CYBER SECURITY

PRACTICAL GUIDE

Name: Chandana Somanath Khatavakar

Project Title: brute force attack on an OWASP vulnerable machine using Burpsuite

1. Introduction

A brute-force attack is a method used to gain unauthorized access to an application by trying every possible combination of credentials until the correct one is found. This guide focuses on using Burp Suite to perform such an attack on an OWASP vulnerable machine. Burp Suite is a powerful web security testing tool, which is widely used by penetration testers.

2. Scope

The goal is to demonstrate how brute-force attacks work and to provide practical experience with Burp Suite. The tutorial assumes you're targeting an OWASP vulnerable machine, like OWASP Juice Shop or OWASP Broken Web Applications (BWA), which are designed for learning security testing.

3. Overview of a Brute Force Attack with Burp Suite

A brute-force attack using Burp Suite generally involves capturing and modifying HTTP requests to automate the submission of different username-password combinations. Burp Suite's Intruder tool is used for this, where you can define payloads (i.e., the list of potential passwords) and customize the attack.

4. Features of a Brute Force Attack Using Burp Suite

- Password Guessing: It uses a wordlist or dictionary to guess passwords for a given username.
- User Enumeration: Identifying valid usernames through response analysis.
- Custom Payloads: You can customize payloads to test various combinations of username and password.
- Automated Process: Burp Suite automates the attack, allowing for quick testing of multiple login combinations.

5. Benefits

- Learn Practical Attack Methods: Understand how attackers use brute force to crack login credentials.
- Security Awareness: Recognize the importance of securing login mechanisms to prevent unauthorized access.
- Hands-On Experience: Gain practical skills with Burp Suite, which is widely used in professional penetration testing.

6. Environment Setup

- Operating System: Kali Linux or any penetration testing OS with Burp Suite installed.
- Target Machine: OWASP Juice Shop, OWASP BWA, or another vulnerable machine running in a controlled environment (e.g., a virtual machine).
- Network Configuration: Both the attacking machine (Kali) and the vulnerable target should be on the same network or within an isolated test network.

Step-by-Step Procedure for Brute Force Attack Using Burp Suite

Step 1: Identify the Target

1.1. **Scan the Target Machine**: Use nmap to identify open ports and services on the OWASP machine.

```
nmap -sV <target_ip>
```

- he scan will list services like HTTP on ports 80 or 8080, which likely contain login forms.

1.2. **Locate the Login Page**: In your browser, navigate to the target machine's IP address and locate the login page.

Step 2: Capture the Login Request

2.1. **Configure Proxy**:

- Open Burp Suite and configure your browser to route traffic through Burp's proxy (by default, Burp listens on 127.0.0.1:8080).
- Install Burp's SSL certificate in your browser if necessary to intercept HTTPS traffic.

2.2. **Intercept the Login Request**:

- Go to the login page of the target in your browser.

- Use Burp Suite’s **Proxy** tab to intercept the login form submission.
- Review the intercepted request to understand the parameters (like username, password, etc.) and the POST request format.

Step 3: Set Up Burp Suite Intruder

3.1. **Configure Intruder**:

- In Burp Suite, go to the **Intruder** tab and click on "New Intruder."
- Select the captured HTTP request (from Proxy history or Intercept tab).
- The **Target** and **Positions** will automatically populate with the HTTP request details.

3.2. **Define Positions**:

- In the **Positions** tab, Burp Suite will highlight parameters like username and password in the intercepted request. You need to **mark** the areas that will change with each attempt:
  - Mark the username and password fields as **Payload Positions** by clicking the "Clear §" button and selecting the areas to be attacked.

Step 4: Prepare Payloads

4.1. **Load the Wordlist**:

- In the **Payloads** tab, you can select a wordlist. Burp Suite allows you to load a list of passwords to use in the attack. The default wordlist in Kali is /usr/share/wordlists/rockyou.txt, but you can use a custom wordlist.
- Select the payload type (e.g., Simple list) and import the wordlist.

Example:

- Username: admin
- Password list: rockyou.txt

4.2. **Configure Payload Settings**:

- You can specify multiple usernames or use the same username and test various passwords. You can also load different payloads for usernames and passwords.

Step 5: Run the Attack

5.1. **Start the Attack**:

- Click the "Start Attack" button. Burp Suite will start sending requests with different combinations of usernames and passwords from the wordlist to the login form.

5.2. **Monitor the Results**:

- As the attack runs, you can monitor the responses in the **Intruder** results tab. Burp Suite will display the status codes and the length of the response for each attempt.

- A **successful login** will often show a different HTTP response (e.g., a 200 OK status or a redirect) compared to failed attempts (usually 403 Forbidden or 401 Unauthorized).

Step 6: Analyze the Results

6.1. **Identify Valid Credentials**:

- Look for successful responses (e.g., a login page redirect or a change in status code) to identify valid username-password combinations.

6.2. **Failed Attempts**:

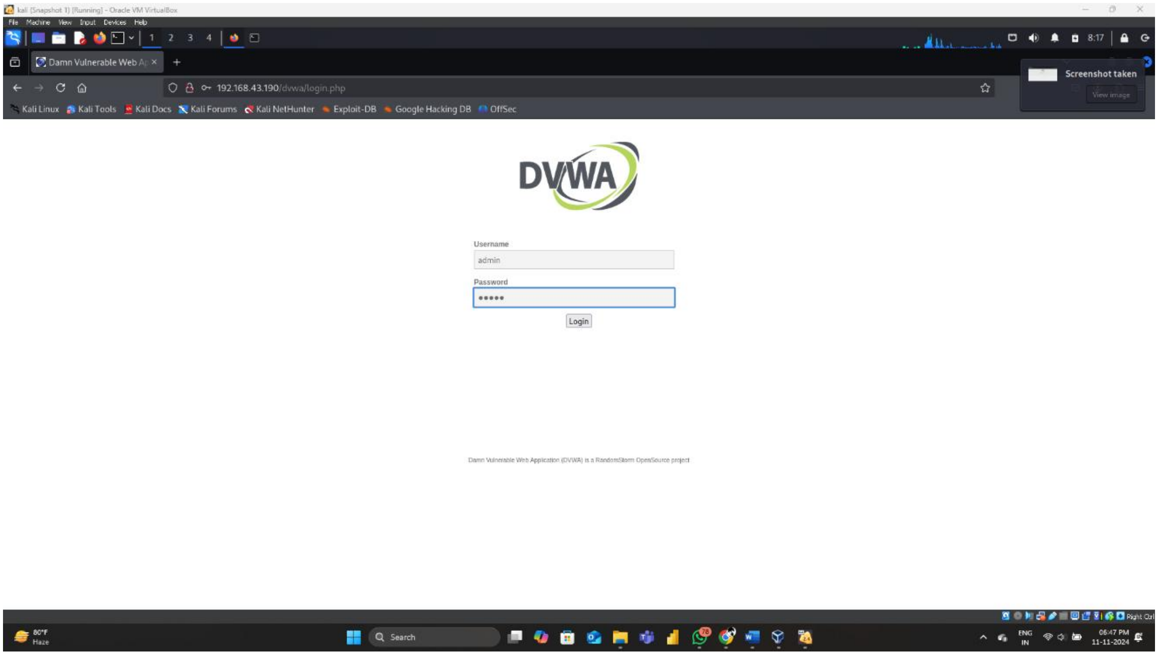
- If no valid credentials are found, review the application for additional security mechanisms like CAPTCHA, account lockouts, or rate limiting.

Step 7: Implement Security Measures

After completing the brute force attack, here are some security measures to prevent such attacks:

- **Rate Limiting**: Implement mechanisms to limit login attempts per IP or account.
- **Strong Password Policies**: Enforce complex password rules (length, character variety).
- **Account Lockout Mechanism**: Lock accounts after several failed attempts.
- **Multi-Factor Authentication (MFA)**: Require multiple factors for authentication to reduce the effectiveness of brute-force attacks.

Images



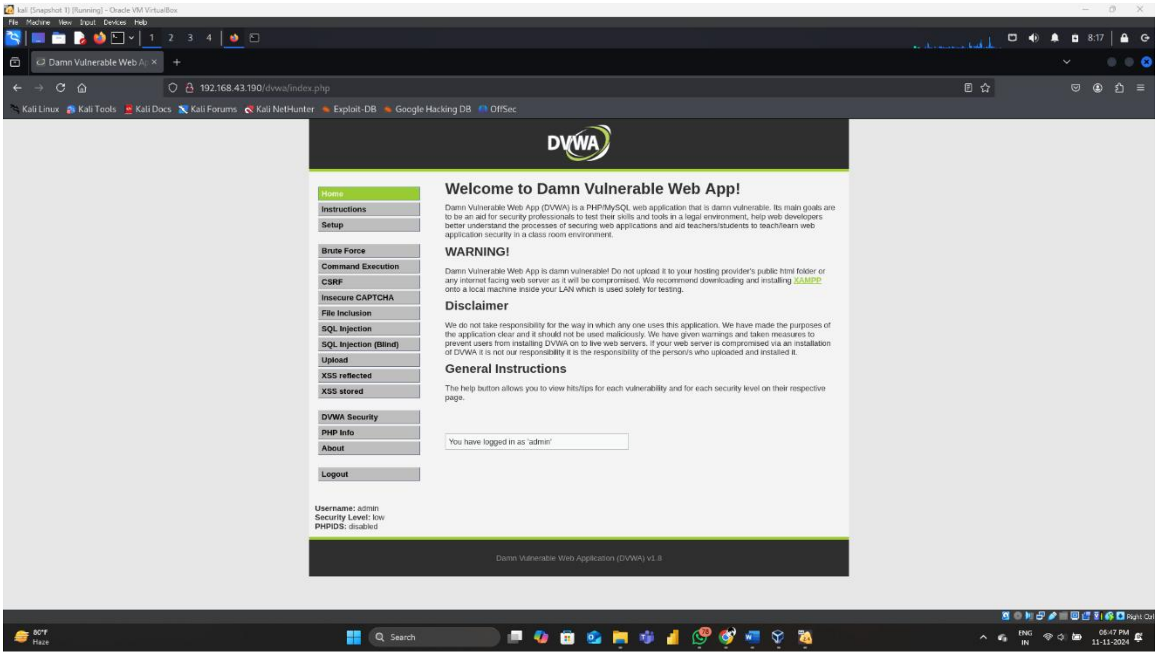
192.168.43.190/dvwa/login.php

Username: admin

Password: *****

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Image 1



192.168.43.190/dvwa/index.php

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are 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 aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. 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.

General Instructions

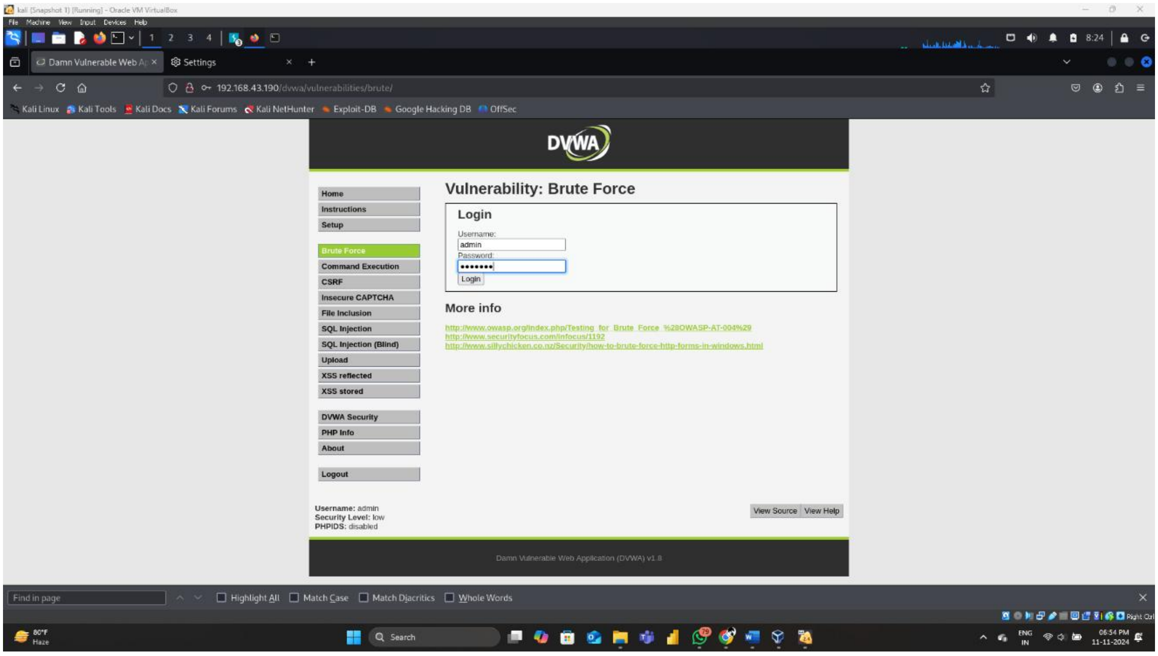
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.8

Image 2



Vulnerability: Brute Force

Login

Username: admin

Password: •••••••

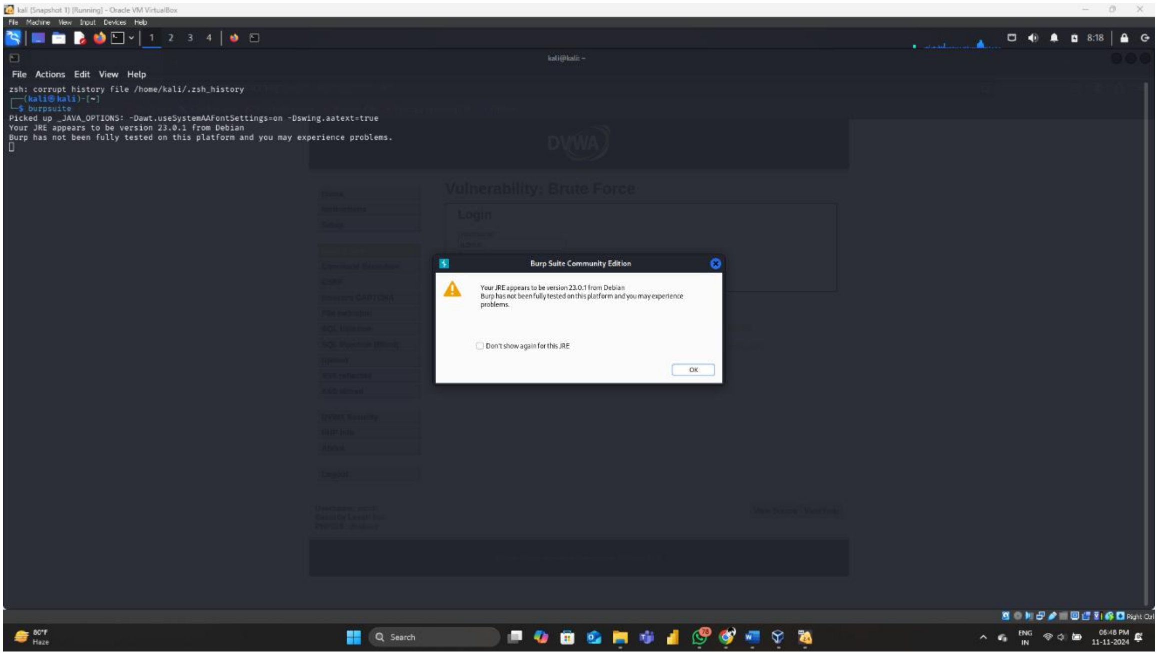
More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
http://www.securityfocus.com/infocus/1192
http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.8

Image 3

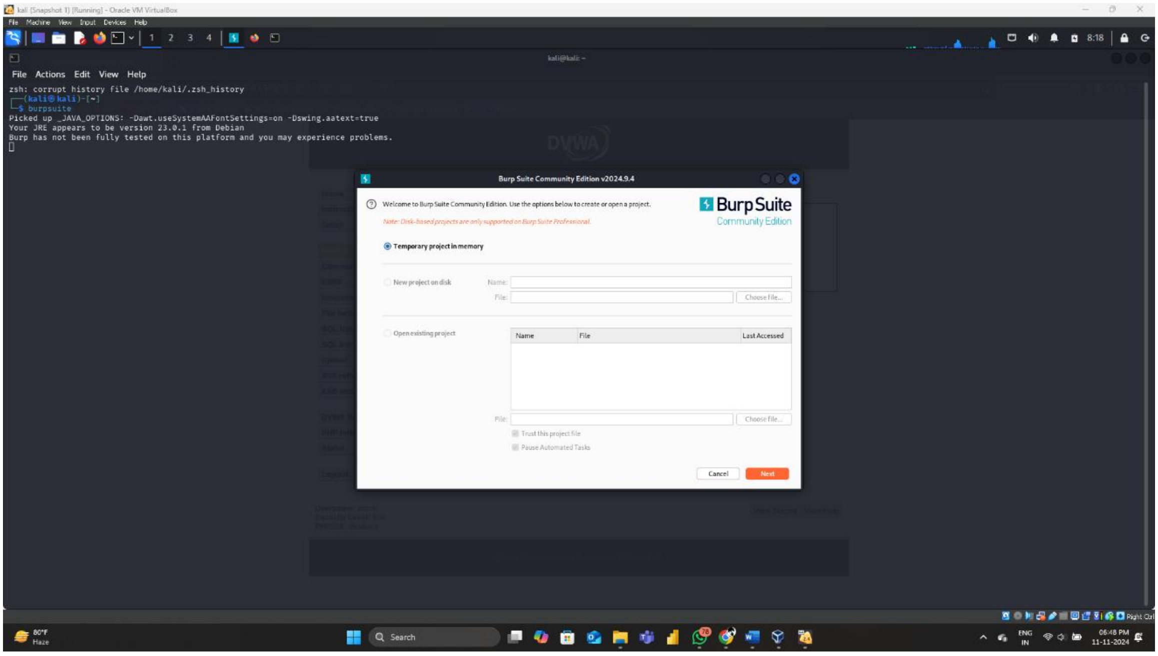

kali [Snapshot 1] [Running] - Oracle VM VirtualBox
kali@kali: ~
File
Actions
Edit
View
Help
Burp Suite Community Edition
OK

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Your JRE appears to be version 23.0.1 from Debian
Burp has not been fully tested on this platform and you may experience problems.
```

Your JRE appears to be version 23.0.1 from Debian
Burp has not been fully tested on this platform and you may experience problems.

□ Don't show again for this JRE

Image 4



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Your JRE appears to be version 23.0.1 from Debian
Burp has not been fully tested on this platform and you may experience problems.
```

Burp Suite Community Edition v2024.9.4

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● Temporary project in memory

○ New project on disk — Name: — File:

○ Open existing project

Name	File	Last Accessed

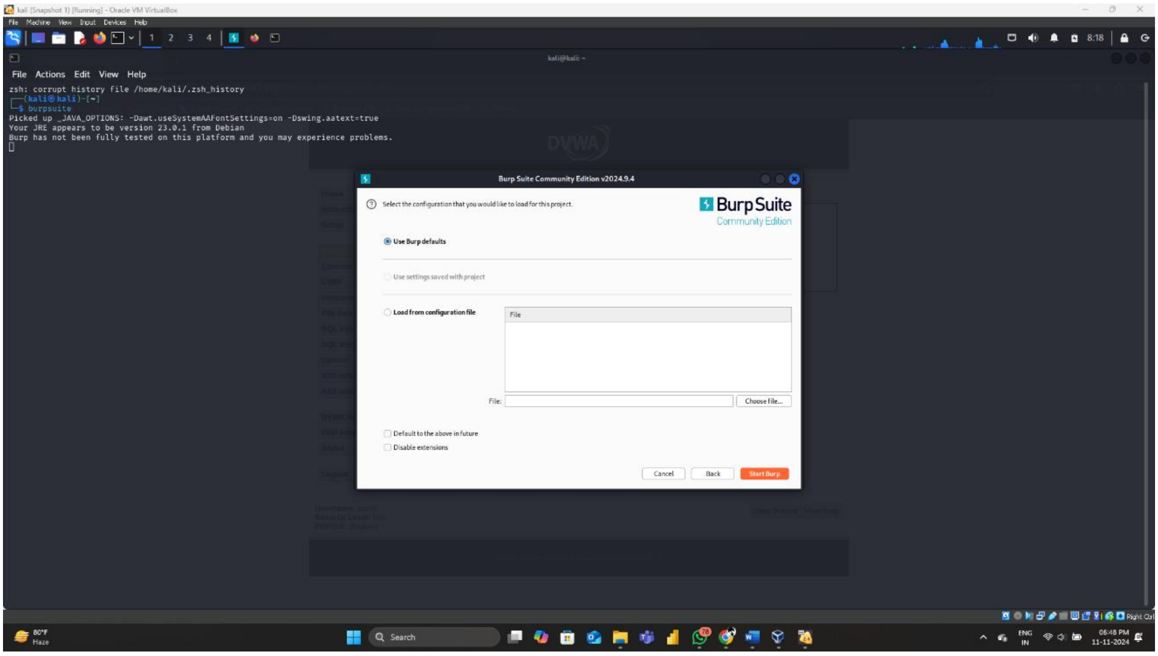
File:

□ Trust this project file

□ Pause Automated Tasks

kali (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Burp Suite
Community Edition
Choose file...
Cancel
Next
80°F
Haze
Search
ENG
IN
06:48 PM
11-11-2024

Image 5



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Your JRE appears to be version 23.0.1 from Debian
Burp has not been fully tested on this platform and you may experience problems.
```

Burp Suite Community Edition v2024.9.4

Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use settings saved with project

○ Load from configuration file

File

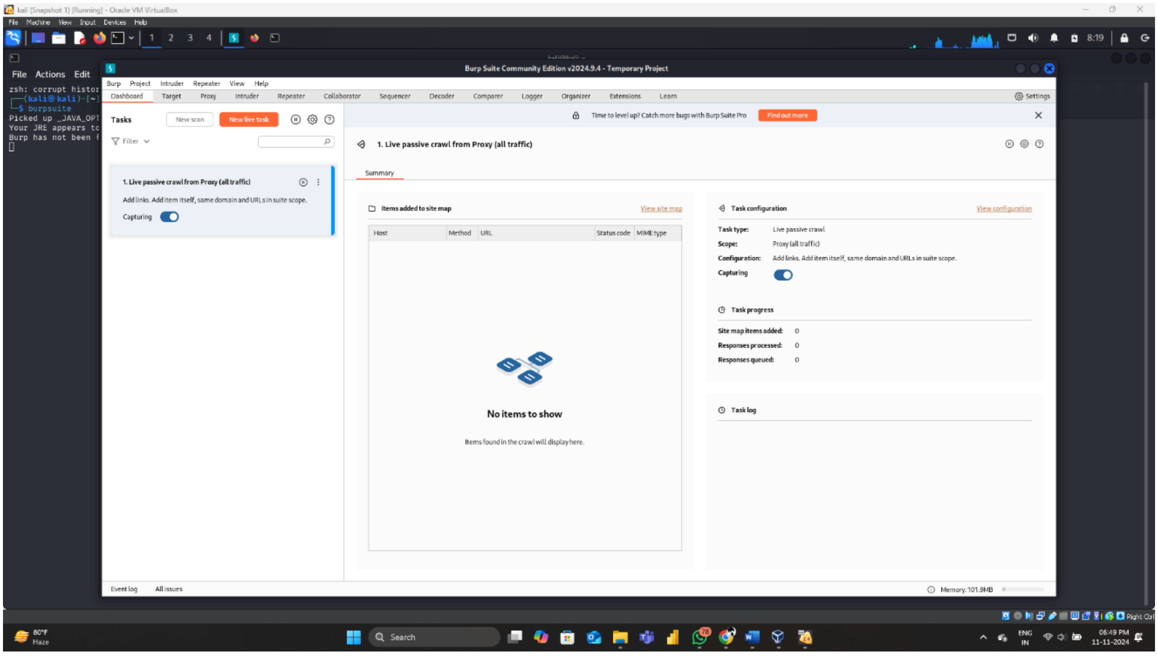
File:

□ Default to the above in future

□ Disable extensions

kali (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Burp Suite
Community Edition
Choose file...
Cancel
Back
Start Burp
80°F
Haze
Search
ENG
IN
06:48 PM
11-11-2024

Image 6


kali (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
New scan
New live task
Filter
Find out more
Summary
View site map
View configuration
Event log
All issues
Memory: 101.9MB

```
zsh: corrupt histor
┌──(kali㉿kali)-[~]
└─$ burpsuite
Picked up _JAVA_OPT
Your JRE appears to
Burp has not been f
```

Tasks

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing

Time to level up? Catch more bugs with Burp Suite Pro

1. Live passive crawl from Proxy (all traffic)

Items added to site map

Host	Method	URL	Status code	MIME type

No items to show

Items found in the crawl will display here.

Task configuration

Task type: Live passive crawl

Scope: Proxy (all traffic)

Configuration: Add links. Add item itself, same domain and URLs in suite scope.

Capturing

Task progress

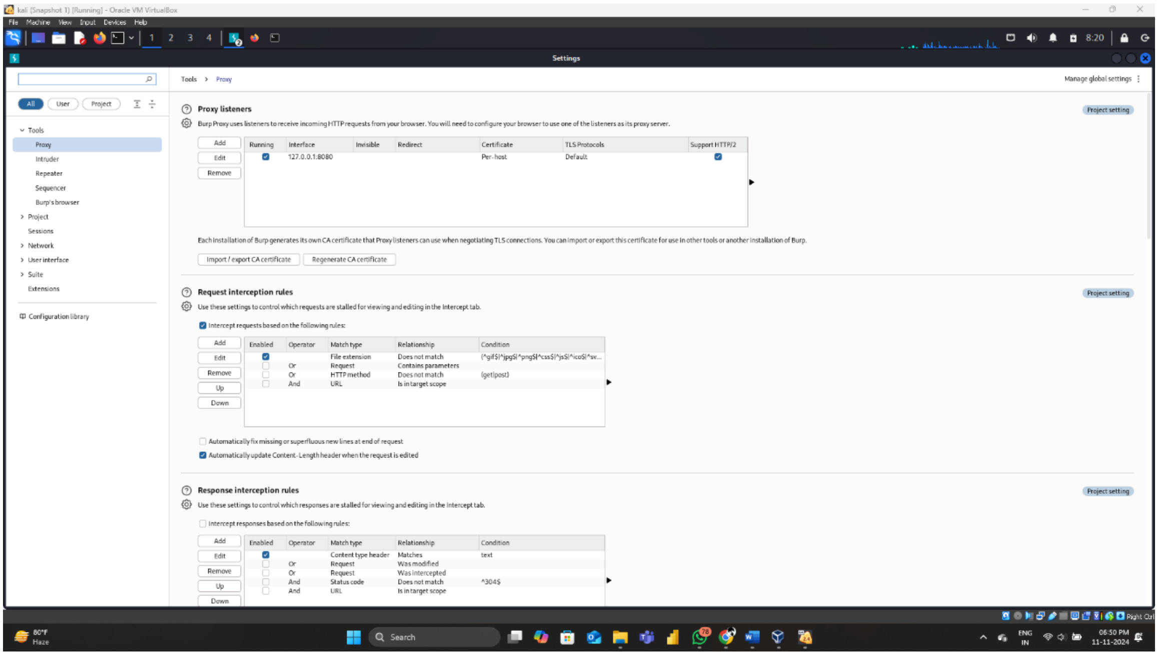
Site map items added: 0

Responses processed: 0

Responses queued: 0

Task log

Image 7



Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols	Support HTTP/2
☑	127.0.0.1:8080			Per-host	Default	☑

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

Request interception rules

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$\|^ico$|^sv...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
□	And	URL	Is in target scope	

□ Automatically fix missing or superfluous new lines at end of request

☑ Automatically update Content-Length header when the request is edited

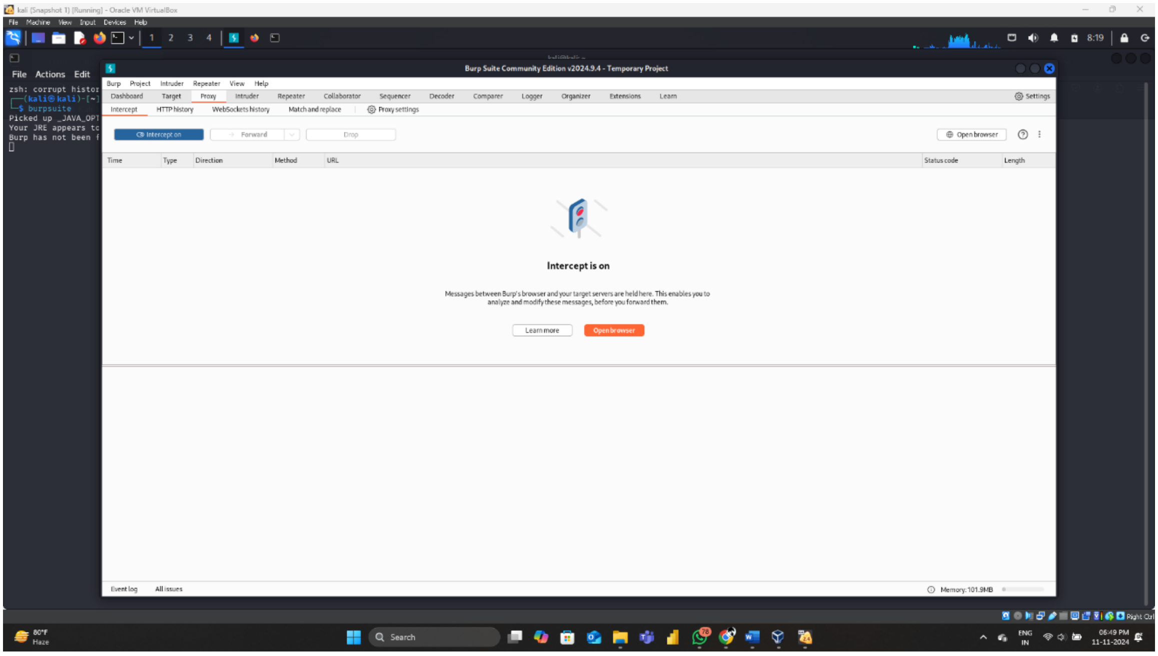
Response interception rules

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

□ Intercept responses based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		Content type header	Matches	text
□	Or	Request	Was modified	
□	Or	Request	Was intercepted	
□	And	Status code	Does not match	^304$
□	And	URL	Is in target scope	

Image 8



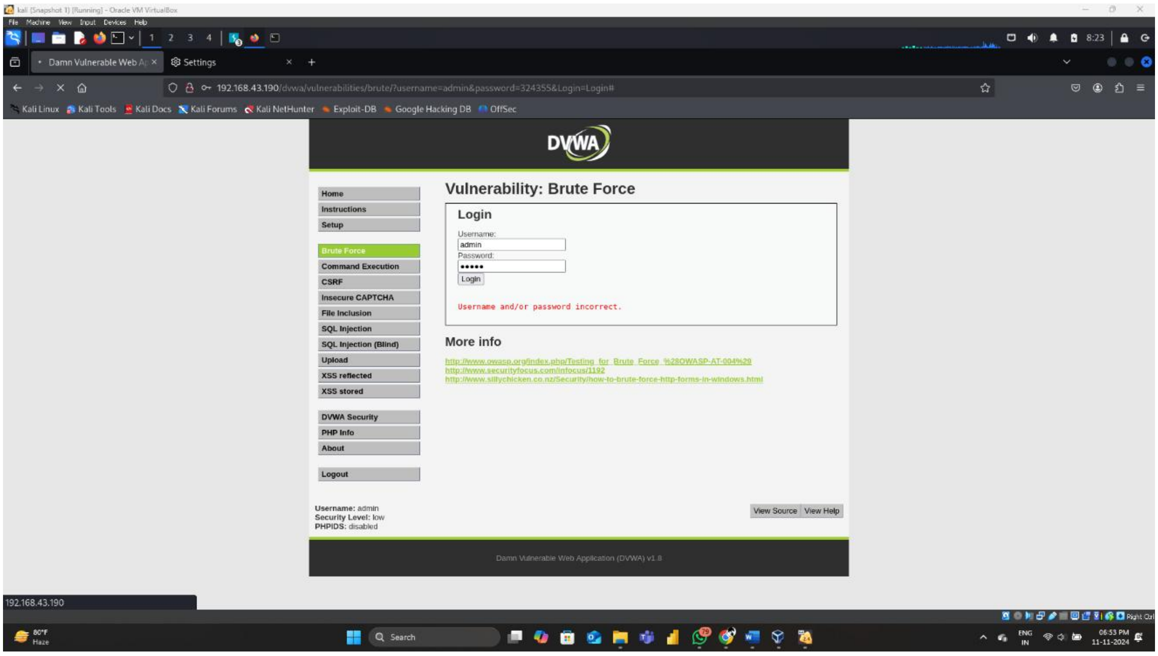
```
zsh: corrupt histor
┌──(kali㉿kali)-[~]
└─$ burpsuite
Picked up _JAVA_OPT
Your JRE appears to
Burp has not been f
```

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.

kali (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit
Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Time Type Direction Method URL Status code Length
Learn more
Open browser
Event log All issues
Memory: 101.9MB
8:19
80°F Haze
Search
ENG IN
06:49 PM 11-11-2024

Image 9



192.168.43.190/dvwa/vulnerabilities/brute/?username=admin&password=324355&Login=Login#

Vulnerability: Brute Force

Login

Username: admin

Password: •••••

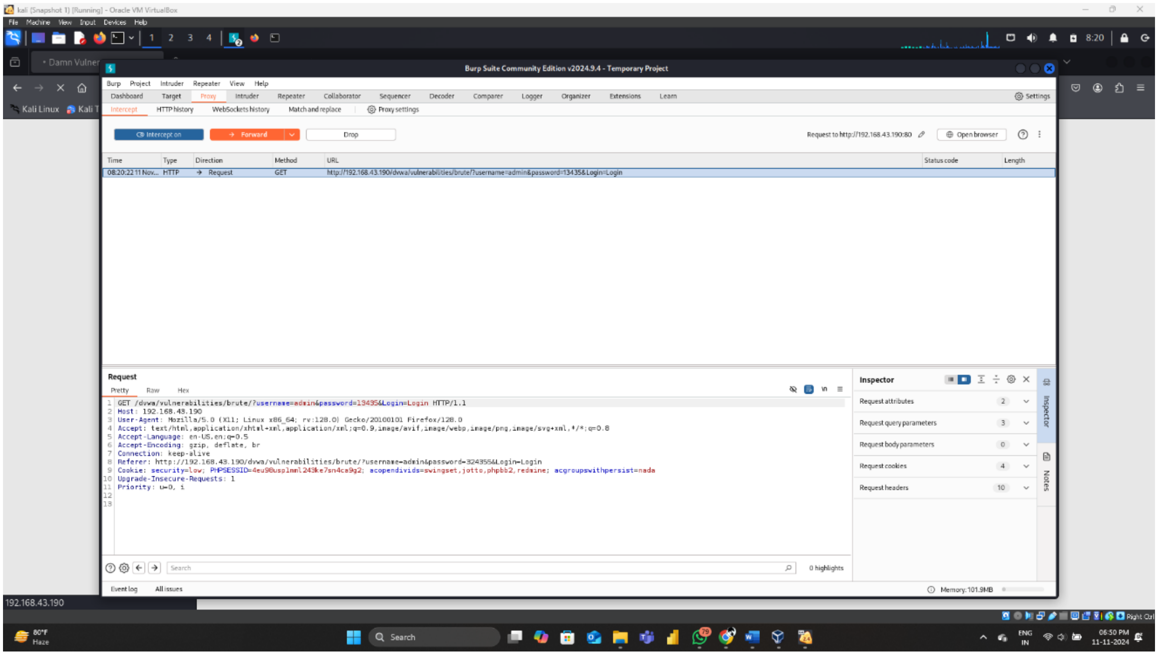
Username and/or password incorrect.

More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
http://www.securityfocus.com/infocus/1192
http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

Username: admin
Security Level: low
PHPIDS: disabled

Image 10


kali (Snapshot 1) [Running] - Oracle VM VirtualBox
Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Inspector
Request attributes 2
Request query parameters 3
Request body parameters 0
Request cookies 4
Request headers 10
Event log All issues
0 highlights
Memory: 101.9MB

Request to http://192.168.43.190:80

Time	Type	Direction	Method	URL	Status code	Length
08:20:22 11 Nov...	HTTP	→ Request	GET	http://192.168.43.190/dvwa/vulnerabilities/brute/?username=admin&password=13435&Login=Login		

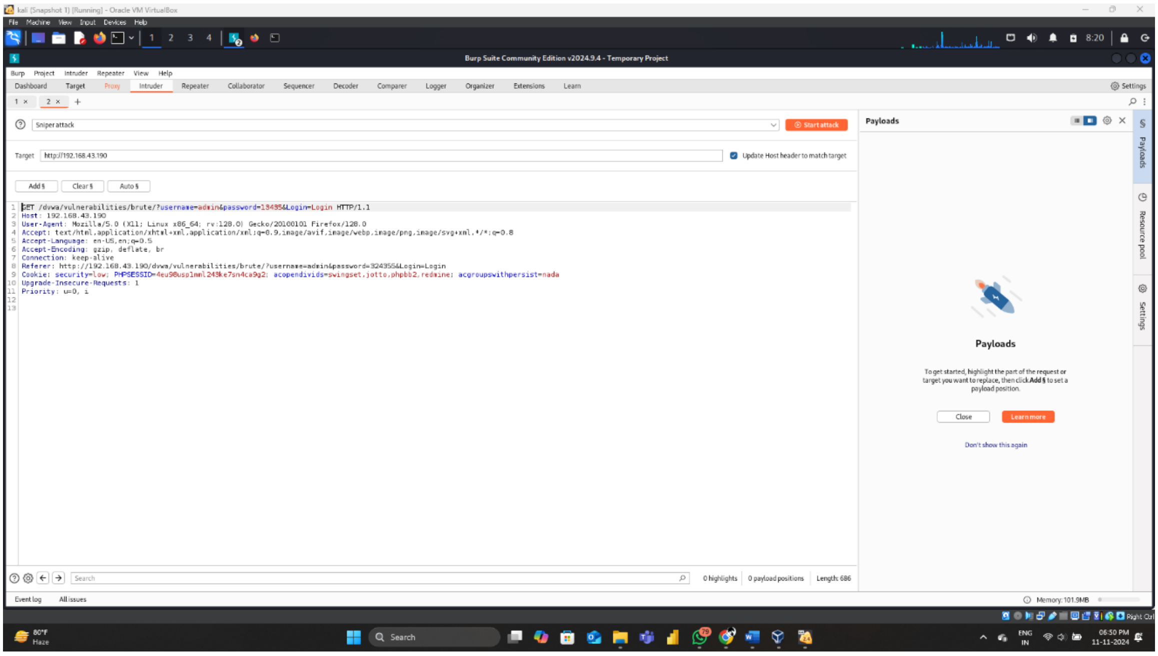
Request

Pretty Raw Hex

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=13435&Login=Login HTTP/1.1
Host: 192.168.43.190
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.43.190/dvwa/vulnerabilities/brute/?username=admin&password=324355&Login=Login
Cookie: security=low; PHPSESSID=4eu98usplmml249ke7sn4ca9g2; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

192.168.43.190

Image 11


kali (Snapshot 1) [Running] - Oracle VM VirtualBox
Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 × 2 × +
Start attack
Add § Clear § Auto §
Payloads
Close
Learn more
Don't show this again
Resource pool
Settings
Event log All issues
0 highlights
0 payload positions
Length: 686
Memory: 101.9MB

Sniper attack

Target http://192.168.43.190

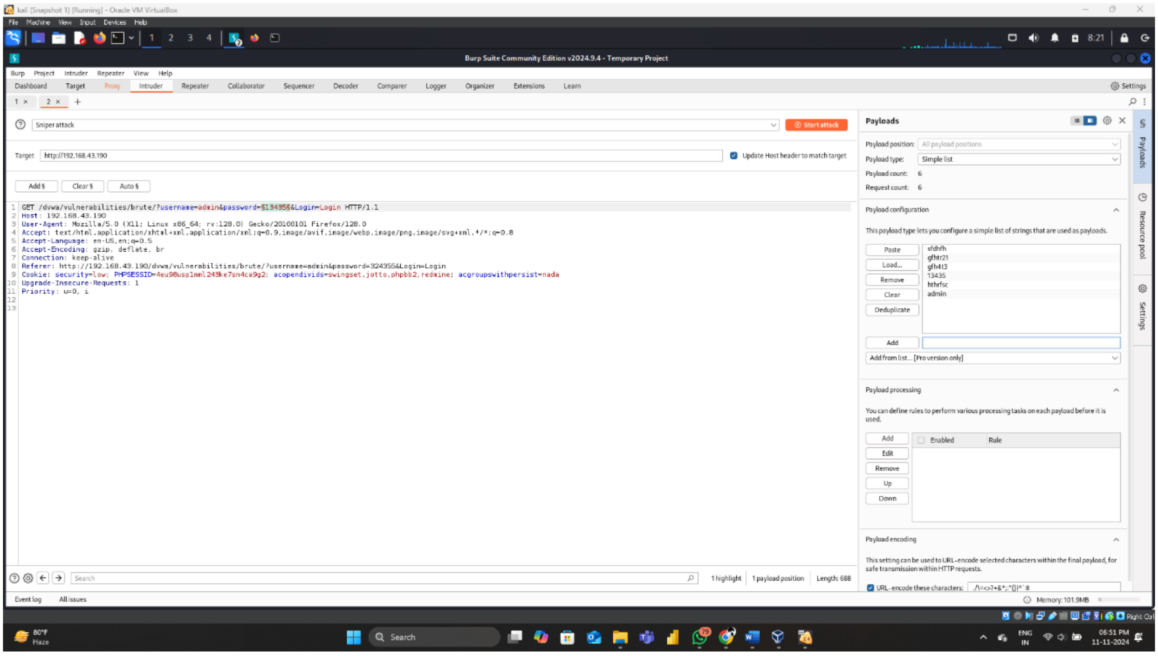
☑ Update Host header to match target

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=13435&Login=Login HTTP/1.1
Host: 192.168.43.190
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.43.190/dvwa/vulnerabilities/brute/?username=admin&password=324355&Login=Login
Cookie: security=low; PHPSESSID=4eu98usplmml249ke7sn4ca9g2; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Payloads

To get started, highlight the part of the request or target you want to replace, then click **Add §** to set a payload position.

Image 12



Sniper attack

Target: http://192.168.43.190

☑ Update Host header to match target

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=§13435§&Login=Login HTTP/1.1
Host: 192.168.43.190
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.43.190/dvwa/vulnerabilities/brute/?username=admin&password=324355&Login=Login
Cookie: security=low; PHPSESSID=4eu98usp1mml243ke7sn4ca9g2; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Payloads

Payload position: All payload positions

Payload type: Simple list

Payload count: 6

Request count: 6

Payload configuration

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

```
sfdhfh
gfhtr21
gfh4t3
13435
hthrfsc
admin
```

Add from list... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

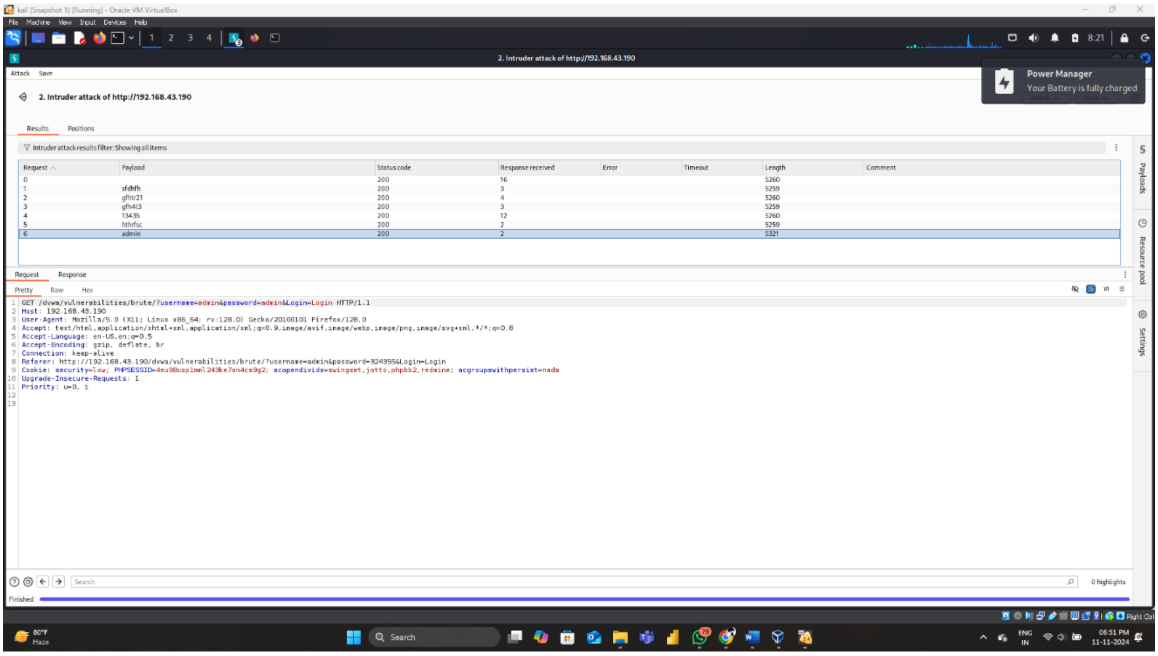
Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters:

1 highlight 1 payload position Length: 688

Image 13



2. Intruder attack of http://192.168.43.190

Power Manager
Your Battery is fully charged

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	16			5260	
1	sfdhfh	200	3			5259	
2	gfhtr21	200	4			5260	
3	gfh4t3	200	3			5259	
4	13435	200	12			5260	
5	hthrfsc	200	2			5259	
6	admin	200	2			5321	

```
GET /dvwa/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.1
Host: 192.168.43.190
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.43.190/dvwa/vulnerabilities/brute/?username=admin&password=324355&Login=Login
Cookie: security=low; PHPSESSID=4eu98usp1mml243ke7sn4ca9g2; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

0 highlights

Image 14

Challenges and Solutions

- **Challenge:** CAPTCHA or account lockout mechanisms.
    - **Solution:** Implement bypass techniques such as using CAPTCHA-solving tools (for educational use only) or focus on highlighting the need for better security configurations.
- **Challenge:** Slow brute-forcing due to network or application delays.
    - **Solution:** Use a targeted wordlist based on common usernames or passwords, reducing the number of attempts needed.

Future Enhancements

- **MFA Implementation:** Encourage the use of multi-factor authentication (MFA) to thwart brute force attacks.
- **Advanced Logging:** Set up intrusion detection systems to monitor brute force attempts in real-time.
- **Account Lockouts and Alerts:** Use alerts and lockout systems to automatically respond to excessive failed attempts.

Project Summary

This guide showed how to use **Burp Suite** for a brute-force attack on an OWASP vulnerable machine. By using Burp Suite's **Intruder** tool and automated payload submission, we demonstrated how attackers try various credentials until they succeed. Implementing security best practices such as rate limiting, account lockouts, and multi-factor authentication can help protect against such attacks.

References

- OWASP Testing Guide
- Burp Suite Documentation
- OWASP Juice Shop