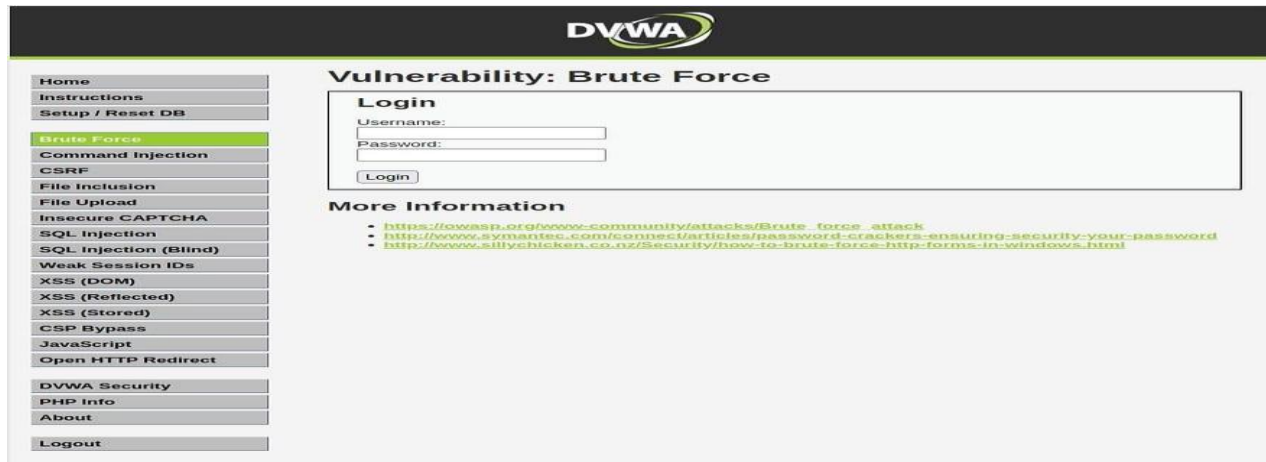


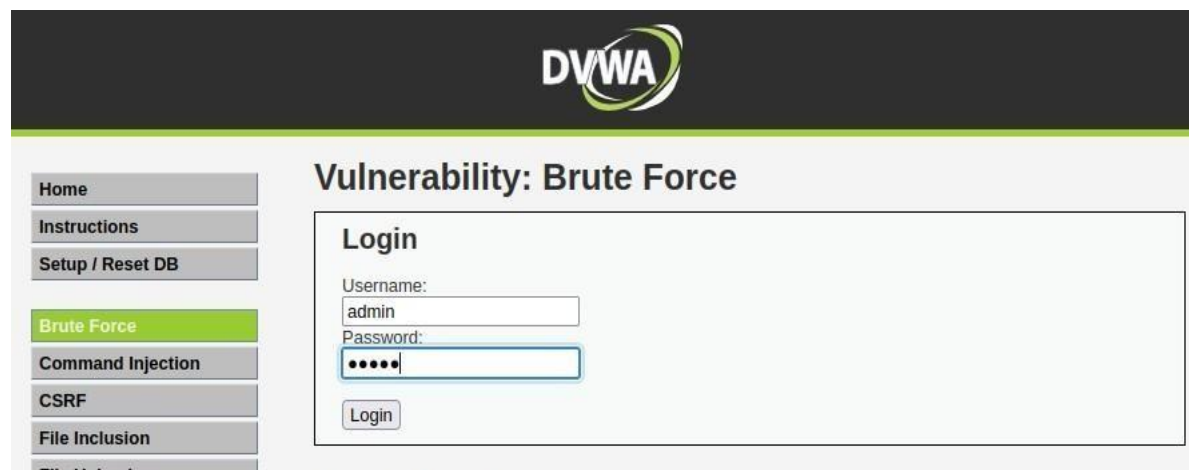
## Experiment-10(Brute Force and Dictionary Attacks-Cyber Security Workshop)

Inside DVWA, select the Brute Force option, which takes user to a Login page.

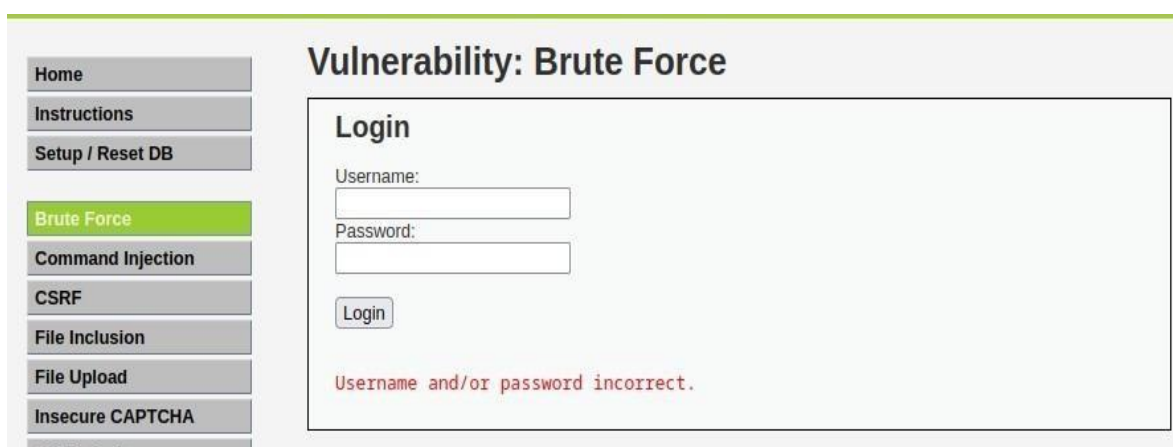


The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The left sidebar contains a menu with options: Home, Instructions, Setup / Reset DB, Brute Force (highlighted), Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, Open HTTP Redirect, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: Brute Force" and features a "Login" form with fields for "Username:" and "Password:", and a "Login" button. Below the form, there is a "More Information" section with three links: [https://owasp.org/www-community/attacks/Brute\\_force\\_attack](https://owasp.org/www-community/attacks/Brute_force_attack), <http://www.symantec.com/connect/articles/password-cracker-ensuring-security-your-password>, and <http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>.

Enter admin for the username and admin for the password, which is the wrong username and password.

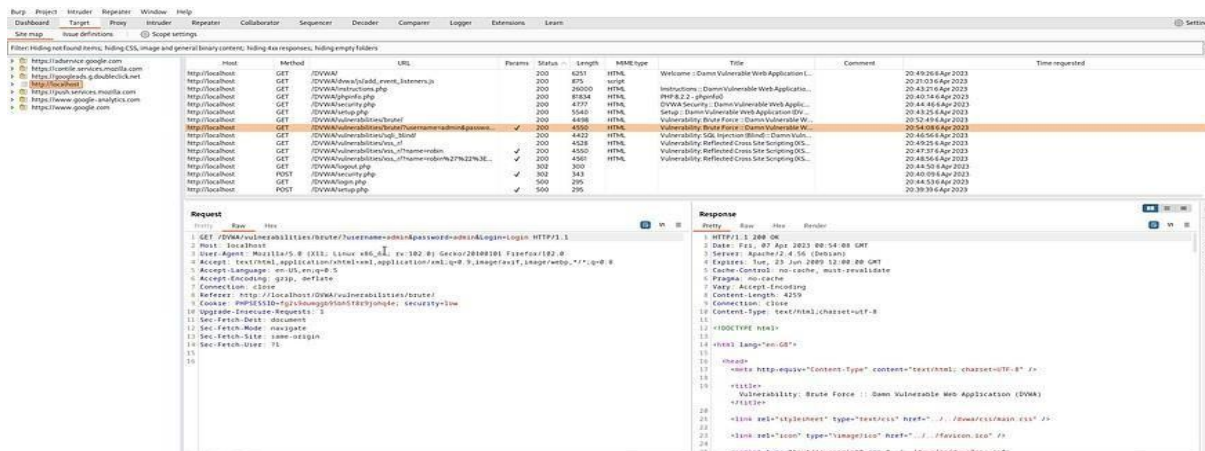


This screenshot shows the DVWA interface after an incorrect login attempt. The "Username:" field contains the text "admin" and the "Password:" field contains five dots. The "Login" button is visible. The left sidebar menu is the same as in the previous screenshot, with "Brute Force" highlighted.

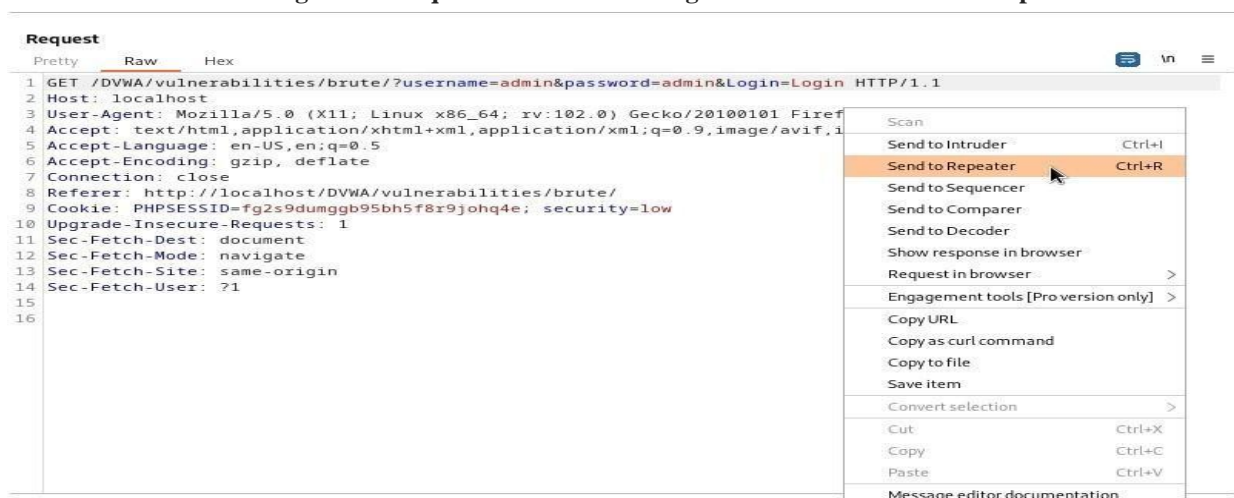


This screenshot shows the DVWA interface after the login attempt. The "Username:" and "Password:" fields are empty. Below the "Login" button, a red error message reads: "Username and/or password incorrect." The left sidebar menu is the same as in the previous screenshots, with "Brute Force" highlighted.

In the Burp Suite tool, follow the path: Target → Site map → http://localhost → URL Containing the following: /DVWA/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.1



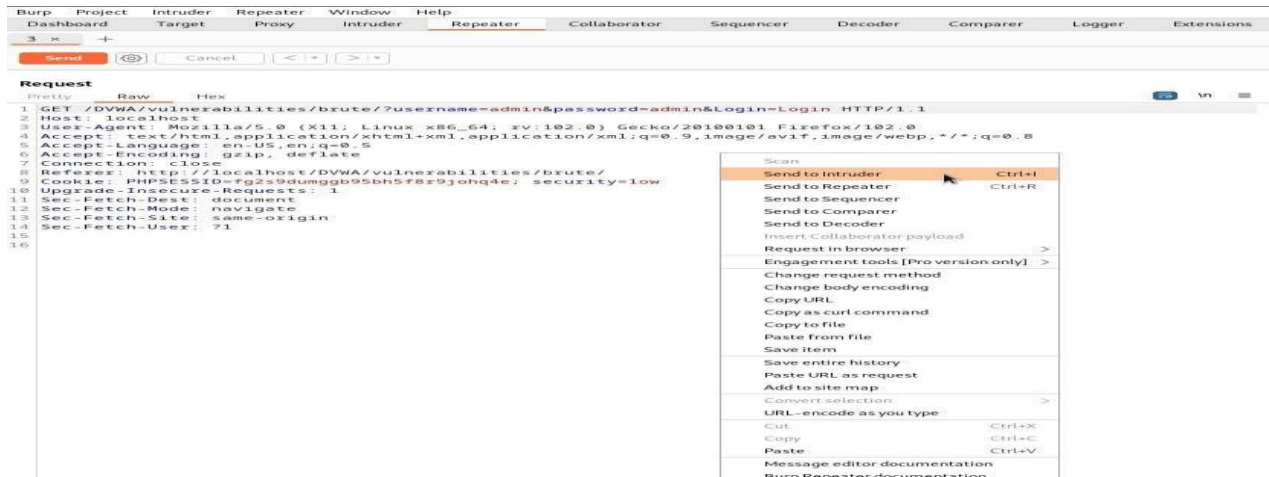
Navigated to Request → Raw tab → Right-click inside → Send to Repeater.



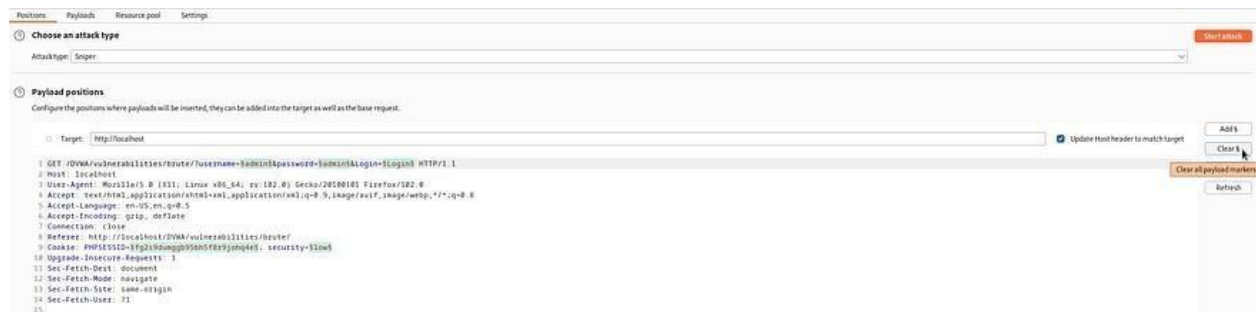
Select the Repeater tab.



Right-click inside the Raw data area → Send to Intruder.



Choose an attack type, Add or Clear payload markers, and Start attack.



All payload markers cleared.



Highlighted admin after username → Selected Add.





**2 Payload sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:  Payload count: 17  
 Payload type:  Request count: 0

---

**2 Payload settings [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

user

administrator

oracle

ftp

pi

puppet

ansible

ec2-user

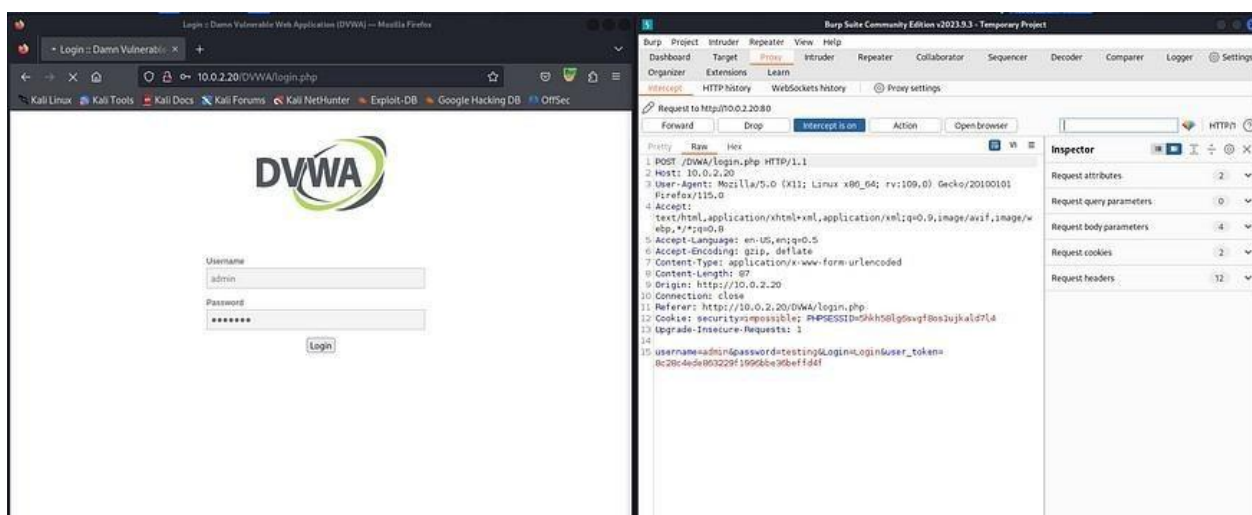
vagrant

azureuser

admin

Add the specified item

## Burp Proxy



## Burp Intruder

