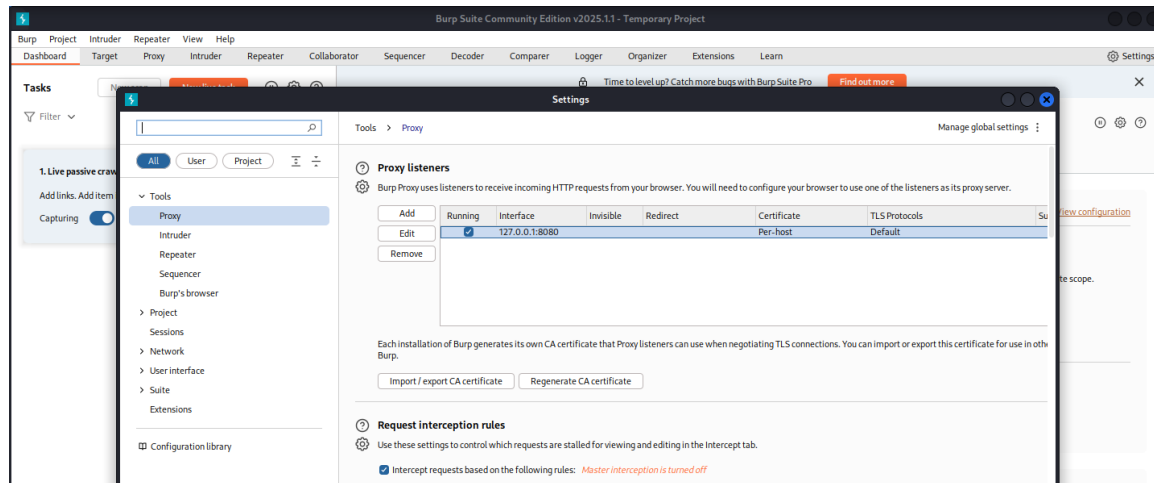


DVWA-Low-Level Brute Force Attack

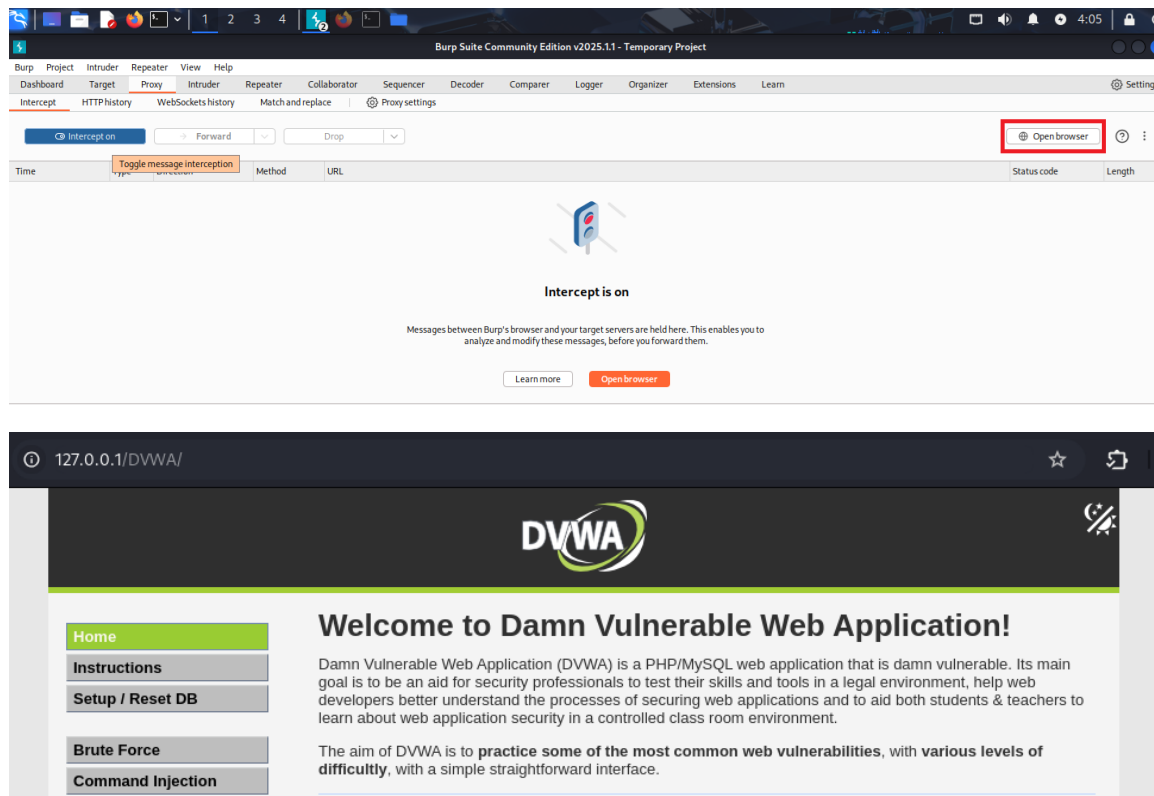
--MagicDragonB

Using the tool called Burp Suite, which has already been installed in Kali Linux 2025.



Once you open this tool, make sure that the proxy listener protocol is running.



Then click Proxy Option → open browser and log in to the DVWA.



Once logged into the DVWA, select the ‘DVWA Security’ option and choose ‘low,’ then submit.



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

JavaScript

Authorisation Bypass

Open HTTP Redirect

Cryptography

API

DVWA Security

PHP Info

About

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

More Training Resources

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

JavaScript

Authorisation Bypass

DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Impossible ▾

Submit

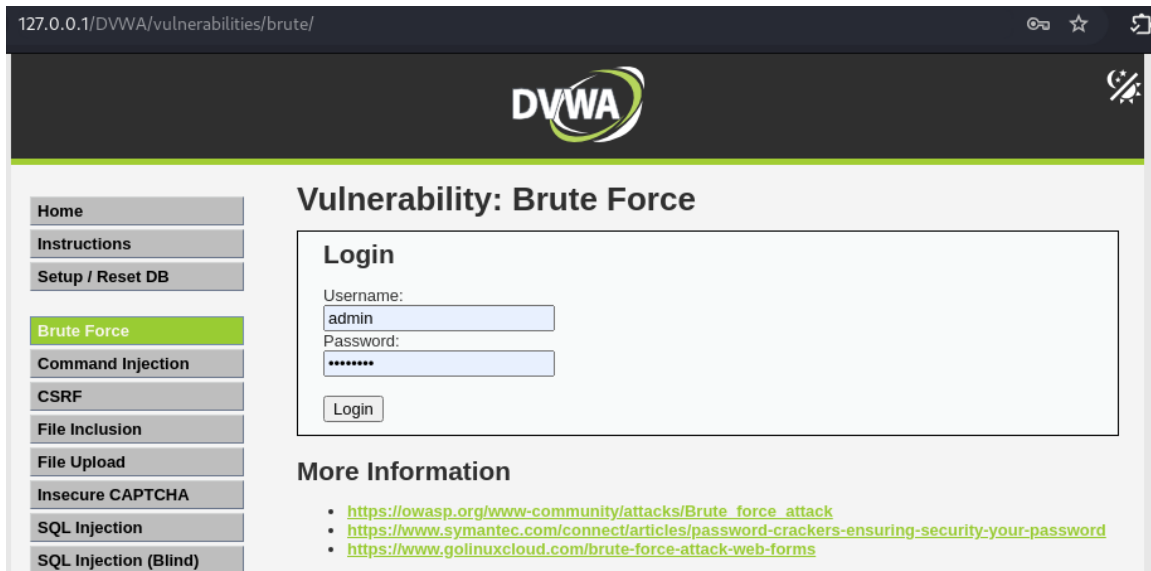
Low

Medium

High

Impossible

Then click Brute Force session, then can start the low-level brute force challenge.



127.0.0.1/DVWA/vulnerabilities/brute/

DVWA

Vulnerability: Brute Force

Login

Username:
admin

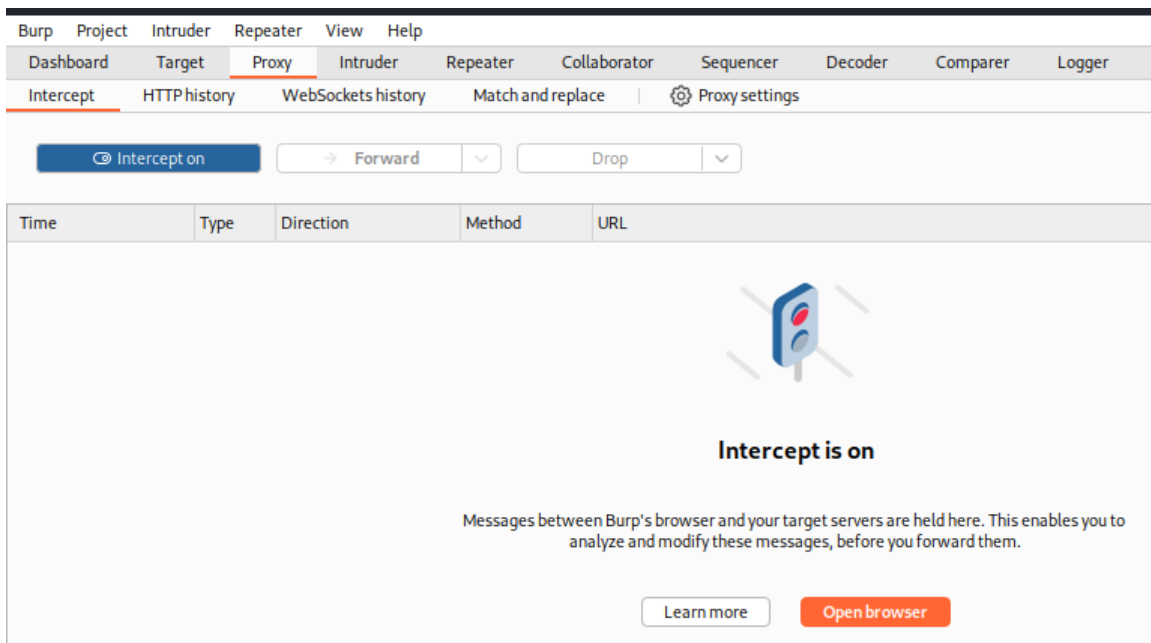
Password:

Login

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>

Turn on the 'intercept' button.

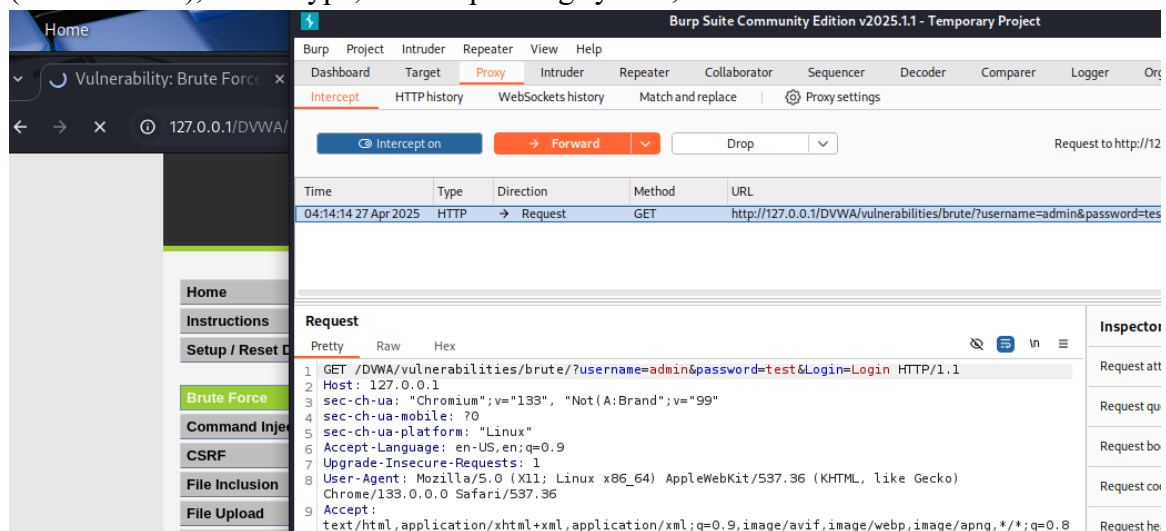


Intercept is on

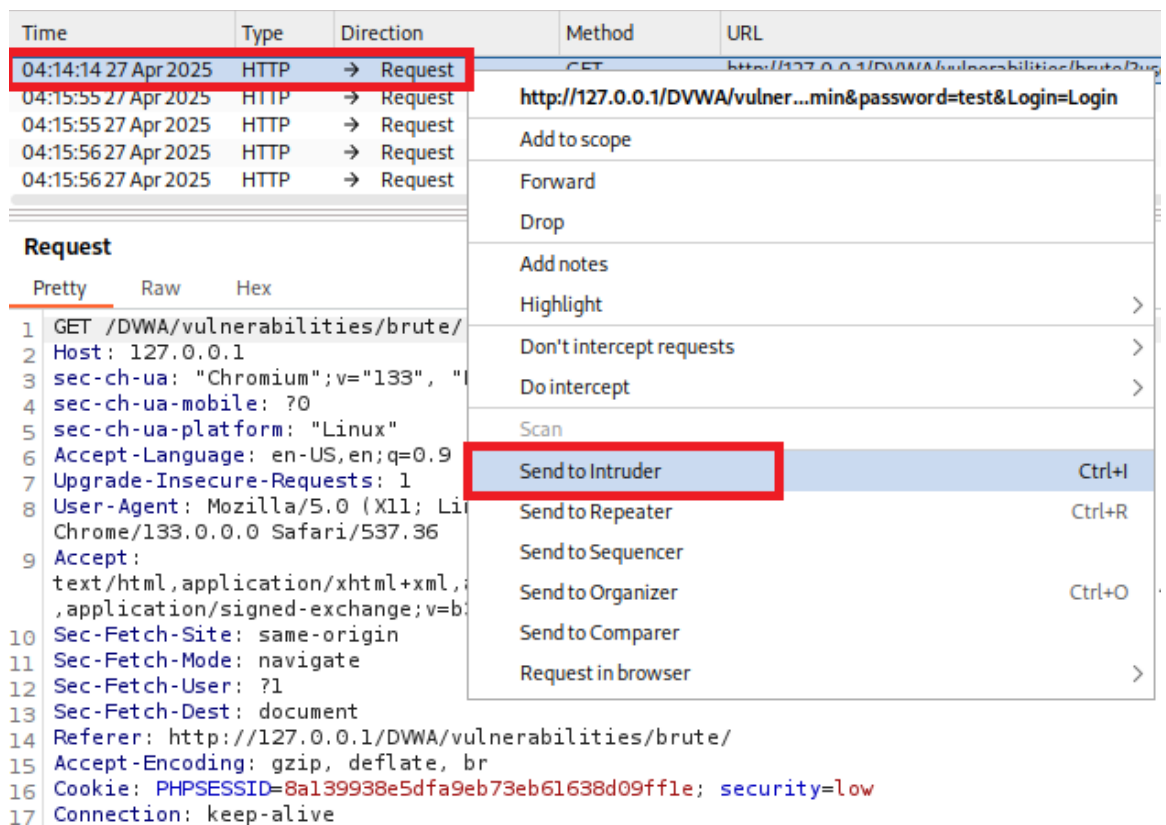
Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

Learn more Open browser

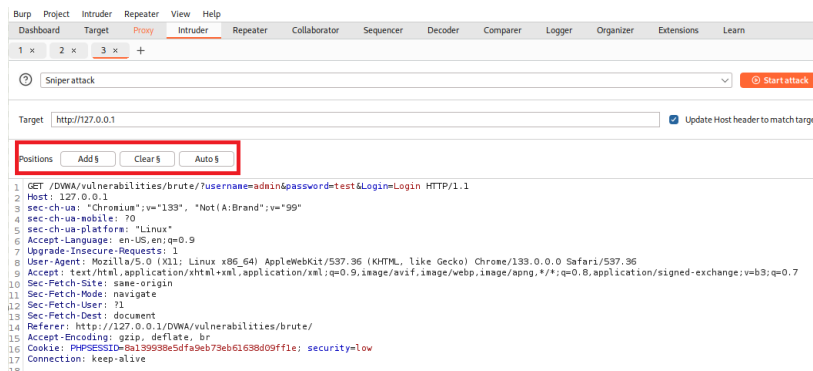
At the password section, enter an incorrect password, such as 'test.' (We know the correct password is 'password.') Then we can capture the message, including the website method (GET method), HTTP type, user's operating system, and more.



Right click on it and click send to intruder



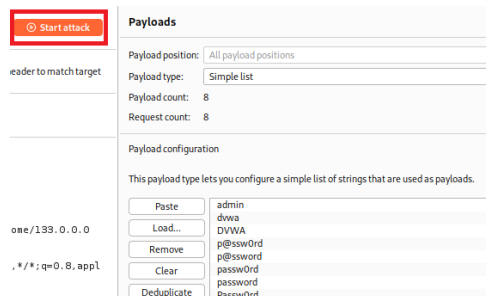
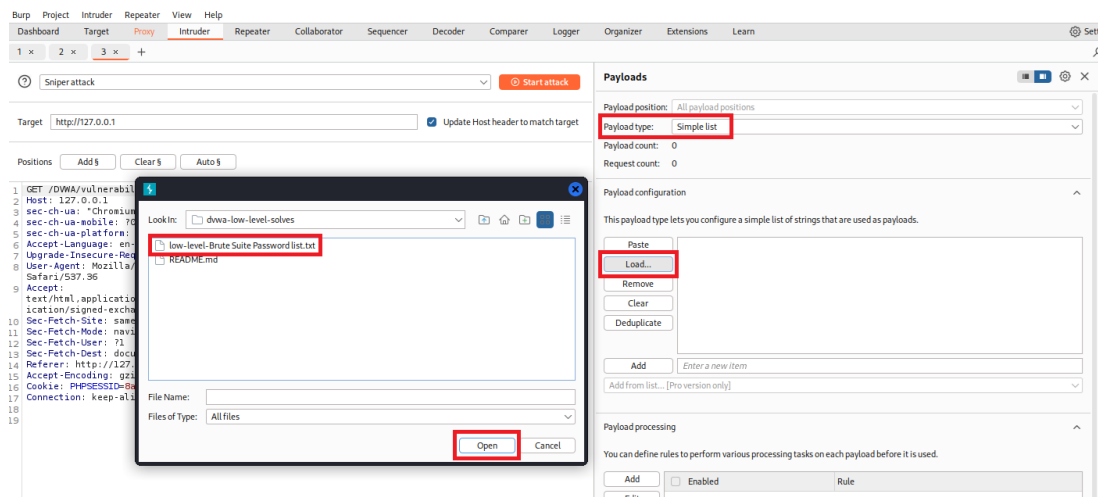
In this page have three options, this option means you can add, clear the attack part. In this session we are focused on the part of password, so we should choose the 'password' and click 'add'



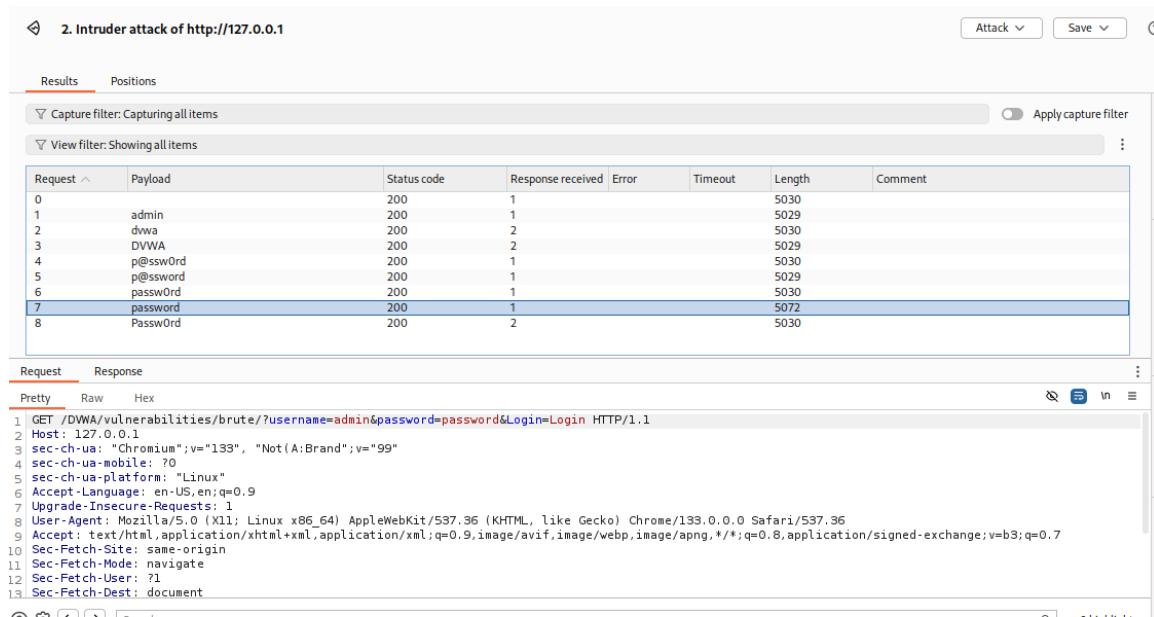
Positions Add \$ Clear \$ Auto \$

1 GET /DWA/vulnerabilities/brute/?username=admin&password=Stest\$&Login=Login HTTP/1.1

The payload page will update after you click "Add." Load the "Low-level-Brute Force Password list" after selecting the "Simple list" Payload Type. Click "start attack" after that.



However, the outcome is difficult to tell which password is wrong and which is right. After that, we may select the Grep-Match option by clicking the settings button.



2. Intruder attack of http://127.0.0.1

Results Positions

Capture filter: Capturing all items Apply capture filter

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	1			5030	
1	admin	200	1			5029	
2	dwva	200	2			5030	
3	DVWA	200	2			5029	
4	p@ssw0rd	200	1			5030	
5	p@ssword	200	1			5029	
6	passw0rd	200	1			5030	
7	password	200	1			5072	
8	Passw0rd	200	2			5030	

Request Response

Pretty Raw Hex

```
1 GET /DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
2 Host: 127.0.0.1
3 sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
```

You will see that the screen will notify you that your 'username and/or password are incorrect' if you have attempted to log in previously with an invalid password.



DVWA

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA

Vulnerability: Brute Force

Login

Username:

Password:

Login

Username and/or password incorrect.

So, we add Username and/or password incorrect into the Grep-Match, after that, we click the attack button again.

Grep - Match

These settings can be used to flag result items containing specified expressions.

☒ Flag responses matching these expressions:

Paste Load... Remove Clear Add

Username and/or password incorrect

Resource pool Settings

Then we can clearly see that the 'password' row does not match, indicating that this is the correct password. We can view the details in the 'Response' option, select 'Render,' and then we can see the successful page.

Request	Payload	Status code	Response received	Error	Timeout	Length	Username and/or password incorrect	Comment
0		200	2			5030	1	
1	admin	200	1			5029	1	
2	dvwa	200	1			5030	1	
3	DVWA	200	1			5029	1	
4	pbshoword	200	2			5030	1	
5	pbshoword	200	1			5029	1	
6	password	200	1			5030	1	
7	password	200	1			5030	1	
8	Password	200	2			5030	1	

Request Response Raw Hex Render

Vulnerability: Brute Force

Home Instructions Setup / Reset DB Brute Force Command Injection CSRF File Inclusion File Upload Insecure CAPTCHA SQL Injection SQL Injection (Blind)

Login

Username: Password: Login

Welcome to the password protected area admin