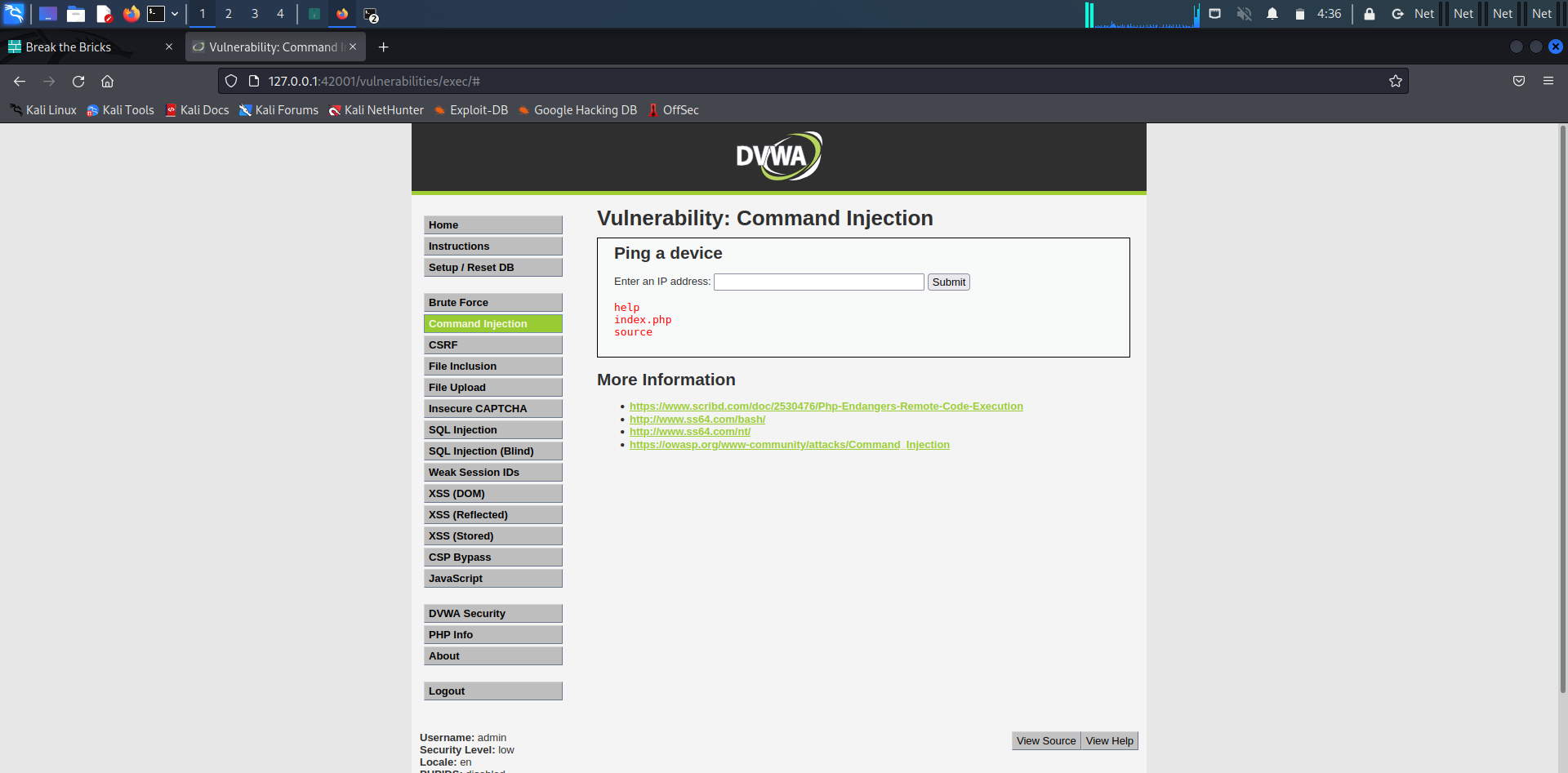
**NAME : SHRAVYA**

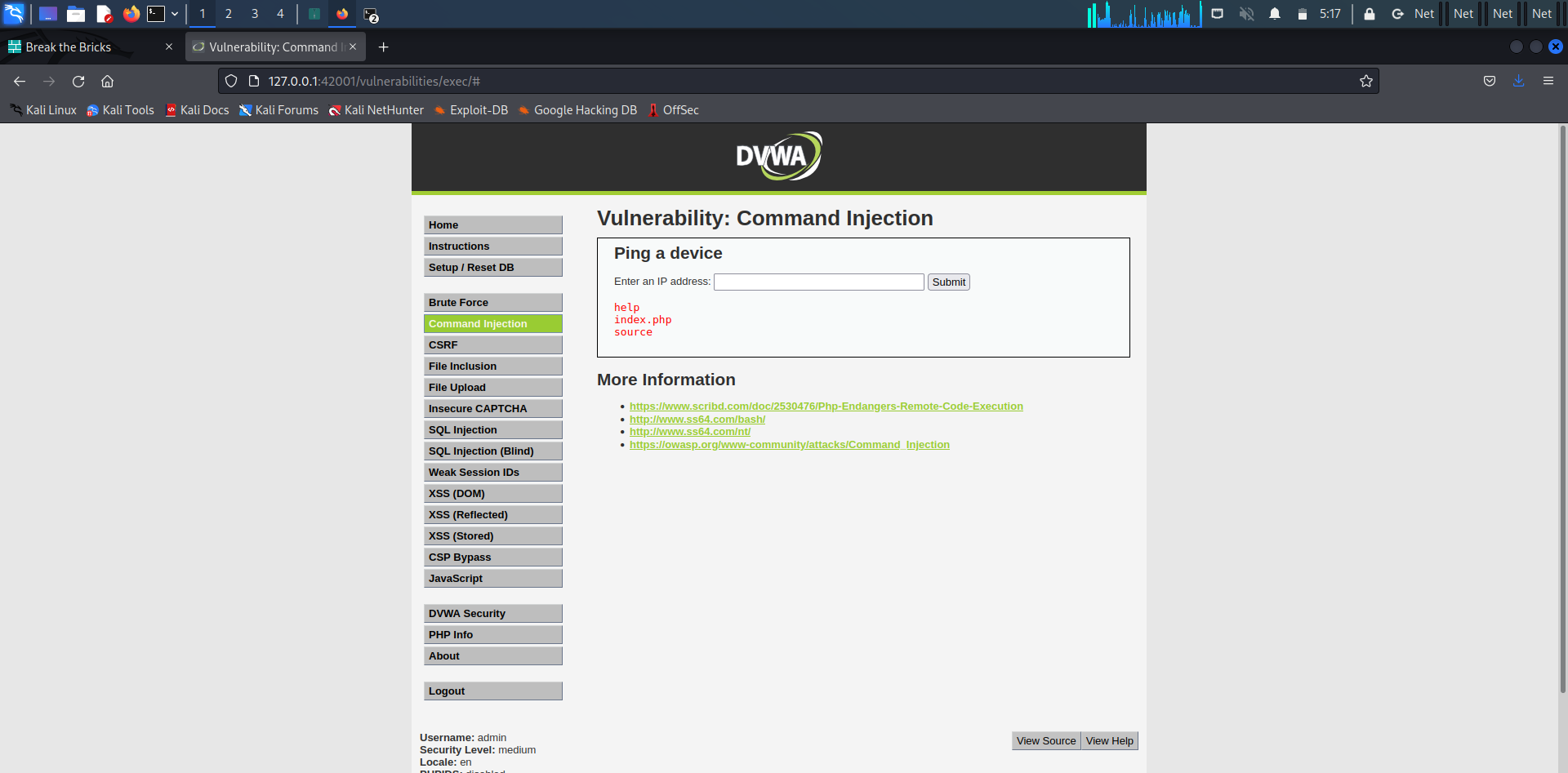
**DATE : 13-03-2023**

**TASK : 3**

1. **Command execution vulnerability:**

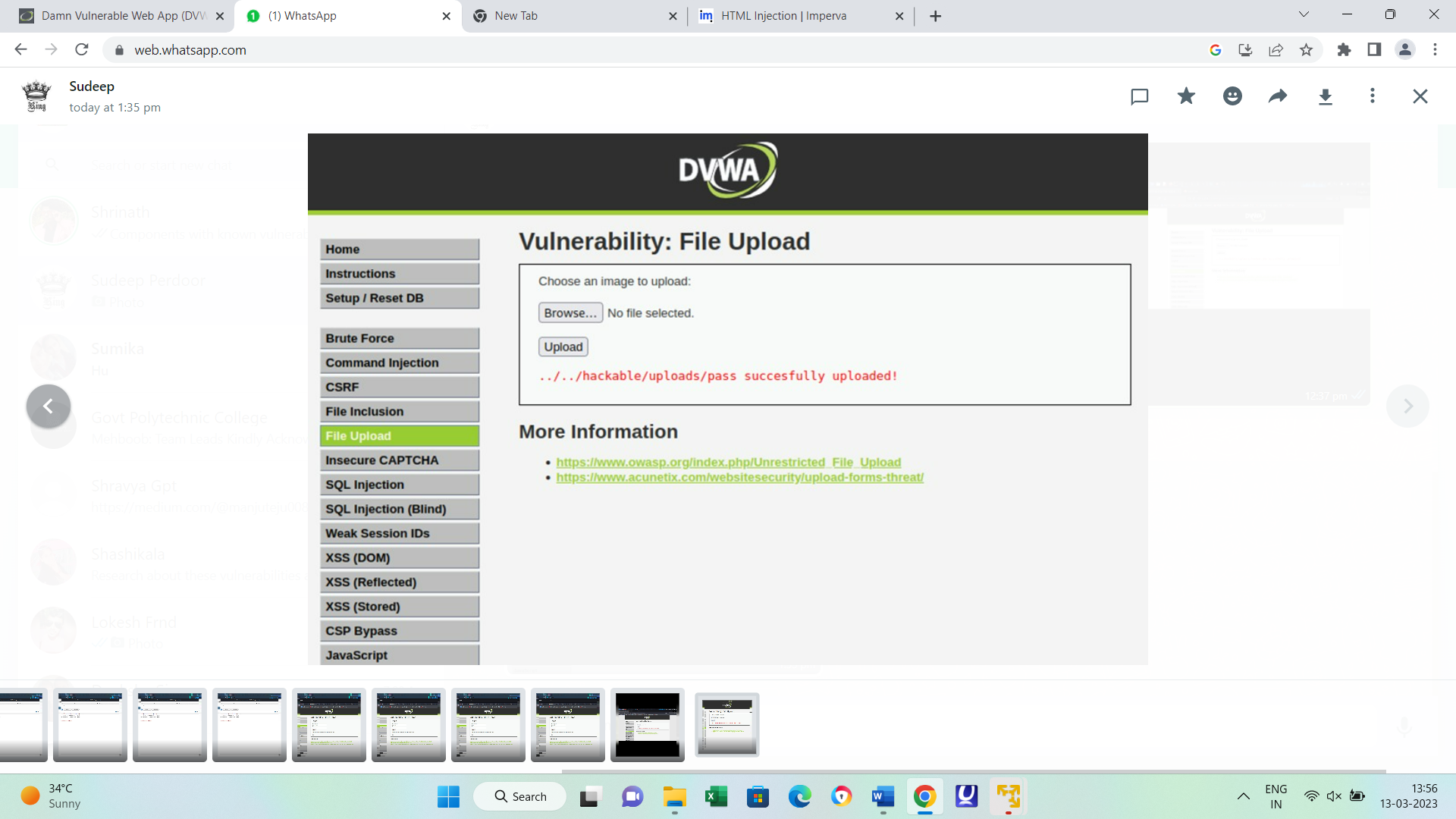
Command injection is a cyber attack that involves executing arbitrary commands on a host operating system (OS). Typically, the threat actor injects the commands by exploiting an application vulnerability, such as insufficient input validation.





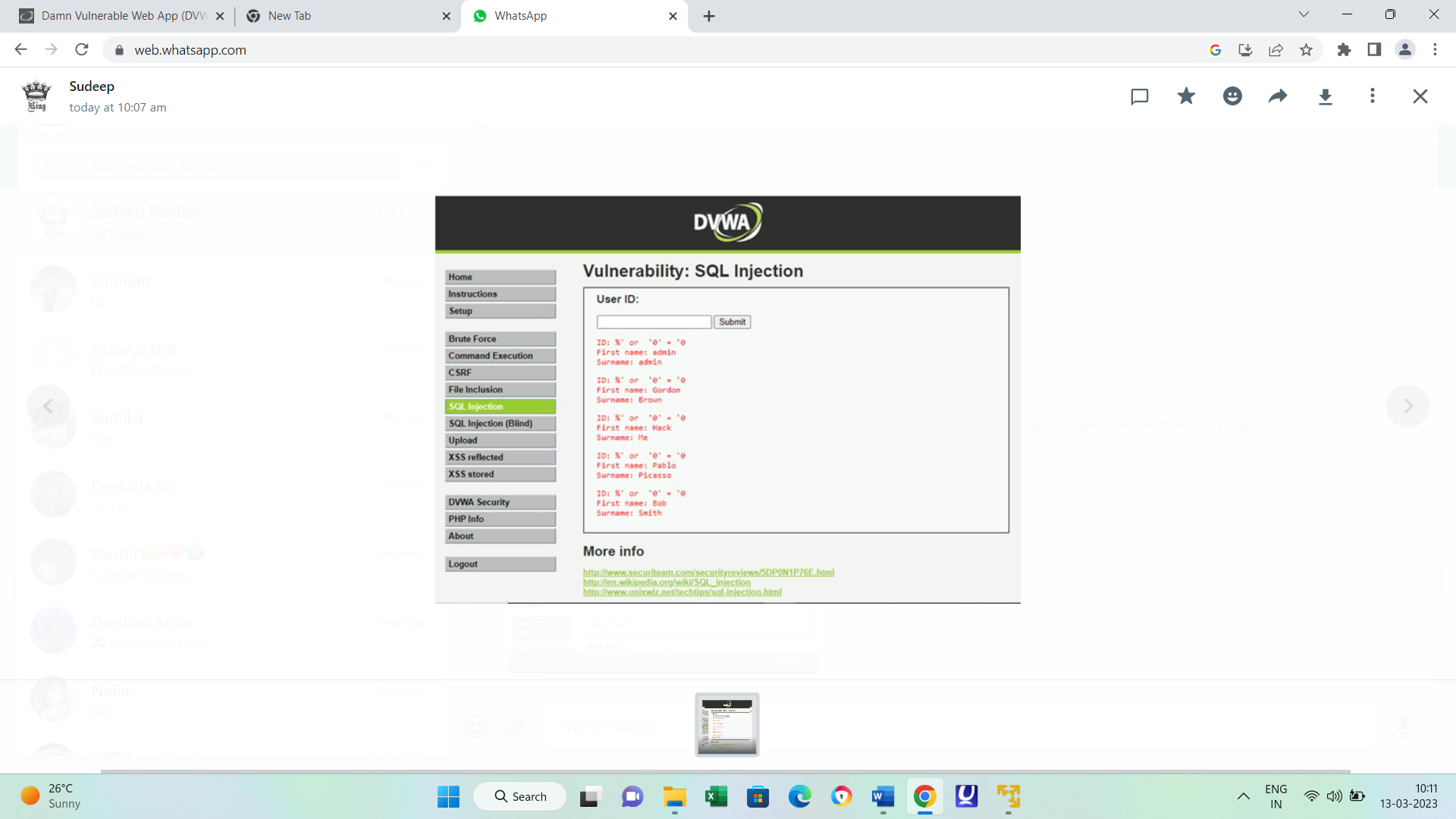
1. **File upload vulnerability:**

File upload vulnerabilities are when a web server allows users to upload files to its filesystem without sufficiently validating things like their name, type, contents, or size.



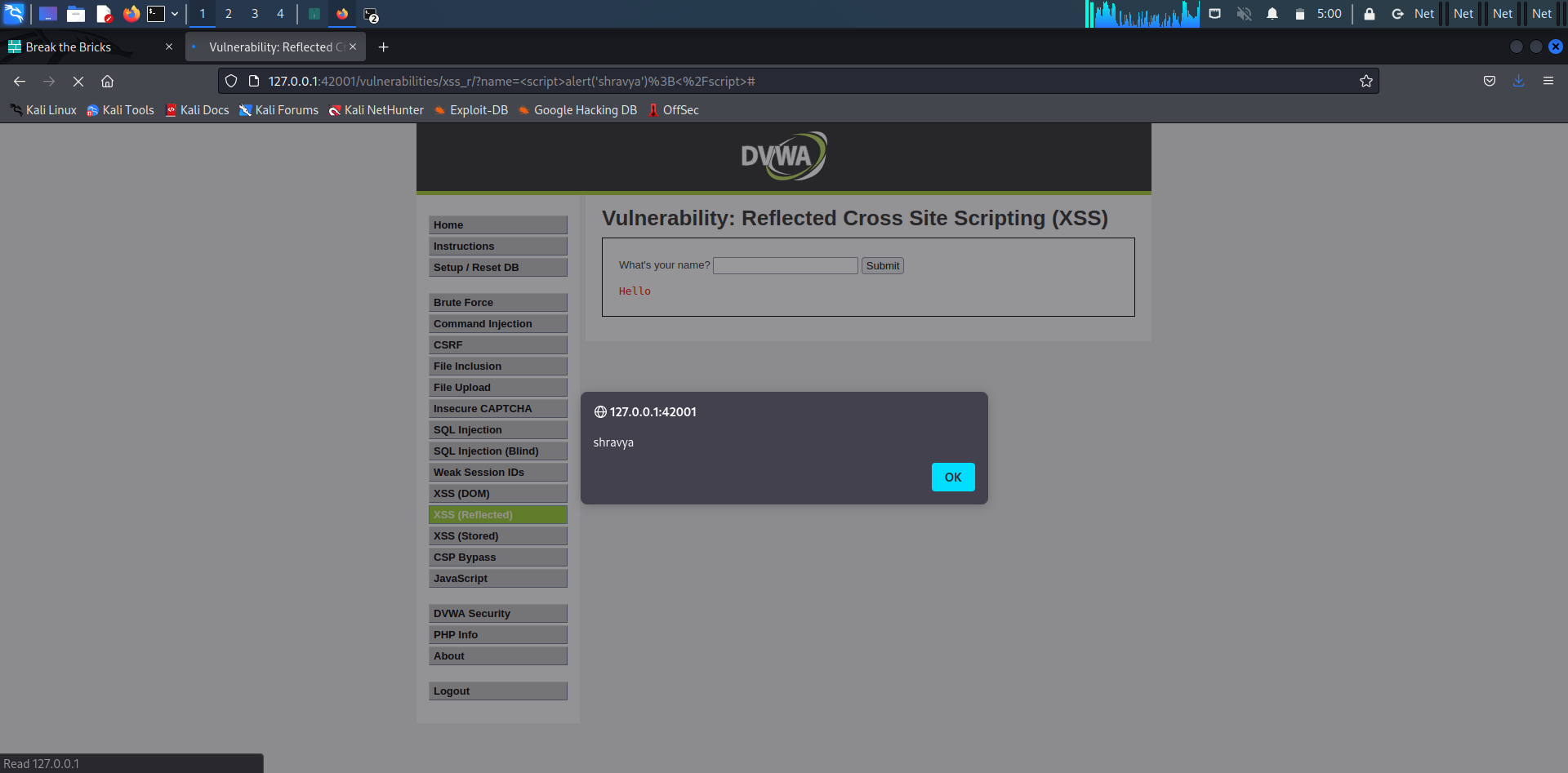
1. **Sql injection vulnerability:**

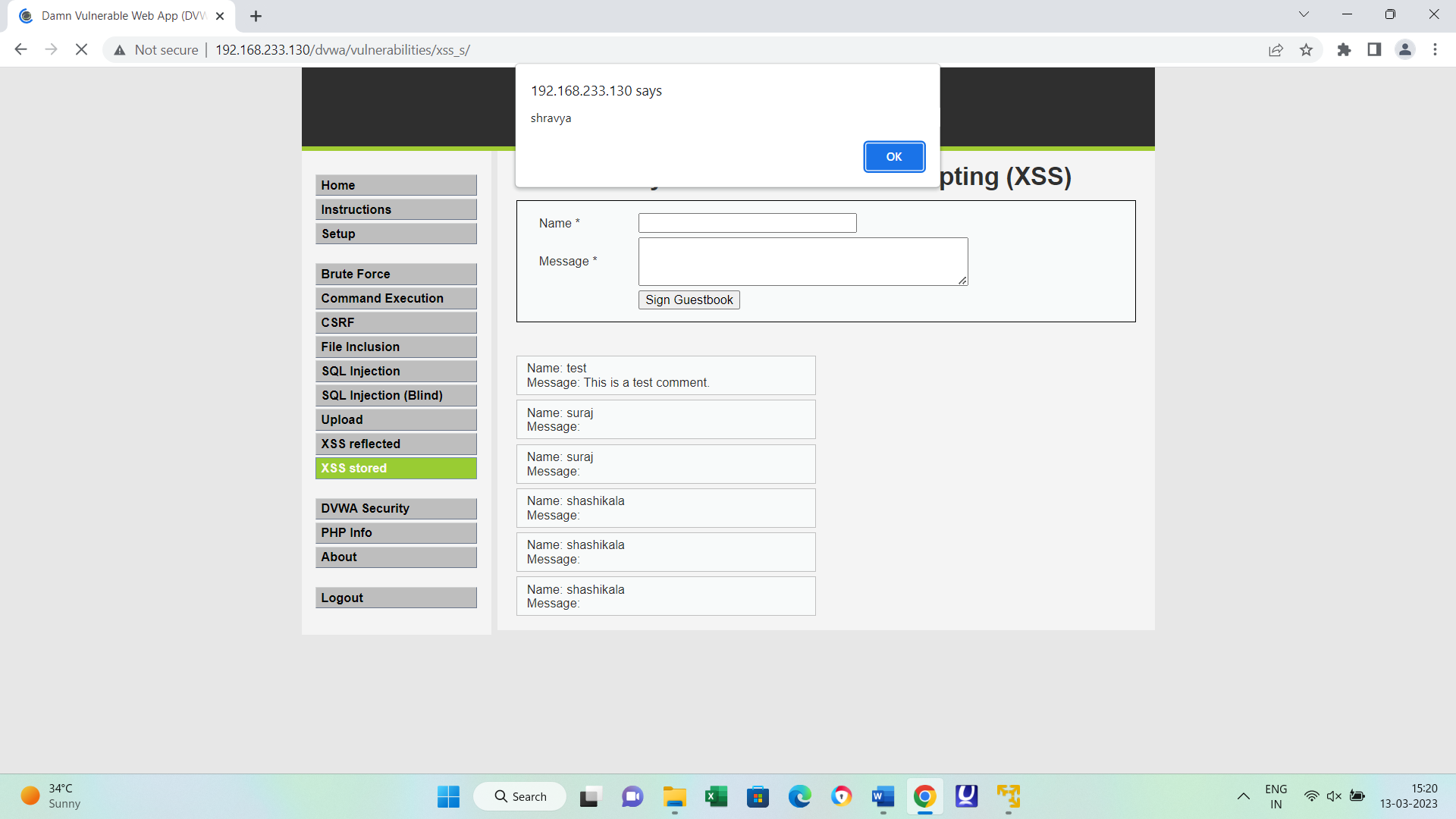
SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.



1. **Cross site scripting:**

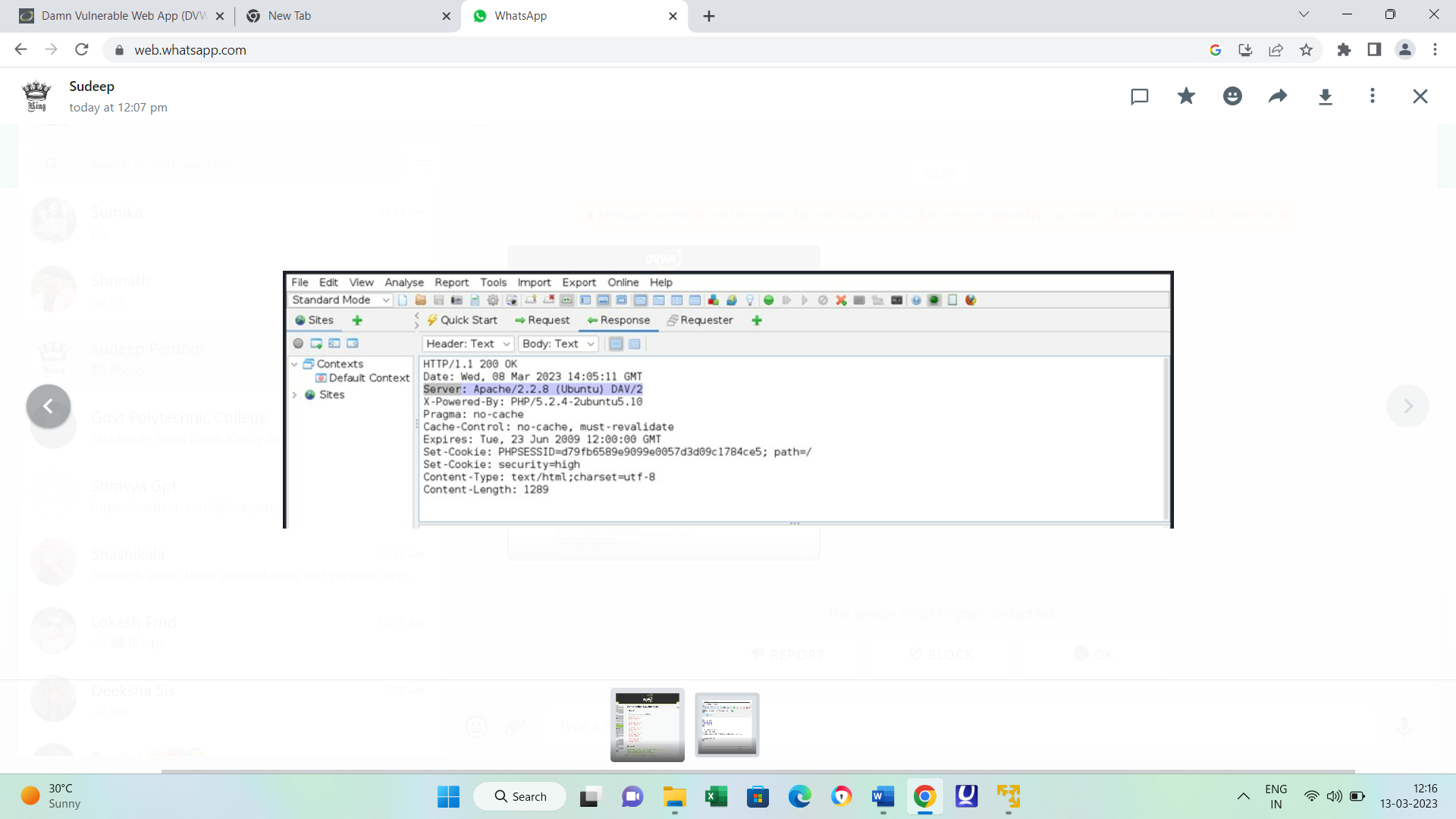
Cross-site scripting is a type of security vulnerability that can be found in some web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.





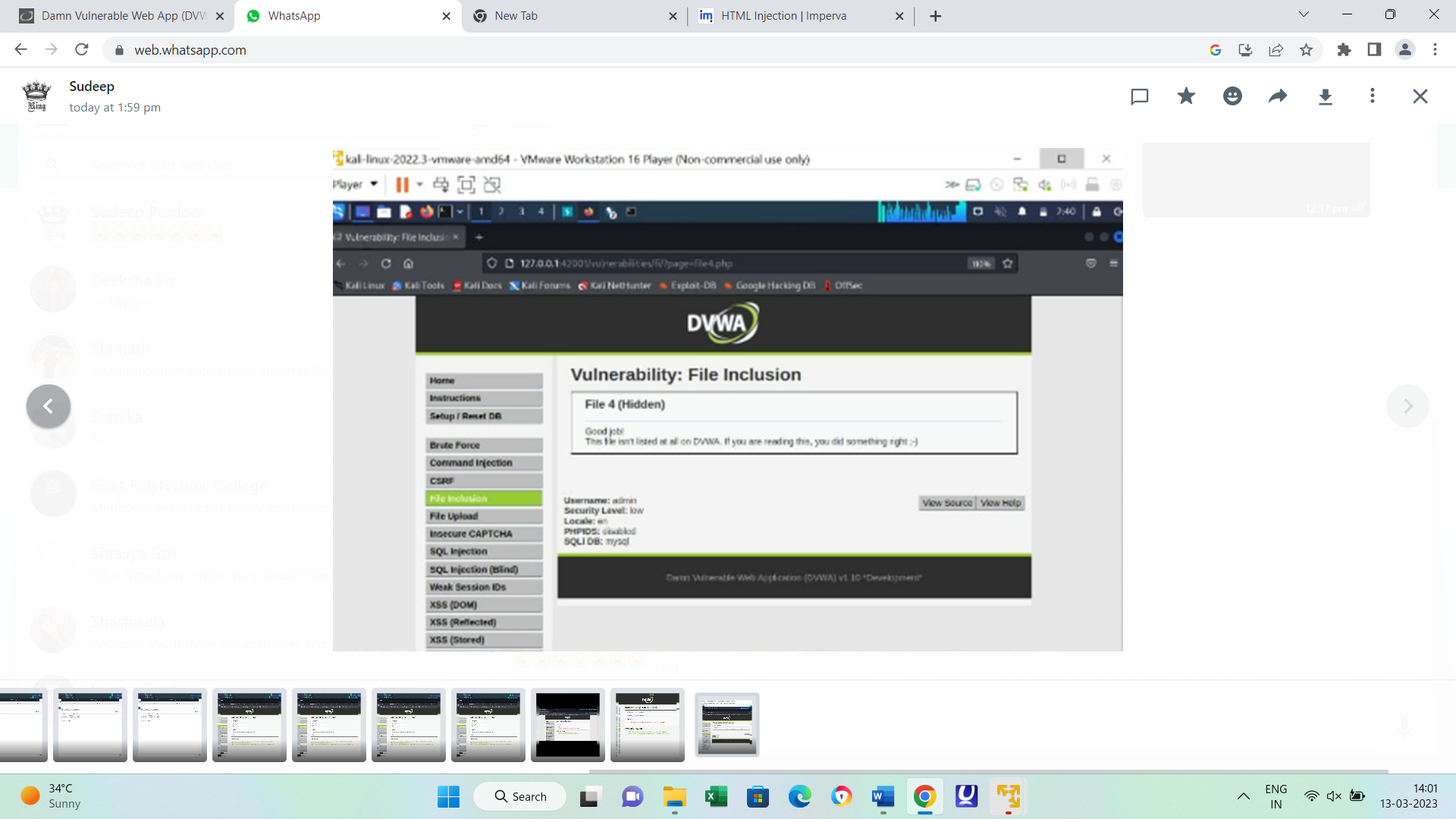
1. **Sensitive information disclosure:**

Information disclosure, also known as information leakage, is when a website unintentionally reveals sensitive information to its users. Depending on the context, websites may leak all kinds of information to a potential attacker, including: Data about other users, such as usernames or financial information.



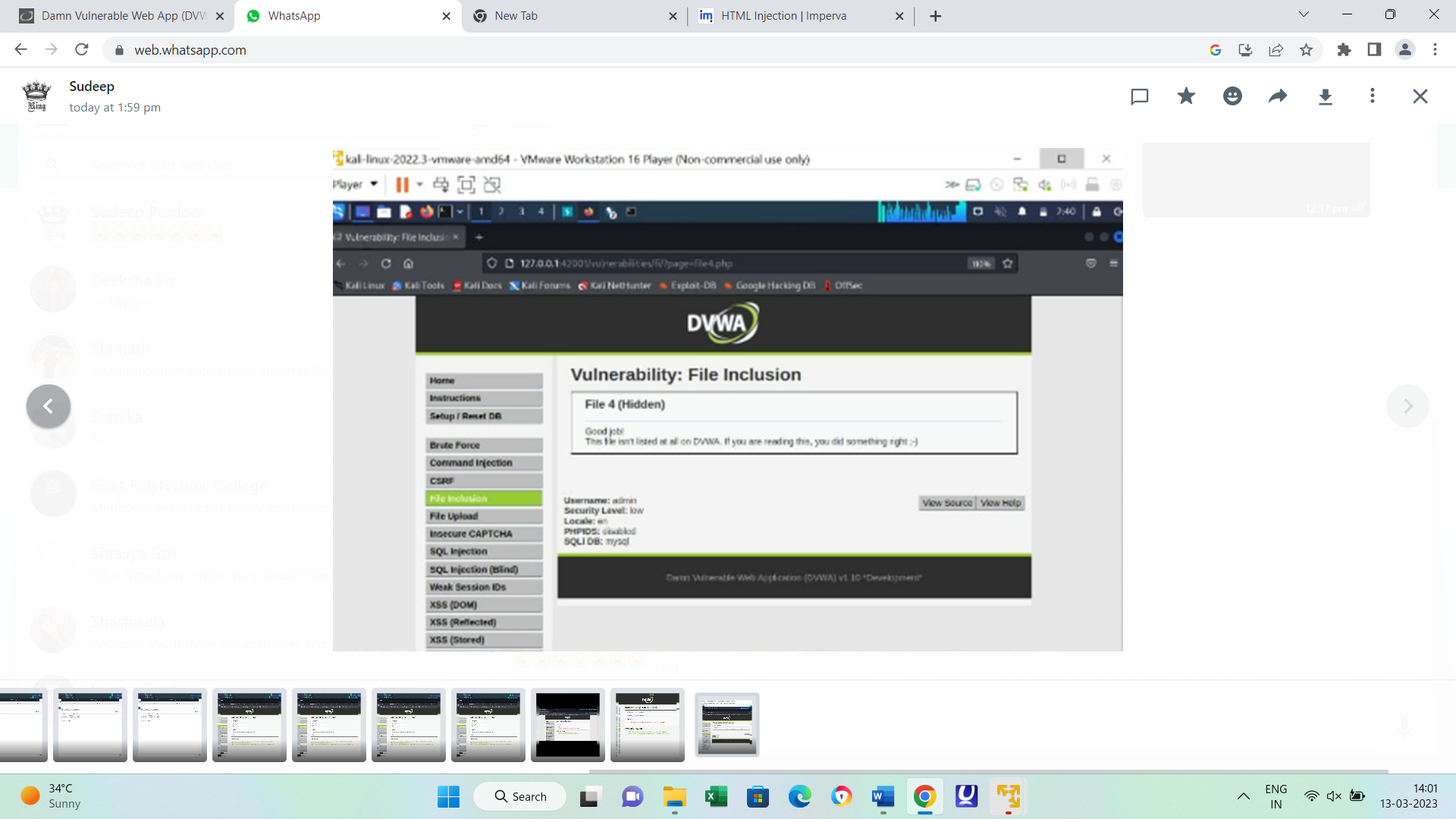
1. **Local file inclusion:**

Local File Inclusion is an attack technique in which attackers trick a web application into either running or exposing files on a web server. LFI attacks can expose sensitive information, and in severe cases, they can lead to cross-site scripting (XSS) and remote code execution.



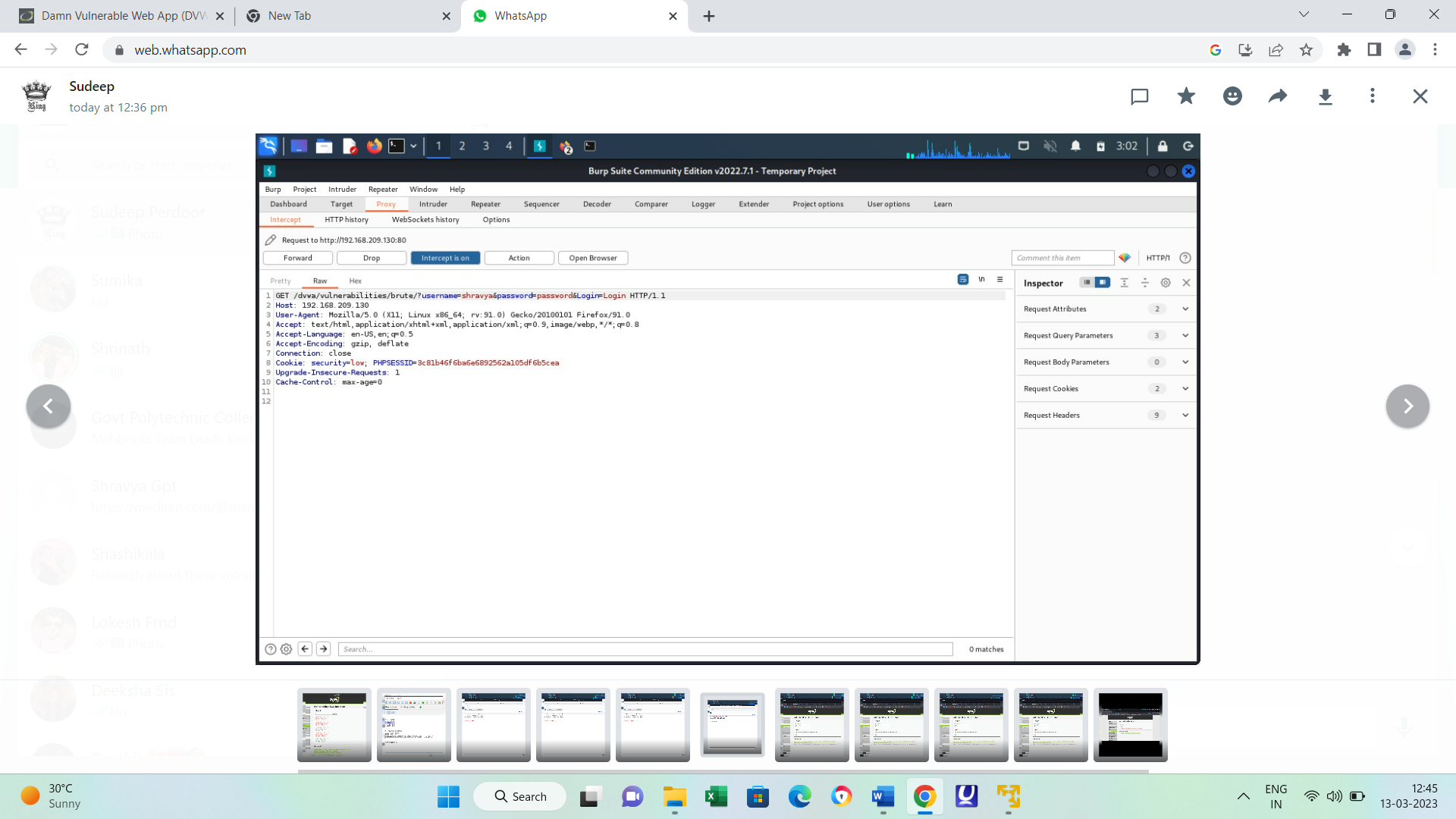
**7) Remote file inclusion:**

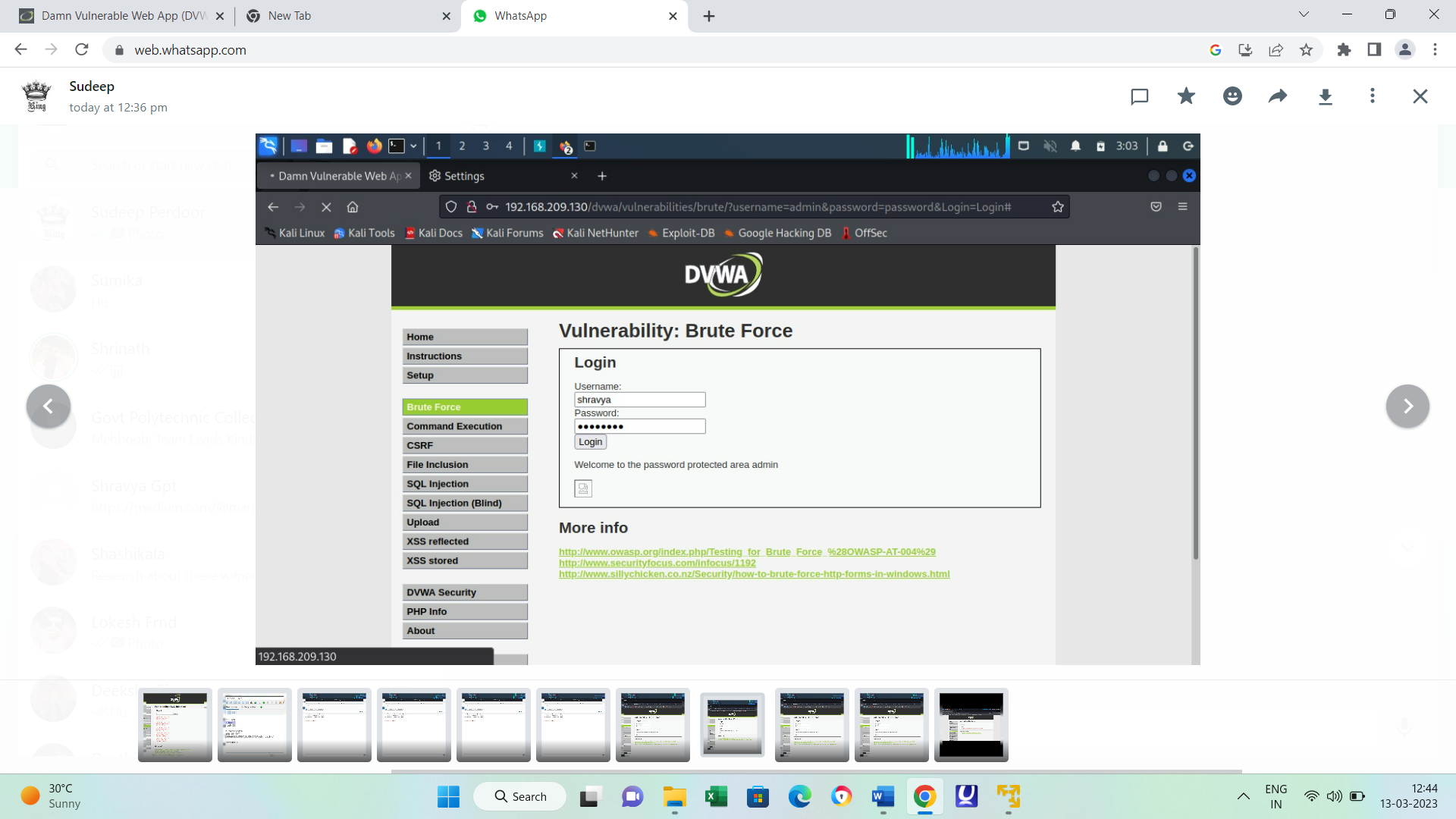
Remote file inclusion (RFI) is an attack targeting vulnerabilities in web applications that dynamically reference external scripts. The perpetrator's goal is to exploit the referencing function in an application to upload malware (e.g., backdoor shells) from a remote URL located within a different domain.



1. **Bruteforce attack:**

A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.





1. **Forced browsing vulnerability:**

Forced browsing is an attack where the aim is to enumerate and access resources that are not referenced by the application, but are still accessible.

An attacker can use Brute force techniques to search for unlinked contents in the domain directory, such as temporary directories and files, and old backup and configuration files. These resources may store sensitive information about web applications and operational systems, such as source code, credentials, internal network addressing, and so on, thus being considered a valuable resource for intruders.

This attack is performed manually when the application index directories and pages are based on number generation or predictable values, or using automated tools for common files and directory names.

This attack is also known as Predictable Resource Location, File Enumeration, Directory Enumeration, and Resource Enumeration.

**10)Components with known vulnerability:**

This kind of threat occurs when the components such as libraries and frameworks used within the app almost always execute with full privileges. If a vulnerable component is exploited, it makes the hacker's job easier to cause a serious data loss or server takeover.

These components can be defined as the third-party apps or software or platforms that are outdated and contain bugs that are public to all, that is- sites like https://www.exploit-db.com contain the full detail as to how to exploit the bugs to put the security of the whole website under severe threat.

This vulnerability arises with the fact that a website finds it difficult to code everything while making its website functional like -transaction, location, chats, etc.

So, in order to ease the process of building the website, many websites use third-party apps which do the tasks. But the main problem is that those apps can be harmful to their system if they are not updated regularly. Components with known vulnerabilities are considered to be one of the top 10 web application vulnerabilities listed by OWASP.

Many websites security gets compromised when they use components having known vulnerabilities.

**11)Html injection:**

HTML Injection also known as Cross Site Scripting. It is a security vulnerability that allows an attacker to inject HTML code into web pages that are viewed by other users.

