Logo

Description automatically generated

**NAMES: Sheikh Muazzin Azeem**

**22-11087**

**INFORMATION AND SECURTIY**

**SECTION: B**

**PROJECT PROPOSAL**

**INTRODUCTION**

**Project title: “ Directory traversal attack “**

**Operating system: kali Linux**

**Software to be used: BurpSuite**

**Directory Traversal attack:**

Directory traversal (also known as file path traversal) is a web security vulnerability that allows an attacker to read arbitrary files on the server that is running an application. This might include application code and data, credentials for back-end systems, and sensitive operating system files. In some cases, an attacker might be able to write to arbitrary files on the server, allowing them to modify application data or behavior, and ultimately take full control of the server

Many applications that place user input into file paths implement some kind of defense against path traversal attacks, and these can often be circumvented.

If an application strips or blocks directory traversal sequences from the user-supplied filename, then it might be possible to bypass the defense using a variety of techniques.

You might be able to use an absolute path from the filesystem root, such as filename=/etc/passwd, to directly reference a file without using any traversal sequences.

**How does a Directory Traversal attack work?**

If there are vulnerabilities in the web application’s code or the server’s configuration, it’s easy to execute a directory traversal attack. For example, let’s examine this PHP code snippet that is prone to directory traversal attacks:  
  
/\*\*  
\* Get the filename from a GET input  
\* Example - https://example-website.com/?file=filename.php  
\*/  
$file = $\_GET[‘file’];

/\*\*  
\* Unsafely include the file  
\* Example: filename.php  
\*/  
file\_get\_contents(‘directory/’ . $file);

In this case, attackers can use the command https://example-website.com/?file=../../../../etc/passwd and manipulate the web application to reveal hidden information of the /etc/passwd system file.

Similar to our example, attackers can use directory traversal vulnerabilities to access credentials, modify files, or take control of the compromised web server.

**STEPS TO COMPLETE THE PROJECT:**

1. Install kali and open burp suite

2. Set the appropriate proxy in web browser

3. Install burpsuite certificate in web browser

4. Enable burpsuite interceptor

5. Go to the target website and select any .jpg file

6. Once you see the jpg file on interceptor, send request to the repeater Module

7. Open repeater module and put in the path of the file you want to fetch in the place of the jpg file

8. Once you know the file exists, we start sending payloads

9. With each payload the content length will keep on increasing and eventually we will fetch the targeted data

**PROJECT OUTCOME:**

After performing these series of steps, we can obtain/modify/manipulate the targeted files from the Database of website and save them locally on our computer too