**COMPLETE APPLICATION TESTING**

**WITH OWASP TOP 7**

**VULNERABILITES**

**Project report submitted in fulfilment of the requirement for the award for the certificate program in Ethical Hacking and Cyber Security**

**In**

** Pace institute of technology &sciences**

**By**

**TUMMALA NAGALAKSHMI (22KQ1A05G2)**

**Cse- c**

**Under the esteemed guidance of**

**Sk. Prem Nazeer**

Certified Ethical Hacker

Licensed Pentester

ABSTRACT:

* Ethical Hacking: The need for cyber security

This abstract from the 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) discusses how hacking is a form of expertise that can be used for both ethical and unethical purposes. It also explains that ethical hackers, also known as white hat hackers, are legally authorized to use hacking techniques to improve security by identifying vulnerabilities before malicious hackers can exploit them. The abstract also mentions that the increasing number of attacks makes it important for people to learn ethical hacking concepts to protect themselves.

* Cybersecurity and cyber defence: national level strategic approach

This abstract from tandfonline.com discusses how cyber security is a broad range of practices, tools, and concepts that are closely related to information and operational technology (OT) security. It also notes that cyber security is unique in that it includes the offensive use of information technology to attack adversaries.

* A Study Of Cyber Security Challenges And Its Emerging ...

This abstract from researchgate.net discusses how cyber security plays an important role in the field of information technology, and how securing information has become a major challenge in today's world. It also mentions that cybercrimes are increasing rapidly, and that governments and companies are taking many measures to prevent them.

The initial very important step of system hacking is password cracking. There are both technical and non-technical methods to cracking a password: examples are Brute-Force Attack and Dictionary Attack for the former and Shoulder Surfing for the latter. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

*INTRODUTION:*

*Myntra was founded in 2007 by Mukesh Bansal, Ashutosh Lawania, and Vineet Saxena. The app serves millions of Indians and offers more than 200,000 items on any given day. Myntra is your one-stop lifestyle online shop. Explore the large variety of beauty, personal care & fashion products. It is a trendy online fashion app. Myntra offers the best online beauty products & online shopping.*

# 

# Application Type: ONLINE SHOPPING

# Languages available: TELUGU, TAMIL, ENGILSH etc….

# *Category: Myntra is an online shopping* app. It's one of India's leading e-commerce stores.

# It is a dynamic app (Up to date)

# Benefits:

* *Super Coins*
* *Rewards*
* *My Style Squad*
* *Priority customer care*

*Features:*

* *Experiences*
* *Product catalog*
* *Shopping assistance*
* *Delivery*
* *Returns and exchange*

## SQL injection:

SQL injection (SQLi) is a common attack vector that uses malicious SQL code to manipulate a database server behind a web application. Attackers can use SQLi to bypass security measures, access sensitive information, and execute unauthorized commands. SQLi attacks can have a wide range of negative impacts on a business, including: unauthorized viewing of user lists, deletion of entire tables, and attacker gaining administrative rights to a database.

SQLi attacks primarily target web applications that use SQL databases, such as MySQL, Oracle, or SQL Server. Attackers can inject malicious SQL code into input fields to manipulate database queries. For example, an attacker can log in as any user without a password by using an SQL comment sequence to remove the password check from a query *is that we can retrieve, delete ,manipulate and select the data from database.*

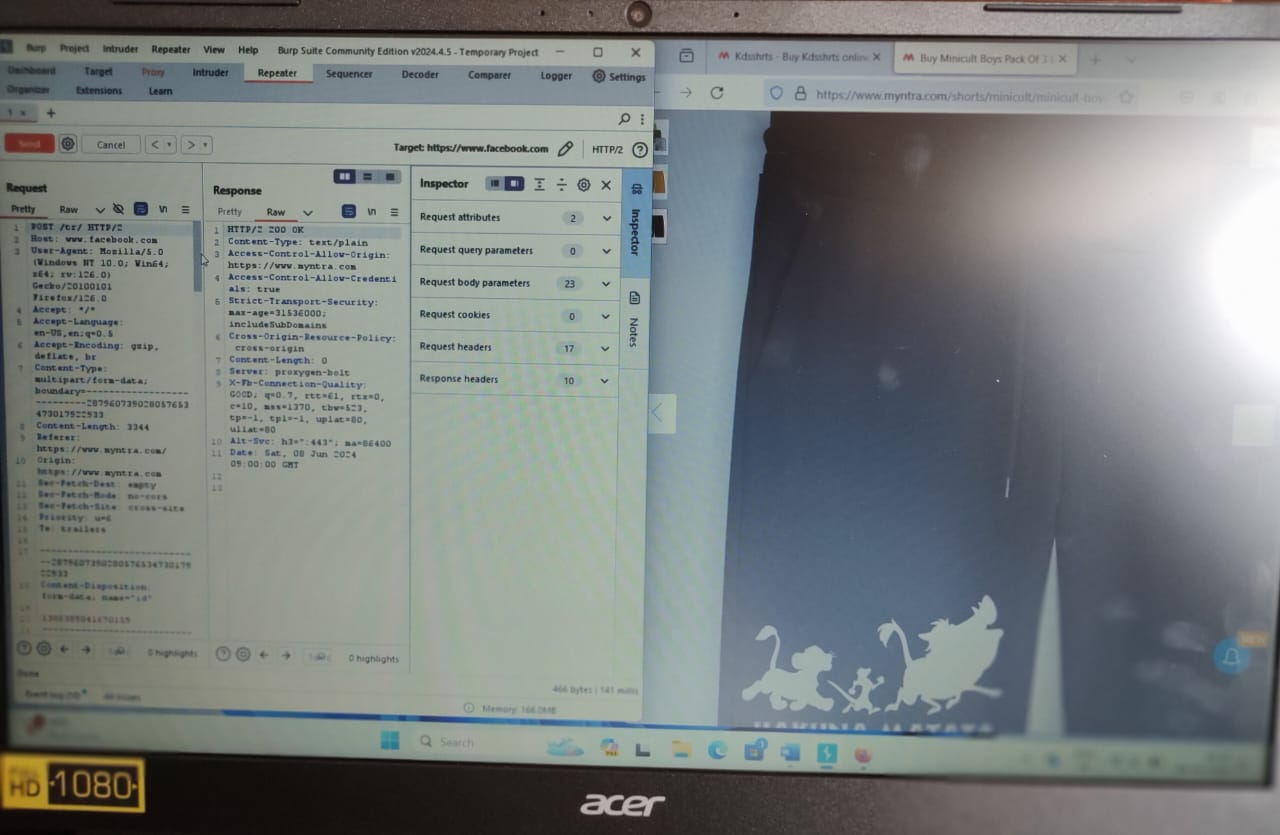
***Impacts of sql injection****:*

· **Data Theft:** *One of the most common objectives of SQL injection attacks is to steal sensitive data from databases. Attackers can manipulate SQL queries to extract information such as usernames, passwords, credit card numbers, and other personally identifiable information.*

· **Data Modification or Deletion*:*** *In addition to stealing data, attackers can use SQL injection to modify or delete existing data in the database. This can lead to loss of critical information, alteration of records, or disruption of services.*

### ***Methodology:***

*1.identify the vulnerabilities in any applications we want to use tool based burp-suite edition*



##### ***mitigation’s :***

***quality of product****: myntra can ensure strict quality control before dispatching items, provide detailed product descriptions and images, and enable customer reviews and ratings for better transparency****.***

***Return and return policies:*** *simplify the return process, provide clear guidelines, and ensure timely processing of refunds. offering free returns can also enhance customer trust****.***

***Conclusion:*** *I had done my sql injection in burp suite and it is not* *implemented*.

***2.cross site scripting:***

***Introduction:***

Cross-site scripting (XSS) is a type of security vulnerability commonly found in web applications. It occurs when a web application allows users to inject malicious scripts into web pages viewed by other users. These scripts are typically written in JavaScript and can be executed in the context of a victim's browser, leading to various malicious activities such as stealing session cookies, accessing sensitive information, or performing actions on behalf of the victim.

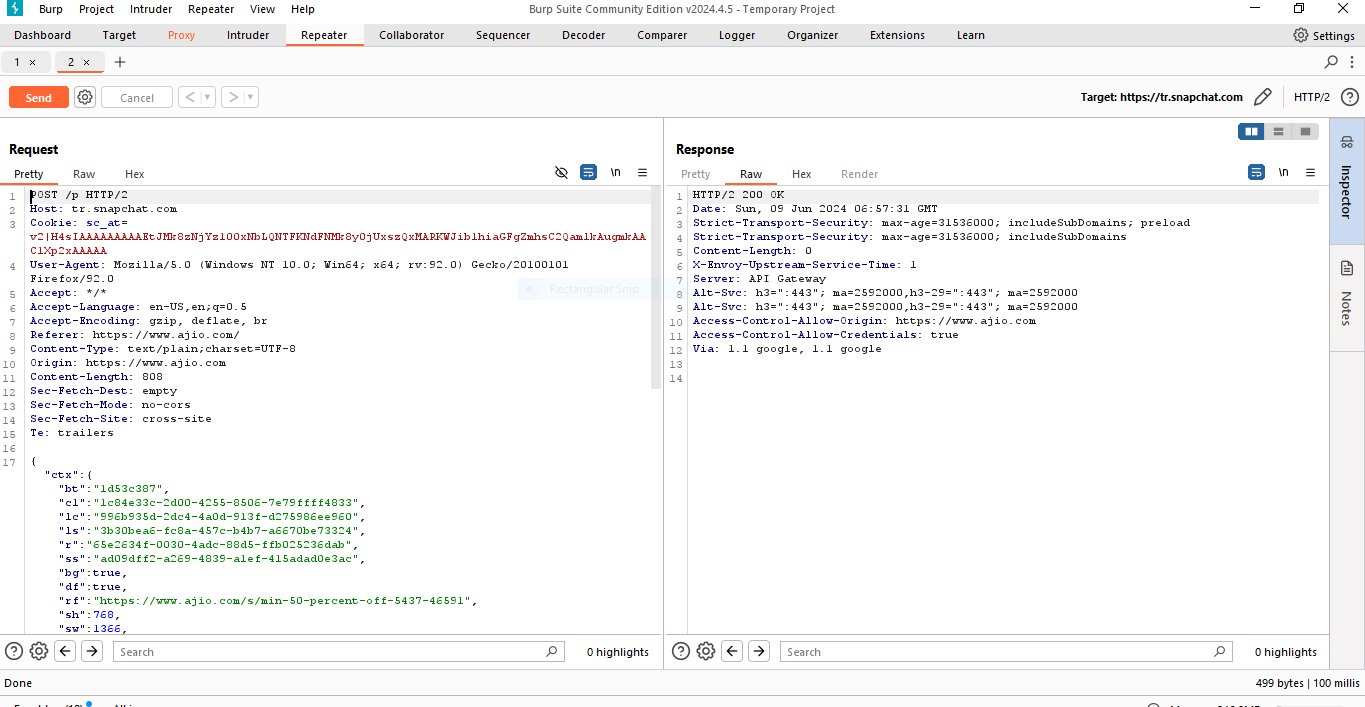
## ***Impacts of cross site scripting:***

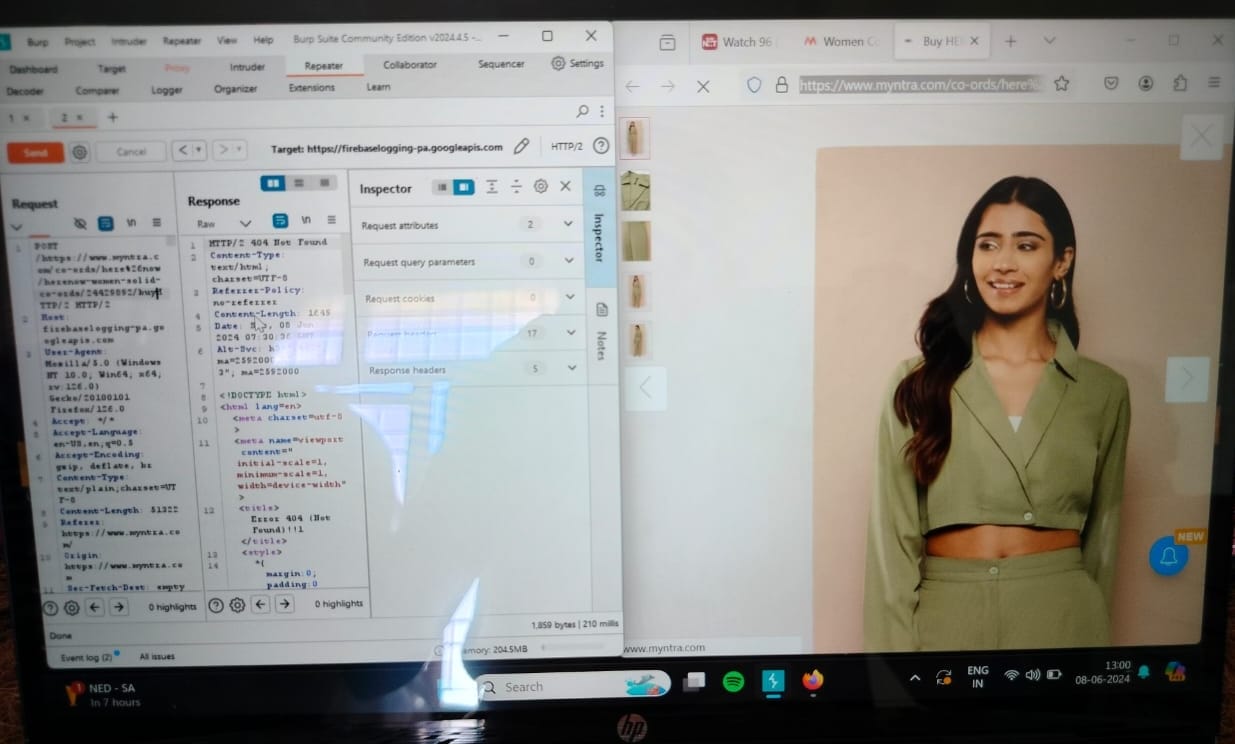
· **Session Hijacking:** *By stealing session cookies through XSS, attackers can hijack user sessions, effectively impersonating legitimate users and gaining unauthorized access to their accounts. This can lead to various malicious activities, such as unauthorized transactions, data manipulation, or identity theft.*

· **Session Hijacking:** *By stealing session cookies through XSS, attackers can hijack user sessions, effectively impersonating legitimate users and gaining unauthorized access to their accounts. This can lead to various malicious activities, such as unauthorized transactions, data manipulation, or identity theft*.

## ***Methodology:***

*1.identify the vulnerabilities in any applications we want to use tool based burp-suite edition*





*By using burp suite we can change the urls and vulnerabilities.*

## ***mitigation’s :***

***data security mitigations****: encryption of sensitive data, such as payment information, stored in database.*

***Access control:*** *implementing strict access controls and authentication mechanisms to prevent unauthorized access to systems and data.*

***Conclusion*:** *I had done my cross site scripting in burp suite and it is implemented*

## ***3.os commands site:***

## ***Introduction:***

*Command injection is a type of security vulnerability where an attacker can execute arbitrary commands on a host operating system by injecting malicious commands into a vulnerable application. These vulnerabilities typically arise when an application uses user-controllable input within a command sent to the operating system's shell or command interpreter without proper validation or sanitization.*

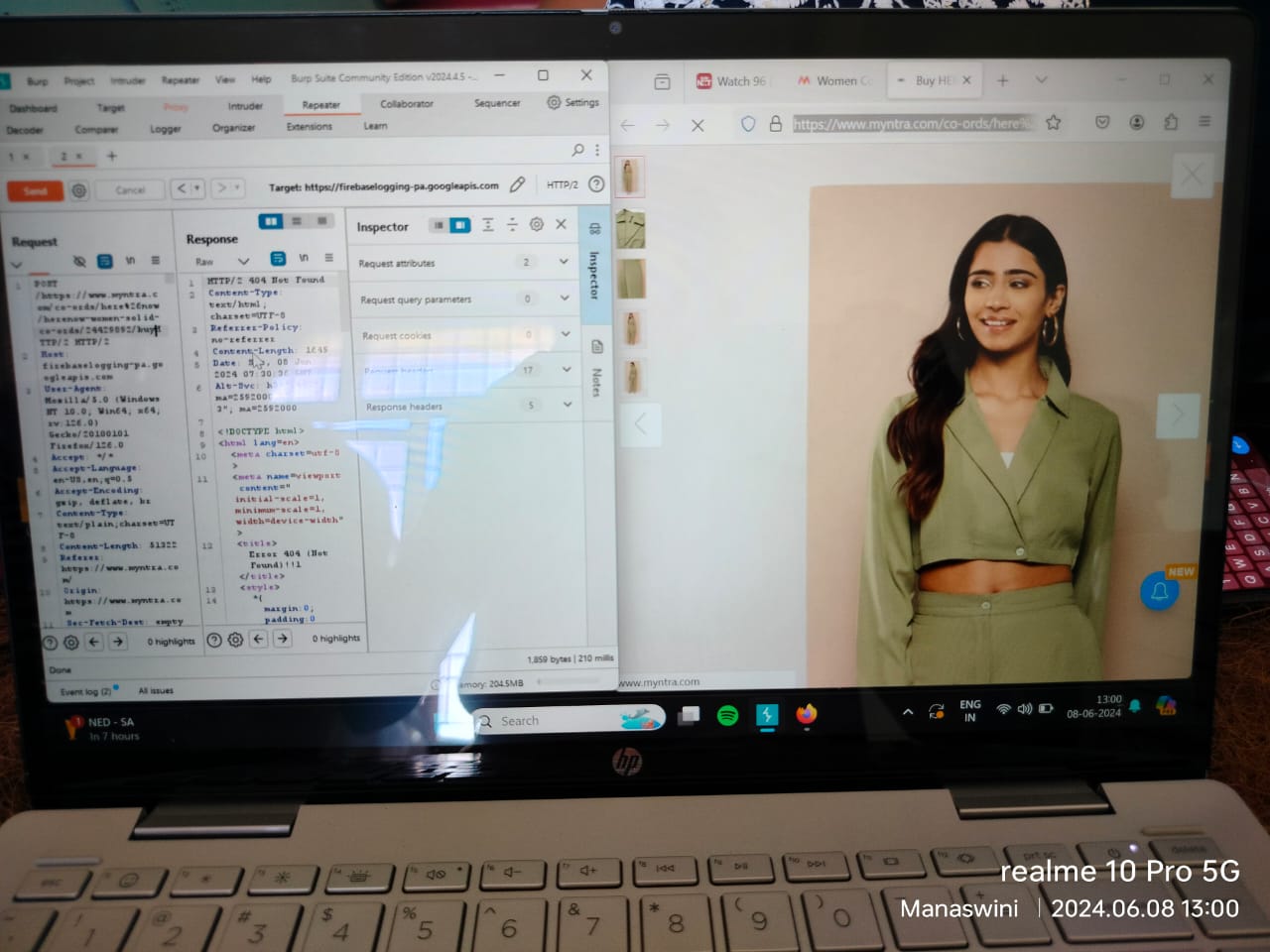
## ***Impacts of os commands site:***

· **Security Risks:** *Allowing users to execute OS commands opens up significant security risks. Malicious users can exploit this functionality to execute arbitrary commands on the server, potentially compromising the entire system.*

*·* ***Server Compromise*:** *If an attacker gains access to the underlying operating system through the site's command execution functionality, they could potentially take full control of the server. This could lead to further attacks, data breaches, or even the distribution of malware.*

## ***Methodology:***

*1.identify the vulnerabilities in any applications we want to use tool based burp-suite edition*



*By using burp suite we can change the urls and vulnerabilities.*

## ***mitigation’s :***

***Limit Access*:** *Restrict access to OS command execution functionality to only authorized users or administrators who require it for legitimate purposes. Implement strong authentication mechanisms, such as multi-factor authentication, to control access to sensitive features*.

***Input Validation*:** *Implement rigorous input validation to ensure that user-supplied commands are sanitized and restricted to prevent injection attacks. Validate input against a whitelist of allowed characters and commands, and reject any input that does not meet the specified criteria.*

***Conclusion:*** *I had done my os command site in burp suite and it is implemented*

## 4***.Authentication:***

## ***Introduction:***

*Authentication is the process of verifying the identity of a user. In the context of web security or computer systems, authentication typically involves the presentation of credentials, such as a username and password, to prove one's identity. The authentication process ensures that only authorized users are granted access to protected resources, while unauthorized users are denied access.*

***Username and Password:*** *This is the most common form of authentication, where users provide a combination of a username (or email address) and a secret password to prove their identity*.

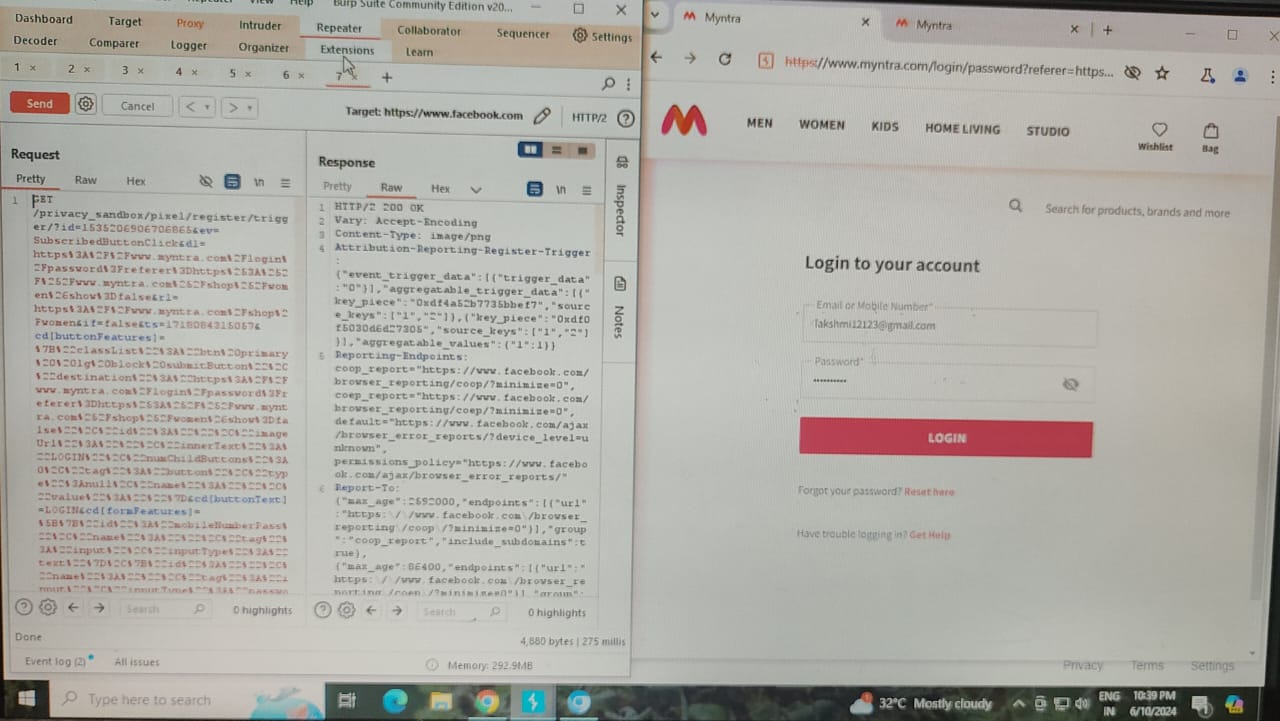
***Single Sign-On (SSO):*** *SSO allows users to authenticate once and gain access to multiple related systems or applications without having to re-authenticate for each one. This improves user experience while maintaining security.*

***Impact of Authentication***:

***Data Security*:** *Authentication plays a crucial role in safeguarding sensitive data from unauthorized access. By verifying the identity of users before granting access to resources, authentication helps prevent data breaches, data theft, and unauthorized modifications to sensitive information.*

## ***Methodology:***

*1.identify the vulnerabilities in any applications we want to use tool based burp-suite edition*

*By using burp suite we can change the urls and vulnerabilities.*

## ***Mitigations:***

· **Strong Password Policies*:*** *Enforce strong password policies that require users to create complex passwords that are difficult to guess. Require passwords to be a minimum length, include a mix of alphanumeric characters, and mandate regular password changes*.

· **Multi-Factor Authentication (MFA):** *Implement multi-factor authentication to add an extra layer of security. Require users to provide additional forms of identification beyond just a password, such as a one-time code sent to their mobile device, a biometric scan, or a hardware token.*

## ***Conclusion:***

## ***5. Directory or Path traversal:***

## ***Introduction:***

*Path traversal, also known as directory traversal or directory climbing, is a web security vulnerability that allows an attacker to access files or directories that are outside of the web server's root directory. This vulnerability arises when an application does not properly sanitize user input, such as file paths, before using it to access files or directories on the server's file system.*

## ***Impacts:***

*path traversal vulnerabilities pose significant risks to the security, integrity, and availability of web applications and servers. It's essential for organizations to proactively identify and mitigate these vulnerabilities to prevent potential security incidents and protect sensitive data.*

*One of the most significant risks of path traversal is that it allows attackers to access sensitive files or directories on the server that they shouldn't have access to. This could include configuration files, databases, user credentials, or any other sensitive data stored on the server.*

## ***Methodology:***

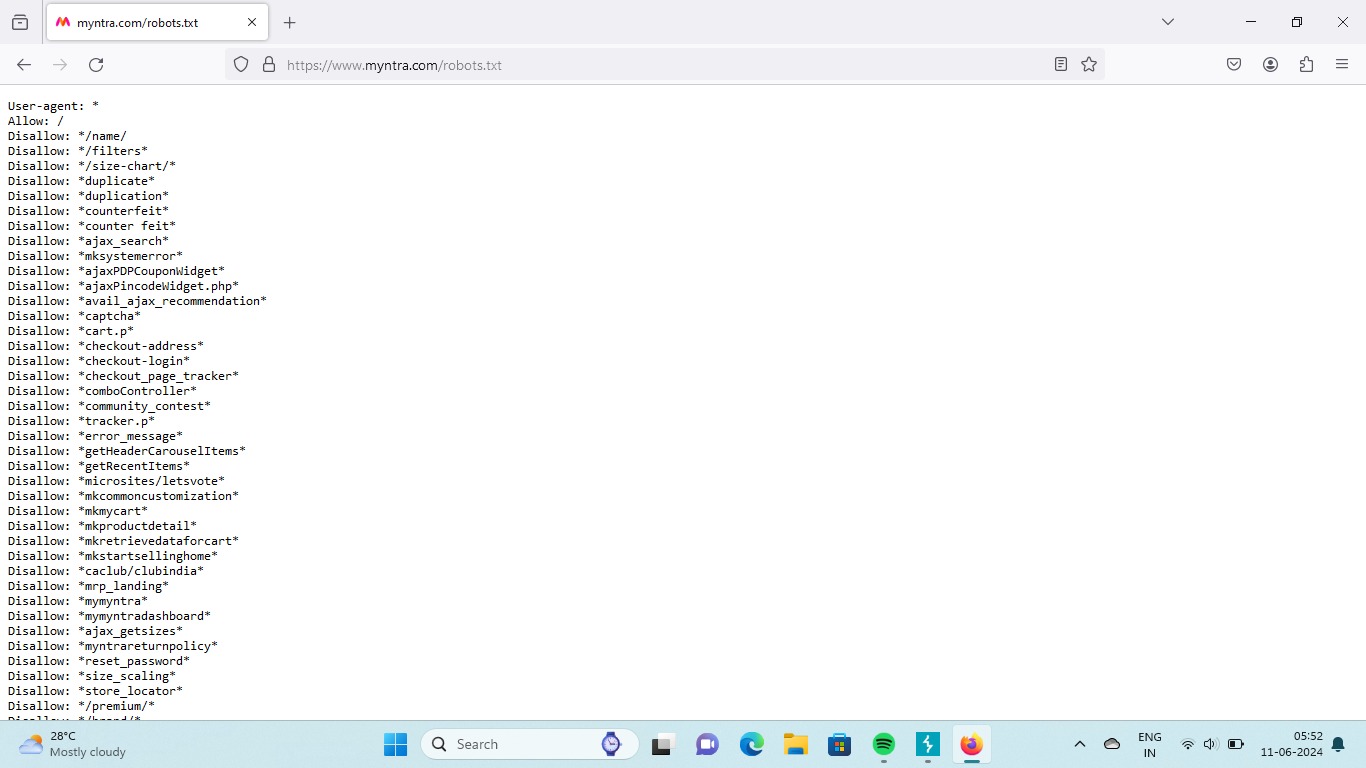
*The directory or path traversel is only solved manually.*

***Roobots.txt:***

*This is directory Path which is used to find all list of urls of entire application.*

*1)first open myntra homepage url and try directory paths after myntra like*

[*https://www.myntra.com/path*](https://www.myntra.com/path)

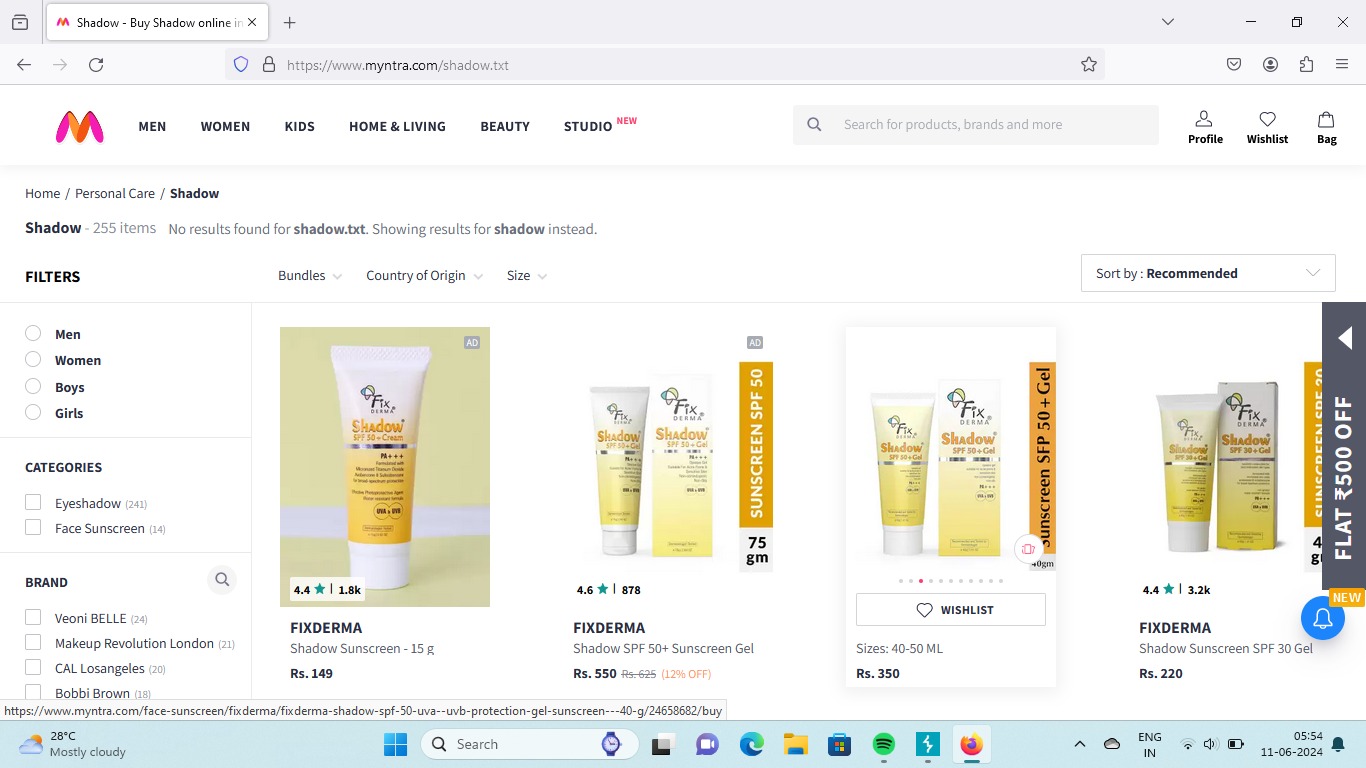


***Shadow.txt:***

*The shadow.txt path show hashed user names and passwords and other account related information which is placed in web application servers*

*That means the application servers have this shadow.txt directory then it acts like a vulnerabilities to give access to get another login credentials.*

*1)first open myntra home page and try to insert shadow.txt path after home page url*

***/etc/passed.txt:***

*The shadow.txt path show hashed user names and passwords and other account related information which is placed in web application servers*

*That means the application servers have this shadow.txt directory then it acts like a vulnerabilities to give access to get another login credentials.*

*1)first open myntra homepage url and try directory paths after myntra like*

*https://www.myntra.com/etc/passed.txt*

***/etc/passed.txt:***

*The shadow.txt path show hashed user names and passwords and other account related information which is placed in web application servers*

*That means the application servers have this shadow.txt directory then it acts like a vulnerabilities to give access to get another login credentials.*

*1)first open myntra homepage url and try directory paths after myntra like*

*https://www.myntra.com/etc/passed.txt*

***Teste.txt:***

*The teste.txt is directory path that useful to visit test case design in our web application.*

*1)first we have to open myntra home page and try to insert teste.txt path after myntra home page url.*

***Mitigations:***

*Mitigating path traversal vulnerabilities requires a combination of secure coding practices. Validate and sanitize all user input, particularly file paths, to ensure that they do not contain any unauthorized characters or sequences that could be used for path traversal.*

*Conclusion:* *We did path traversal with amazon application it doesnot seem any output in amazon application because we use normal burp suite community edition tool.*

***6.Brute force attack****:*

*Introduction:*

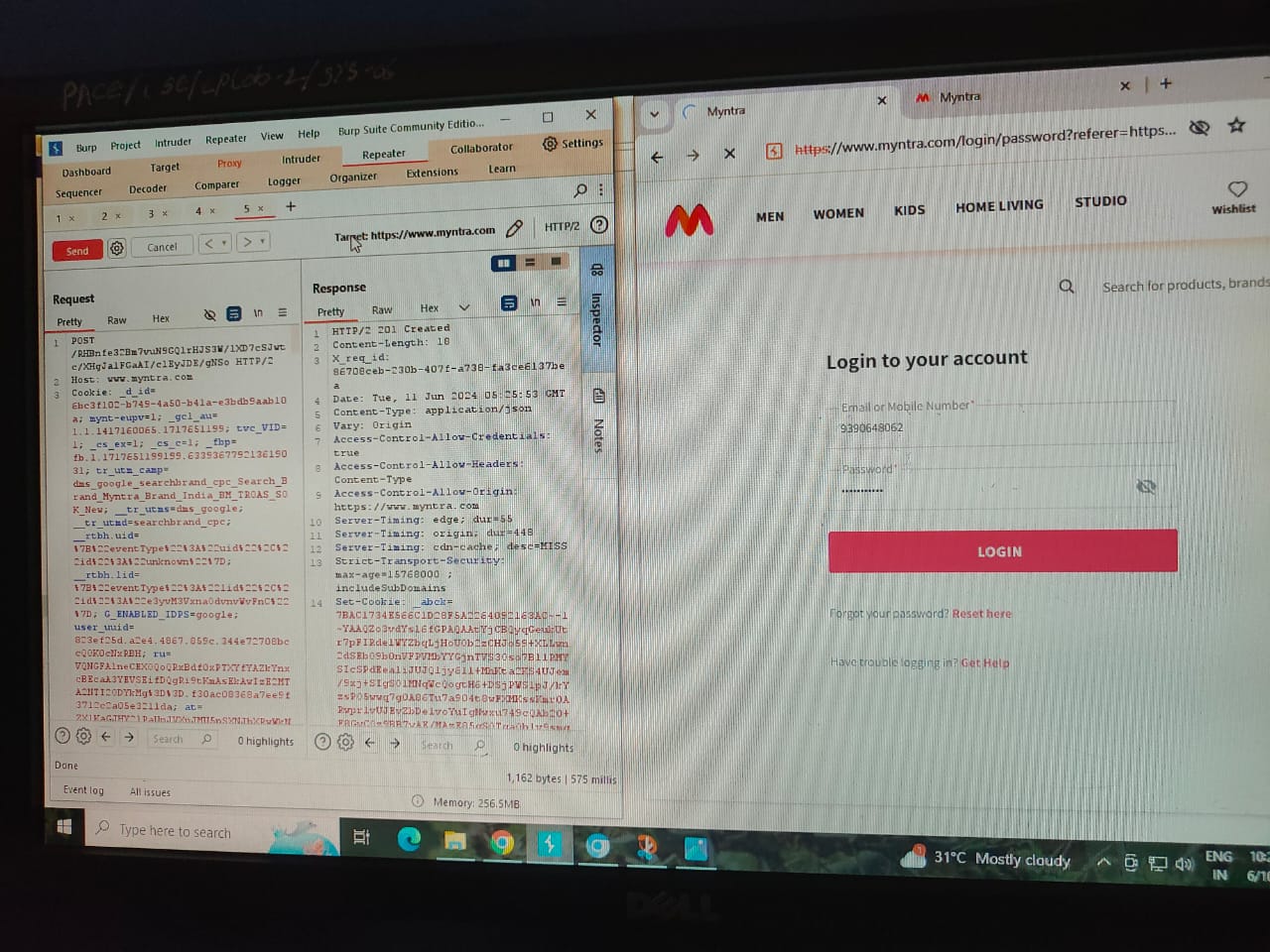
*A brute force attack is a type of cybersecurity attack where an attacker tries to gain unauthorized access to a system or an account by systematically trying all possible combinations of usernames, passwords, or encryption keys until the correct one is found. This method relies on the sheer computational power of the attacker's resources to try all possible combinations within a reasonable amount of time.*

## ***Impacts:***

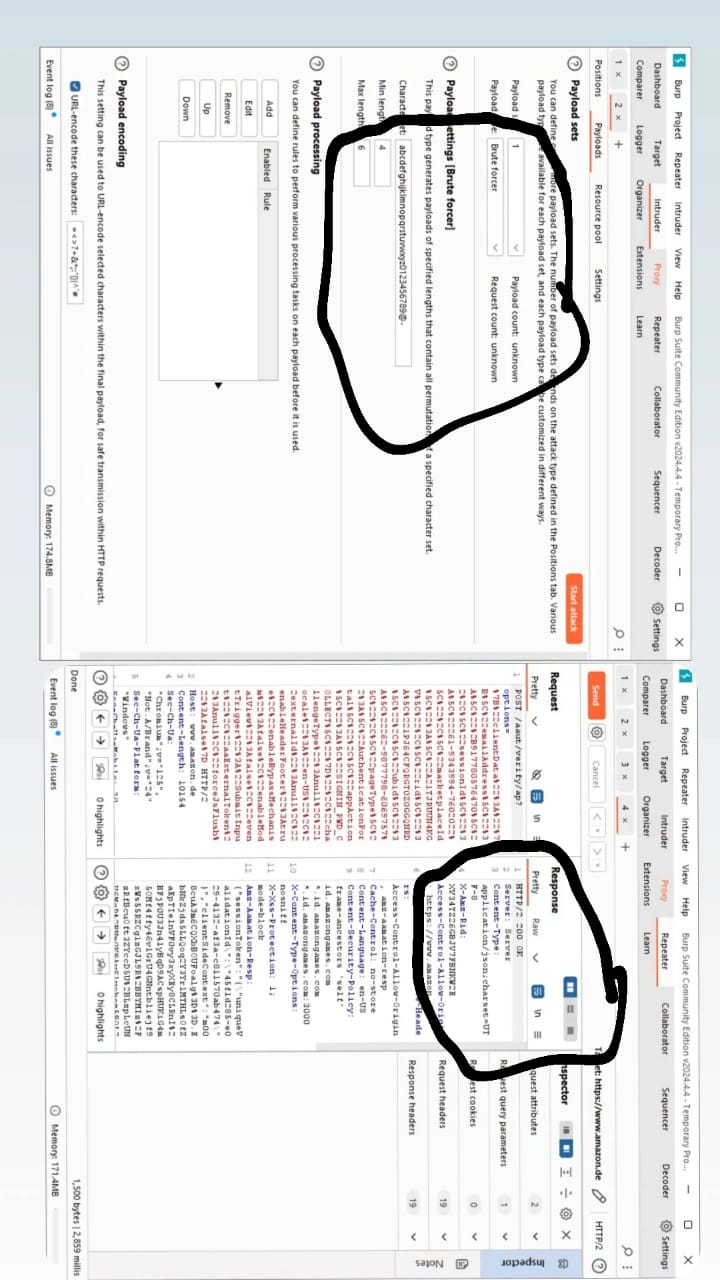
*The primary impact of a successful brute force attack is unauthorized access to user accounts, systems, or sensitive data. Attackers can gain control over accounts, steal personal information, manipulate data, or perform malicious activities on behalf of the compromised user.*

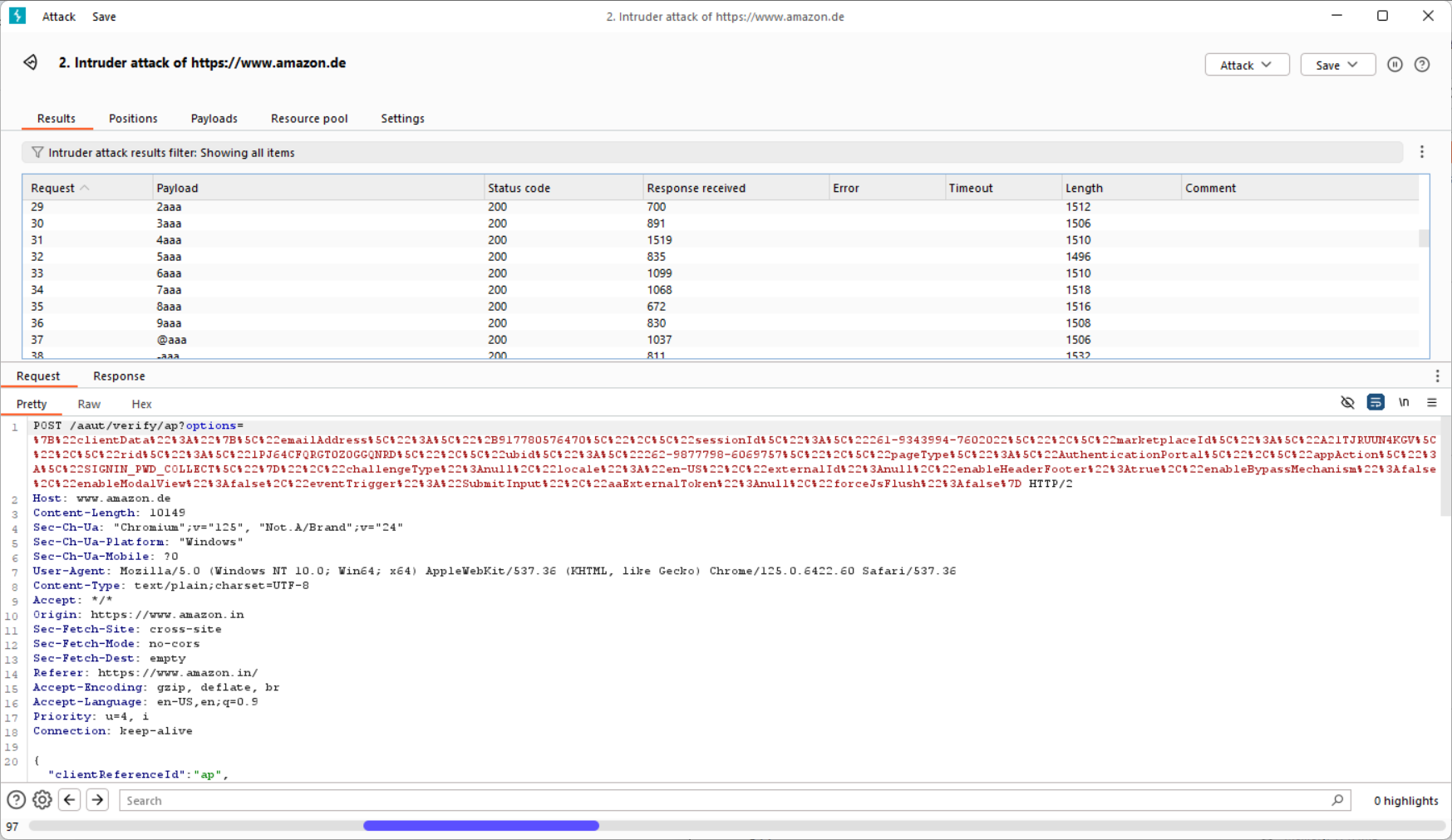
## ***Methodology:***

Step 1:*Firstly we have to login in myntra application next we have to login with our gmail (or)phone number& give a unreal password ,before sign in we have to on intercept in burp and next sign.*



*Step 2:When we on the intercept the code will appear as upper fig ,next we have to send the code to the repeater to see response. the response will seen as 200 Ok. Next we have to send the code to the intruder as shown in fig, in intruder we have to add positions. next set the payload type: brute forcer, give min length:4,max length:6 at last start attack*



Step 3:Here the result when we start attack,it takes lot of time to complete this.

## ***Mitigations:***

*Enforce strong password policies that require users to create complex passwords containing a mix of uppercase and lowercase letters, numbers, and special characters. Discourage the use of easily guessable passwords, such as dictionary words or common phrases.*

Conclusion: We take myntra application to test the OS command injection vulnerability, we did the steps ,in our app it does not seem any result because we use normal burp suite community edition tool

## ***7.Server side request forgery:***

## ***Introduction:***

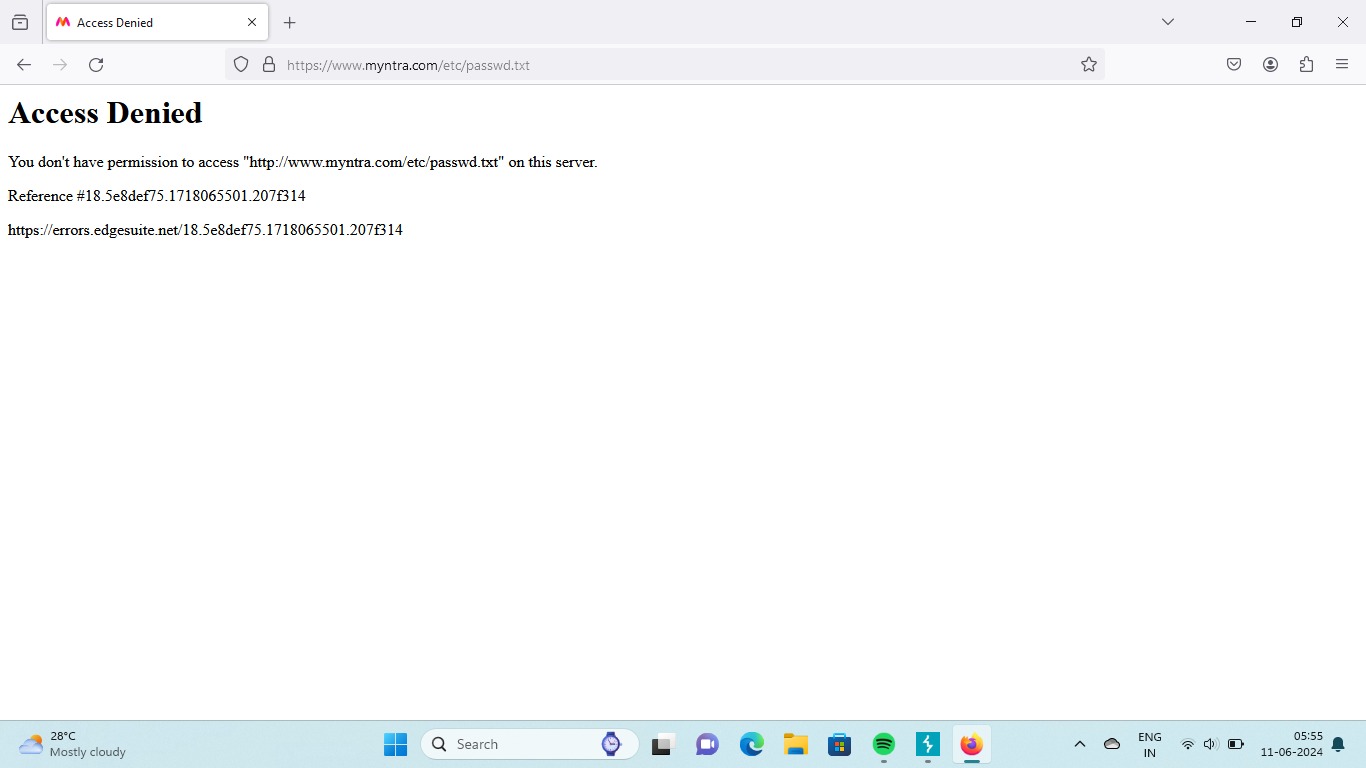
*Server-Side Request Forgery (SSRF) is a type of web security vulnerability where an attacker can trick a server into making unauthorized requests on its behalf. In SSRF attacks, the attacker can manipulate the server into accessing or interacting with resources that it should not have access to, potentially leading to data disclosure, unauthorized access to internal systems, or even remote code execution*.

## Impacts:

*One of the primary impacts of SSRF is the potential exposure of sensitive data. Attackers can leverage SSRF to access internal resources, such as databases, configuration files, or APIs, leading to data leakage. This can include personally identifiable information (PII), financial data, intellectual property, or other confidential information*.

*One of the primary impacts of SSRF is the potential exposure of sensitive data. Attackers can leverage SSRF to access internal resources, such as databases, configuration files, or APIs, leading to data leakage. This can include personally identifiable information (PII), financial data, intellectual property, or other confidential information*.

## ***Methodology:***



## ***Mitigations:***

*Implement strict input validation and sanitization to ensure that user-supplied URLs or input cannot be used to craft malicious requests. Validate and sanitize input to only allow trusted and expected URLs or IP addresses.*

## Conclusion: When we check SSRF vulnerability with myntra application we see some codes and didn’t see any result in myntra application because we use normal burp suite community edition tool.