#### Project report on

**Brute forcing password using SSH**

**A Dissertation submitted in partial fulfillment of the Academic requirements for the award of the degree of**

**Bachelor of Technology**

## In

**Computer Science & Engineering (Cyber Security)**

**Submitted by**

GUDALA DHEERAJ - 22H51A6218

MARMAMLA SUMA - 22H51A6233

NAYAKWADI SAHITHI - 22H51A6236

**Under the esteemed Guidance of**

**Dr.R.Venkateswara Reddy (Associate Professor and HOD,CSC)**

**Department of Cyber Security**

**CMR COLLEGE OF ENGINEERING & TECHNOLOGY**

**(Autonomous)**

**(NAAC Accredited with ‘A+’ Grade & NBA Accredited) (Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)**

**KANDLAKOYA, MEDCHAL ROAD, HYDERABAD-501401**

#### CMR COLLEGE OF ENGINEERING & TECHNOLOGY

**(Autonomous)**

**(NAAC Accredited with ‘A+’ Grade & NBA Accredited) (Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)**

**KANDLAKOYA, MEDCHAL ROAD, HYDERABAD-501401**

**DEPARTMENT OF CYBER SECURITY**



#### CERTIFICATE

This is to certify that the Mini Project -1 report entitled “**Brute forcing password using SSH**” being submitted by **G. Dheeraj (22H51A6218), M. Suma (22H51A6233), N. Sahithi(22H51A6236)** in partial fulfillment for the award of **Bachelor of Technology in Computer Science and Engineering (Cyber Security)** is a record of bonafide work carried out his/her under my guidanceand supervision.

The results embodied in this project report have not been submitted to any other University or Institute for the award of any Degree.

U. Nirmala Nish Dr. R. Venkateswara Reddy

Assistant Professor Associate Professor & HOD

Dept. of CSC Dept. of CSC

#### ACKNOWLEDGEMENT

With great pleasure I want to take this opportunity to express my heartfelt gratitude to all the people

`who helped in making this project a grand success.

I am grateful to  **U. Nirmala Nishi**, Assistant Professor, Dept. of Computer Science and Engineering for her valuable suggestions and guidance during the execution of this project.

I would like to thank **Dr. R. Venkateswara Reddy**, Head of the Department of Computer Science and Engineering, for his moral support throughout the period of my study in CMRCET.

I am highly indebted to **Major Dr. V.A. NARAYANA**, Principal CMRCET, for giving permission to carry out this project in a successful and fruitful way.

I would like to thank the Teaching & Non- teaching staff of the Department of Computer Science and Engineering for their co-operation.

Finally, I express my sincere thanks to **Mr. CH. GOPAL REDDY**, Secretary, CMR Group of Institutions, for his continuous care. I sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project work.

G. DHEERAJ

(22H51A6218)

M. SUMA (22H51A6233)

N. SAHTHI (22H51A6236)

#### ABSTRACT

* Trying to guess or "brute force" SSH passwords, where you repeatedly try different combinations until one works, is both unethical and illegal.
* It violates privacy and security standards and can lead to serious consequences.
* If you're having trouble accessing a system, it's best to seek help from system administrators or support rather than attempting unauthorized access.
* There are proper procedures for password recovery or resetting that should be followed instead of resorting to such methods.

**Table Of Content**

|  |  |  |
| --- | --- | --- |
| **CHAPTERS** | **DESCRIPTION** | **PAGE NUMBERS** |
| 1 | INTRODUCTION | 2 |
| 1.1 | AIM | 3 |
| 1.2 | SCOPE | 4 |
| 2 | LITERATURE REVIEW | 6 |
| 3 | EXISTING SOLUTIONS | 8 |
| 4 | PROPOSED SYSTEM | 11 |
| 4.1 | REQUIREMENT ANALYSIS | 12 |
| 4.1.1 | HARDWARE REQUIREMENTS | 12 |
| 4.1.2 | SOFTWARE REQUIREMENTS | 12 |
| 4.2 | MERITS AND DEMERITS | 13 |
| 5 | DESIGN DESCRIPTION | 15 |
| 5.1 | CONCEPTUAL DESIGN | 15 |
| 6 | IMPLEMENTATION AND DISCUSSION | 16 |
| 6.1 | IMPLEMENTATION | 17 |
| 7 | RESULT | 20 |
| 8 | CONCLUSION AND FUTURE ENHANCEMENT | 21 |
| 8.1 | CONCLUSION | 21 |
| 8.2 | ENHANCEMENT | 21 |
| 8.3 | REFERENCES | 24 |

# CHAPTER 1

1

#### INTRODUCTION

* Brute forcing SSH passwords represents a serious threat to the integrity of systems and data.
* This malicious technique involves automated or manual attempts to guess login credentials by systematically trying various combinations of usernames and passwords.
* Despite its simplicity, brute forcing poses significant risks, including unauthorized access, data breaches, and potential legal repercussions.
* Understanding the implications of brute force attacks underscores the importance of implementing robust security measures, such as multi-factor authentication and password policies, to defend against such threats.
* Effective cybersecurity strategies are essential for protecting sensitive information and maintaining the trust of users and stakeholders in the digital landscape.

#### AIM

* Brute force SSH attacks systematically attempt username and password combinations to gain unauthorized access to remote systems, posing a serious cybersecurity threat.
* Weak or commonly used passwords are exploited, leading to potential data breaches and compromised system integrity.
* Effectively detecting and mitigating these attacks requires implementing strong password policies, multi-factor authentication, and intrusion detection systems.
* Safeguarding against brute force SSH attacks is crucial to maintaining the security of sensitive information in the digital realm.

#### SCOPE

* + Brute force SSH attacks work by systematically trying different username and password combinations to gain unauthorized access to remote systems.
  + Attackers use automated tools to repeatedly test these combinations until they find the correct credentials.
  + They exploit weak or commonly used passwords to breach system defenses.
  + To prevent such attacks, organizations should implement strong password policies, multi-factor authentication, and intrusion detection systems.
  + Regular monitoring and updating of security protocols are essential to thwart unauthorized access attempts and safeguard sensitive data.

# CHAPTER 2

#### LITERATURE REVIEW

**Methods and Tools for Brute-Forcing SSH**

**1.1. Techniques**:

Brute force attacks on Secure Shell (SSH) protocols involve systematically attempting various password combinations until the correct one is found, exploiting the weaknesses in password policies and user habits. SSH, widely used for secure remote command-line access, remains a prime target due to its critical role in network management. While Burp Suite, a comprehensive web security testing tool, is not traditionally designed for SSH brute forcing, its versatile intruder tool can be adapted for such tasks. This adaptation involves configuring Burp Suite to capture and modify SSH traffic, automating repeated login attempts using curated lists of common passwords. However, modern SSH implementations often incorporate defenses like rate-limiting and IP blocking, which challenge the effectiveness of brute force attacks and necessitate advanced strategies, such as distributed attacks from multiple IP addresses.

Despite the technical feasibility of using Burp Suite for SSH brute forcing, ethical and legal constraints must be rigorously observed. Unauthorized brute-forcing is illegal and unethical, emphasizing the need for explicit permission during penetration testing. Moreover, the evolving landscape of cybersecurity has led to the deployment of robust defenses, such as CAPTCHA, two-factor authentication (2FA), and account lockout policies, which significantly mitigate brute force risks. The literature underscores the importance of these measures and the necessity for strong password policies to protect against unauthorized access. While Burp Suite remains a potent tool for security professionals, its application in brute force attacks should be carefully managed within legal and ethical boundaries.

# 

# CHAPTER 3

#### EXISTING SOLUTION

* The current approach to brute force attacks against SSH passwords involves using scripts and tools that systematically try different password combinations to gain unauthorized access.
* This method is often time-consuming and can be easily detected by security systems, putting the attacker at risk of being identified and blocked.
* To stop bad actors from breaking into systems via SSH brute force attacks, we have a few tricks up our sleeve.
* First off, we make sure people use strong passwords that are hard to guess.
* Then, we add an extra layer of security with something like a code sent to your phone when you log in.
* We also keep an eye on how many times someone tries to log in – if they're trying too much too fast, we block them automatically.
* Instead of using just passwords, we can use special keys that are much harder for the bad guys to crack.
* Robust security measures such as strong password policies, multi-factor authentication, and intrusion detection systems are commonly employed to mitigate brute force SSH attacks.
* These solutions aim to strengthen access controls, detect suspicious login attempts, and prevent unauthorized access to remote systems.
* Regular monitoring and updating of security protocols play a crucial role in identifying and addressing potential vulnerabilities to safeguard against such attacks effectively.

# CHAPTER 4

#### PROPOSED SYSTEM

* The proposed system will utilize a brute force attack to guess the SSH password of a target system.
* This will involve using a custom script to systematically try different password combinations until the correct one is found.
* The system will leverage a large dictionary of common passwords and passphrases to increase the chances of success.
* The system will also incorporate techniques to evade detection and bypass security measures, such as rotating IP addresses, using encrypted connections, and mimicking legitimate user behavior.
* This will allow the attack to proceed undetected and increase the likelihood of gaining unauthorized access to the target system.

**>ADVANTAGES OF PROPOSED SYSTEM:**

**1. \*\*Higher Success Rate\*\*:** With a large dictionary of common passwords and passphrases, the system may have a better chance of guessing the correct password compared to manual attempts.

**2. \*\*Efficiency\*\*:** Automated scripts make the brute force attack process faster and less labor-intensive than manual methods.

**3. \*\*Stealthy Approach\*\*:** Techniques like rotating IP addresses and using encrypted connections could help the attack go unnoticed by security systems.

**4. \*\*Tailored Attacks\*\*:** Custom scripts allow attackers to adapt their approach to the specific characteristics of the target system, potentially increasing effectiveness.

**5. \*\*Learning Opportunity\*\*:** Developing and using the system may provide attackers with insights into cyber security, albeit through unethical means.

#### REQUIREMENT ANALYSIS

##### Software Requirements

* + - * Windows 7 or later, Linux, or macOS
      * User Interface
      * Module to generate password combinations
      * SSH Connectivity
      * Burp suite community edition

##### Hardware Requirements

* Powerful CPU
* Ample RAM
* High-Speed Storage
* Dedicated GPU



##### MERITS AND DEMERITS Merits:

* Higher Success Rate
* Efficiency
* Stealthy Approach
* Tailored Attacks
* Learning Opportunity

##### Demerits:

* Inconvenience to legitimate users due to additional login steps.
* Inability to entirely prevent determined attackers from exploiting vulnerabilities.
* Resource-intensive maintenance and updating of security protocols.
* Risk of false positives in intrusion detection systems, leading to unnecessary alerts.

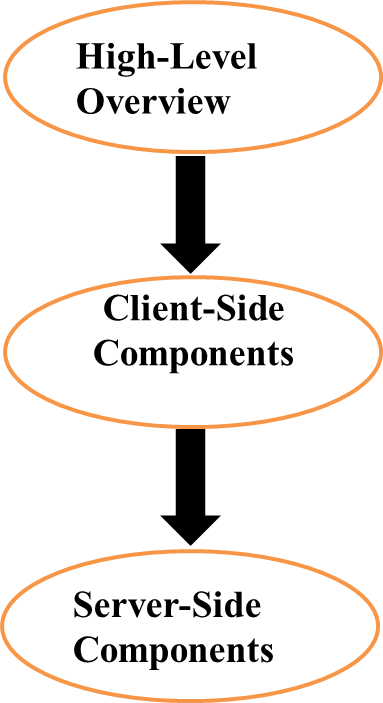
# CHAPTER 5

14

#### DESIGN DESCRIPTION

##### 5.1 CONCEPTUAL DESIGN

The diagram shows the steps involved in Brute forcing password using SSH.



**Fig 6:** Architecture for Brute forcing password using SSH

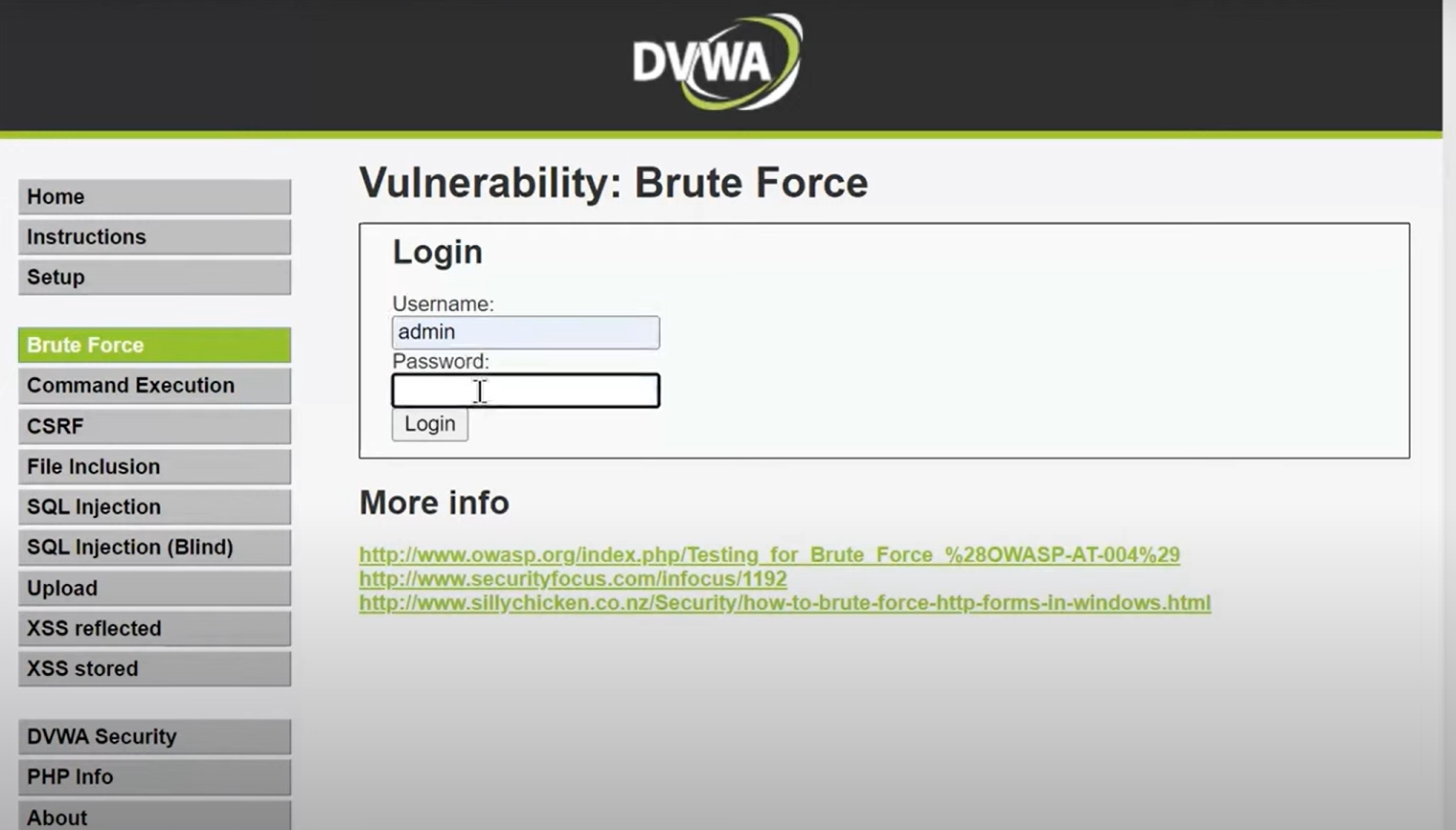
# CHAPTER 6

#### IMPLEMENTATION AND DISCUSSION

* 1. **IMPLEMENTATION**

**Brute force:**

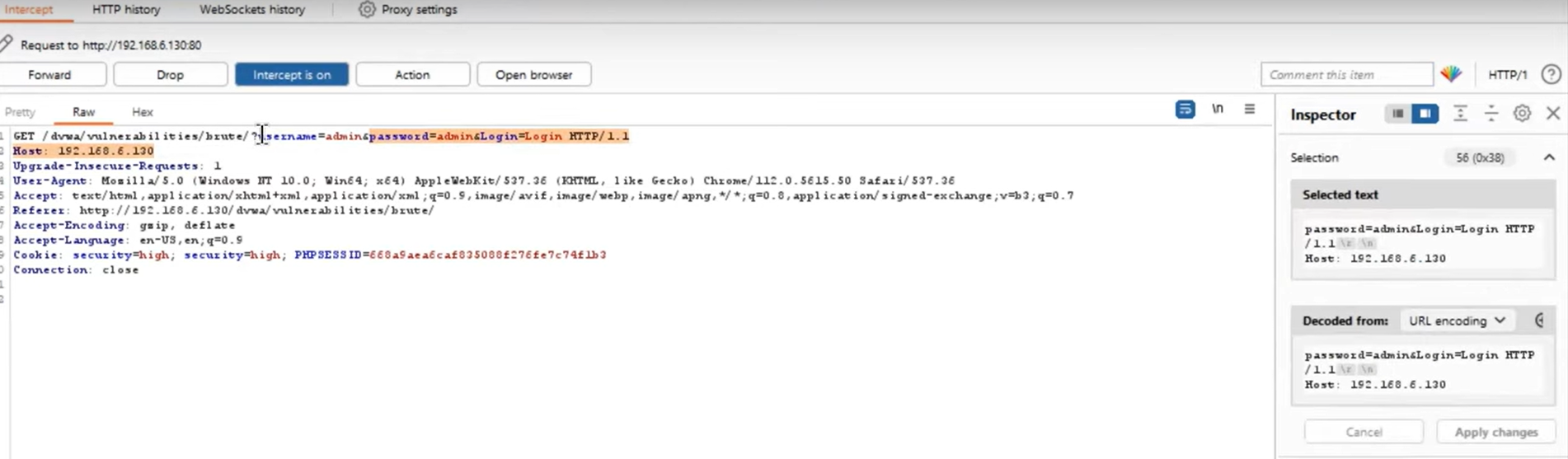
A brute force attack is a technique used by hackers to get into someone's account by guessing their login credentials. It is an uncomplicated approach for gaining unauthorized access to personal accounts, wherein the hacker repeatedly attempts various usernames and passwords until they manage to find the correct login information.

****

**Fig 6**

## Scanning:

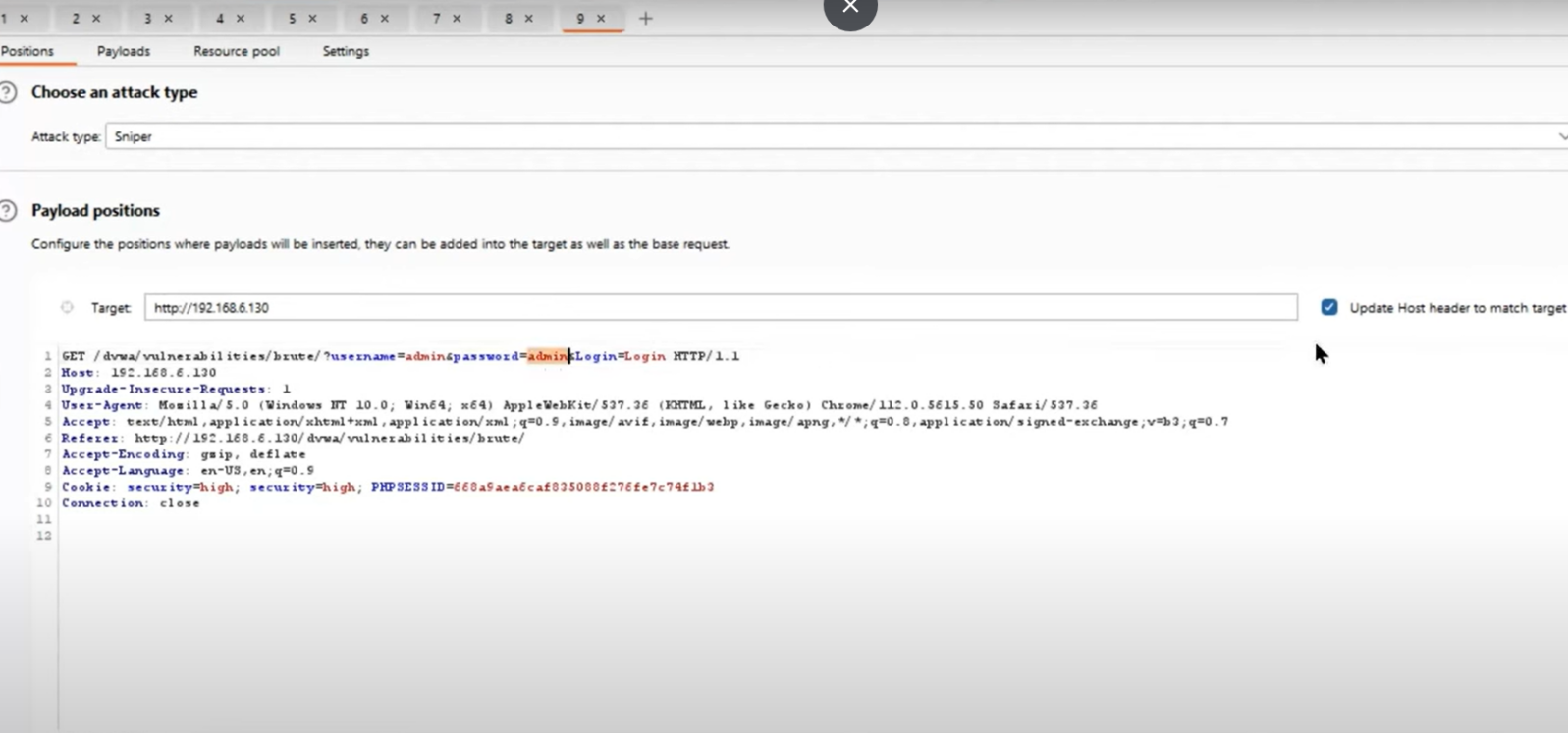
It is the methodical process of inspecting systems, applications, and networks to find any potential flaws, incorrect setups, or vulnerabilities.



**Fig 7:**Scanning

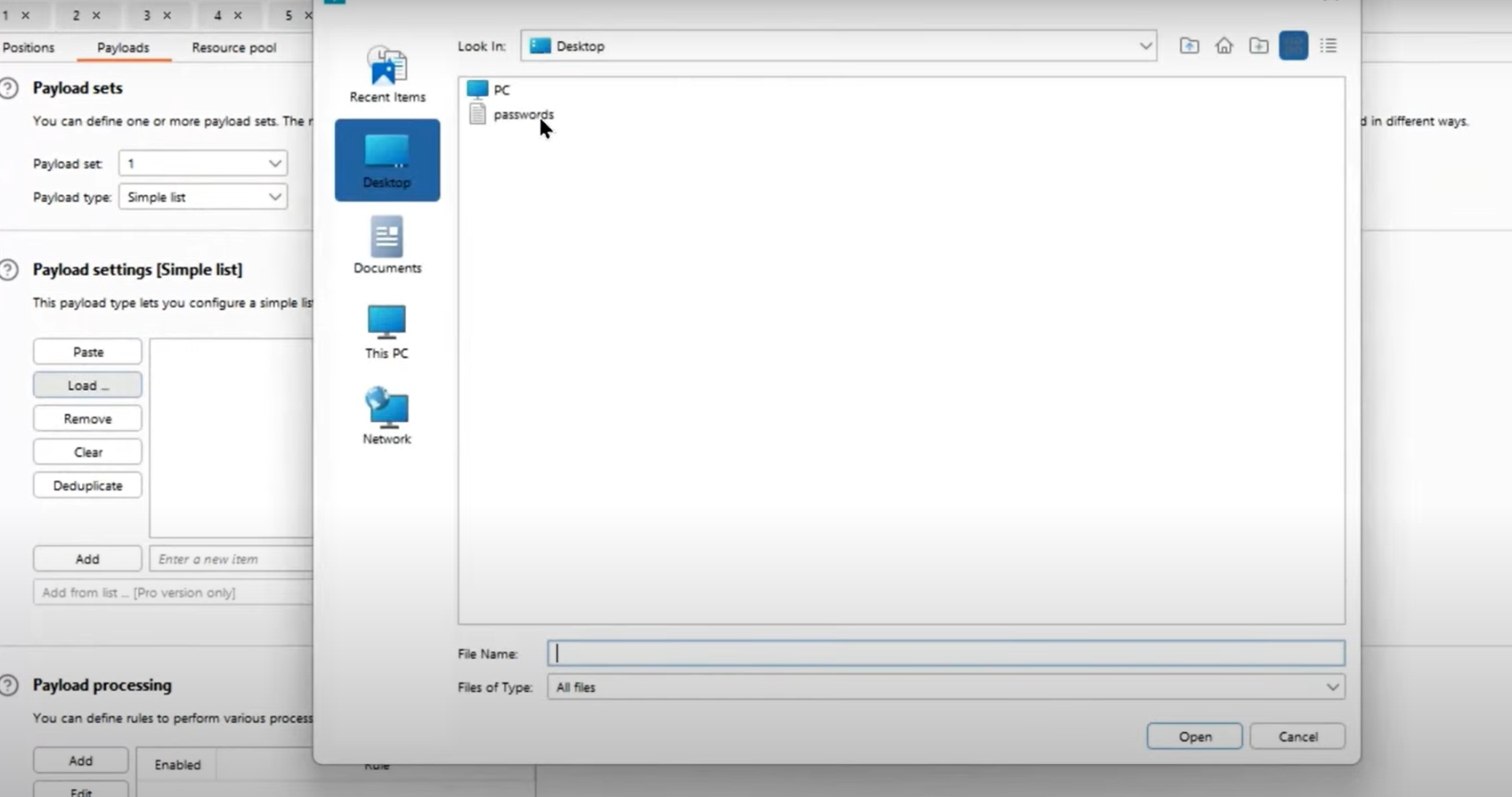
## Gaining access:

It is the phase where an attacker obtains control over the target. Be it a network or a web application, “Gaining Access” is only the beginning.



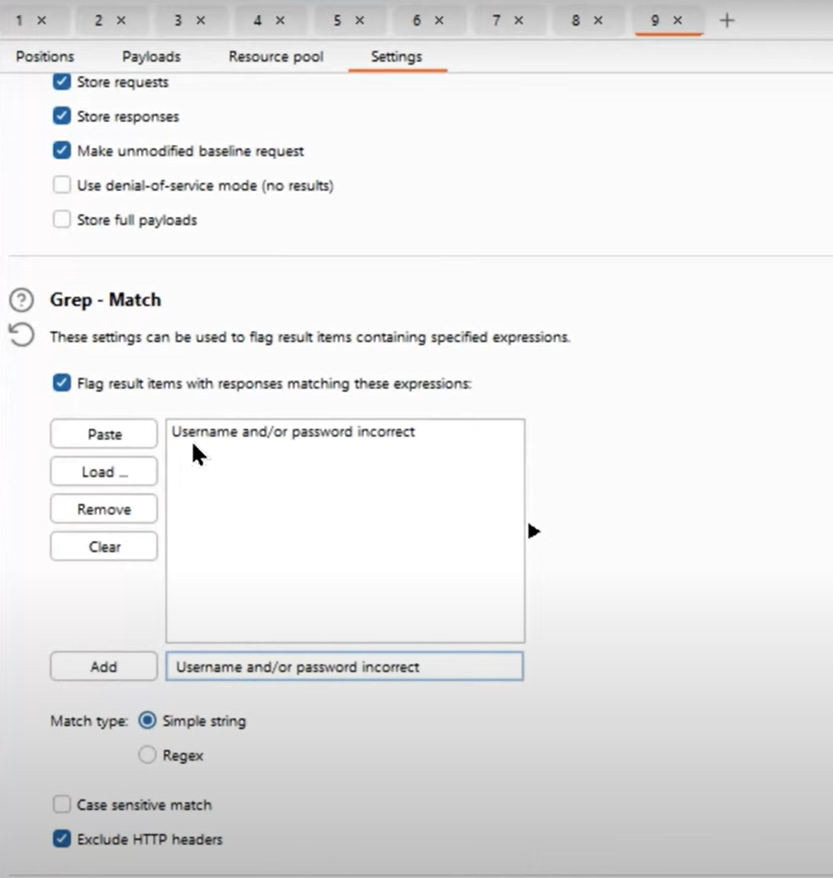
**Fig 8**

**LOAD:**

******

**Fig 9**

**FLAG RESULTS:**

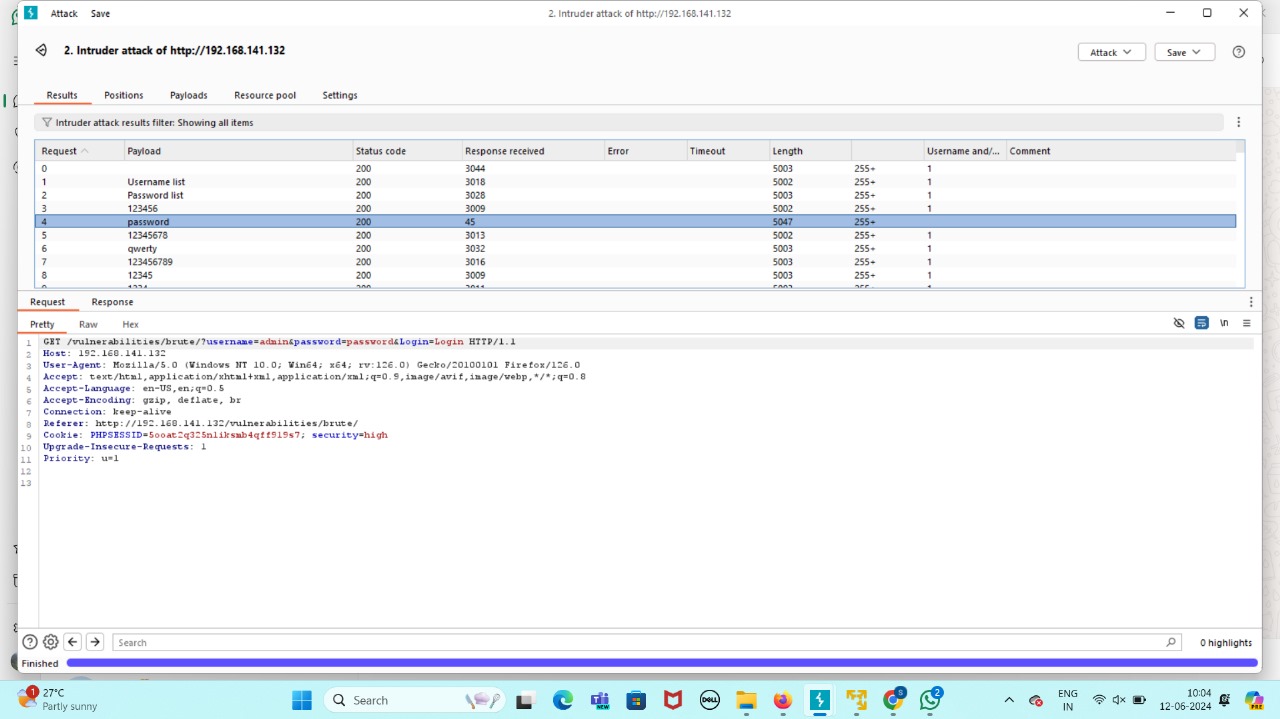
******

**Fig 10**

# CHAPTER 7

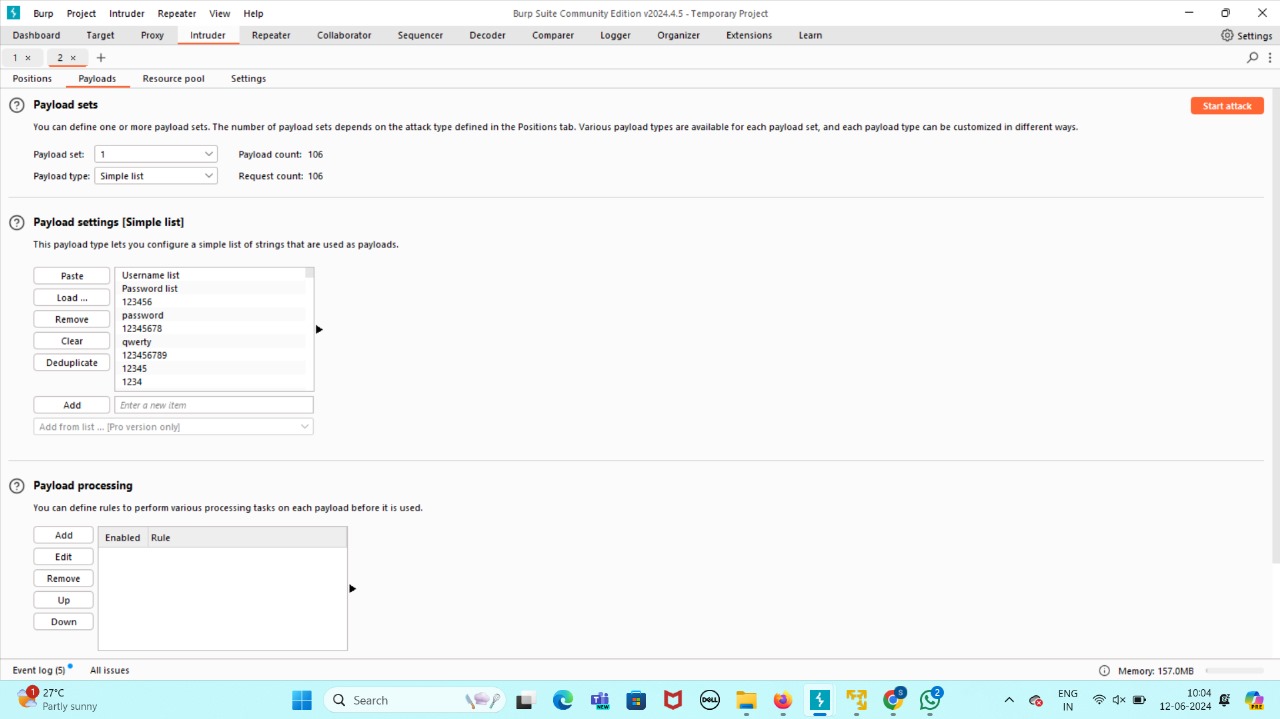
#### RESULT

we have successfully gained the access to the vulnerable system .Now we can take control of system



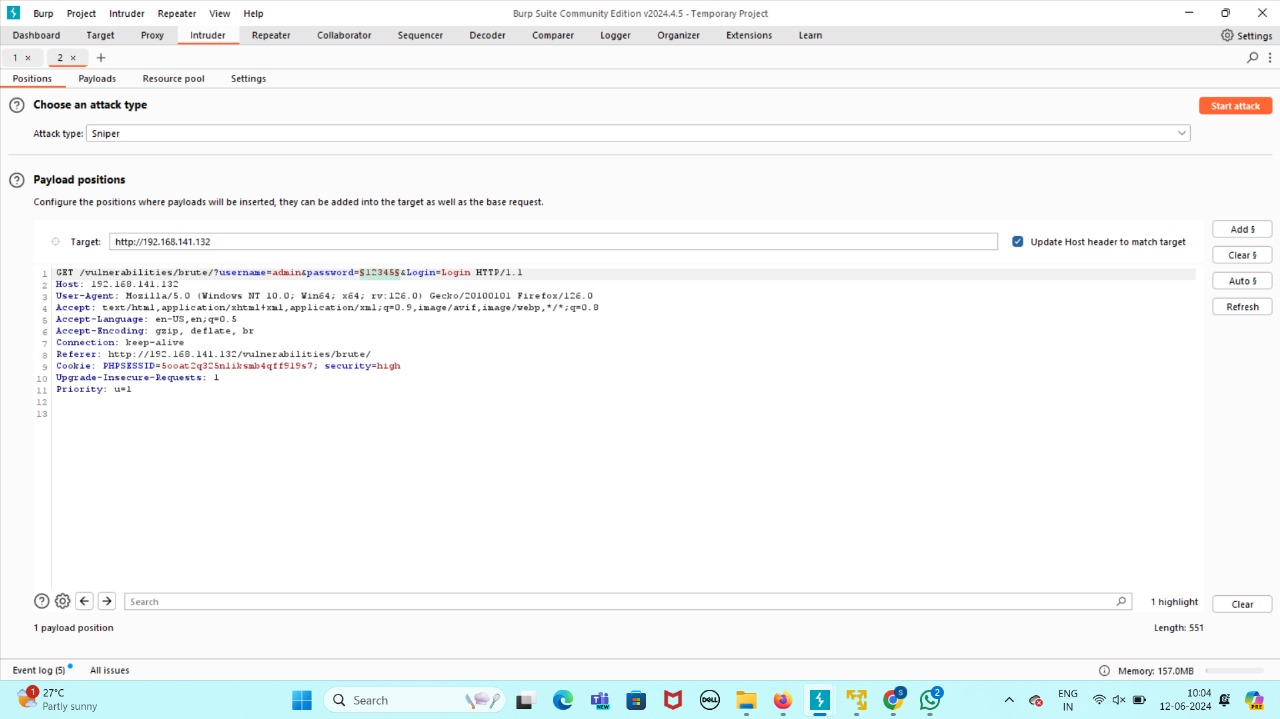
**Fig 11**

**Website interaface:**

****

**Fig 12**

## Uploading the report:

****

**Fig 13**

# CHAPTER 8

#### CONCLUSION AND FUTURE ENHANCEMEMT

##### 8.1. CONCLUSION

* Increase password Length (At least 14-character long)
* Increase password complexity (Mixed-case letters, digits, and special characters)
* Use multi-factor authentication (Password + Verification Code)
* Limit login attempts (Account lockouts after failed attempts)

##### FUTURE ENHANCEMENTS

brute force password attacks in Burp Suite could include optimized word list management with dynamic word lists that adapt based on previous successes and up-to-date password lists from leaked databases. Additionally, implementing multi-threading and distributed brute force attacks could significantly speed up the process by sharing the load across multiple machines. Enhancements in intelligent guessing, such as incorporating machine learning algorithms to predict and prioritize likely password candidates based on patterns and user behavior, could also increase the efficiency and success rate of these attacks.

#### REFERENCES

* **Research Papers**

Consult scholarly articles and papers on password cracking techniques, SSH security, and brute-force attack methodologies.

* **Online Tutorials**

Explore detailed online guides and tutorials on implementing SSH brute-forcing tools and understanding their inner workings.

* **Expert Blogs**

Read blog posts and insights from cybersecurity experts discussing the latest trends and best practices in password security.

* **Open-Source Projects**

Examine the source code and documentation of popular open-source SSH brute-forcing tools to learn from their implementation.