Security Testing Report

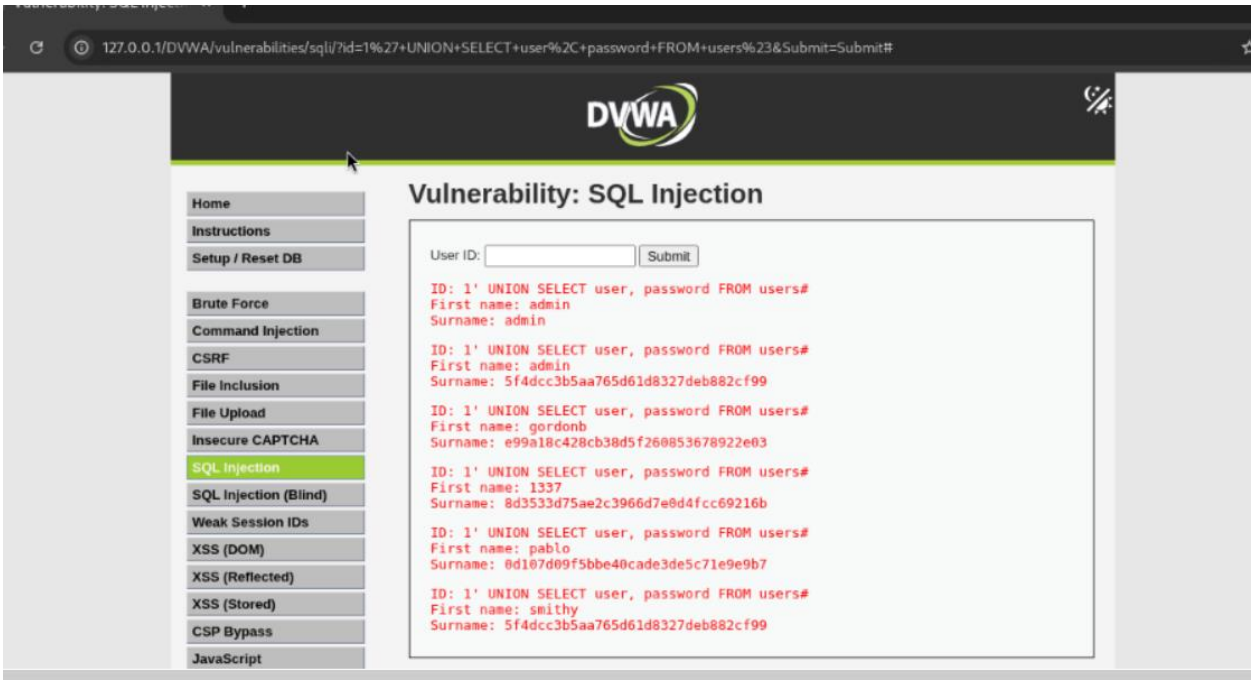
Aman Jiwani

Date:9/10/25

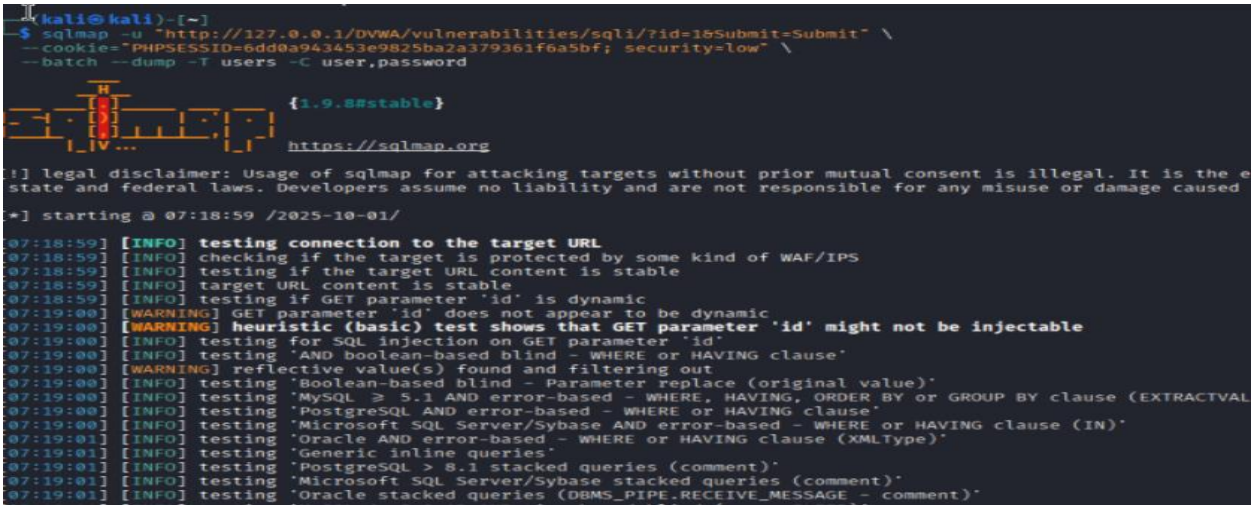
1. SQL Injection

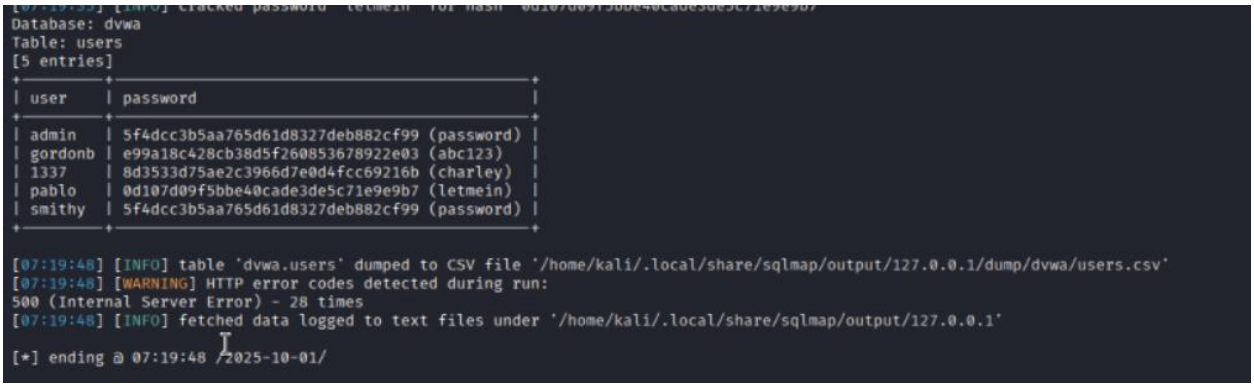
SQL injection (SQLi) is a class of vulnerability where untrusted input is incorporated into SQL commands so an attacker can change the intended query. That can lead to data theft, data corruption, authentication bypass, and full system compromise.

A. Manual SQL Injection (union-based)



B. Automated dump using sqlmap





2. Cross Site Scripting XSS

XSS is a class of web vulnerability where an application includes untrusted data in web pageswithout proper validation or escaping, allowing an attacker to execute arbitraryJavaScript (or other active content) in victims' browsers under the site's origin. Thatscript can steal tokens, perform actions as the user, alter page content, or load furthermalicious content.

A. Stored XSS

Description: Malicious script is saved by the application (e.g., in a comment or profile field) and runs when other users view the stored content.

Example payload used:

```
<body onload=alert('test')>
```

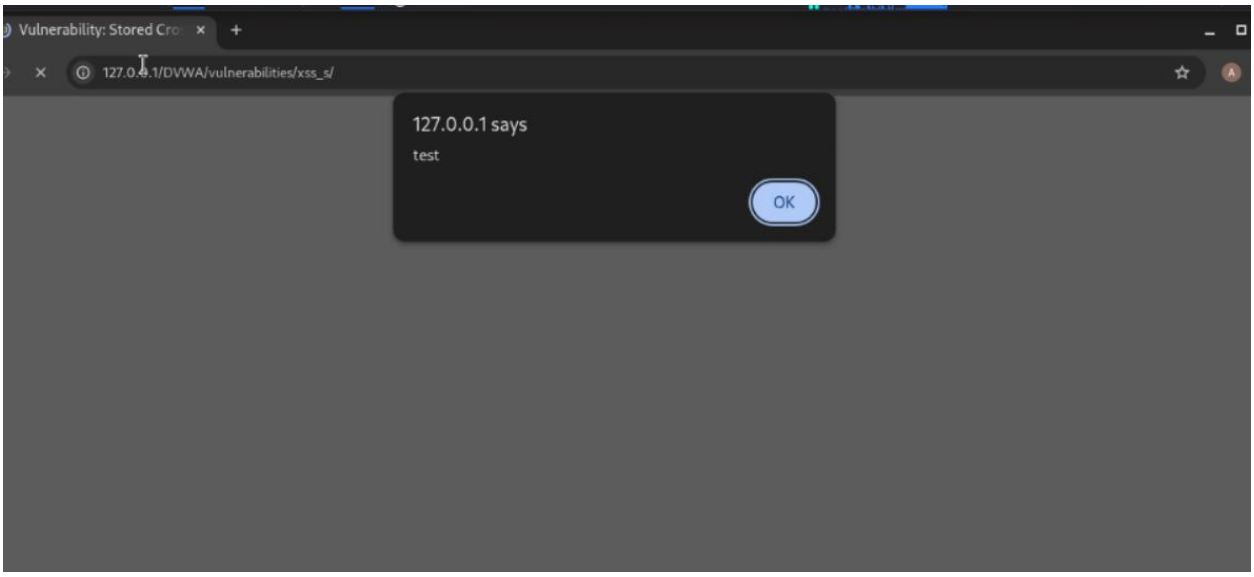
This payload triggers a browser alert when the stored HTML is rendered directly into a page without encoding.

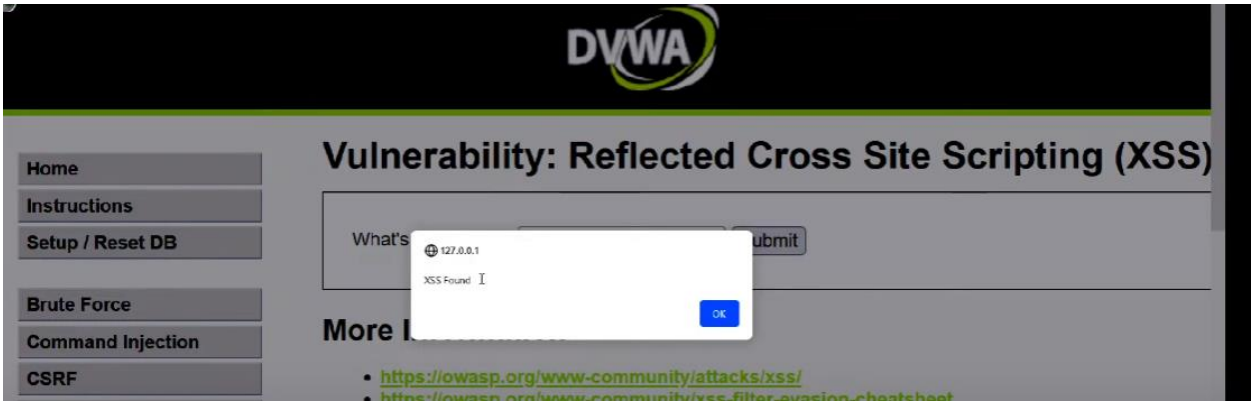
B. Reflected XSS

Description: Attacker-controlled input is reflected in the server response and executed immediately (e.g., search, error messages, query parameters).

Example payload used:

```
<script>alert("XSS Found");</script>
```





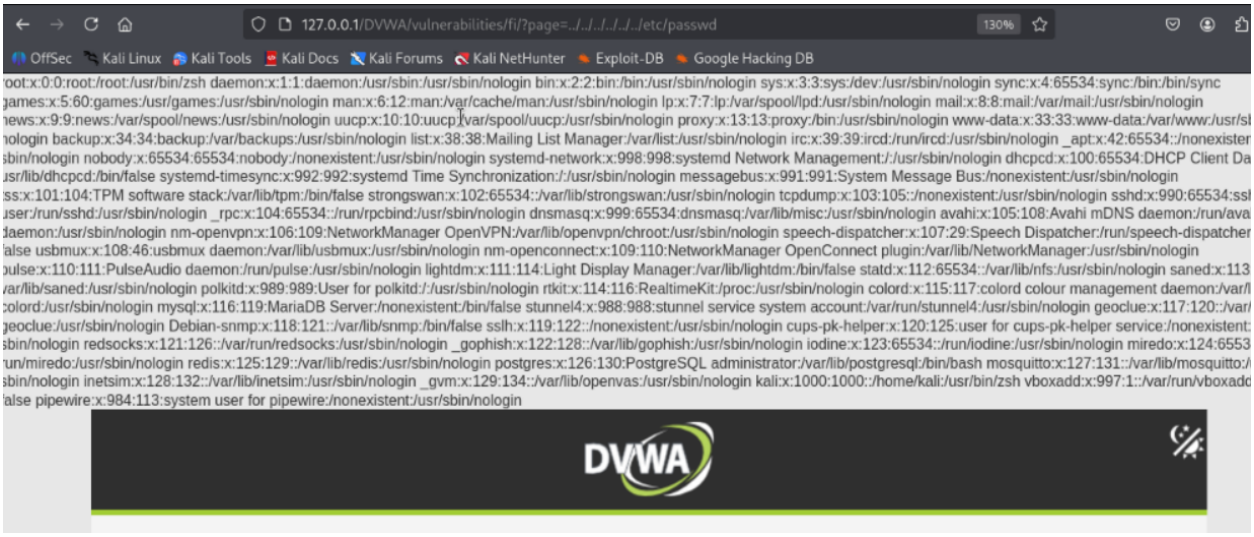
3.File Inclusion Attack

It is an attack that allows an attacker to include a file on the web server through a php script. This vulnerability arises when a web application lets the client submit input into files or upload files to the server. A file include vulnerability is distinct from a generic Directory Traversal Attack, in that directory traversal is a way of gaining unauthorized file system access, and a file inclusion vulnerability subverts how an application loads The flaw in this code is a Cross-Site Request Forgery (CSRF) vulnerability. The code uses the HTTP Referer header to check if the request came from the same server, assuming it's a trusted source. However, the Referer header can be easily manipulated by an attacker. This allows an attacker to create a malicious website or craft a URL that makes a request to this script, tricking the user's browser into performing an unwanted action on their behalf, such as changing their password without their knowledge or consent. 4. What is File Inclusion Attack? code for execution. Successful exploitation of a file include vulnerability will result in remote code execution on the web server that runs the affected web application. Now start your machine and login to DVWA, then go to DVWA security tab and

change the difficulty level to low. Go to file inclusion tab and change the URL from incude.php to ?page= ../../../../../../etc/passwd. LFI vulnerabilities allow an attacker to read (and sometimes execute) files on the victim machine. This can be very dangerous because if the web server is misconfigured and running with high privileges, the attacker may gain access to sensitive information. If the attacker is able to place code on the web server through other means, then they may be able to execute arbitrary commands. RFI vulnerabilities are easier to exploit but less common. Instead of accessing a file on the local machine, the attacker is able to execute code hosted on their own machine. Remote File inclusion (RFI) and Local File Inclusion (LFI) are vulnerabilities that are often found in poorly-written web applications. These vulnerabilities occur when a web application allows the user to submit input into files or upload files to the server

A.LFI

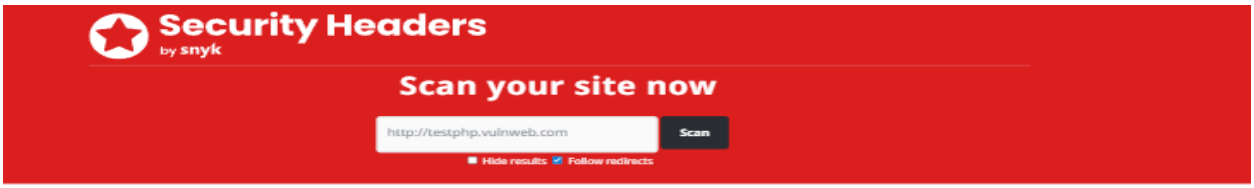
?page= ../../../../../../etc/passwd.

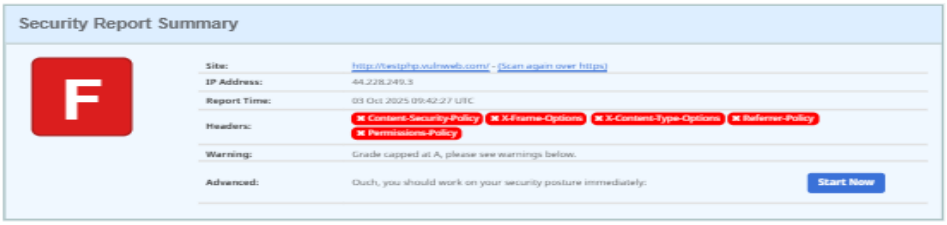


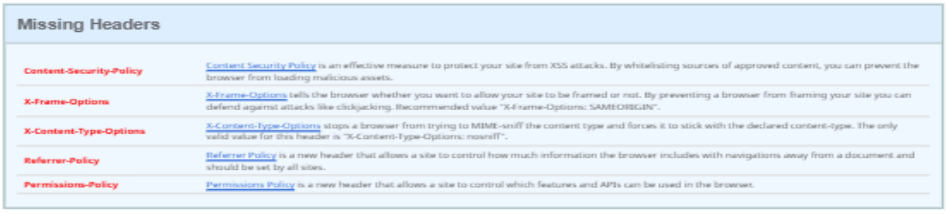
B.RFI

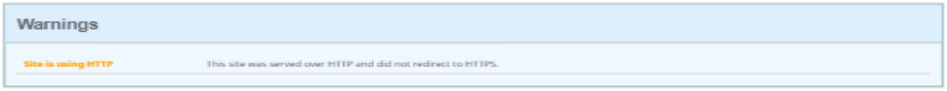
4. Web Header Security

A. Security Header Scan

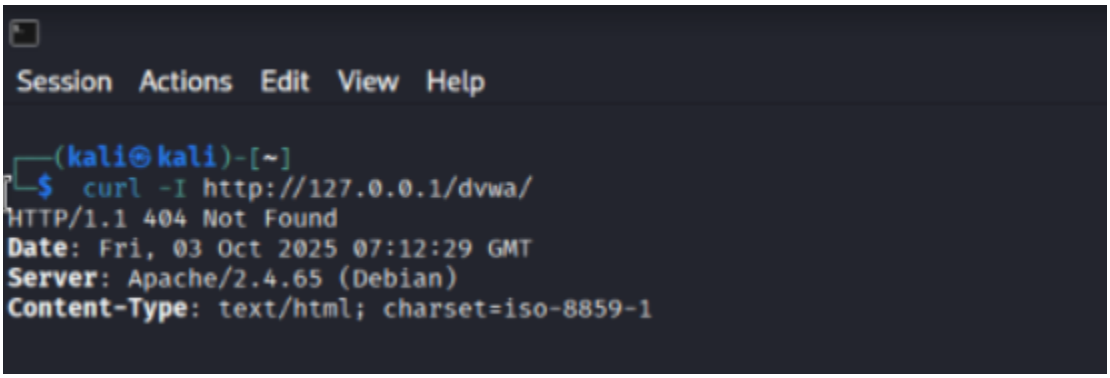






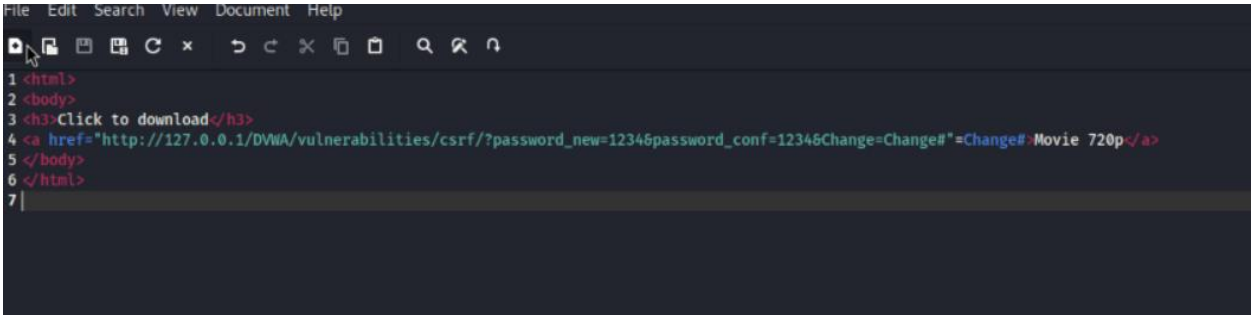


B. ADD Http header

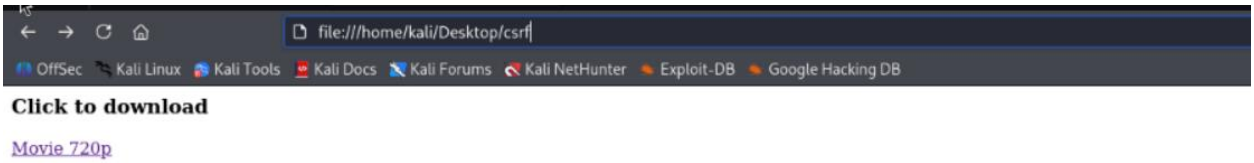


5.CSRF

A.Html code



B.Htmlpage



C.Paswword change to 1234