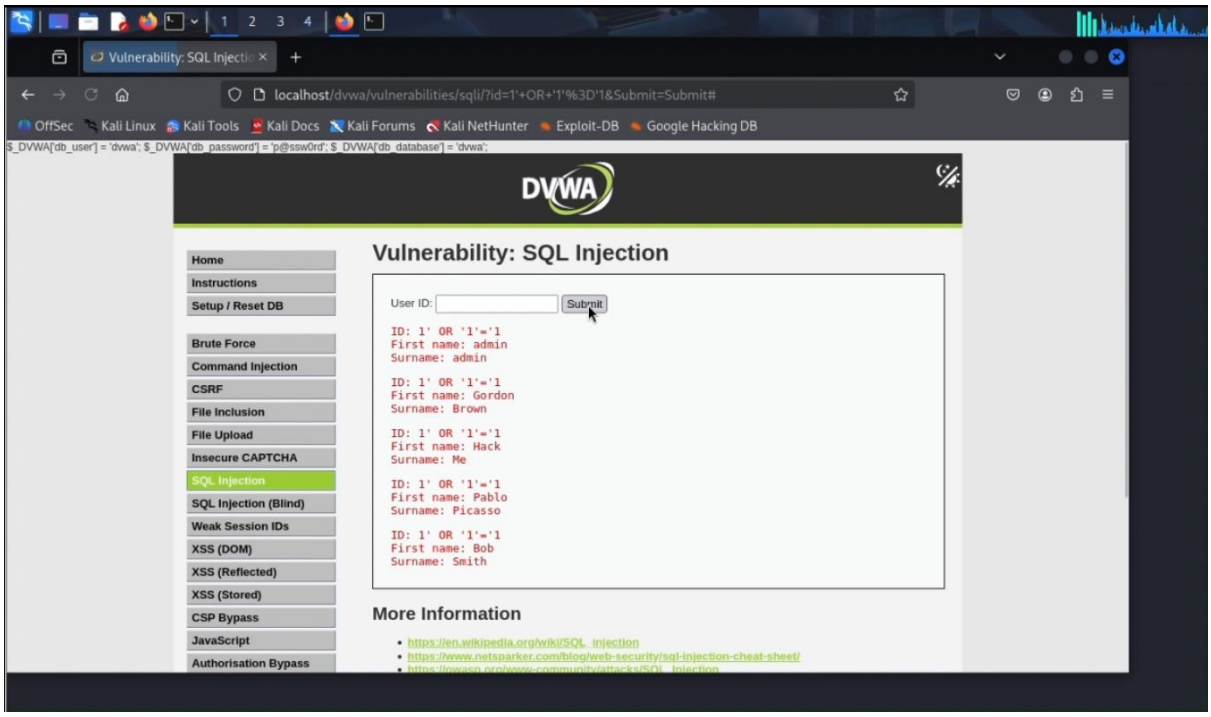
Task 3

Security Testing Report

SQL Injection :

SQL Injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It happens when user input is not properly validated or sanitized, and the attacker inserts malicious SQL commands into input fields which are then executed by the database.

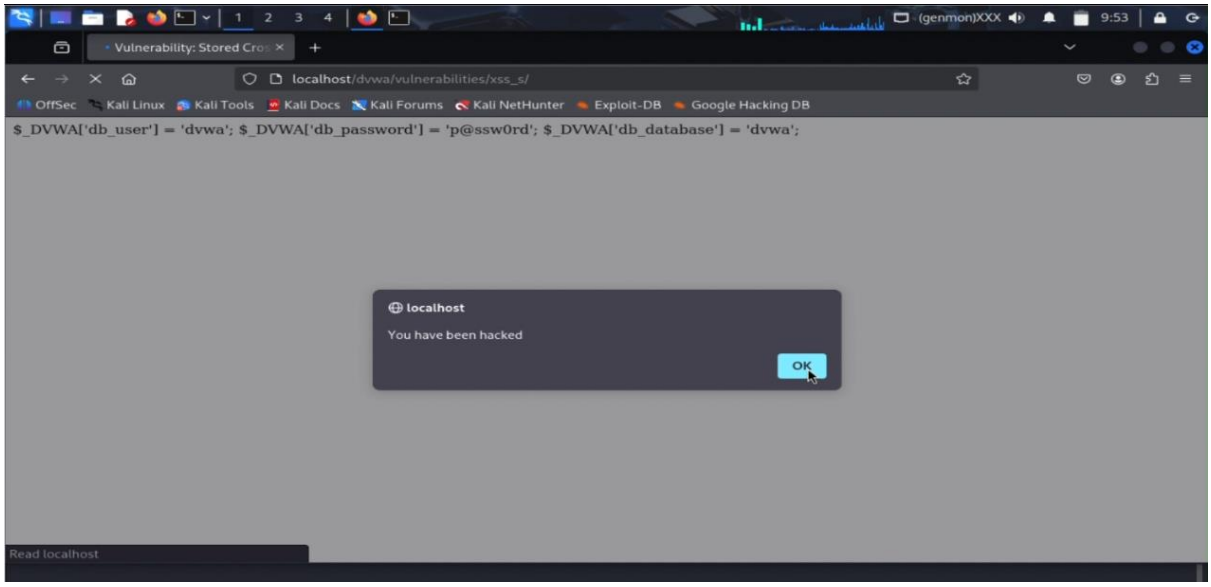


Cross-Site Scripting(XSS) :

XSS(Cross Site Scripting) is a web security vulnerability that allows an attacker to inject malicious scripts (usually JavaScript) into web pages that are viewed by other users. These scripts run inside the victim's browser, making it possible for attackers to steal information, hijack sessions, or alter the appearance or behavior of a website. There are two types of XSS

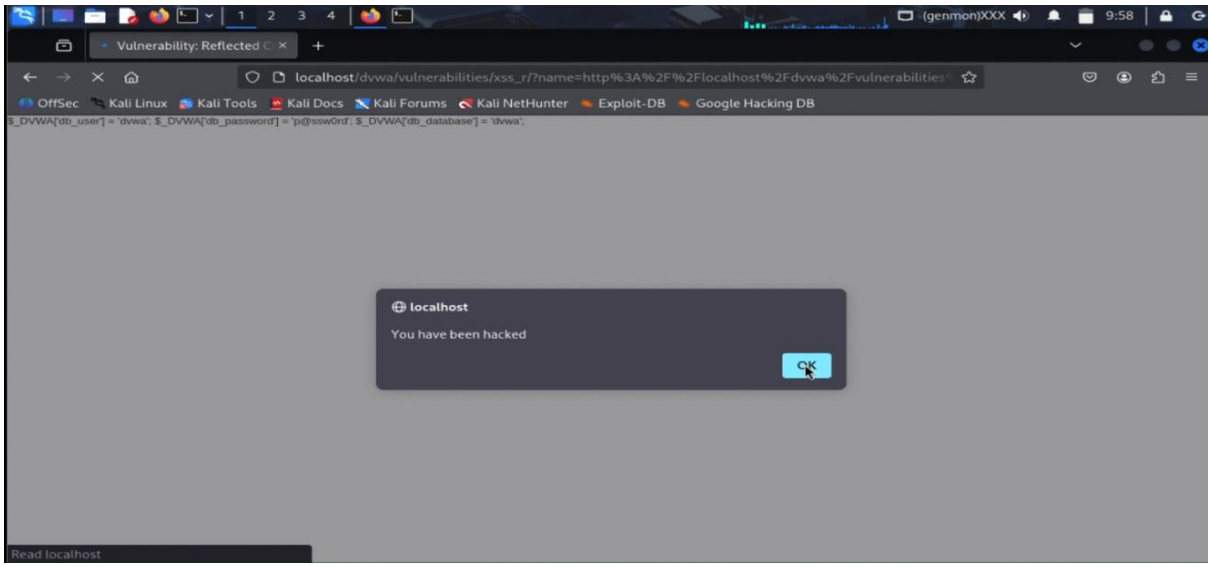
i) Stored

The script is saved in the database. It executes whenever another user views the affected page. More dangerous because it affects many users over time.



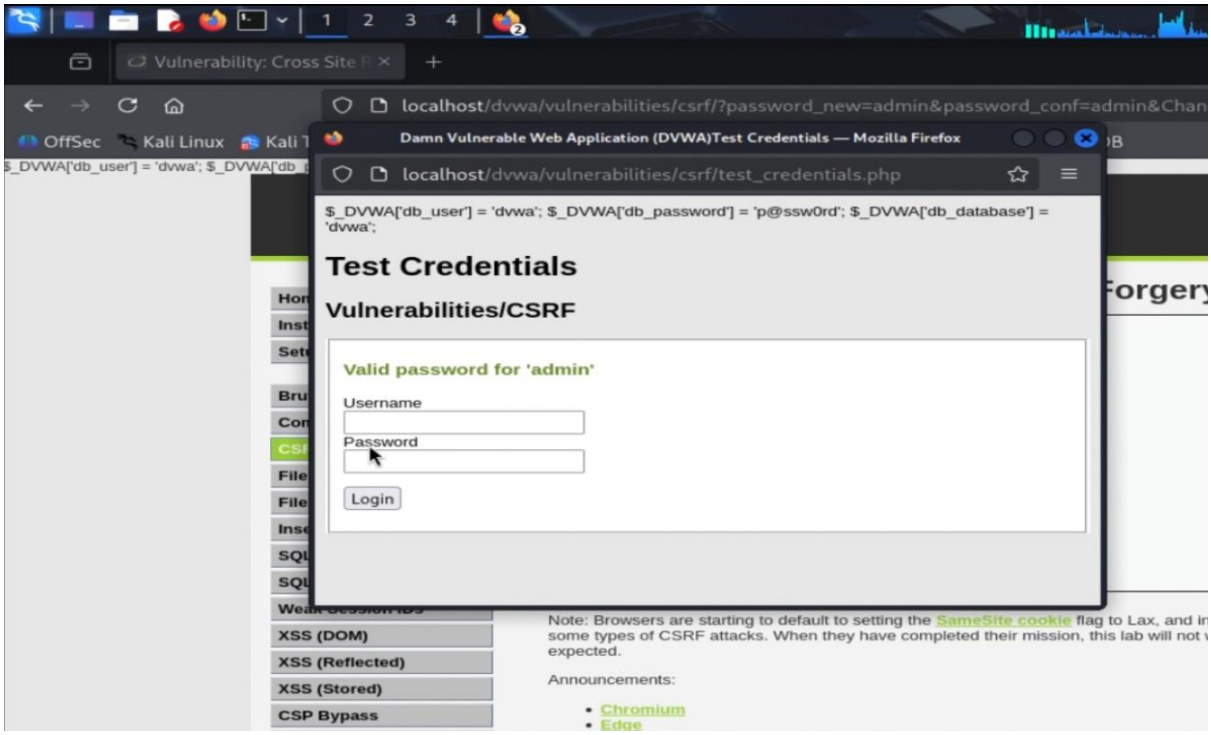
ii) Reflected

Malicious script comes from the current HTTP request. Triggered when the server reflects untrusted input back in the response.



Cross Site Request Forgery (CSRF) :

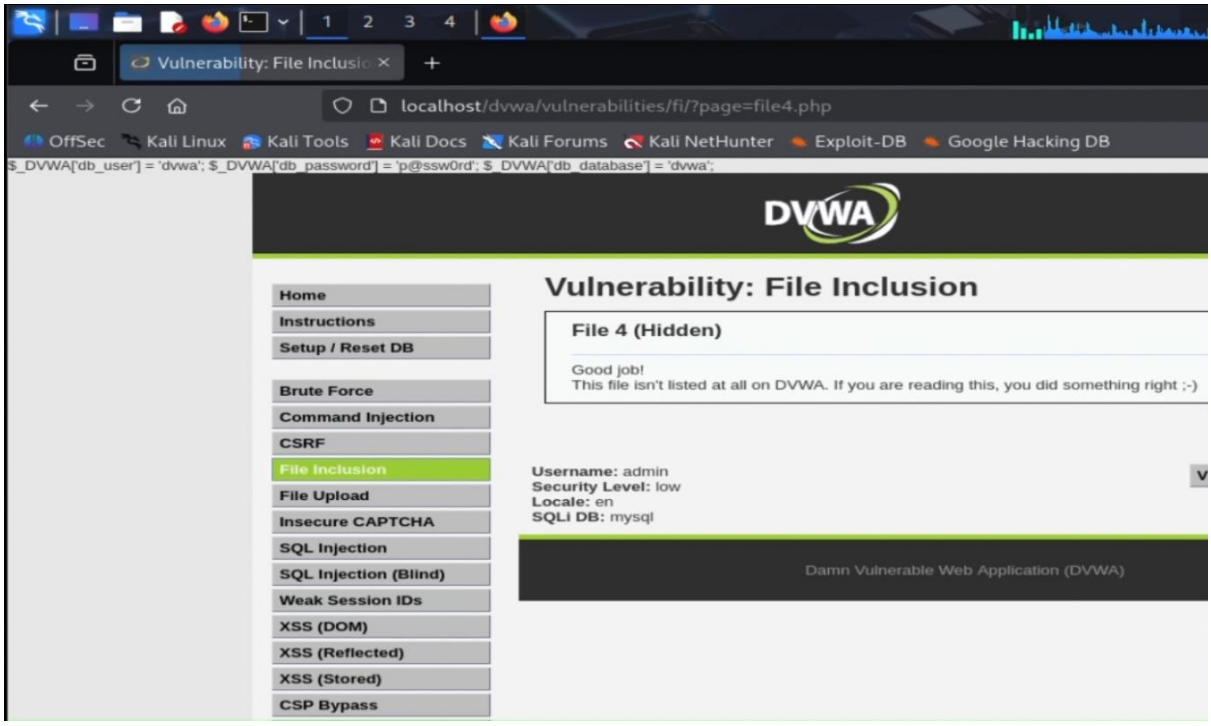
CSRF is a web security vulnerability that allows an attacker to trick a logged-in user's browser into making unintended requests to a web application on behalf of that user.



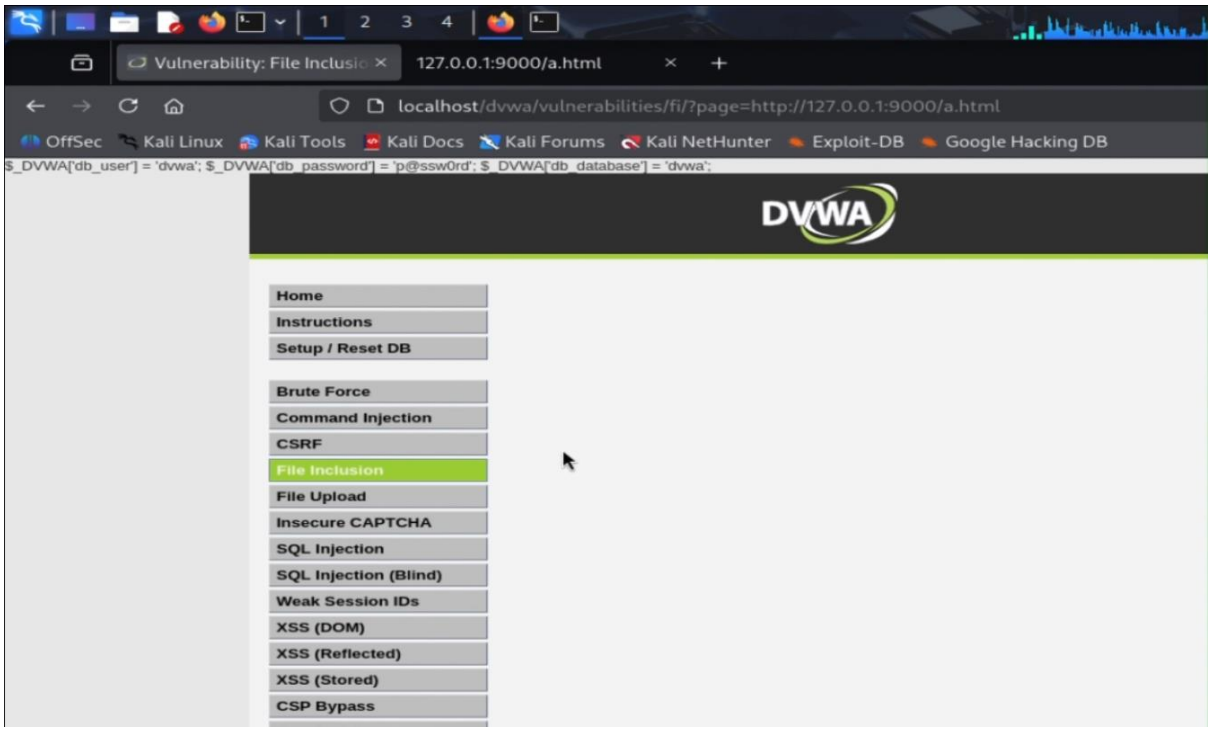
File Inclusion :

A File Inclusion Attack happens when a web application dynamically loads files based on user input but doesn't properly validate that input. Attackers can exploit this to include unauthorized files — either from the local server or from a remote server — and execute malicious code, read sensitive data, or take over the server. There are two types of file inclusion attacks:

i) Local File Inclusion

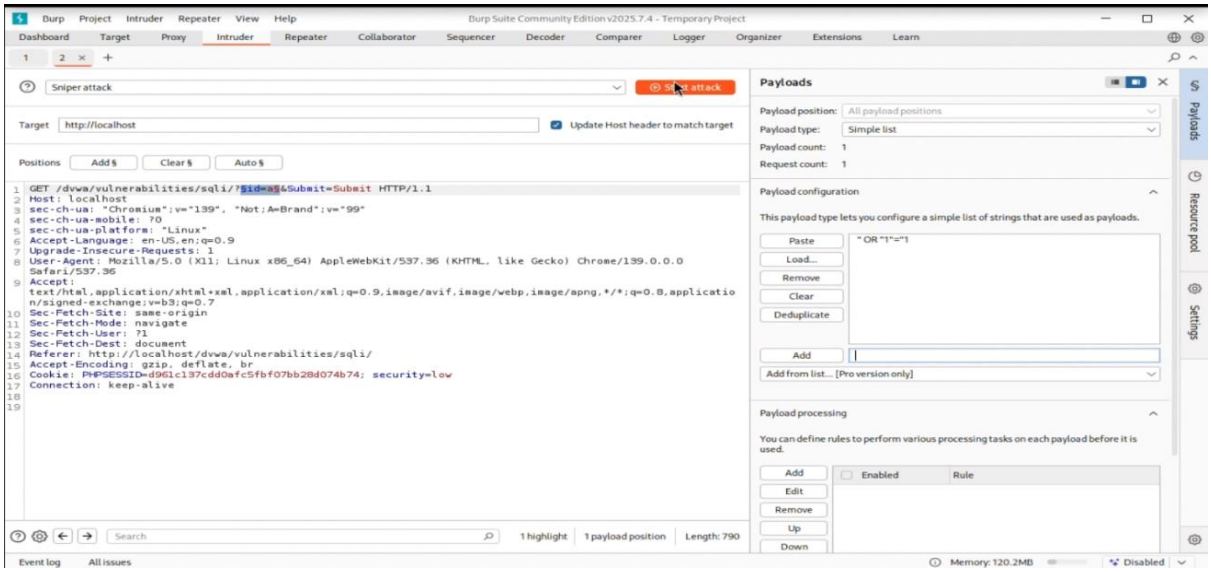


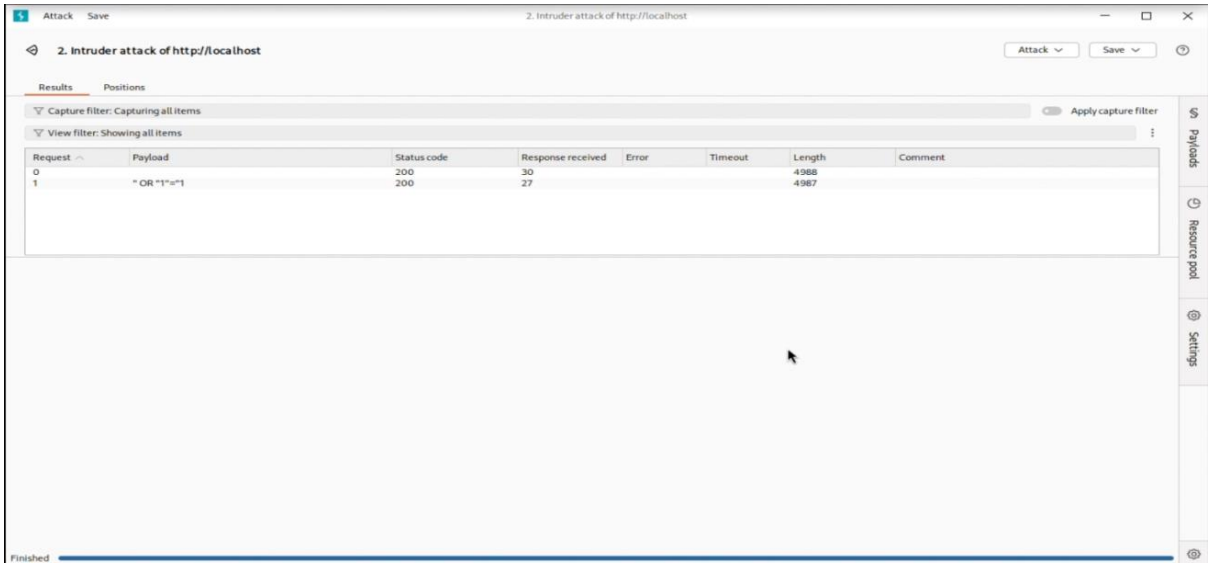
ii) Remote file inclusion



Burpsuite :

Burp Suite is a powerful web application security testing tool developed by PortSwigger. It acts like a proxy between the browser and the target web application, allowing to inspect, modify, and analyze every request and response. It can also be used for intercepting and modifying login requests.




Attack
Save
2. Intruder attack of http://localhost
2. Intruder attack of http://localhost
Attack
Save
Results
Positions
Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items
Request
Payload
Status code
Response received
Error
Timeout
Length
Comment
0
200
30
4988
1
" OR "1"="1
200
27
4987
Payloads
Resource pool
Settings
Finished