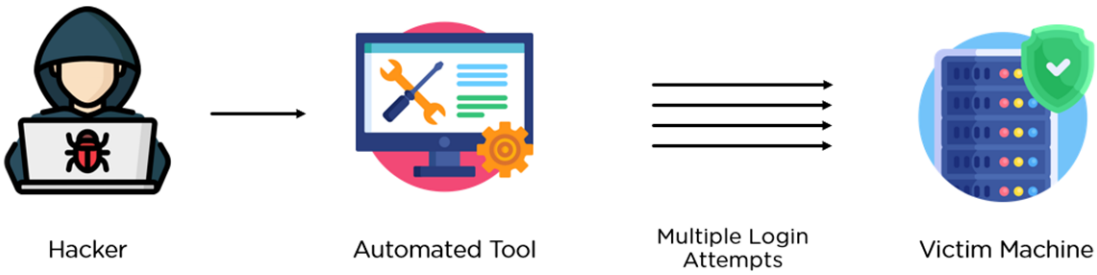
Report On Brute Force Attack Simulation



Anuja Panchariya

Brute Force Attack Simulation Report

Objective

The objective of this simulation is to demonstrate a brute force attack on a deliberately vulnerable web application, OWASP Bricks. The attack aims to identify valid credentials (username and password) by using automated tools and analyzing server responses.

Tools Used

The tools used in this simulation are:

1. Burp Suite (Community Edition): A powerful web vulnerability scanner and testing tool that provides automation for tasks like brute force attacks.

2. OWASP Bricks: A vulnerable web application designed for training and testing security tools and skills.

Setup and Steps

1. Target Configuration

The target application for this simulation was hosted at:

URL: http://192.168.1.69

The vulnerable login endpoint accepts the following parameters in a POST request:

username=$test$&passwd=$test$&submit=Submit

Positions for the username and password were marked in Burp Suite for inserting payloads.

2. Payloads

Two sets of payloads were prepared for this attack:

- Payload Set 1 (Usernames): Included common usernames such as: admin, root, manager, user, etc.
- Payload Set 2 (Passwords): Included commonly used or default passwords, such as:
  12345, password, admin, default, etc.

These payloads were selected to mimic real world scenarios where attackers leverage default credentials or leaked username password combinations.

3. Attack Type

The Cluster Bomb attack type in Burp Suite was selected for this simulation. This method ensures that every username in the first payload set is paired with every password in the second payload set. The total number of combinations is calculated as: Payload Set 1 Count x Payload Set 2 Count

This exhaustive approach maximizes the chances of identifying valid credentials.

4. Execution

The attack was executed by configuring Burp Suite Intruder to send a sequence of HTTP POST requests to the target application. Each request included a unique username password pair generated from the payload sets. Burp Suite logged the server's response for each request, which was then analyzed to identify successful login attempts.

Findings

1. Response Analysis

The server's responses were analyzed to detect successful logins. Key indicators included:

- Response Length: A shorter or different length response indicated successful login.
- HTTP Status Code: A status code of 200 (OK) accompanied by specific messages or page redirects.
- Response Content: A unique page or confirmation message that differed from the failed login responses.

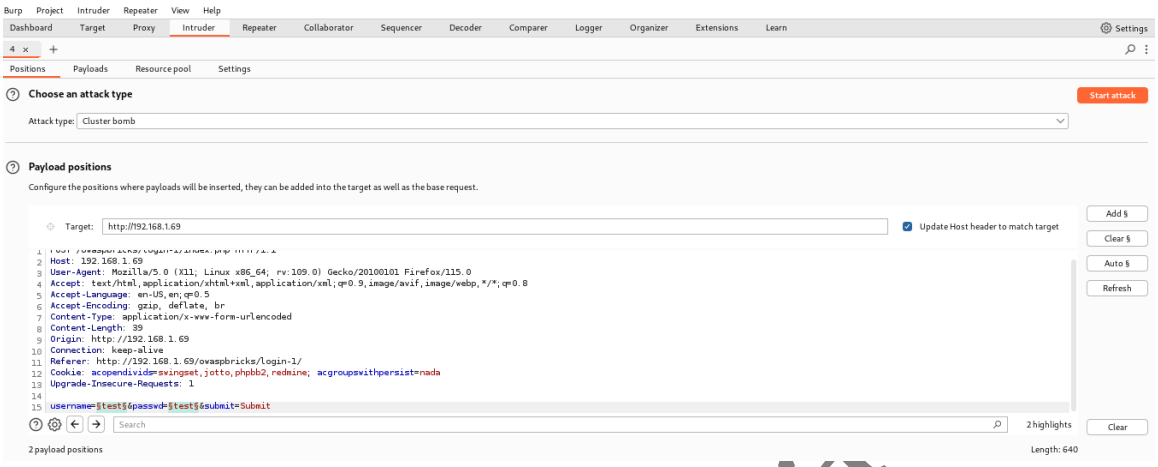
Using these indicators, the valid username password combination was identified successfully.

2. /etc/passwd File Usage

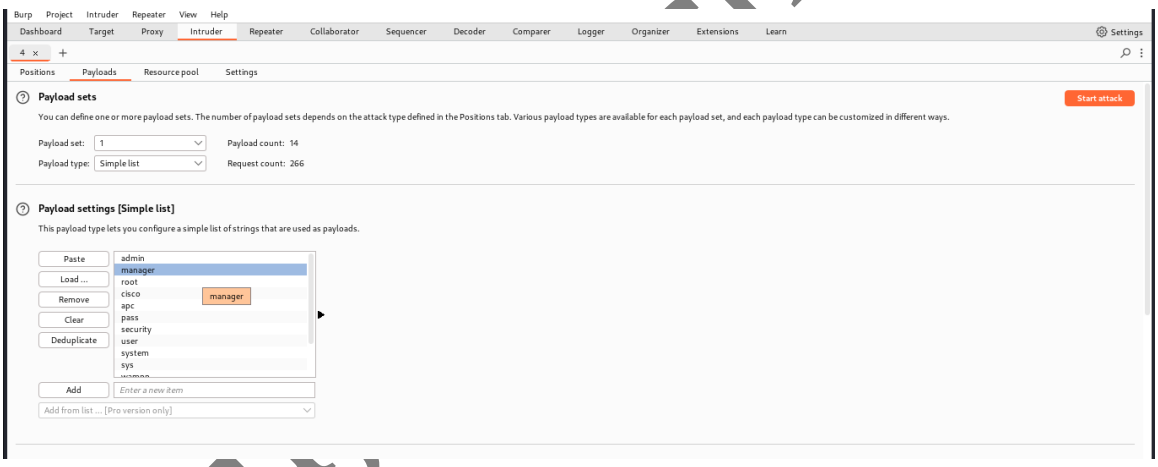
The simulation referenced potential usernames derived from the `/etc/passwd` file. This file, common in UNIX based systems, contains a list of system users. Attackers often extract this list to target default or poorly secured credentials.

Output :

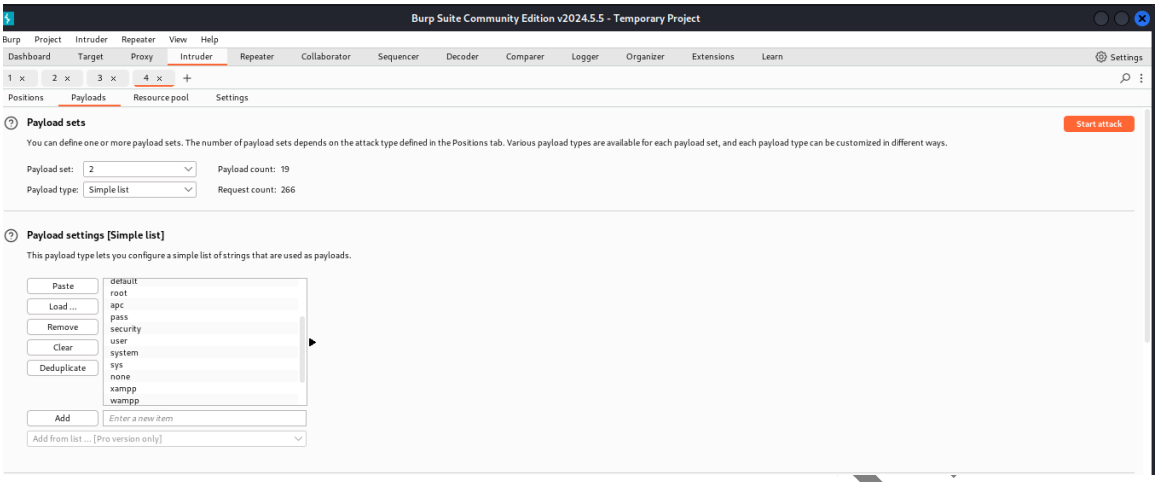
- Go to OWASP Bricks >Bricks>login >Intercept ON



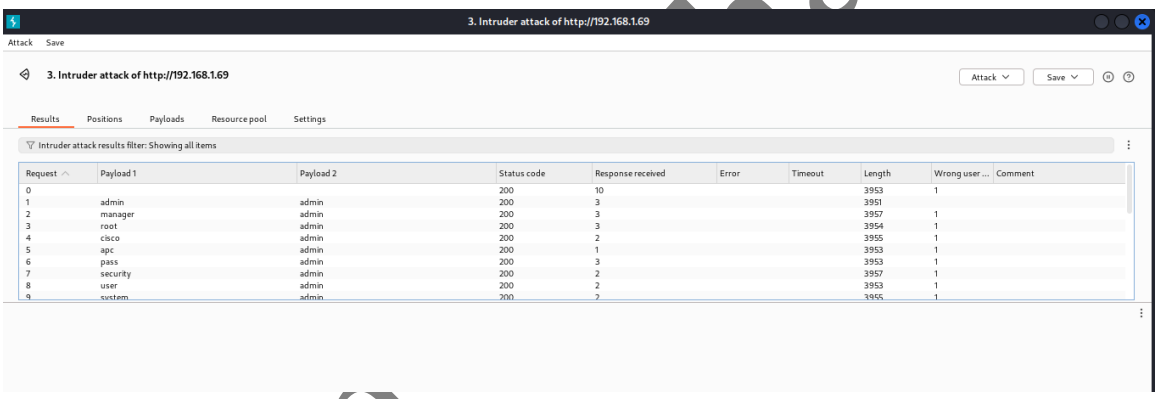
- Select payload type as 1 and import users



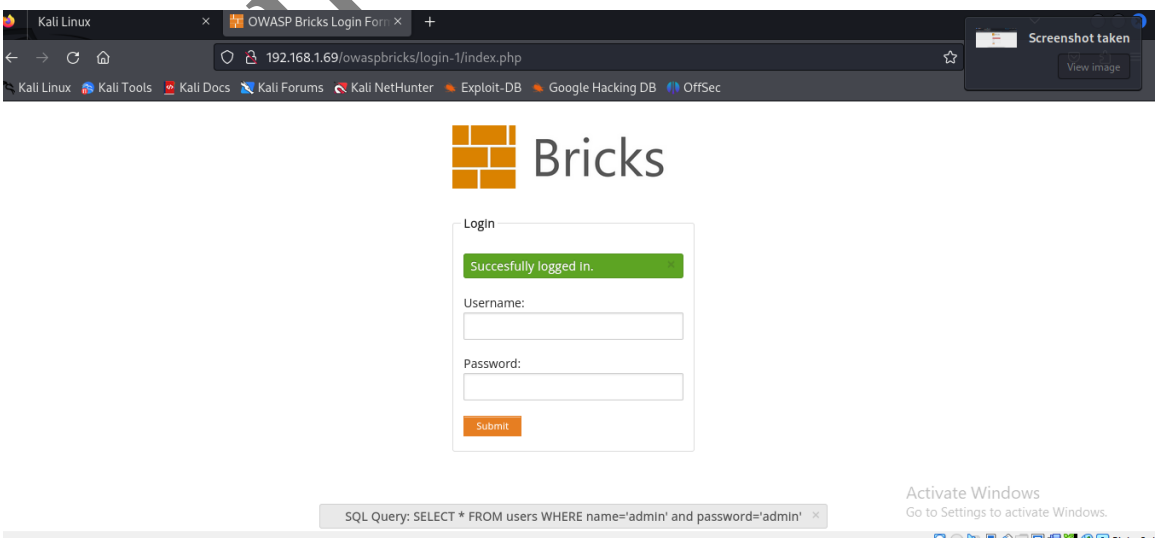
- Select payload type as 2 and import Password



- Go to options then grepmatch and you will find user and password .



- You successfully logged in!



Recommendations

1. Mitigation Strategies

- Account Lockout Policies: Implement account lockout mechanisms after a defined number of failed login attempts.
- CAPTCHA Integration: Use CAPTCHA on login pages to prevent automated attacks.
- Strong Password Policies: Enforce policies requiring users to create strong, unique passwords.

2. Best Practices

- Monitor Login Attempts: Regularly monitor and analyze failed login attempts for patterns indicative of brute force attacks.
- Secure Default Accounts: Disable default accounts or change their default credentials.
- Regular Security Audits: Periodically audit web applications to identify and patch vulnerabilities.
- System Updates: Ensure all applications and systems are updated with the latest security patches.

Conclusion

This simulation of a brute-force attack on a vulnerable application, OWASP Bricks, demonstrated the effectiveness of automated tools like Burp Suite in identifying weak or default credentials. The exercise highlighted the critical importance of implementing robust security measures to protect against such attacks.

The findings underscore the necessity for organizations to enforce strong password policies, implement account lockout mechanisms, and regularly monitor system logs for suspicious login activity. By adopting proactive security practices, organizations can significantly reduce the risk of unauthorized access and data breaches.

It is important to note that this simulation was conducted in a controlled environment for educational purposes. Organizations should always prioritize legal and ethical guidelines when conducting penetration tests or using vulnerability assessment tools.