DVWA: Brute Force Attack Exploitation Lab

By: Belizaire Bassette II

School: Syracuse University

Major: Information Management & Technology (Information Security Concentration)

Minor: Computer Science

Overview & Professional Relevance

This lab was conducted in a controlled environment using the Damn Vulnerable Web Application (DVWA) to simulate a real-world brute force attack scenario. The goal was to gain hands-on experience with the tools, techniques, and workflows commonly used in penetration testing engagements and security operations.

Key outcomes of this exercise include:
- Identifying and exploiting authentication weaknesses.
- Leveraging automated tools for password cracking.
- Understanding attacker workflows for improved defense strategies.

In practice, these skills translate to real-world cybersecurity roles by:
- Strengthening offensive capabilities to identify weaknesses before attackers do.
- Enhancing defensive readiness through recognition of brute force indicators.
- Developing professional reporting skills for both technical and executive audiences.

Lab Environment & Tools Used

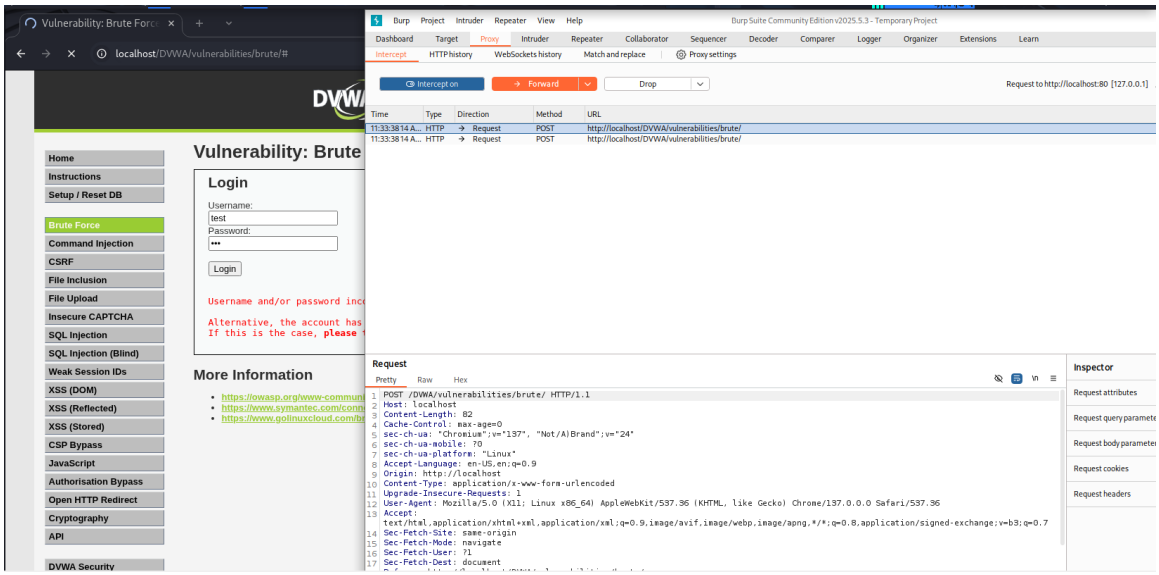
- Operating Systems: Kali Linux, Ubuntu Linux
- Web Application Target: DVWA (Damn Vulnerable Web Application)
- Tools & Utilities:
  - Nmap: Network scanning and service enumeration.
  - Burp Suite: HTTP traffic interception and analysis.
  - Hydra: Automated password cracking for brute force testing.
  - rockyou.txt: Common password wordlist from the 2009 RockYou breach.

Step 1 — Target Identification

Confirmed DVWA was hosted locally at 127.0.0.1 (localhost). Accessed the application and navigated to the Brute Force module.

Step 2 — Manual Reconnaissance

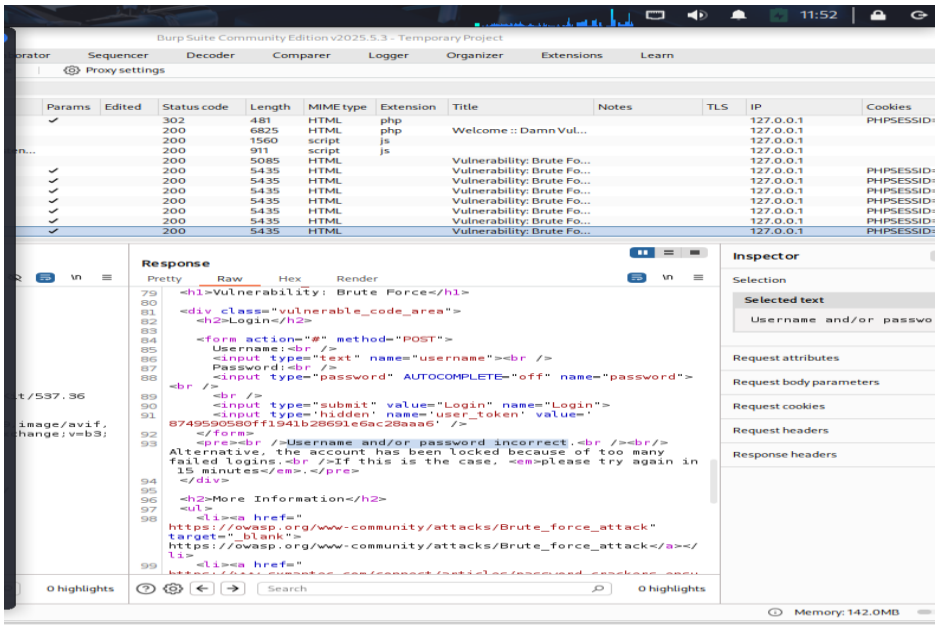
Attempted a manual login to observe the server's response to invalid credentials. Identified the error message: 'Username and/or password incorrect'. This provided the failure condition for Hydra's automated attack.



Step 3 — Traffic Interception & Parameter Discovery

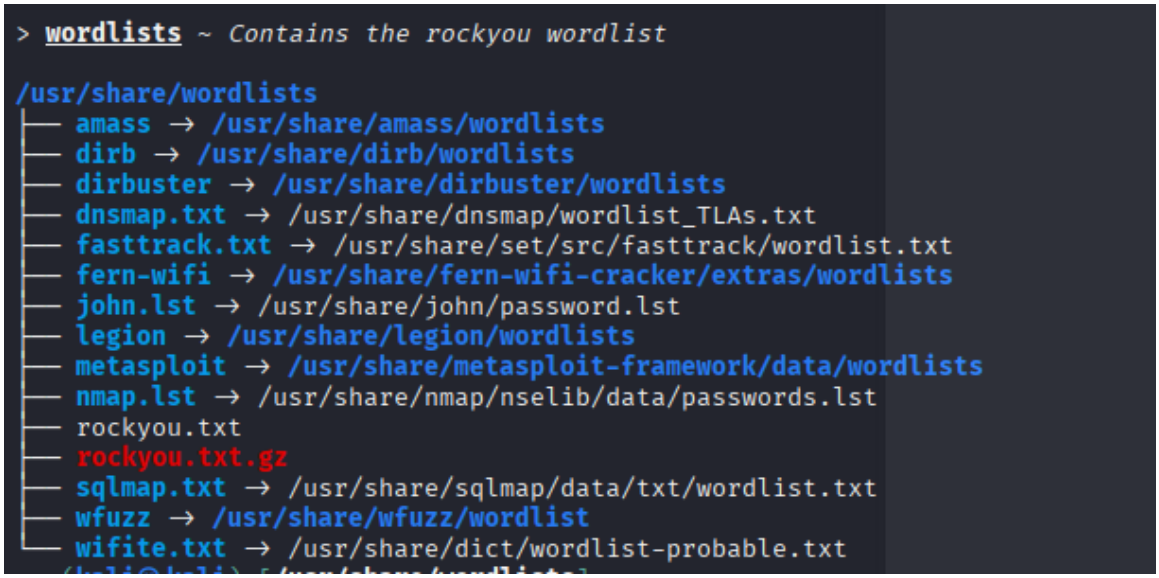
Using Burp Suite, intercepted the login request to identify POST parameters and the exact form structure.

Parameters Identified:
- username
- password
- Login (submit field)



Step 4 — Wordlist Preparation

Selected rockyou.txt as the password list due to its large dataset of real-world passwords from the 2009 RockYou breach.



Step 5 — Hydra Execution

The following command was executed to perform the brute force attack:

```
hydra -l admin \
    -P /usr/share/wordlists/rockyou.txt \
    127.0.0.1 \
    http-post-form \

"/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:Username and/or password incorrect" \
    -V
```

Command Breakdown:

- `-l admin`: Specifies the username to test.

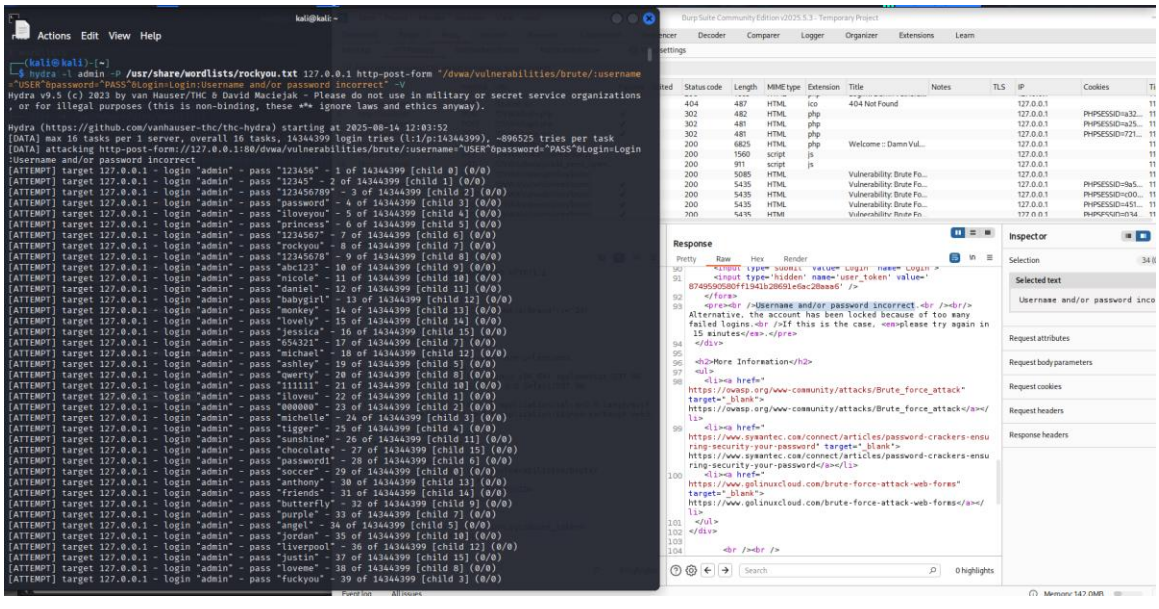
- `-P /usr/share/wordlists/rockyou.txt`: Path to the wordlist.

- `127.0.0.1`: Target IP (localhost).

- `http-post-form`: Specifies the attack type (form-based login).

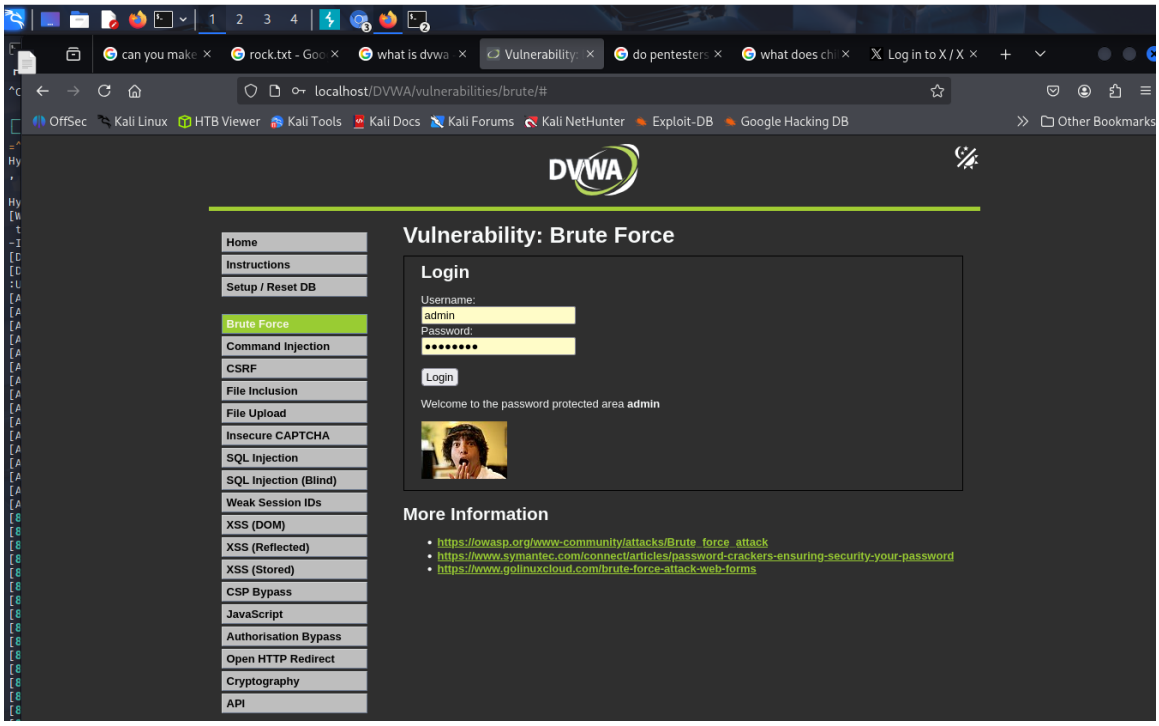
- `"/DVWA/...incorrect"`: Login form path, parameters, and failure message.

- `-V`: Verbose mode for detailed output.



Step 6 — Results & Findings

The correct password was found after 4 attempts, successfully logging into the application and capturing the flag.



Step 7 — Security Recommendations

- Implement account lockout policies after a set number of failed attempts.
- Enforce strong password complexity requirements.
- Enable multi-factor authentication (MFA).
- Monitor for repeated failed login attempts using SIEM alerts.