Brute-force Attacks Project Report

Title: Brute-force Attacks using Burp Suite and Hydra
Name: Balasani Sai Vardhan
Tools Used: Kali Linux, Burp Suite, Hydra, bWAPP (OWASP BWA)
Target IP: 10.0.2.5

---

1. Introduction

Brute-force attacks are a type of cyberattack where an attacker tries multiple username and password combinations to gain unauthorized access to a system. Weak authentication mechanisms in web applications are highly vulnerable to such attacks if proper security controls like account lockout, CAPTCHA, or rate limiting are not implemented.

The objective of this project is to simulate and analyze brute-force attacks against a vulnerable web login form using Burp Suite Intruder (manual attack) and Hydra (automated attack), and demonstrate how valid credentials can be discovered and mitigated.

---

2. Lab Environment Setup

- Operating System: Kali Linux (VirtualBox)
- Vulnerable Application: bWAPP (OWASP BWA)
- Tools Used:
    - Burp Suite (Intruder)
    - Hydra
- Target URL:

http://10.0.2.5/bWAPP/login.php

💉 **Lab 1: Brute-force Using Burp Suite (Cluster Bomb)**

3.1 Objective

To perform a brute-force attack on the bWAPP login form using Burp Suite Intruder with the Cluster Bomb attack type and identify valid credentials through response analysis.

3.2 Procedure

1. Opened bWAPP login page in the browser.
2. Configured Burp Suite proxy and enabled interception.
3. Entered dummy credentials to capture the login request.
4. Sent the intercepted request to Intruder.

5. Set payload positions for:
    - login (username)
    - password
6. Selected attack type as **Cluster Bomb**.
7. Loaded username and password wordlists.
8. Launched the attack and analyzed response length differences.

Figure 1: bWAPP Login Page

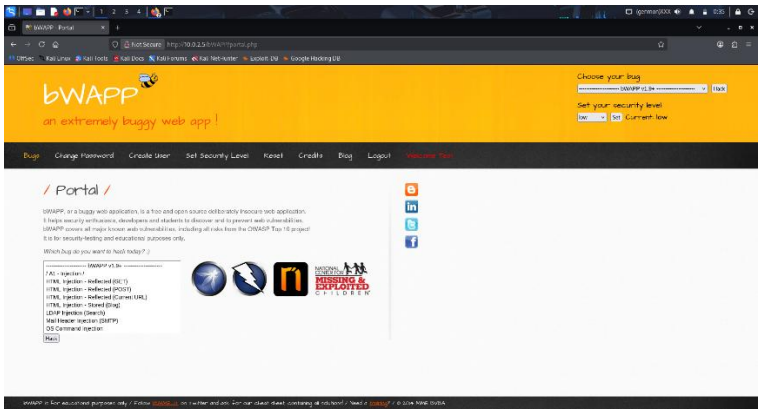


Figure 2: Burp Suite Intercepted Login Request

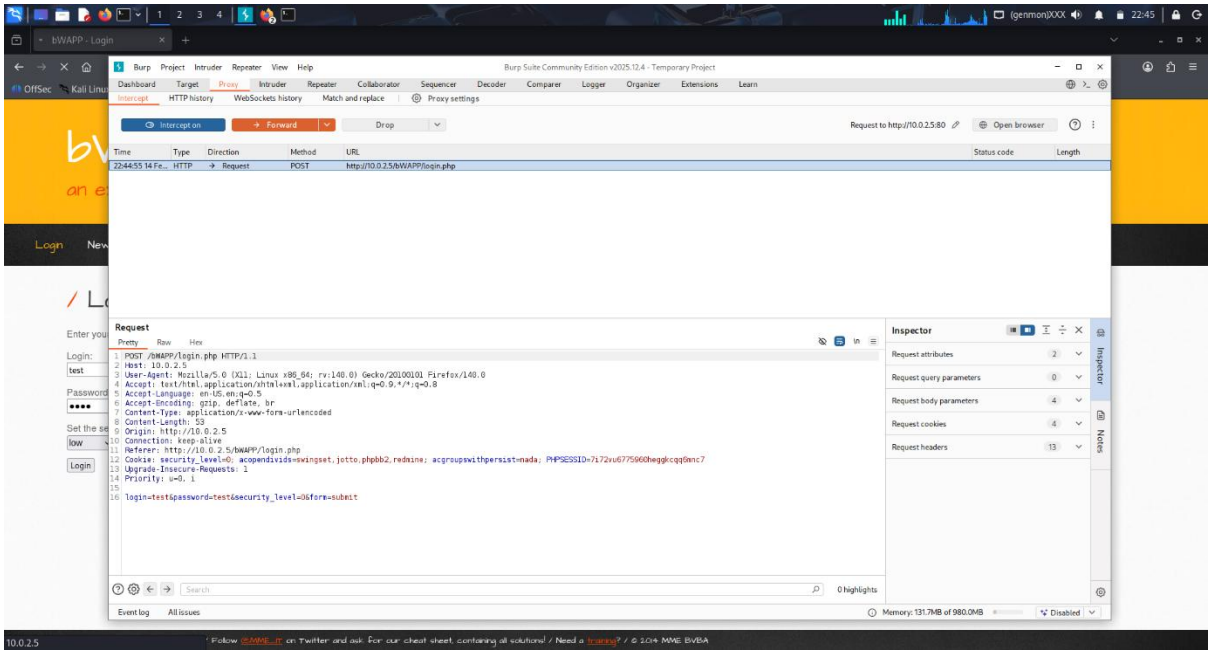
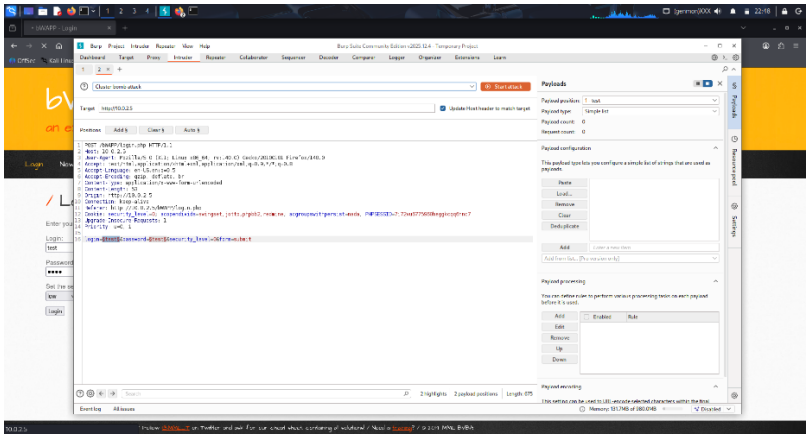


Figure 3: Intruder Payload Positions (Cluster Bomb Setup)



3.3 Payload Configuration

Usernames:

admin

bee

test

user

Passwords:

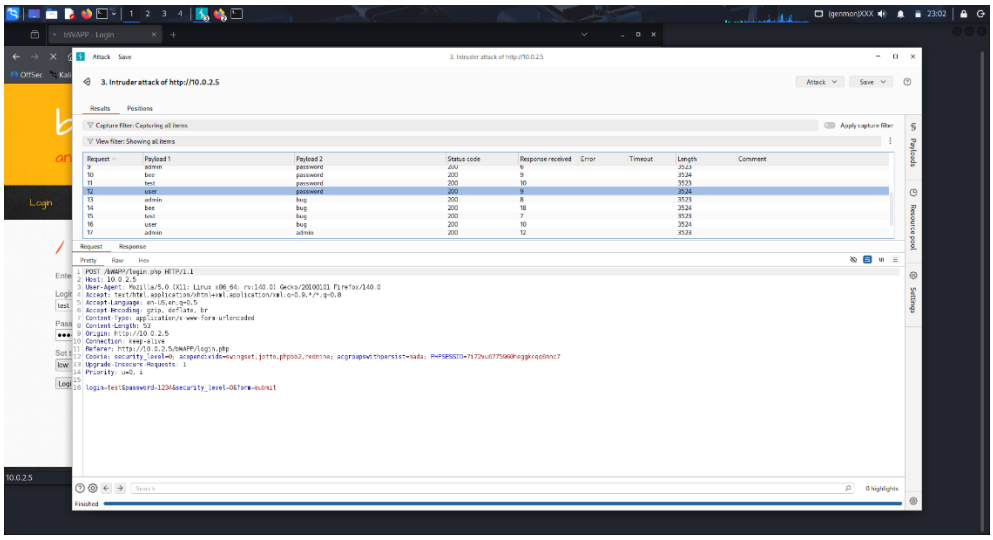
1234

password

admin

bug

Figure 4: Burp Intruder Attack Results (Response Length Analysis)



3.4 Results and Analysis

All requests returned HTTP status code 200, which is common for login forms. Therefore, response length was used to detect successful logins.
Most failed attempts had a response length of 3523, while a different response length (3524) indicated a successful login.

Valid credentials identified:

- Username: bee
- Password: bug

This confirms that response analysis is an effective technique in brute-force testing.

3.5 Conclusion of Lab 1

The Burp Suite Cluster Bomb attack successfully demonstrated how weak authentication systems can be brute-forced manually. The valid credentials were discovered by analyzing response length differences, indicating the application lacks proper brute-force protection.

💉 Lab 2: Hydra Web Form Brute-force (bWAPP Login)

4.1 Objective

To automate brute-force attacks on the bWAPP login form using Hydra and discover valid credentials by analyzing server responses.

4.2 Identifying Form Parameters

Using Burp Suite interception, the login POST request parameters were identified as:

login=USERNAME

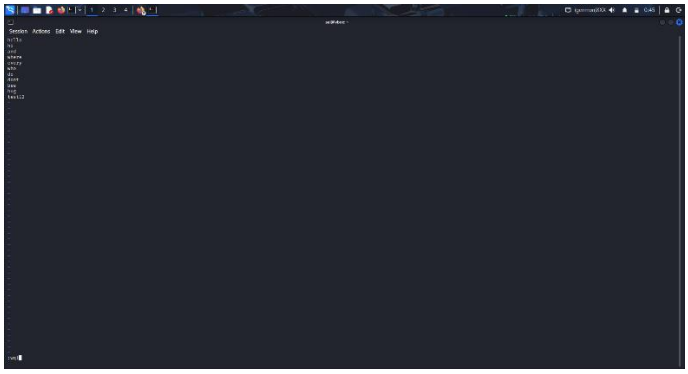
password=PASSWORD

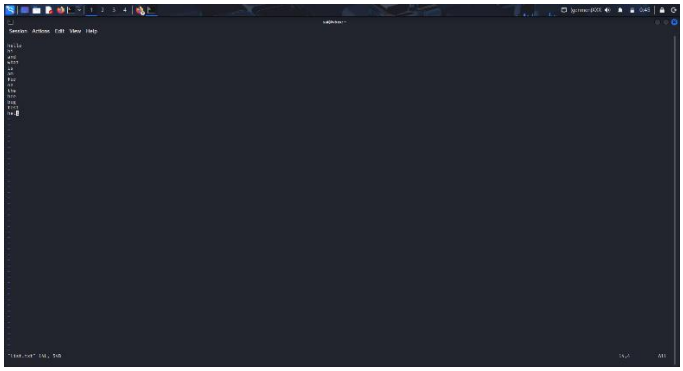
form=submit

Failure Message Observed:

Invalid credentials or user not activated

📸 **Figure 5: Username and Password Wordlists (list.txt & pass.txt)**





4.3 Hydra Command Used

hydra 10.0.2.5 http-post-form "/bWAPP/login.php:login=^USER^&password=^PASS^&form=submit:Invalid credentials or user not activated" -L list.txt -P pass.txt

Explanation:

- http-post-form → Web login brute-force module
- login & password → Form field names
- form=submit → Hidden form parameter
- Failure string used to detect incorrect logins

📸 Figure 6: Hydra Command Execution in Kali Linux

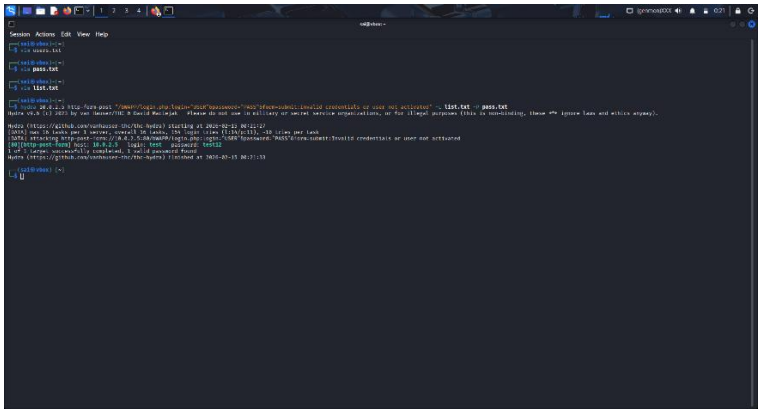
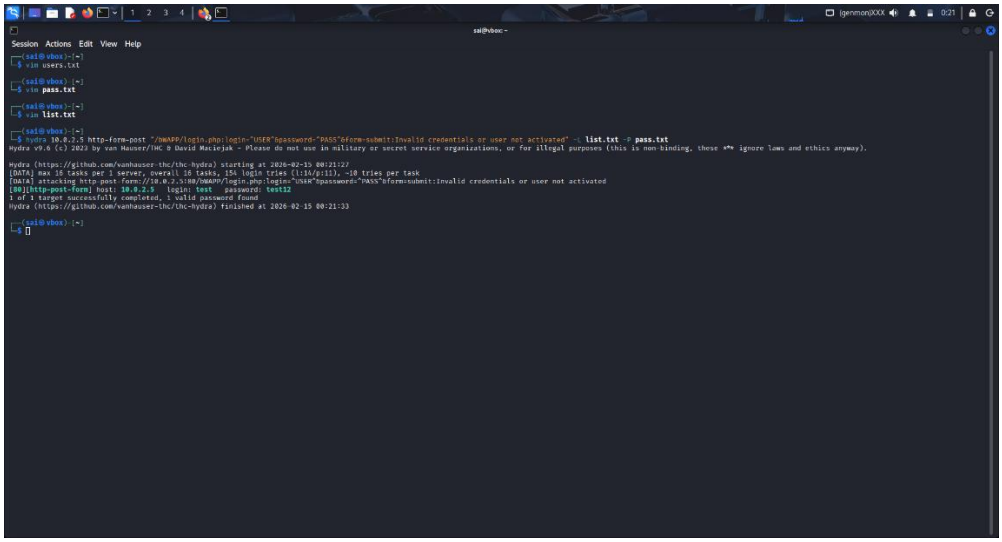


Figure 7: Hydra Successful Output (Valid Credentials Found)



4.4 Results

Hydra successfully performed the automated brute-force attack and discovered valid credentials:

- Username: test
- Password: test12

This confirms that the login system is vulnerable to automated brute-force attacks due to lack of account lockout and rate limiting.

---

5. Successful Credentials (Lab Purpose Only)

- Lab 1 (Burp Intruder): bee : bug
- Lab 2 (Hydra): test : test12

---

6. Mitigation Checklist (Prevention of Brute-force Attacks)

To protect web applications from brute-force attacks, the following security measures should be implemented:

- Account lockout after multiple failed attempts
- CAPTCHA on login forms
- Strong password policies
- Multi-Factor Authentication (MFA)
- Rate limiting on login requests

- Monitoring and logging failed login attempts
- Web Application Firewall (WAF)
- Removal of default and weak credentials

---

7. Final Conclusion

This project successfully demonstrated brute-force attacks on a vulnerable web application using both manual (Burp Suite Intruder) and automated (Hydra) techniques. The experiments proved that weak authentication mechanisms can be easily exploited to obtain valid credentials. The results highlight the importance of implementing strong authentication controls, rate limiting, and security best practices to prevent unauthorized access and enhance overall web application security.