Experiment 06

AIM - Perform various attacks using Burp Suite for security testing of web applications

Learning Objective: Students should be able to understand and test brute force attack using Burp Suite.

Tools: Virtual Machine/Linux, Burp Suite

Theory:

A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks. The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.

The name "brute force" comes from attackers using excessively forceful attempts to gain access to user accounts. Despite being an old cyberattack method, brute force attacks are tried and tested and remain a popular tactic with hackers.

Types of Brute Force Attacks

There are various types of brute force attack methods that allow attackers to gain unauthorized access and steal user data.

1. Simple Brute Force Attacks : A simple brute force attack occurs when a hacker attempts to guess a user's login credentials manually without using any software. This is typically through standard password combinations or personal identification number (PIN) codes.

These attacks are simple because many people still use weak passwords, such as "password123" or "1234," or practice poor password etiquette, such as using the same password for multiple websites. Passwords can also be guessed by hackers that do minimal reconnaissance work to crack an individual's potential password, such as the name of their favorite sports team.

2. Dictionary Attacks : A dictionary attack is a basic form of brute force hacking in which the attacker selects a target, then tests possible passwords against that individual's username. The attack method itself is not technically considered a brute force attack, but it can play an important role in a bad actor's password-cracking process.

The name "dictionary attack" comes from hackers running through dictionaries and amending words with special characters and numbers. This type of attack is typically time-consuming and has a low chance of success compared to newer, more effective attack methods.

3. Hybrid Brute Force Attacks : A hybrid brute force attack is when a hacker combines a dictionary attack method with a simple brute force attack. It begins with the hacker knowing a username, then carrying out a dictionary attack and simple brute force methods to discover an account login combination.

The attacker starts with a list of potential words, then experiments with character, letter, and

number combinations to find the correct password. This approach allows hackers to discover passwords that combine common or popular words with numbers, years, or random characters, such as "SanDiego123" or "Rover2020."

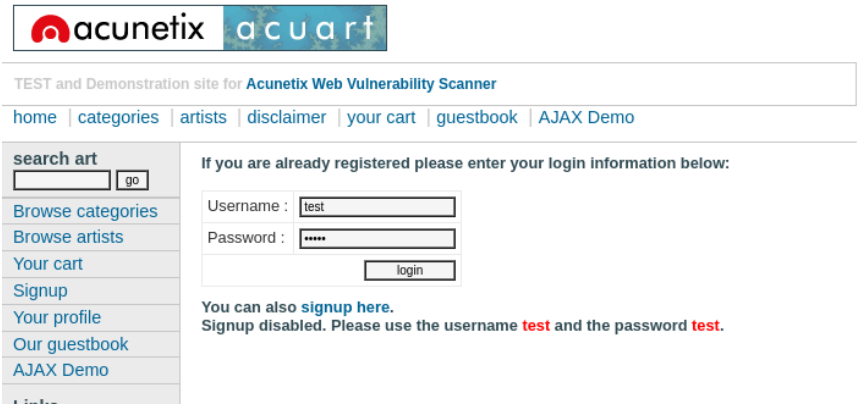
4. Reverse Brute Force Attacks : A reverse brute force attack sees an attacker begin the process with a known password, which is typically discovered through a network breach. They use that password to search for a matching login credential using lists of millions of usernames. Attackers may also use a commonly used weak password, such as "Password123," to search through a database of usernames for a match.

5. Credential Stuffing : Credential stuffing preys on users' weak password etiquettes. Attackers collect username and password combinations they have stolen, which they then test on other websites to see if they can gain access to additional user accounts. This approach is successful if people use the same username and password combination or reuse passwords for various accounts and social media profiles.

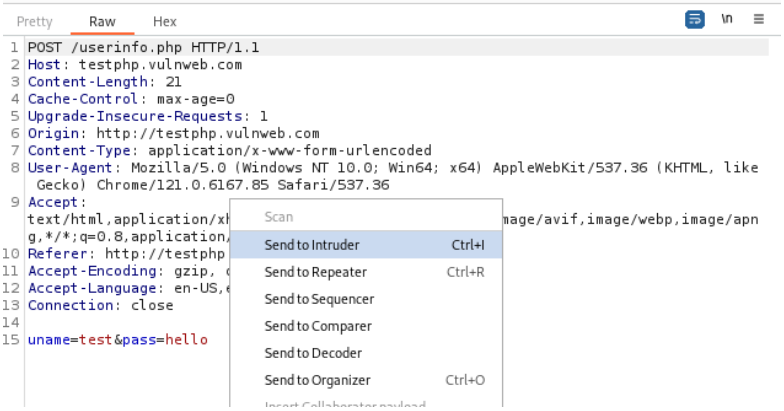
Working of Brute Force Attack :

<u>Brute Force using Burp Suite</u> :

Username is known with a random password and Intercept is Off

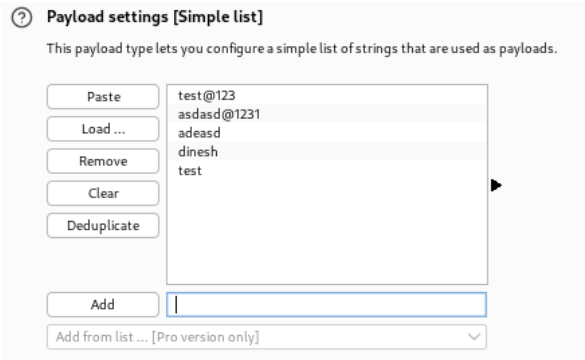


Intercept on and send the data to the intruder



Go to Positions and highlight the password as payload position

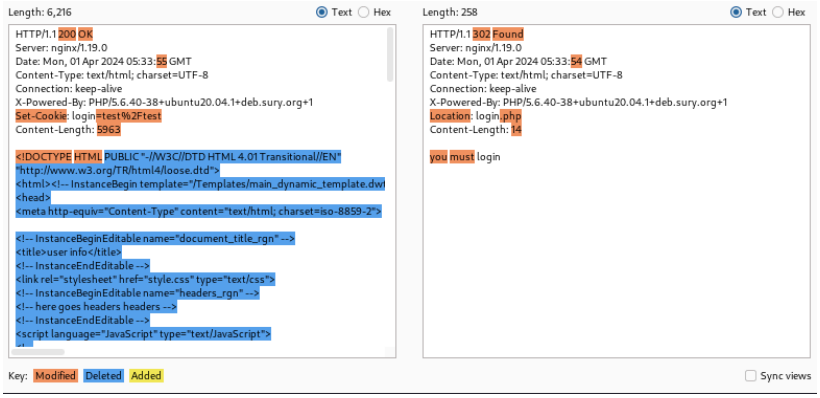
Go to PayLoad and add password to the list click on Start Attack



One with different status code or length would be the most possible correct password

Requ...	Payload	Status code	Error	Timeout	Length	Comment
0		302			258	
1	test@123	302			258	
2	asdasd@1231	302			258	
3	adeasd	302			258	
4	dinesh	302			258	
5	test	200			6216	

Compare two password by sending any two password to comparer and compare it by word or byte



Learning Outcomes:

The student should be able to understand various attacks using Burp Suite
LO1: To describe & understand Brute Force Attack
LO2: To implement Brute Force Attack

Course Outcomes: Upon completion of the course students will be able to understand & implement Brute force attack using Burp Suite.

Conclusion:

From this experiment, we were able to understand what Brute Force Attack is, its types and working and implemented the same using Burp Suite in Kali Linux.

For Faculty Use:

Correction Parameters	Formative Assessment [40%]	Timely completion of Practical [40%]	Attendance / Learning Attitude [20%]	
Marks Obtained				