Vulnerability Name:	Brute Force Attack
Affected Vendor:	DVWA
Affected Product Name:	http://dvwa/vulnerabilities/brute/
Product Official Website URL	http://dvwa/
Affected Components:	Affected parameters: - login page username, password

Description: - A cyberattack method that involves systematically trying all possible combinations of passwords or keys until the correct one is found.

Root Cause: - Weak password policies, lack of account lockout mechanisms, or inadequate protection against automated login attempts.

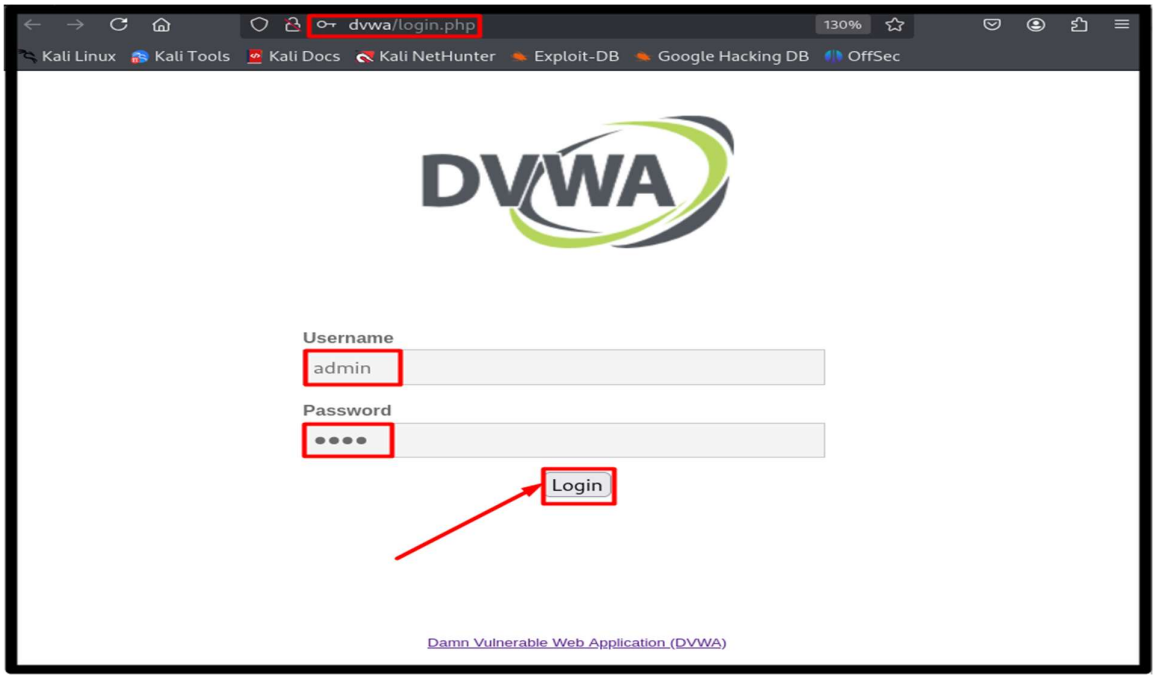
Impact: - Account compromise, data theft, unauthorized access, or denial of service.

Mitigation: - Implement account lockout mechanisms, enforce strong password policies, use multi factor authentication, and monitor for suspicious login attempts to mitigate Brute Force Attacks.

Remediation: - To remediate a brute force attack, implement an Account Lockout Policy to lock accounts after multiple failed login attempts, use CAPTCHA & Rate Limiting to slow down repeated login attempts, and enforce Multi-Factor Authentication (MFA) for an additional verification step. Strengthen security with Strong Password Policies requiring complex passwords and periodic changes, while Monitoring & Logging help detect and block suspicious login attempts. Deploy IP Blocking & Web Application Firewall (WAF) to block malicious IPs and use Credential Stuffing Protection tools to prevent the use of breached passwords.

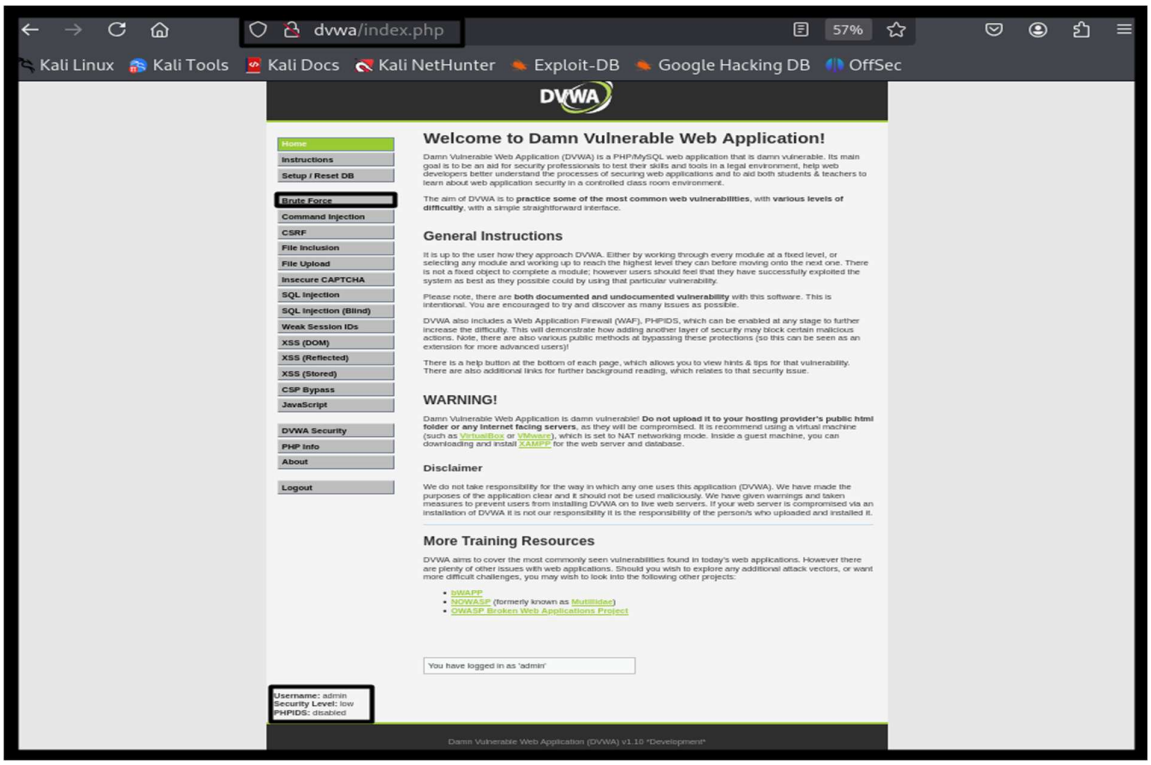
Proof of Concept

Step: -1 First navigate to http://dvwa/login.php and login with username and Password.

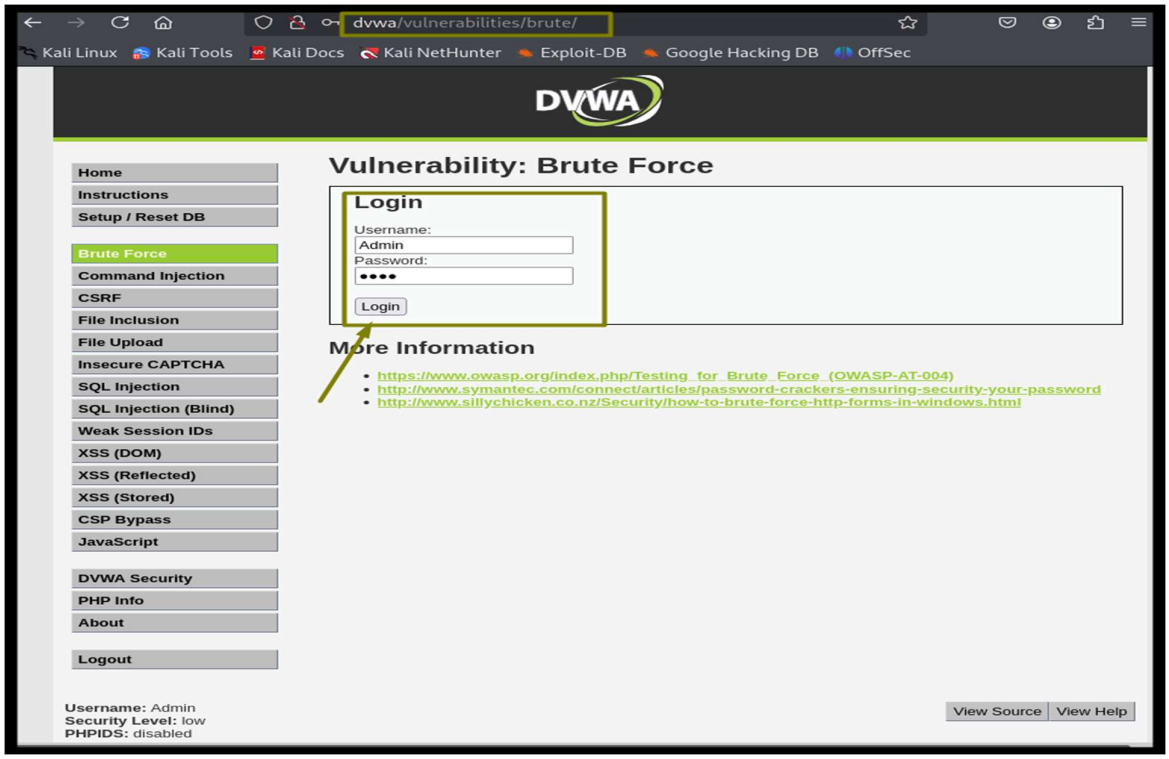


Step: -2 log in the home page of DVWA then click to the brute force section.

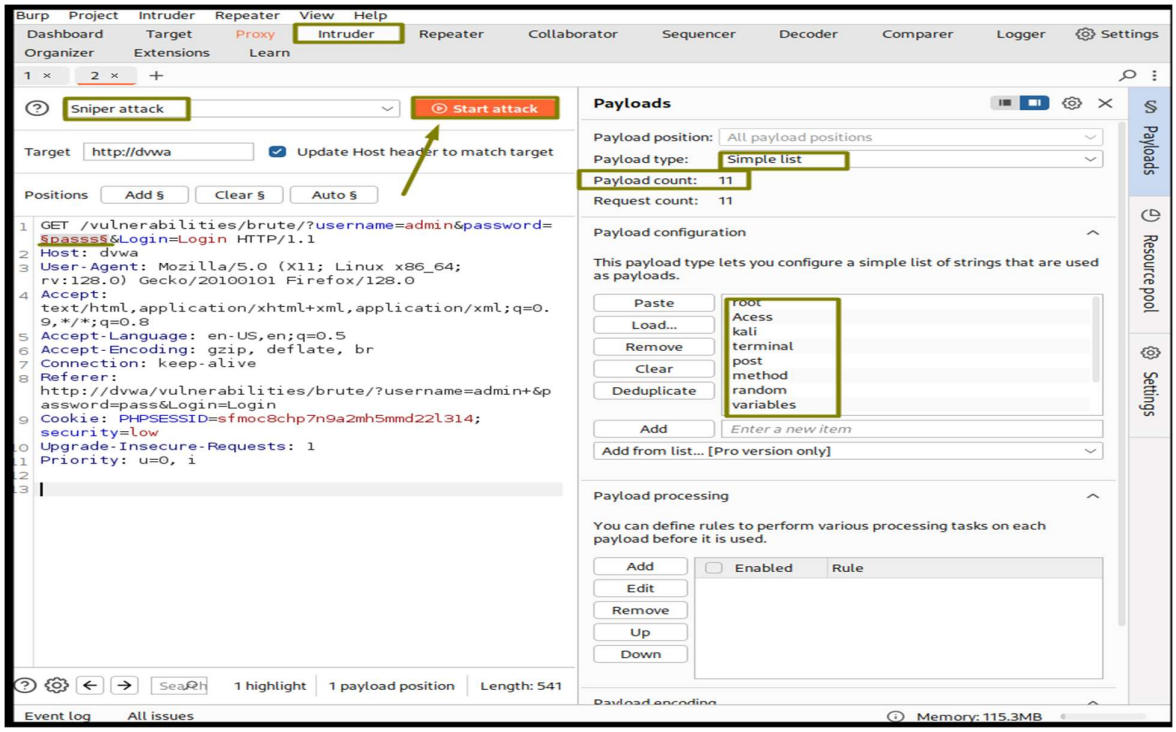
SECURITY LEVEL: - LOW (all level is same process)



Step:-3 In this step, start a penetration testing tool, open Burp Suite, and accept the website request within Burp Suite and request send to intruder.



Step:-4 In this step, set the payload positions, configure the payloads, and then click "Start Attack."



Step:-5 In this step, analyze all response times and lengths, review the responses, verify the response codes, and then click "Render."