



Brute Force & Authentication Attacks (Hydra)

WEEK 5: TASK 15

Submitted by: Aasima Noureen

Student ID: TBS-INT-2026-030

Company Name: TECH BIZ SECURITY

Date of Submission: 04-08-2026

Table of Contents

1. Executive Summary
2. Objective
3. Scope
4. Testing Environment
5. Methodology
6. Attack Execution
7. Results and Findings
8. Risk Assessment
9. Mitigation Recommendations
10. Conclusion
11. References

1. Executive Summary

A password brute-force assessment was performed against the DVWA login interface using Hydra from a Kali Linux attack machine. The objective was to determine whether weak credentials and the absence of brute-force protection could allow unauthorized access.

The attack successfully demonstrated that automated password guessing can compromise user accounts when strong authentication controls are not implemented.

2. Objective

The objectives of this assessment were:

- Identify whether the web login page is vulnerable to brute-force attacks.
- Evaluate the effectiveness of the authentication mechanism.
- Demonstrate automated password attacks using Hydra.
- Recommend security controls to prevent password attacks.

3. Scope

Target Application	DVWA
Target IP	127.0.0.1
Operating System	Kali Linux
Attack Tool	Hydra
Item	Description
Attack Type	HTTP GET Form Brute Force

4. Testing Environment

Component	Details
Attacker Machine	Kali Linux
Target Machine	DVWA
Authentication Method	HTTP GET Login Form
Password Wordlist	rockyou.txt
Username Tested	admin

5. Methodology

The assessment followed these phases:

1. Reconnaissance

The login page was identified, and the authentication parameters were inspected using the browser.

2. Form Analysis

The login request contained:

- Username parameter
- Password parameter

The application returned the message:

"Username and/or password is incorrect"

This failure message was used by Hydra to distinguish unsuccessful login attempts.

3. Password Attack

Hydra was configured to automate login attempts using the **admin** username and the **rockyou.txt** password dictionary.

6. Attack Execution

Command Used

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 127.0.0.1 http-get-form  
"/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&login=lo  
gin:H=cookie:PHPSESSID=0dd96716586a9971e298a66ef7c0da29;security=low:F  
=username and/or password incorrect" -t 30
```

Command Breakdown

Option	Purpose
-l admin	Specifies the username
-P rockyou.txt	Uses the RockYou password dictionary
127.0.0.1	Target IP address

http-post-form	Performs brute force against an HTTP POST form
user=^USER^	Username field placeholder
password=^PASS^	Password field placeholder
F=	Failure string returned after unsuccessful login

Hydra automatically replaces the placeholders with every username and password combination until valid credentials are discovered or the wordlist is exhausted.

```

root@10:~/home/kali
# hydra -l admin -P /usr/share/wordlists/rockyou.txt 127.0.0.1 http-get-form "/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=cookie:PHPSESSID=0dd96716586a9971e298a6b0f7c0da29; security=low:F=Username and/or password incorrect." -t 30
Hydra v9.7 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-08-04 22:08:23
[DATA] max 30 tasks per 1 server, overall 30 tasks, 14344299 login tries (l:1/p:14344399), ~478147 tries per task
[DATA] attacking http-get-form://127.0.0.1:80/DVWA/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=cookie:PHPSESSID=0dd96716586a9971e298a6b0f7c0da29; security=low:F=Username and/or password incorrect.
[80][http-get-form] host: 127.0.0.1 login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-08-04 22:08:27

root@10:~/home/kali

```

7. Results and Findings

Observation

Hydra was able to automate thousands of login attempts against the authentication portal.

If the correct password exists in the supplied wordlist, Hydra reports valid credentials and demonstrates successful authentication.



The screenshot displays the DVWA web application interface. At the top, there is a dark header with the DVWA logo and a small icon in the top right corner. Below the header, the page is divided into three main sections. On the left is a sidebar with a list of vulnerability categories: Home, Instructions, Setup / Reset DB, Brute Force (highlighted in green), Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, and JavaScript Attacks. The main content area is titled 'Vulnerability: Brute Force' and contains a 'Login' form. The form has two input fields for 'Username:' and 'Password:', a 'Login' button, and a message that says 'Welcome to the password protected area admin' accompanied by a small image of a person with a surprised expression. Below the login form, there is a 'More Information' section with two links: https://owasp.org/www-community/attacks/Brute_force_attack and <https://www.golinuxcloud.com/brute-force-attack-web-forms>.

Vulnerability Identified

Weak Password / Brute Force Authentication

Description

The application allows repeated login attempts without implementing adequate protection mechanisms such as account lockout, CAPTCHA, or rate limiting. This

enables attackers to automate password guessing attacks and potentially gain unauthorized access.

Impact

- Unauthorized account access
- Credential compromise
- Privilege escalation
- Data disclosure
- Increased risk of account takeover

8. Risk Assessment

Metric	Rating
Vulnerability	Weak Authentication / Brute Force
Severity	High
Likelihood	High
Impact	High
CVSS (Approximate)	8.1 (High)

Severity Chart

Risk Level	Description
 Low	Minimal impact
 Medium	Limited security impact
 High	Authentication can be bypassed through brute force
 Critical	Complete compromise of sensitive systems

Assessment:  High

10. Mitigation Recommendations

Recommendation	Description
Strong Password Policy	Enforce complex passwords with minimum length requirements.
Account Lockout	Temporarily lock accounts after multiple failed login attempts.
Rate Limiting	Restrict the number of login requests within a defined time period.
CAPTCHA	Require CAPTCHA after several failed login attempts.
Multi-Factor Authentication	Add a second authentication factor for user accounts.
Login Monitoring	Log and alert on repeated failed authentication attempts.
Password Hashing	Store passwords securely using modern hashing algorithms such as Argon2, bcrypt, or PBKDF2.

11. Conclusion

The brute-force assessment demonstrated that automated password attacks can effectively target weak authentication mechanisms in a controlled DVWA lab environment. Hydra rapidly tested credentials from a password dictionary, highlighting the importance of strong passwords and defensive controls.

Organizations should implement layered protections—including rate limiting, account lockout, CAPTCHA, and multi-factor authentication—to reduce the risk of successful brute-force attacks and protect user accounts from unauthorized access.

12. References

1. The Open Web Application Security Project. *OWASP Web Security Testing Guide (WSTG)*.
2. The Open Web Application Security Project. *OWASP Top 10 – Identification and Authentication Failures*.
3. THC. *Hydra Documentation*.
4. Offensive Security. *Kali Linux Tools Documentation*.
5. Damn Vulnerable Web Application. *DVWA Documentation*.
6. TRYHACKME: <https://tryhackme.com/room/hydra>
7. TRYHACKME: <https://tryhackme.com/room/bruteit>

TRYHACKME:

HYDRA:

The screenshot shows the TryHackMe interface for the 'Hydra' room. The top navigation bar includes 'Dashboard', 'Learn', 'Practice', 'Compete', and 'HH 2026'. The room title 'Hydra' is prominently displayed with a green dragon icon. Below the title, a description states: 'Learn about and use Hydra, a fast network logon cracker, to bruteforce and obtain a website's credentials.' The room statistics show a duration of 45 minutes and 264,554 participants. A row of buttons includes 'Share your achievement', 'Start AttackBox', 'Save Room', '5367 Recommend', 'Connectivity', and 'Options'. A green progress bar at the bottom indicates 'Room completed: 100%'. The 'Video' tab is selected in the bottom navigation bar.

BRUTE IN:

The screenshot shows the TryHackMe interface for the 'Brute It' room. The top navigation bar is consistent with the previous screenshot. The room title 'Brute It' is displayed with a red and blue pixelated icon. The description reads: 'Learn how to brute, hash cracking and escalate privileges in this box!'. The room statistics show a duration of 45 minutes and 48,966 participants. The row of buttons includes 'Share your achievement', 'Start AttackBox', 'Save Room', '1689 Recommend', 'Connectivity', and 'Options'. A green progress bar at the bottom indicates 'Room completed: 100%'. The bottom navigation bar shows 'Chart', 'Scoreboard', and 'Write-ups' tabs, with 'Chart' being the active tab.