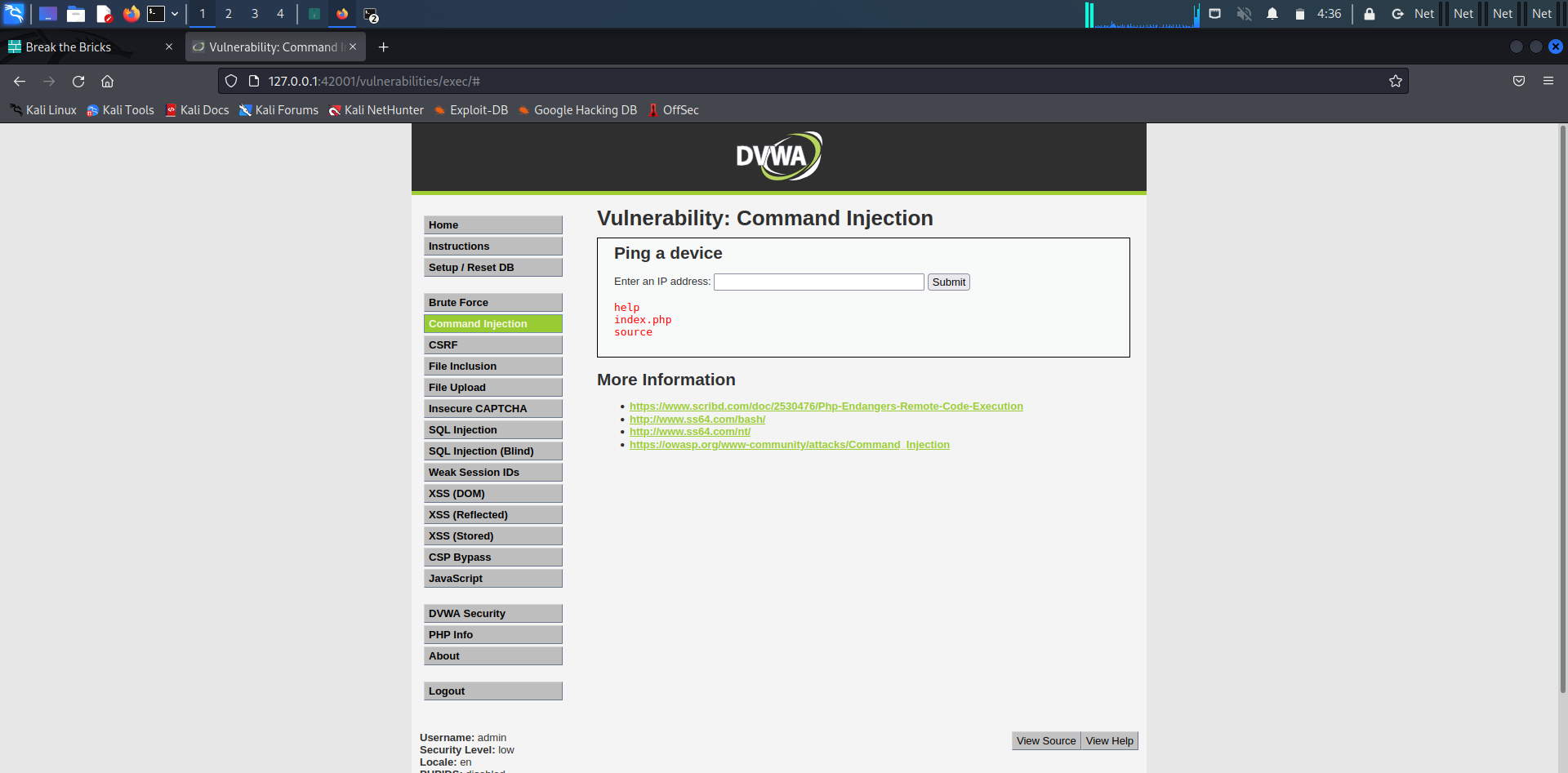
**NAME: SURAJ**

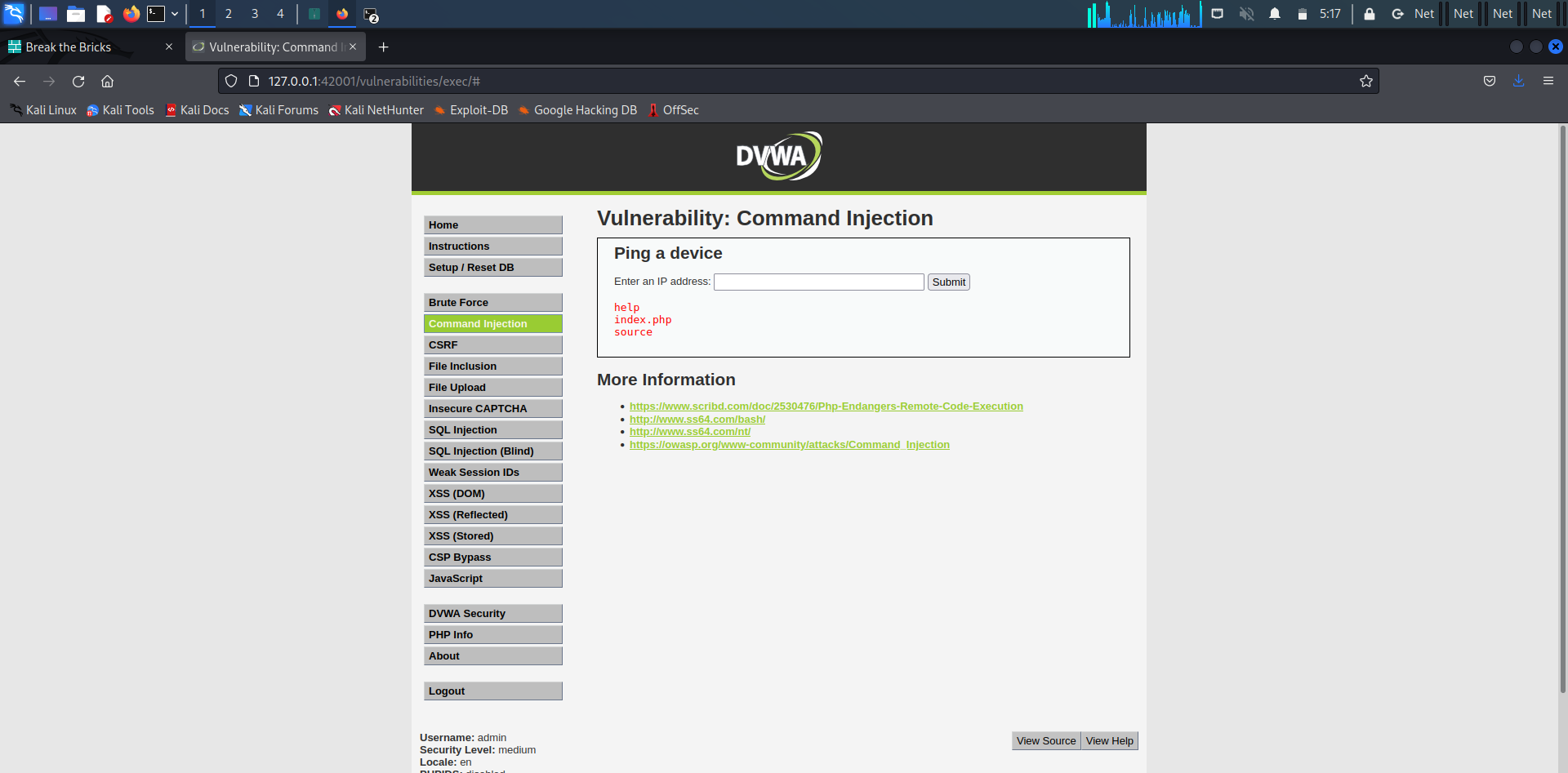
**DATE: 13/03/2023**

**TASK-03**

**1)Command execution vulnerability:**

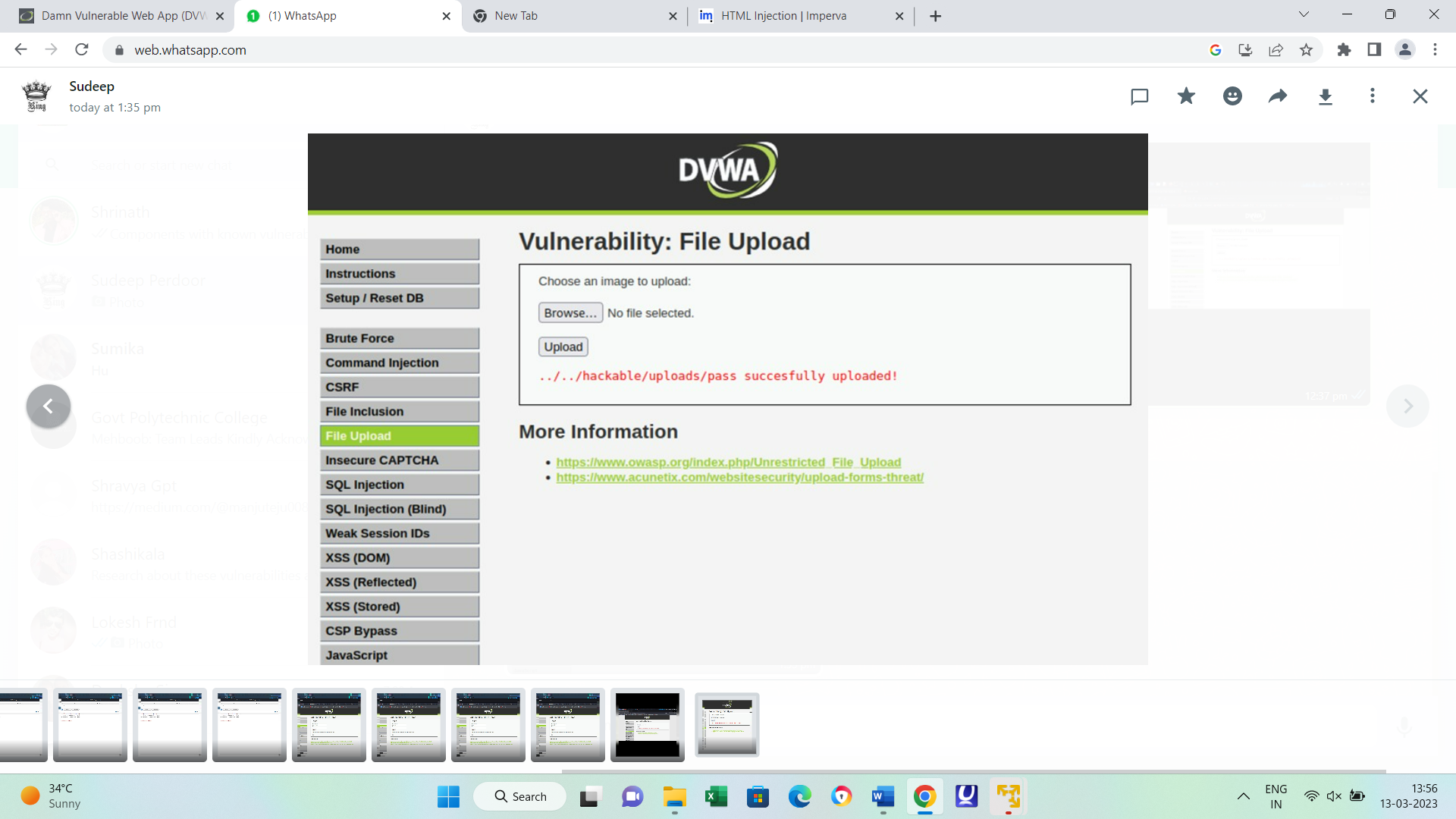
A command execution vulnerability is a security flaw that allows an attacker to execute arbitrary commands or code on a system by exploiting a weakness in an application or software component. This vulnerability occurs when an application fails to properly validate input from a user, and instead of treating the input as data, the application interprets it as a command.





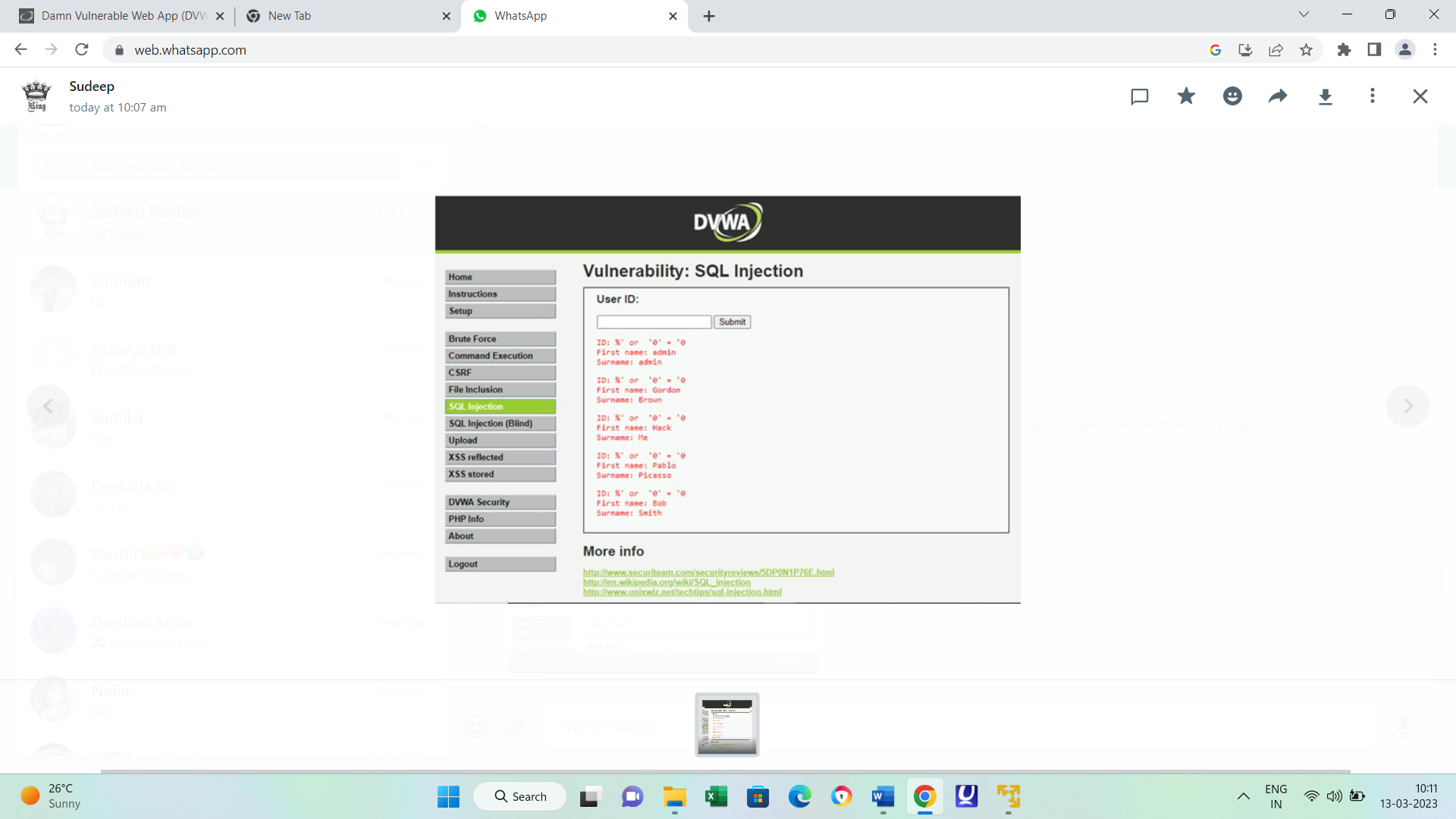
**2) File upload vulnerability :**

File upload vulnerability refers to a security flaw in web applications that allows attackers to upload and execute malicious files on the server. This type of vulnerability occurs when a web application does not properly validate the file being uploaded, allowing an attacker to upload a file with malicious code.



**3)sql injection vulnerability:**

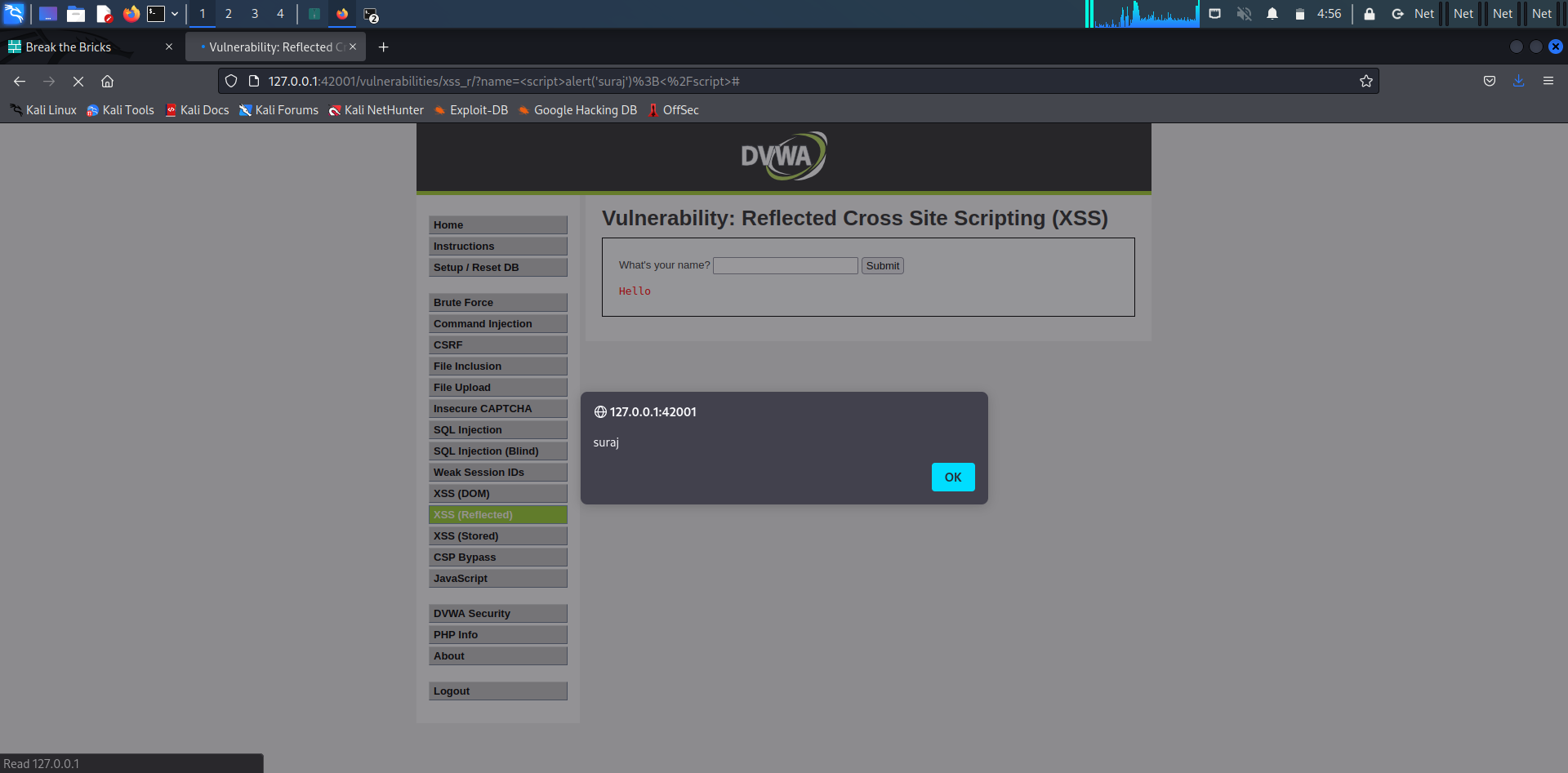
SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

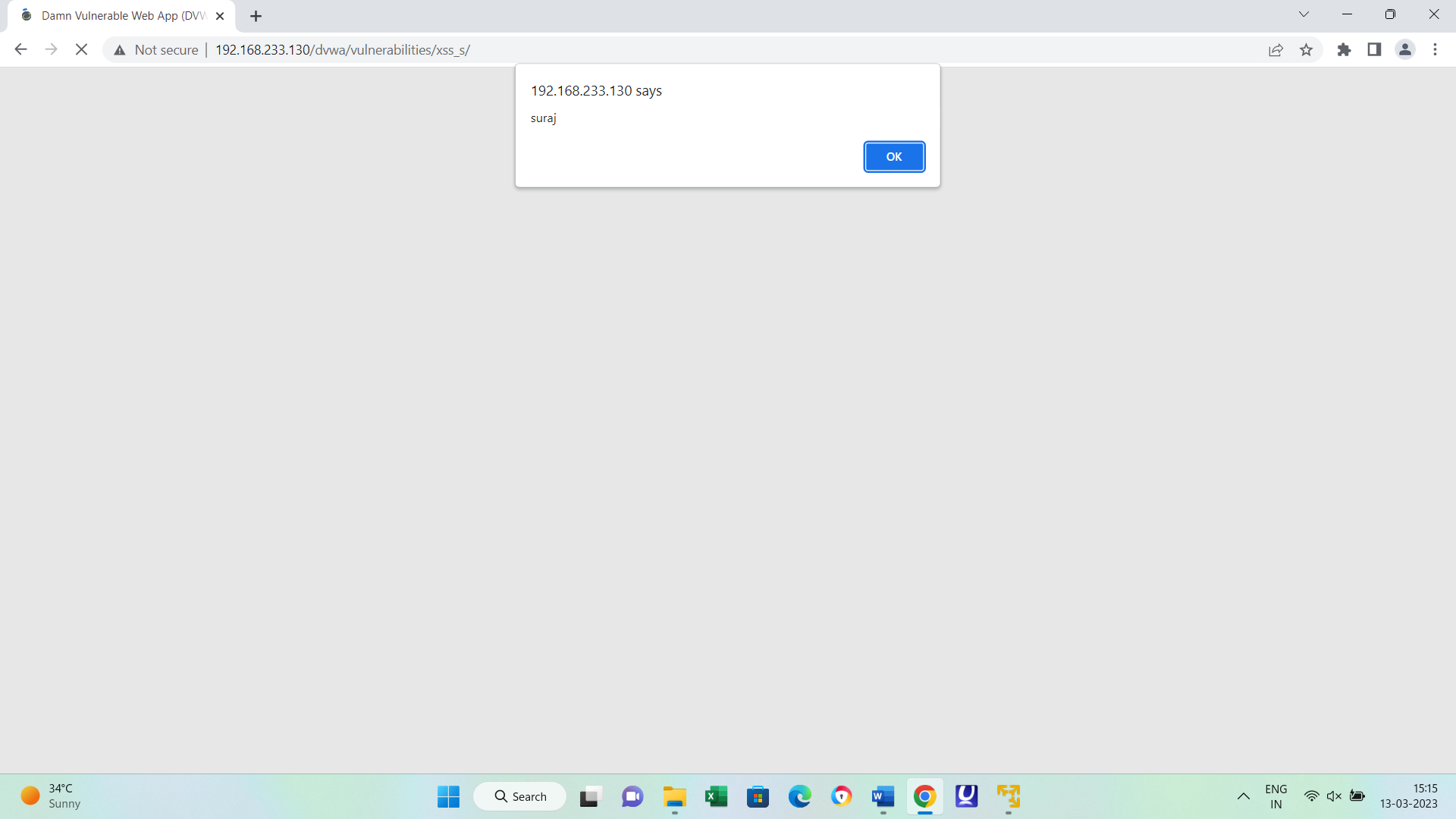


**4) Cross site scripting :**

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

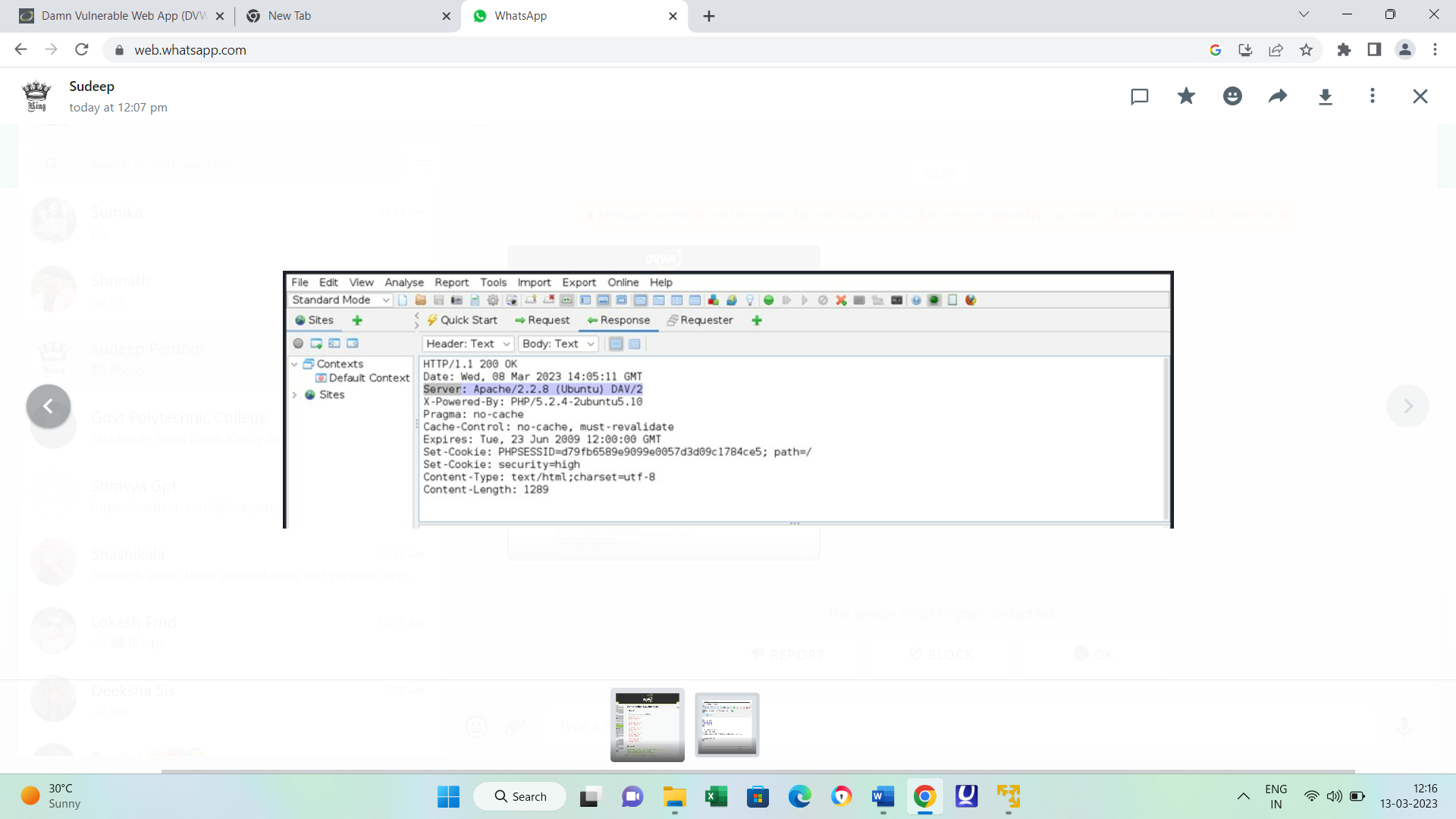
An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.





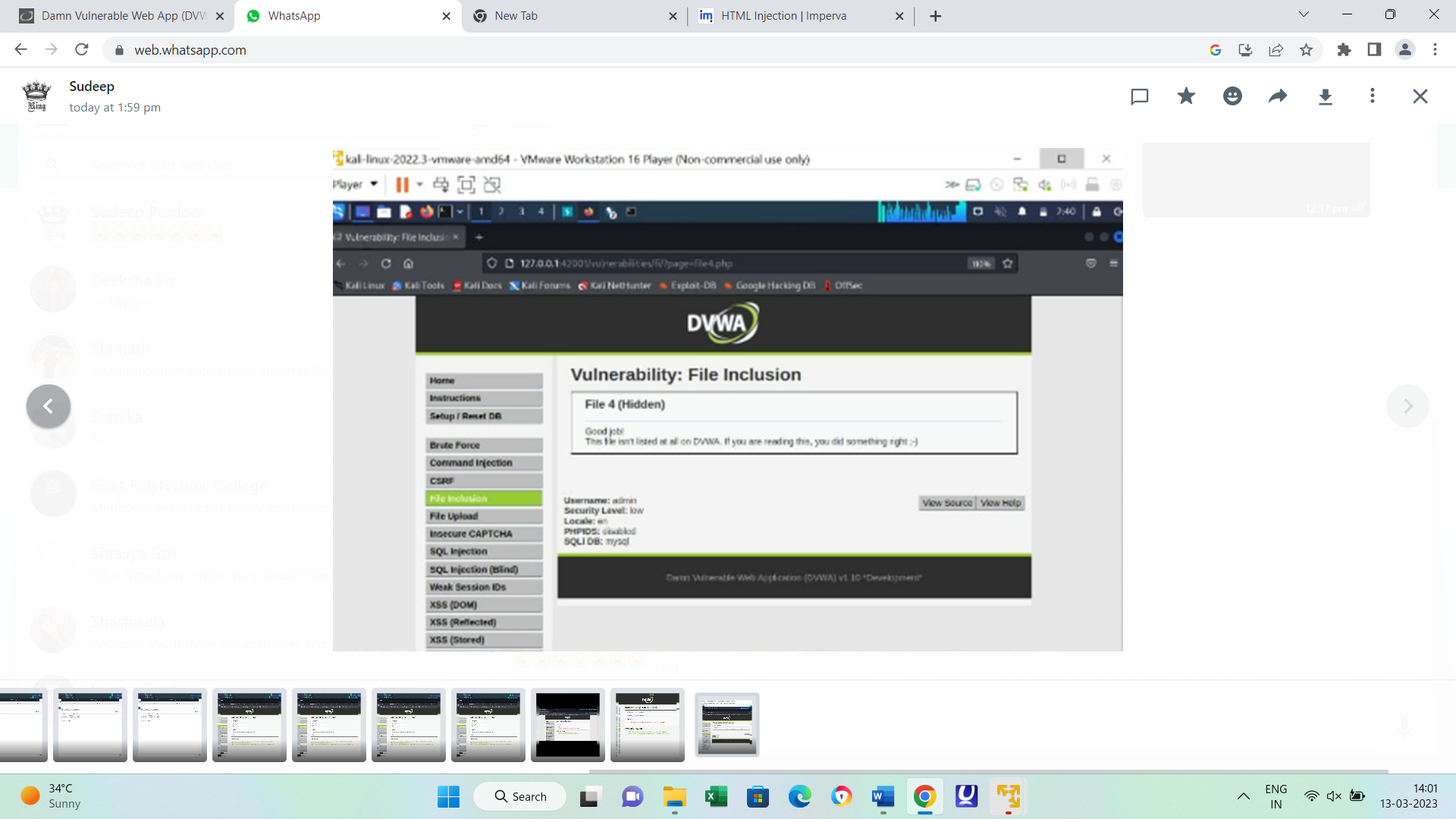
**5)Sensitive information disclosure :**

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.



**6) Local file inclusion :**

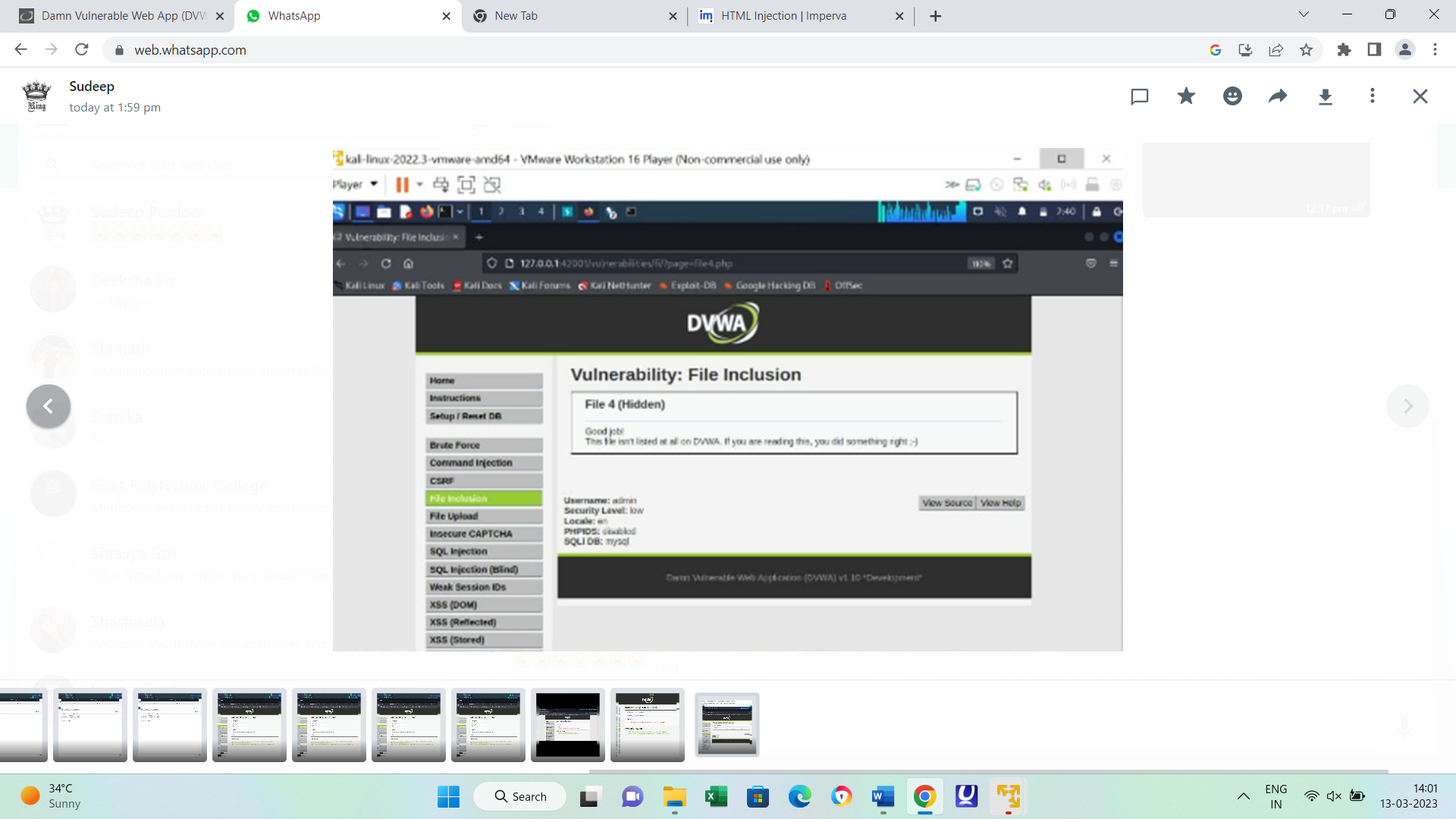
Local file inclusion (also known as LFI) is the process of including files, that are already locally present on the server, through the exploiting of vulnerable inclusion procedures implemented in the application. This vulnerability occurs, for example, when a page receives, as input, the path to the file that has to be included and this input is not properly sanitized, allowing directory traversal characters (such as dot-dot-slash) to be injected. Although most examples point to vulnerable PHP scripts, we should keep in mind that it is also common in other technologies such as JSP, ASP and others.



**7)Remote file inclusion**

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

The consequences of a successful RFI attack include information theft, compromised servers and a site takeover that allows for content modification.

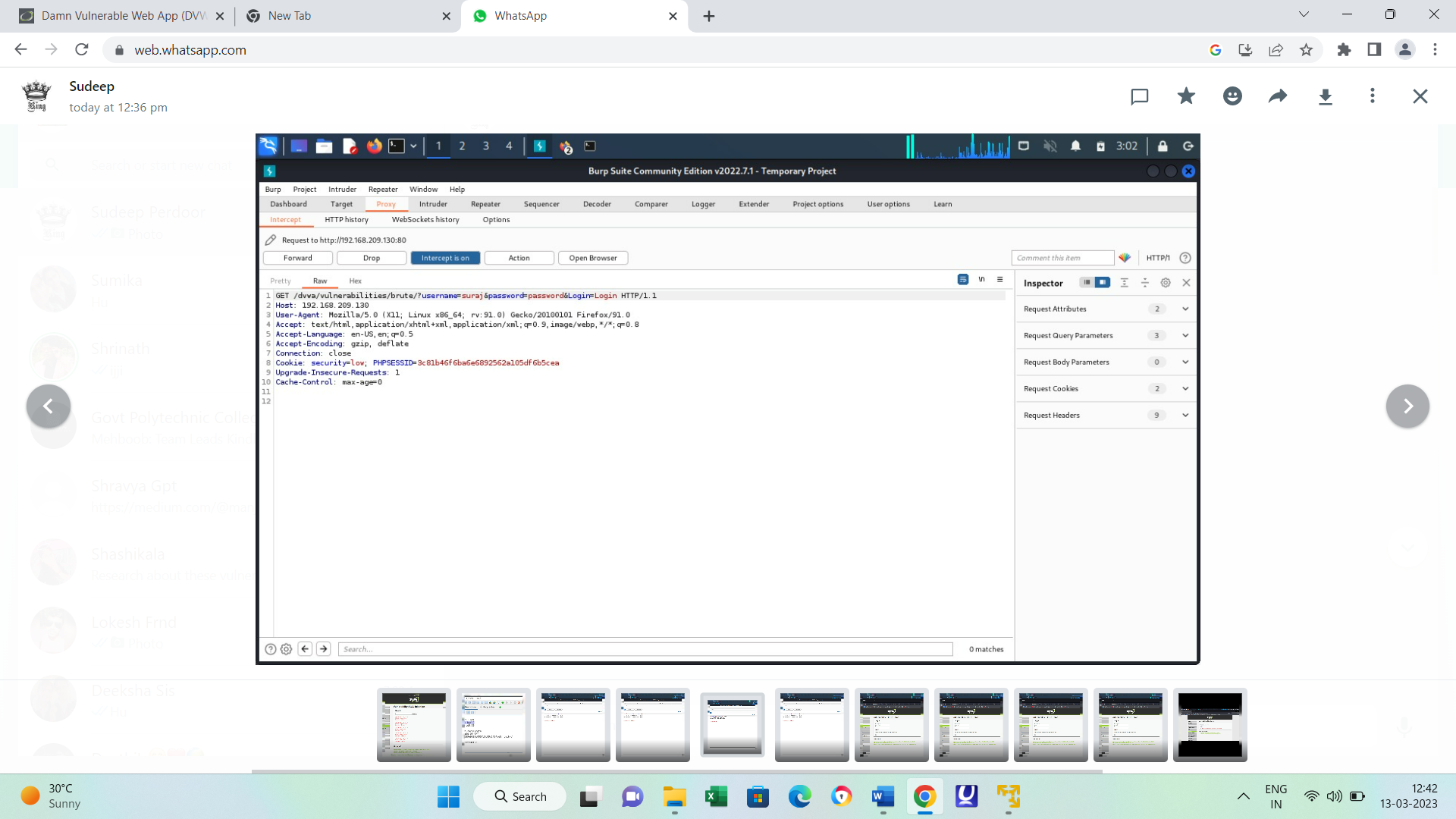


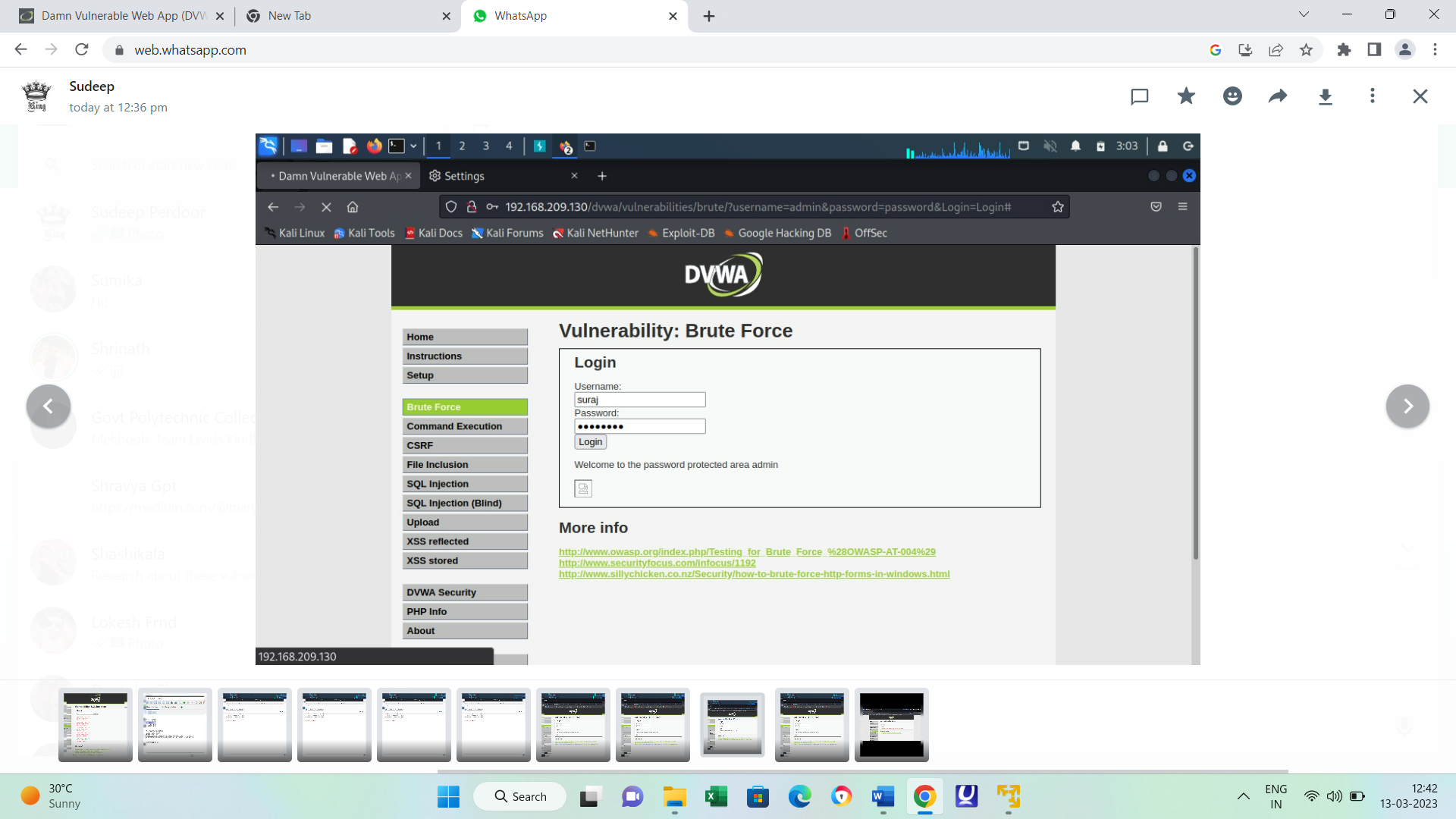
**8)Bruteforce attack:**

A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly.

These attacks are done by ‘brute force’ meaning they use excessive forceful attempts to try and ‘force’ their way into your private account.

This is an old attack method, but it's still effective and popular with hackers. Because depending on the length and complexity of the password, cracking it can take anywhere from a few seconds to many years.





**9) Forced browsing vulnerability:**

Forced browsing attacks are the result of a type of security misconfiguration vulnerability. These kinds of vulnerabilities occur when insecure configuration or misconfiguration leave web application components open to attack. Misconfiguration vulnerabilities may exist in subsystems or software components.

Forced browsing attacks are the result of a type of security misconfiguration vulnerability. These kinds of vulnerabilities occur when insecure configuration or misconfiguration leave web application components open to attack.

Misconfiguration vulnerabilities may exist in subsystems or software components. Some examples of this include remote administration functionality and other unneeded services that software may have enabled, or sample configuration files or scripts, or even default user accounts that web server software may arrive with. These existing features leave access to the system an attacker can exploit.

**10)Components with known vulnerability :**

Components with known vulnerabilities are hardware or software components that have a known weakness or flaw that could be exploited by an attacker. This vulnerability could be related to a programming error, a design flaw, or a configuration issue.

These components can be defined as a third party apps or software or platforms that are outdated and contains books that are public to all that is sites like HTTPS:// [www.exploit-db.com](http://www.exploit-db.com) contain the full detail as to how to exploit the bugs to put the security of the whole website under the server threat.

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

**11)Html injection:**

HTML is the language that determines how application data gets presented to users in their web browser. This language contains visualization commands, like the color of the page’s background and the size of embedded pictures. It also contains links to other web pages, and additional commands intended for the user’s browser. Furthermore, automated tools that collect useful information from the web on behalf of users often do so by systematically accessing and parsing the relevant information in the application’s HTML pages

