3. Selected the Injection Point
   Identified and highlighted the OTP parameter as the injection target.
4. Chose Attack Type: Sniper
   Selected Sniper mode, which replaces the marked payload position one at a time.
5. Configured Payloads
   Added a numeric list of OTP values ranging from 000000 to 999999.
6. Started the Attack
   Launched the brute force attack, allowing Burp to cycle through the payloads.
7. Monitored Responses
   - Successful OTP attempts were indicated by status code 200 or distinct content length.
   - Invalid attempts typically returned 401 or 403.
   - Applied filters using Grep Match and Content Length to automatically highlight anomalies.

By Ritesh Kumar Gupta CRN : 2315195 URN : 2302650

Outcome :

The simulation successfully demonstrated that OTP endpoints without proper security measures are vulnerable to brute force attacks using Sniper Mode in Burp Suite.

This highlights the critical need for implementing:

- Rate Limiting
- CAPTCHA on OTP forms
- Account Lockouts after failed attempts
- Logging and monitoring suspicious OTP attempts

Ethical Note :

This activity was conducted in a controlled environment strictly for educational and ethical training purposes. Never perform brute force or penetration testing on systems without explicit permission.