Experiment No. 8

Title: Password Cracking - Burp suite

Batch: A3 **Roll No.:16010421059** **Experiment No.:08**

Aim: To implement password cracking using Burp suite

Resources needed: Burp suite Professional or open source tool, XAMPP

Theory

1. Password-Based Authentication Systems:

Password-based authentication systems rely on something the user knows, which is typically a secret password. Here are some key points about these systems:

- User Credentials: Users have a combination of a username or email and a password. The username is often public, while the password is kept secret.

- Authentication Process: The system checks the entered password against the stored password associated with the given username/email. If they match, the user gains access.

- Strengths: Simplicity, ease of use, and familiarity for users.

- Weaknesses: Vulnerable to various attacks, especially if users choose weak passwords, reuse passwords, or fall victim to social engineering.

2. Attacks on Password-Based Authentication Systems:

Password-based authentication systems are vulnerable to several types of attacks, including:

a. Brute Force Attack: An attacker systematically tries every possible password until the correct one is found. This can be mitigated by account lockouts or rate limiting.

b. Dictionary Attack: Attackers use a list of common words or phrases as potential passwords. This is often more efficient than brute force.

c. Phishing: Attackers trick users into revealing their passwords by posing as a legitimate entity via email, websites, or other means.

d. Keylogging: Malware records the keystrokes of users, capturing passwords as they are typed.

e. Rainbow Tables: Precomputed tables of password hashes are used to quickly look up corresponding plaintext passwords.

f. Password Spraying: Attackers try a few common passwords against many accounts to avoid detection from account lockout mechanisms.

g. Credential Stuffing: Attackers use known username/password combinations from breaches on multiple websites to gain unauthorized access.

h. Man-in-the-Middle (MitM): An attacker intercepts communication between the user and the server, potentially capturing the password during login.

i. Online and Offline Attacks: In online attacks, the attacker interacts with the authentication system in real-time. In offline attacks, the attacker has obtained a password hash and can attempt to crack it without being connected to the target system.

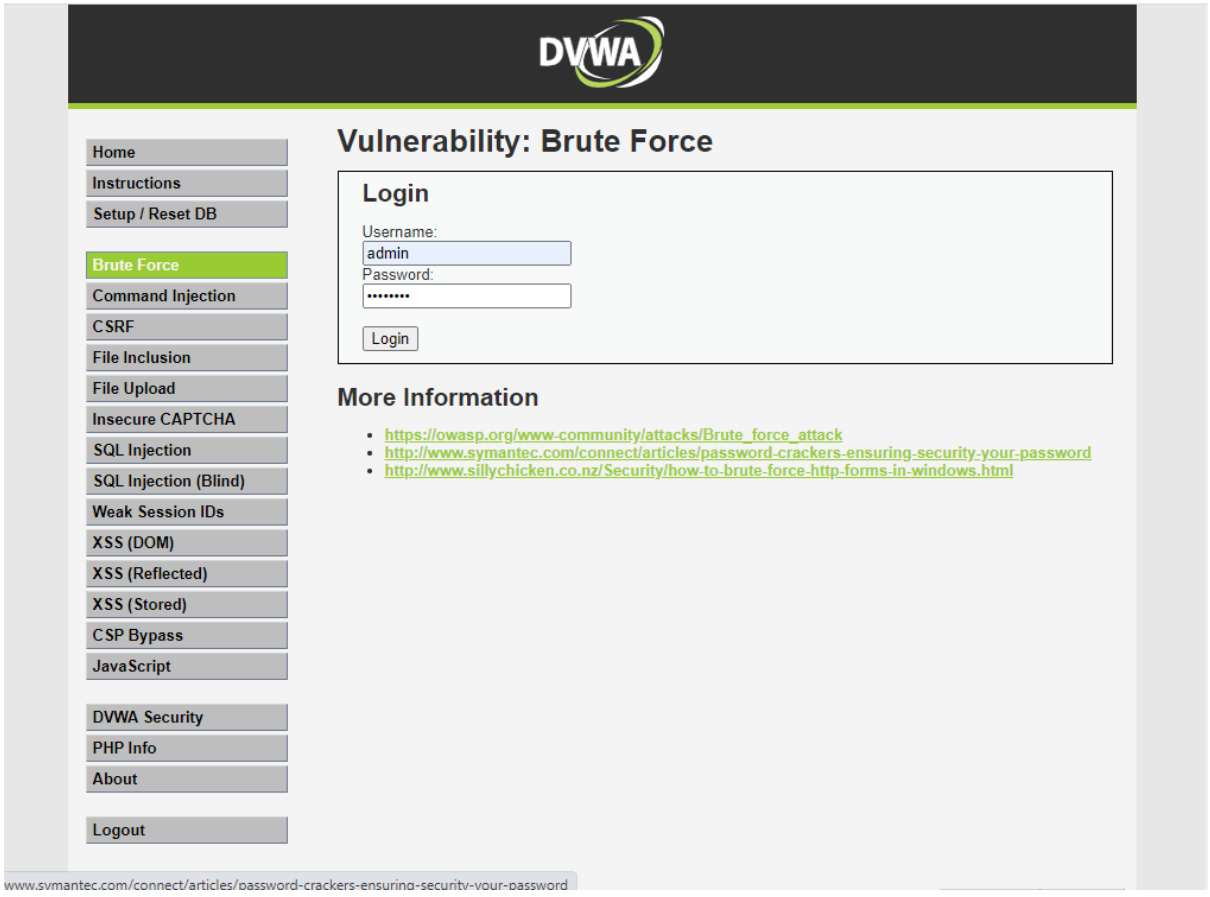
j. Social Engineering: Attackers manipulate individuals into revealing their passwords through deception or psychological manipulation.

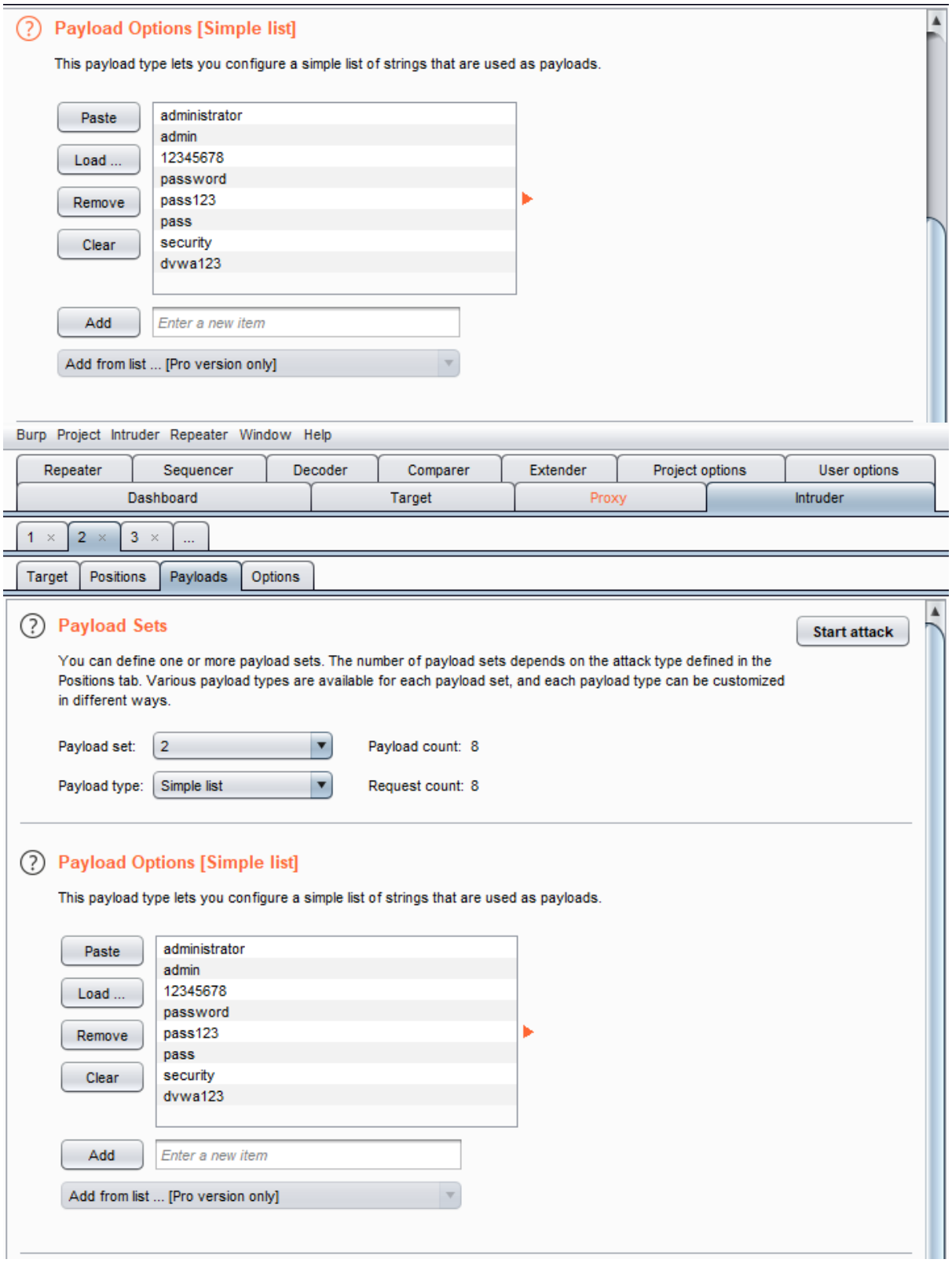
To enhance the security of password-based authentication systems, best practices include using strong, unique passwords, implementing multi-factor authentication (MFA), and following security guidelines for secure password storage (e.g., using salted and hashed passwords). Additionally, educating users about the risks of password-based attacks and how to recognize phishing attempts is essential for overall security.

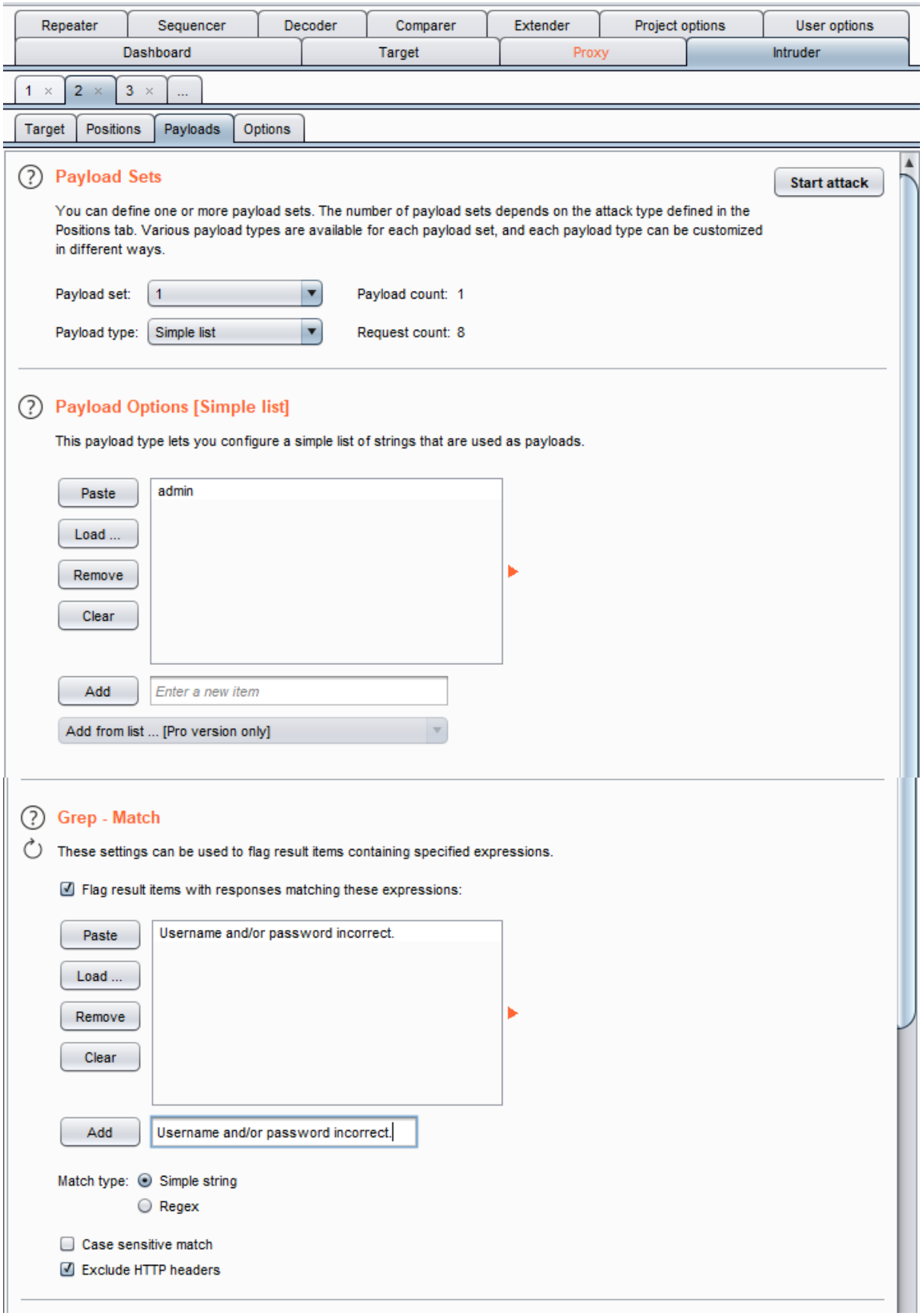
Procedure / Approach /Algorithm / Activity Diagram:

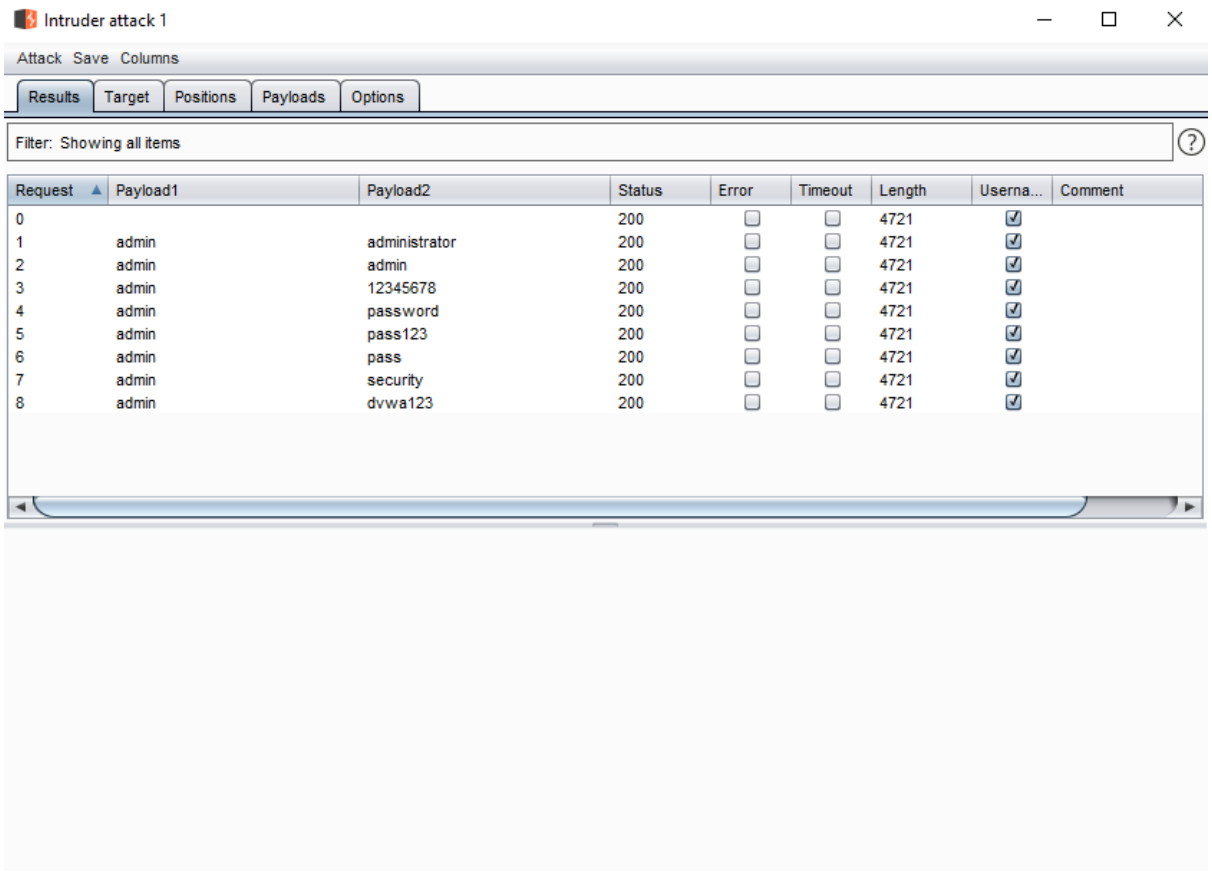
1) **Installation of Burp suite and other utilities (open source/ freeware/ trial versions)**
2) **Perform password cracking using Burp suite (refer to sample video uploaded)**

SCREENSHOTS:

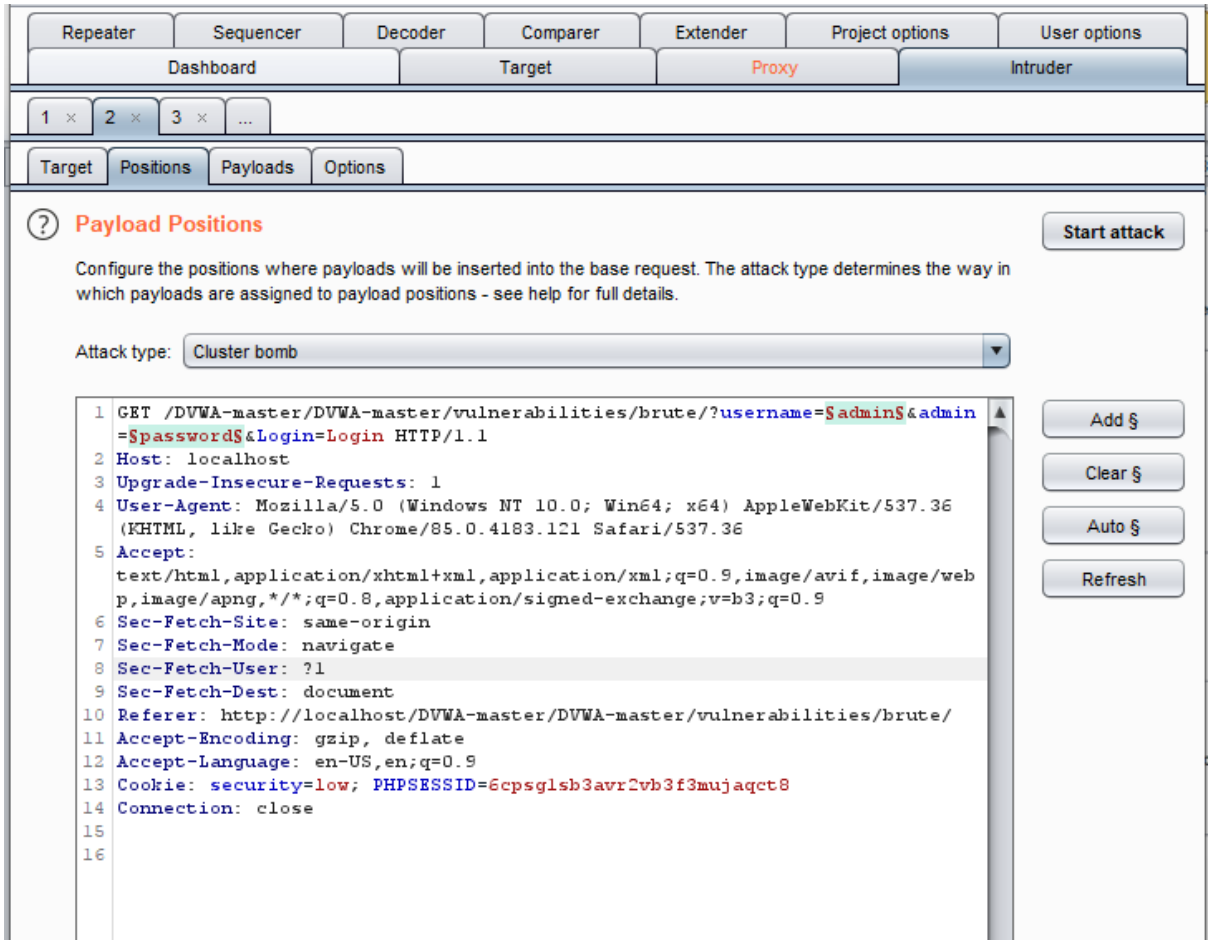



Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
administrator
admin
12345678
password
pass123
pass
security
dvwa123
Add
Enter a new item
Add from list ... [Pro version only]
Burp Project Intruder Repeater Window Help
Repeater Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder
1 2 3 ...
Target Positions Payloads Options
Payload Sets
Start attack
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: 2
Payload count: 8
Payload type: Simple list
Request count: 8
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
administrator
admin
12345678
password
pass123
pass
security
dvwa123
Add
Enter a new item
Add from list ... [Pro version only]


Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options
Dashboard
Target
Proxy
Intruder
1
2
3
...
Target
Positions
Payloads
Options
Payload Sets
Start attack
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: 1
Payload count: 1
Payload type: Simple list
Request count: 8
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
admin
Add
Enter a new item
Add from list ... [Pro version only]
Grep - Match
These settings can be used to flag result items containing specified expressions.
Flag result items with responses matching these expressions:
Paste
Load ...
Remove
Clear
Username and/or password incorrect.
Add
Username and/or password incorrect.
Match type:
Simple string
Regex
Case sensitive match
Exclude HTTP headers



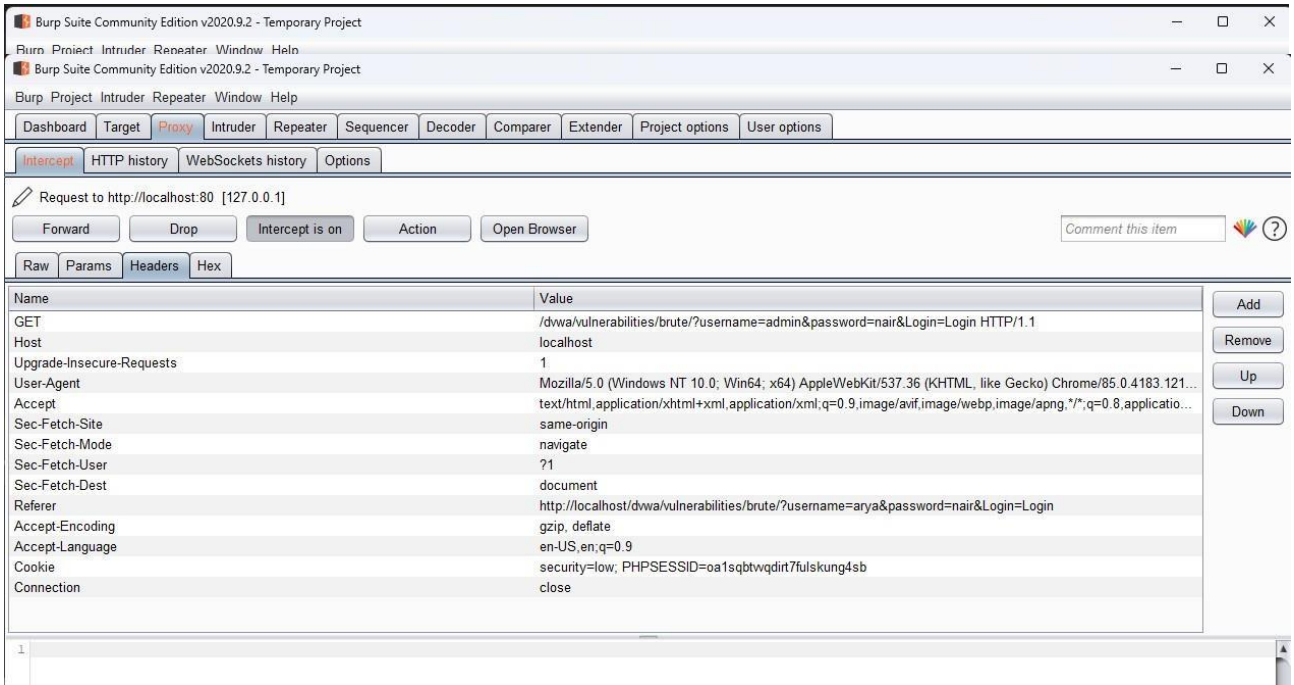
Request	Payload1	Payload2	Status	Error	Timeout	Length	Userna...	Comment
0			200	☐	☐	4721	☑	
1	admin	administrator	200	☐	☐	4721	☑	
2	admin	admin	200	☐	☐	4721	☑	
3	admin	12345678	200	☐	☐	4721	☑	
4	admin	password	200	☐	☐	4721	☑	
5	admin	pass123	200	☐	☐	4721	☑	
6	admin	pass	200	☐	☐	4721	☑	
7	admin	security	200	☐	☐	4721	☑	
8	admin	dvwa123	200	☐	☐	4721	☑	



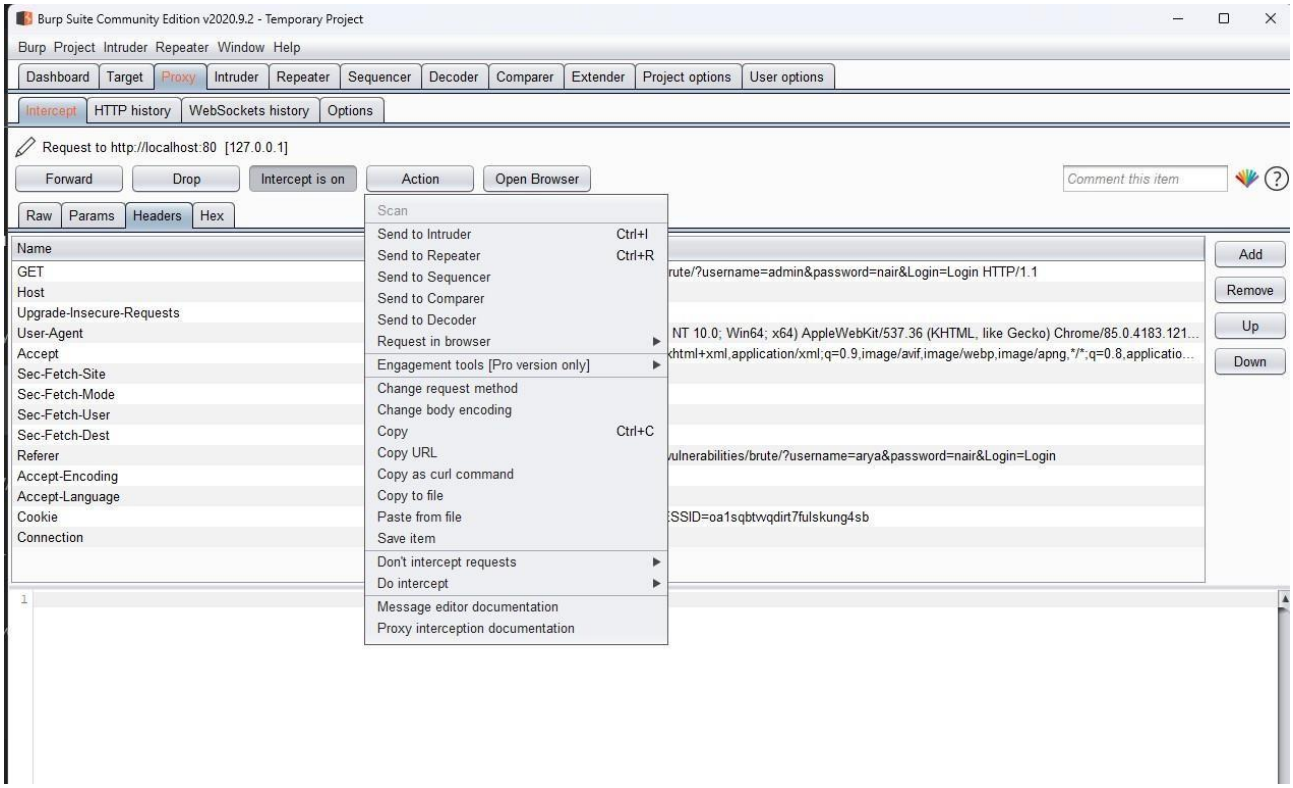
Implementation: Audio-Video recording of the mentioned activities performed with your own voice.(upload .mp4 file along with final writeup)

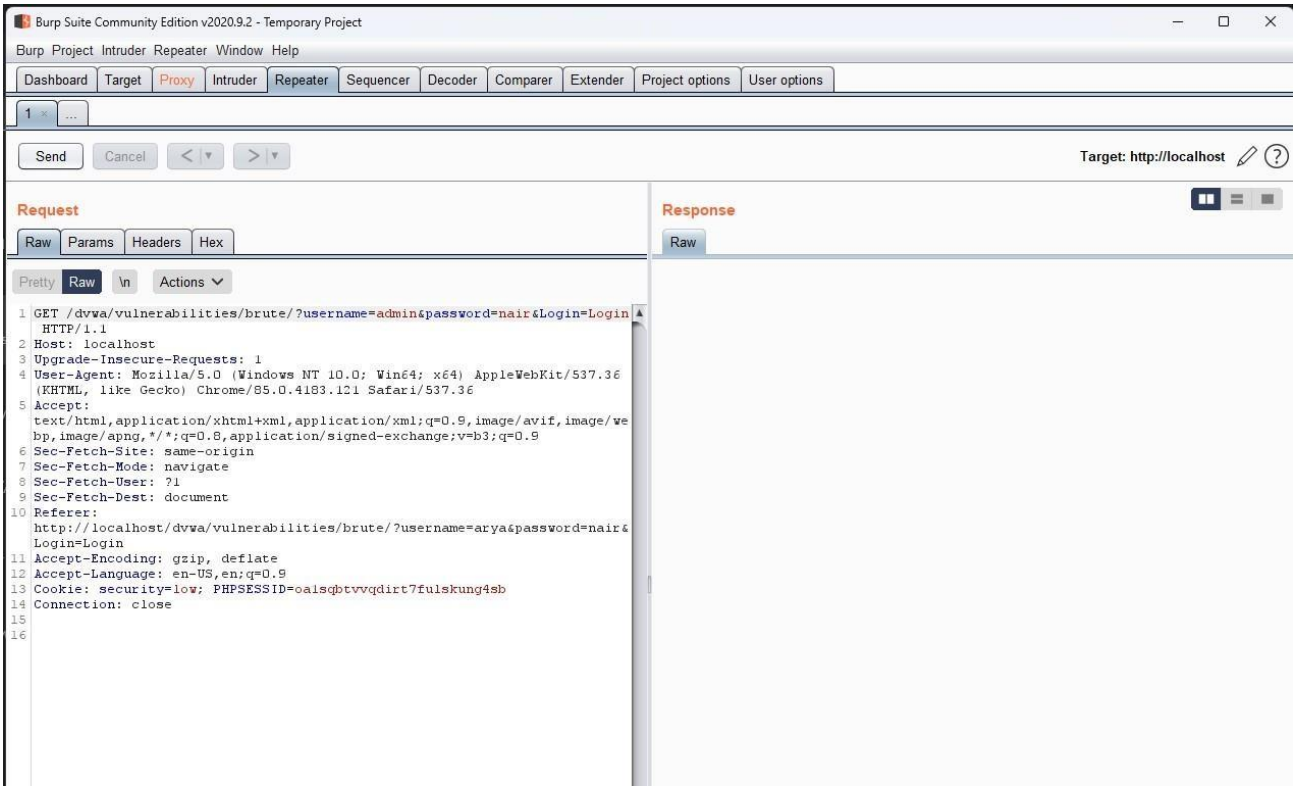
Questions:

1) Explore any other use of Burp suite. Perform it using burp suit and add the screen shots of the same.



We used burpsuite to intercept the request from the user to the server. Then after eavesdropping we can send it further





Then we can modify and send the request using repeater

Outcomes:

CO 4: Understand Security issues related to Software, Web and Networks.

Conclusion: (Conclusion to be based on the objectives and outcomes achieved**)**

Implemented password cracking using Burp suite successfully in lab.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

References:
Books/ Journals/ Websites:

1. **https://portswigger.net/burp/pro**
2. **https://www.apachefriends.org/download.html**