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

Topics Covered:

- Brute Force Attack using Burp Suite Professional
- Setting up and running an attack in Sniper Mode
- Bypassing OTP on Quantower (simulated)

Attack Overview:

A Brute Force OTP Attack tries many OTP values to find the right one. This works if OTP verification isn't secure.

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

Steps Performed:

1. **Captured OTP Request:** Intercepted the OTP request after submitting the form on Quantower.
2. **Sent Request to Intruder:** Right-clicked and sent it to the Intruder module.
3. **Selected Injection Point:** Highlighted the OTP parameter.
4. **Chose Attack Type: Sniper:** Replaces one payload position at a time.
5. **Configured Payloads:** Added numbers from 000000 to 999999.
6. **Started Attack:** Launched the attack.
7. **Monitored Responses:** Looked for successful attempts (status 200 or different content length). Invalid attempts were 401 or 403. Used filters to find anomalies.

Outcome:

The simulation showed that OTP endpoints without good security are vulnerable to brute force attacks with Burp Suite's Sniper Mode. This means we need:

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

Ethical Note:

This was for education only. Never do penetration testing without permission.