

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.

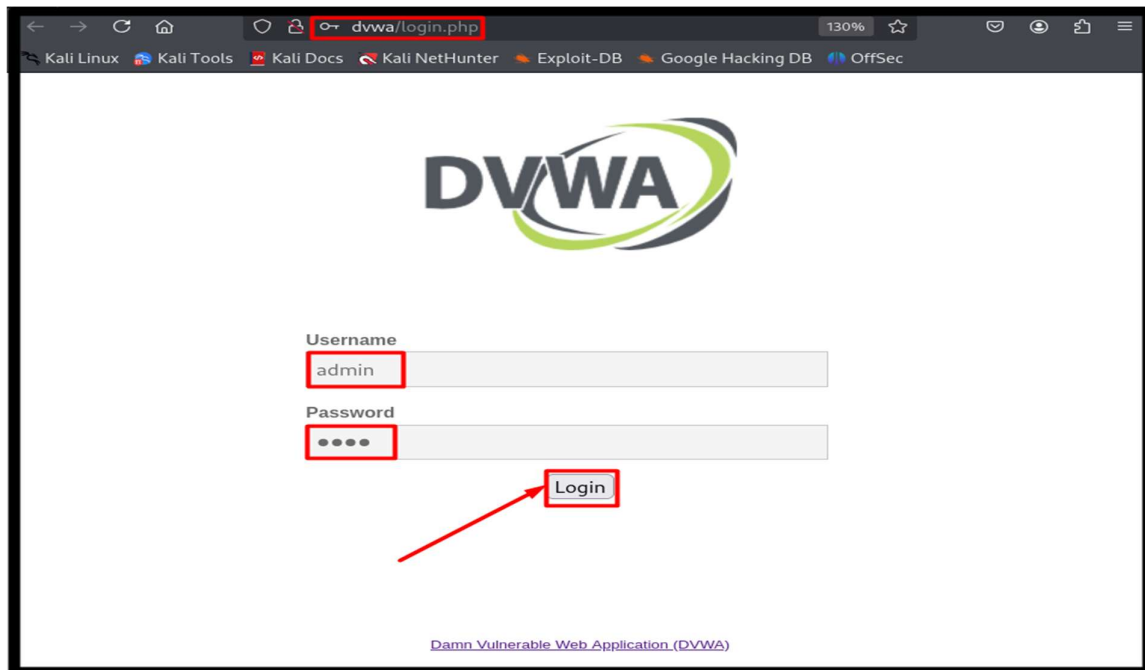
Impact: - Account compromise, data theft, unauthorized access, or denial of service.

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.

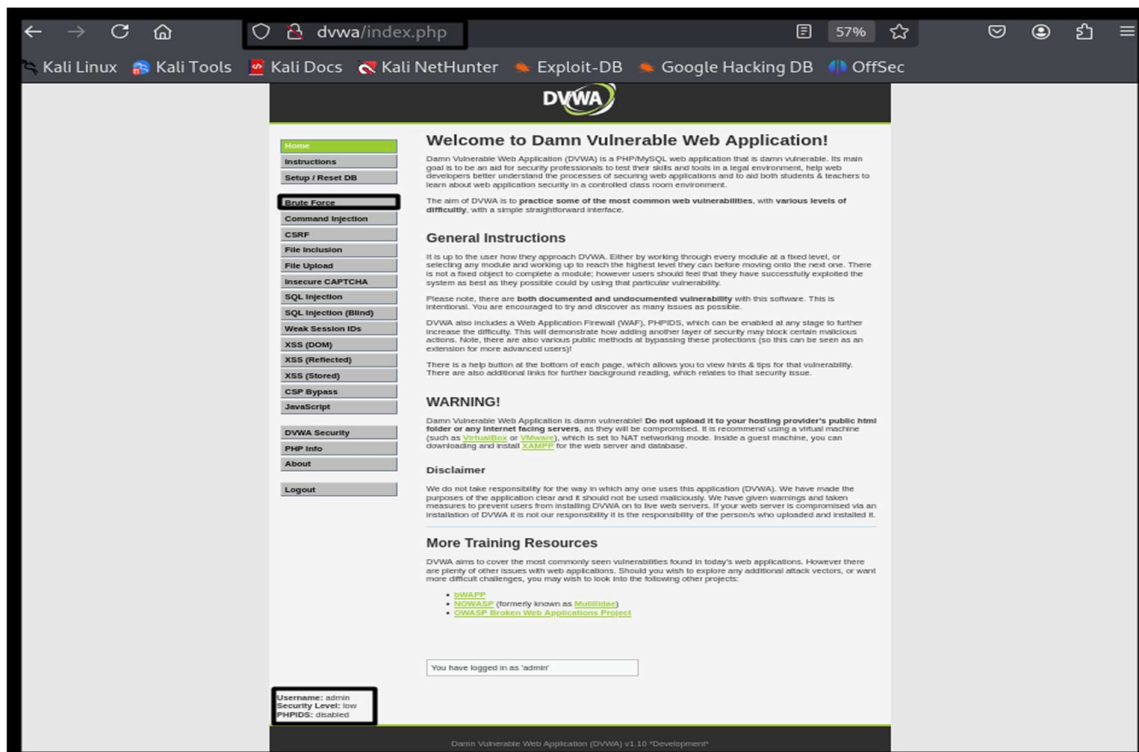
Proof of Concept

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

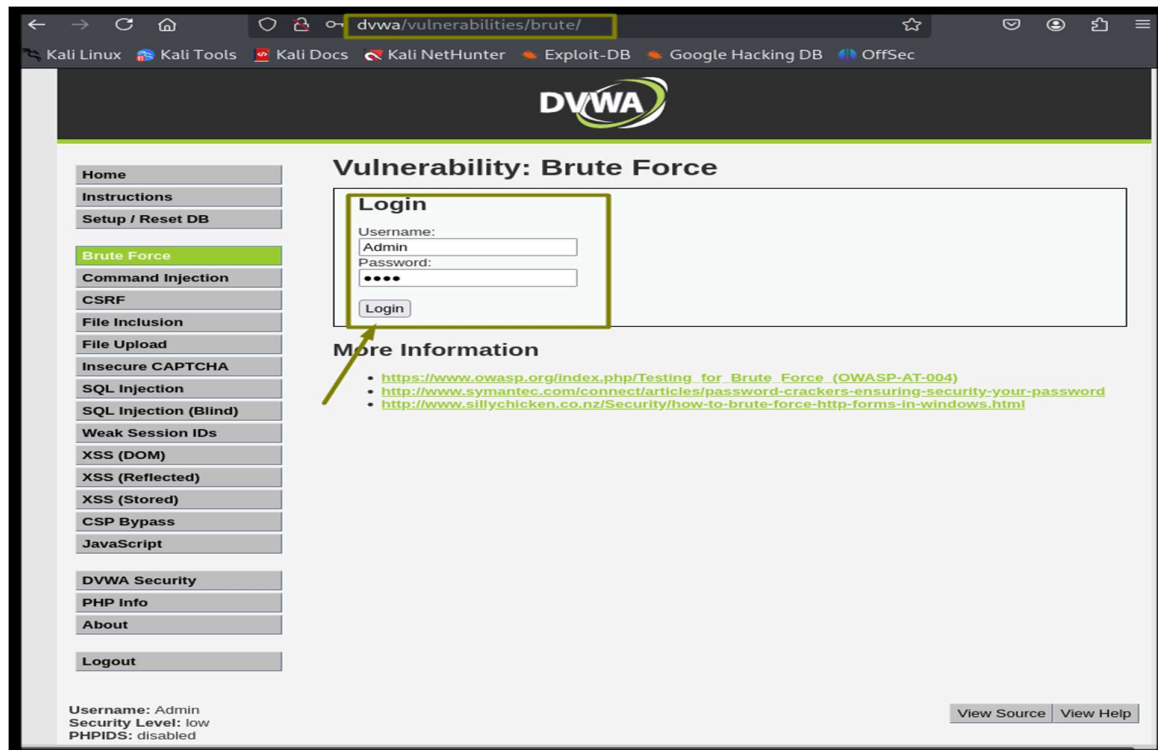


Step: -2 log in the home page of DVWA then click to the brute force section.

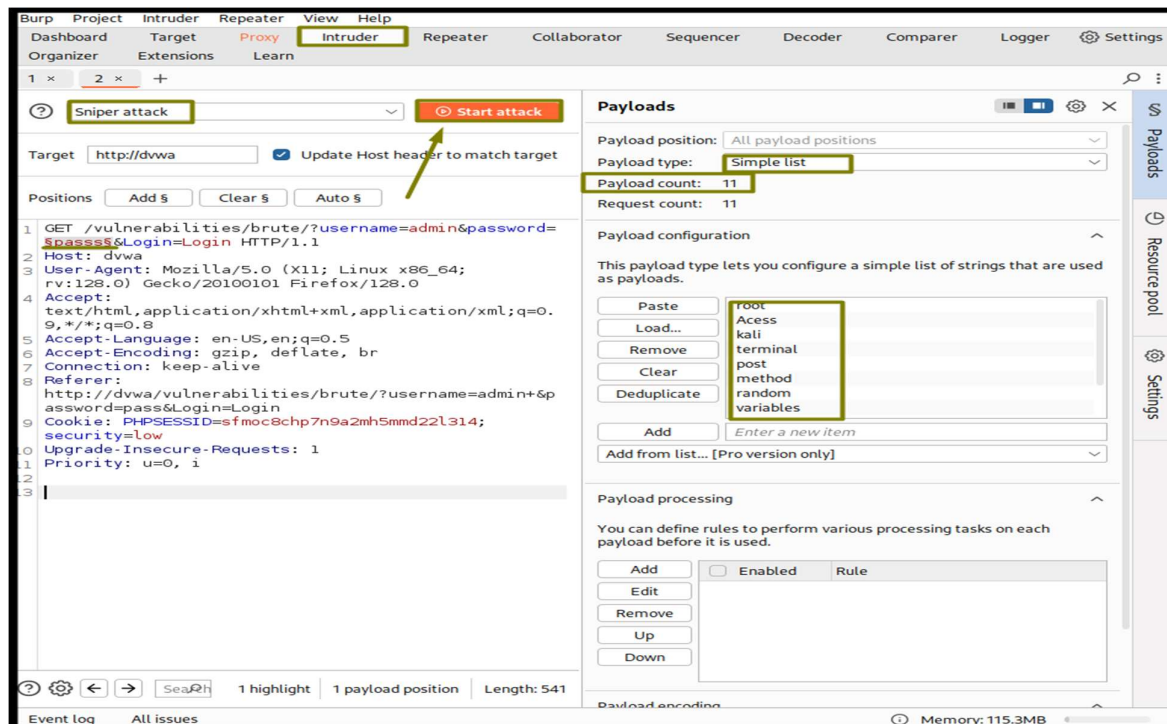
SECURITY LEVEL: - LOW (all level is same process)



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."

Attack Save

2. Intruder attack of http://dvwa

Attack Save

Results Positions

Capture filter: Capturing all items Apply capture filter

View filter: Showing all items

Request	Payload	Status code	Response...	Error	Timeout	Length	Comment
9	test	200	14			4740	
3	kali	200	8			4702	
0		200	6			4703	
2	Acess	200	5			4703	
4	terminal	200	5			4703	
8	variables	200	5			4703	
10	password	200	5			4703	
1	root	200	4			4702	
5	root	200	4			4702	

Request Response

Pretty Raw Hex **Render**

DVWA

Vulnerability: Brute Force

Login

Username:

Password:

Login

Welcome to the password protected area admin

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

Finished

Attack Save

2. Intruder attack of http://dvwa

Attack Save

Results Positions

Capture filter: Capturing all items Apply capture filter

View filter: Showing all items

Request	Payload	Status code	Response...	Error	Timeout	Length	Comment
9	test	200	14			4740	
3	kali	200	8			4702	
0		200	6			4703	
2	Acess	200	5			4703	
4	terminal	200	5			4703	
8	variables	200	5			4703	
10	password	200	5			4703	
1	root	200	4			4702	
5	root	200	4			4702	

Request Response

Pretty Raw Hex **Render**

```
1 HTTP/1.1 200 OK
2 Date: Fri, 28 Feb 2025 06:37:24 GMT
3 Server: Apache/2.4.25 (Debian)
4 Expires: Tue, 23 Jun 2009 12:00:00 GMT
5 Cache-Control: no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 4413
9 Keep-Alive: timeout=5, max=99
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=utf-8
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
14 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
15
16 <html xmlns="http://www.w3.org/1999/xhtml">
17
18 <head>
19 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
20
21 <title>
22 Vulnerability: Brute Force :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*
```

Finished

