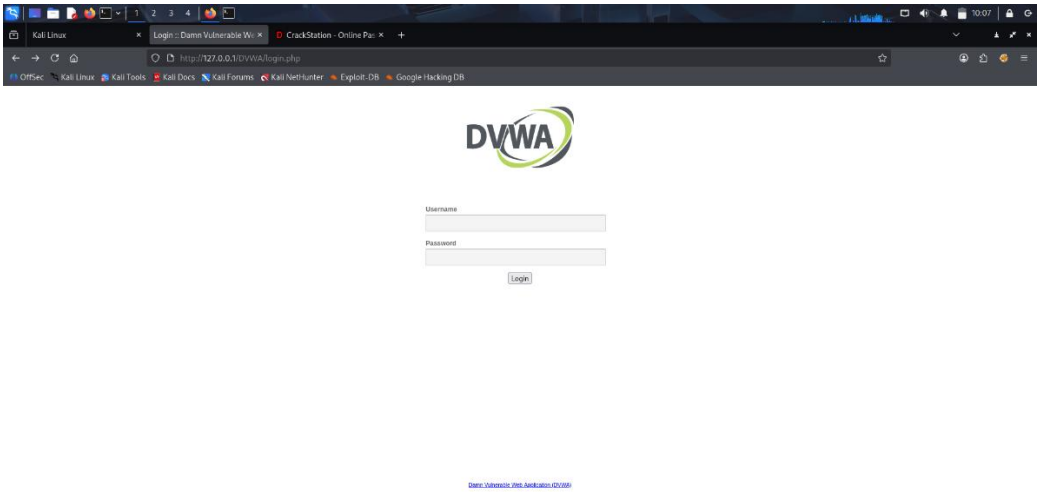
Task 3 — Web Application Security

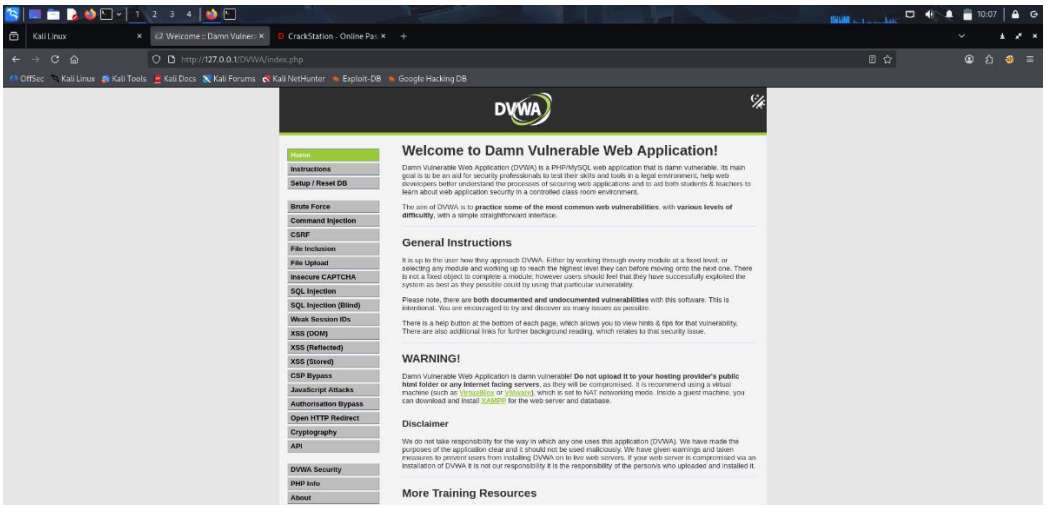
Intern Name: **Nitesh Sharma** Date: **05/10/2025**

Objective:-

In a controlled lab environment identify, validate and safely exploit OWASP Top 10 vulnerability to assess application security, all testing will be authorized, non-destructive, and aimed at improving security posture through documented findings and remediation recommendations.

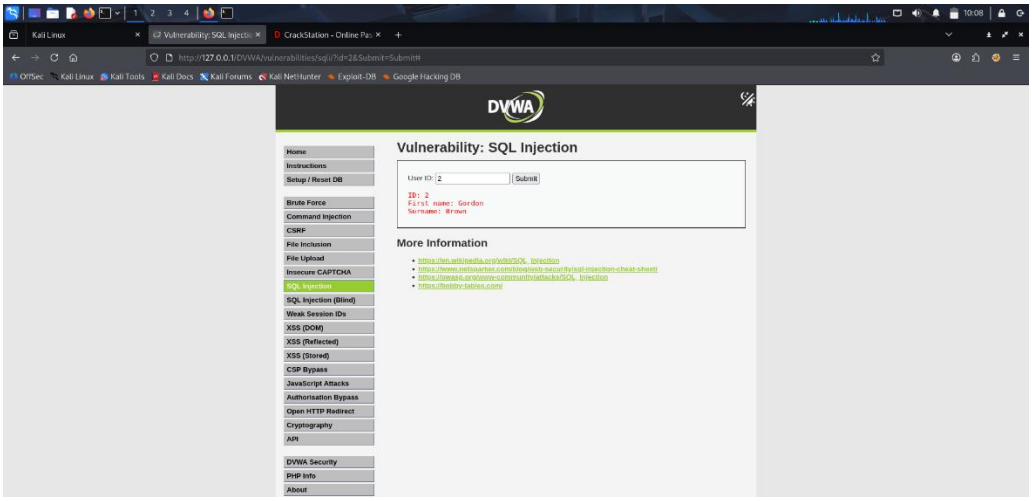
1. **SQL Injection:-**

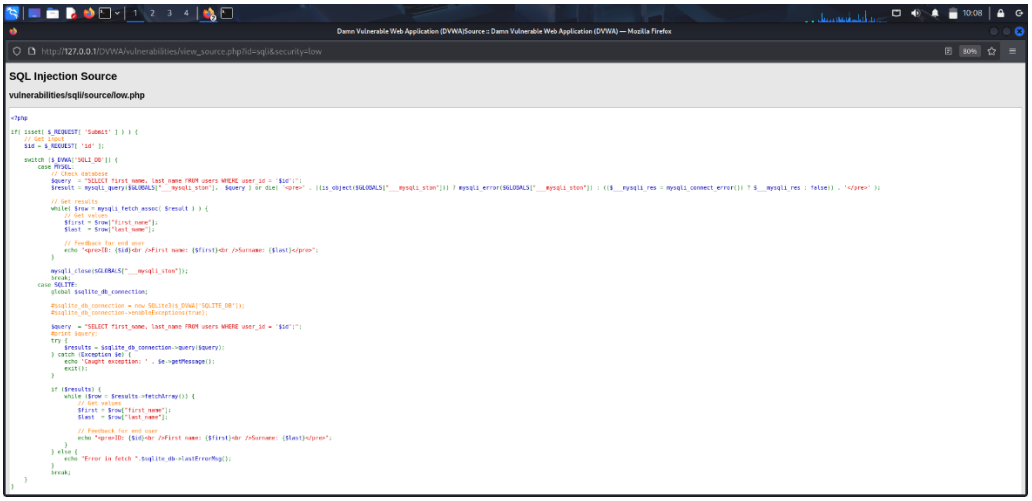


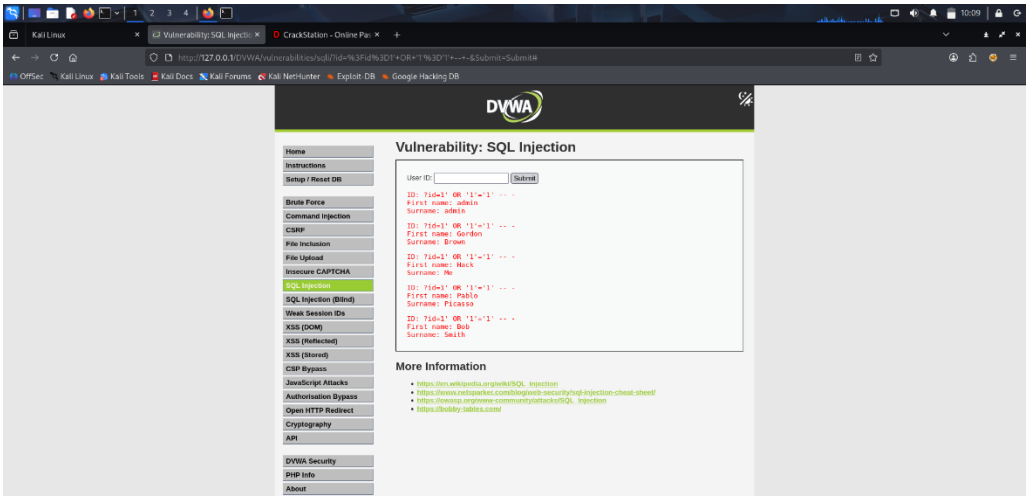


Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**

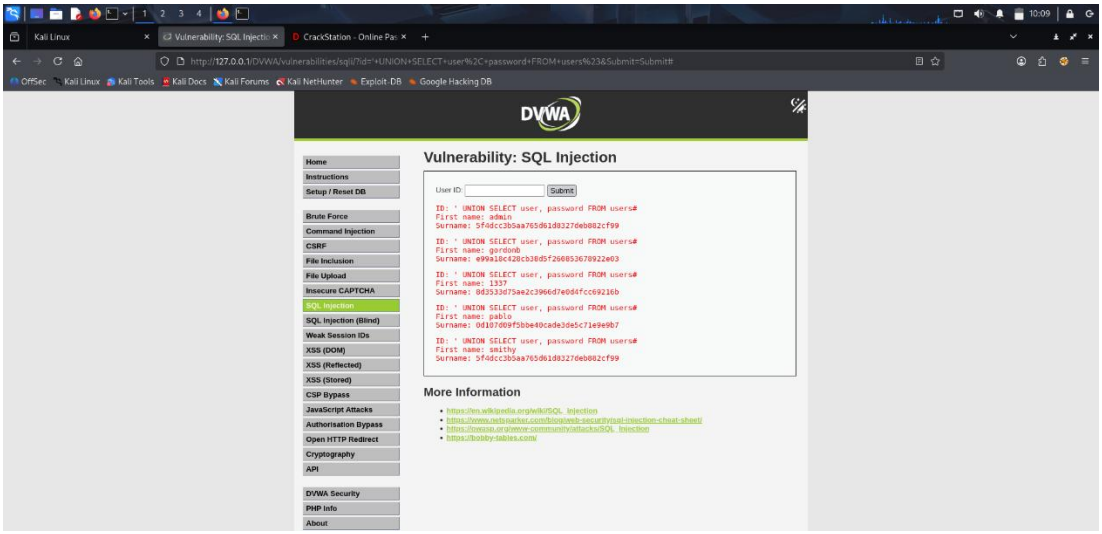


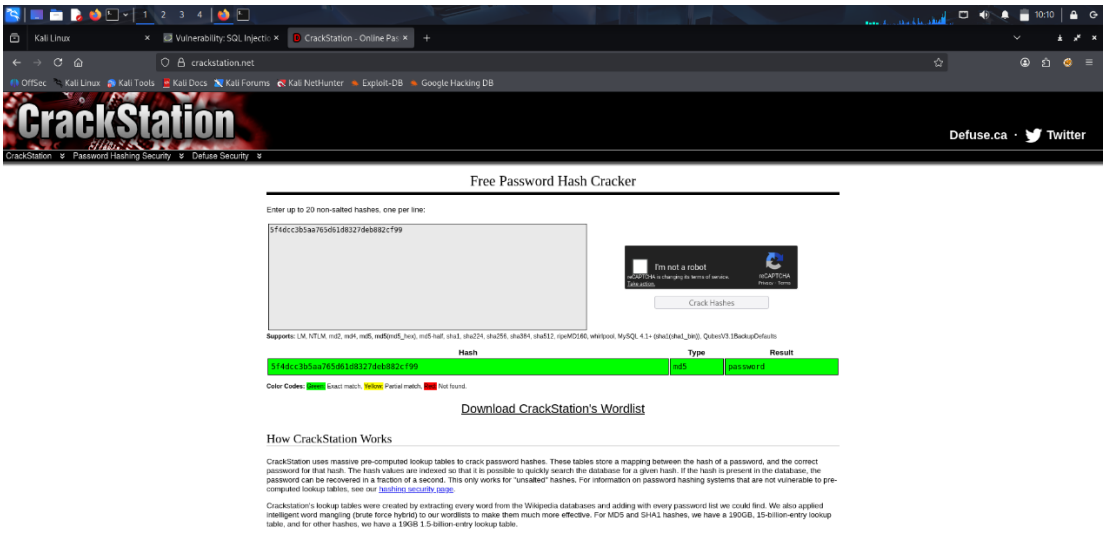




Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**





Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**

(Demonstrate prevention using Prepared Statement):-

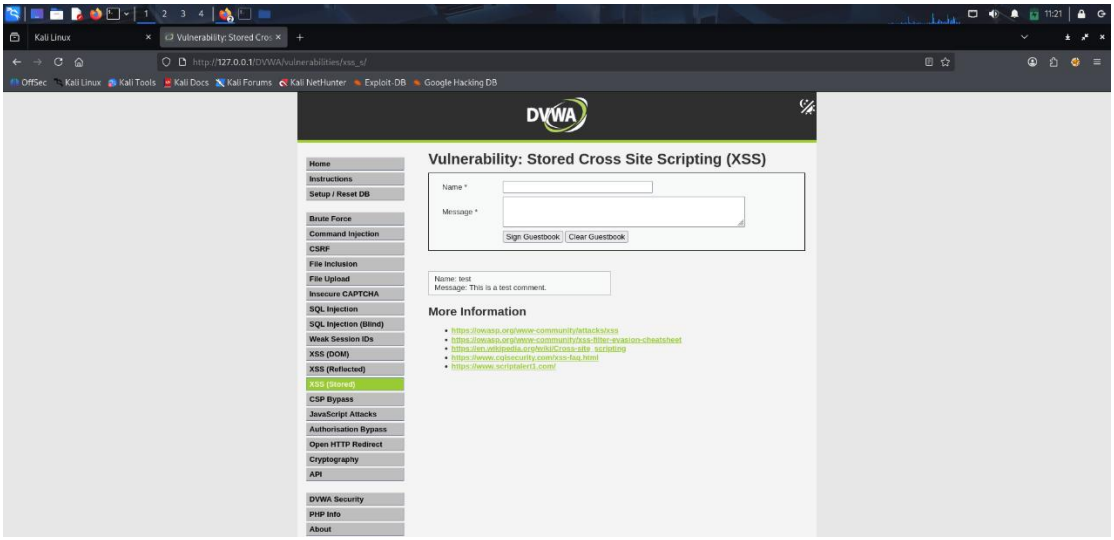
```
<?php

if( isset( $_REQUEST['Submit'] ) ) {
  // Get input
  $id = $_REQUEST['id'];

  switch ($_DVWA['SQLI_DB']) {
    case MYSQL:
      // Check database connection
      $query  = "SELECT first_name, last_name FROM users WHERE user_id = ?";

      // Prepare statement
      if ($stmt = mysqli_prepare($GLOBALS["___mysqli_ston"], $query)) {
        // Bind the input parameter
        mysqli_stmt_bind_param($stmt, "i", $id); // "i" means integer

        // Execute the statement
        mysqli_stmt_execute($stmt);

        // Get the result
        $result = mysqli_stmt_get_result($stmt);

        // Fetch results
        while ($row = mysqli_fetch_assoc($result)) {
          $first = $row["first_name"];
          $last = $row["last_name"];
          echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
        }

        // Close statement
        mysqli_stmt_close($stmt);
      } else {
        echo "Failed to prepare the query.";
      }

      // Close connection
      mysqli_close($GLOBALS["___mysqli_ston"]);
      break;

    case SQLITE:
      global $sqlite_db_connection;

      $query = "SELECT first_name, last_name FROM users WHERE user_id = :id";

      try {
        // Prepare statement
        $stmt = $sqlite_db_connection->prepare($query);
```

Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**

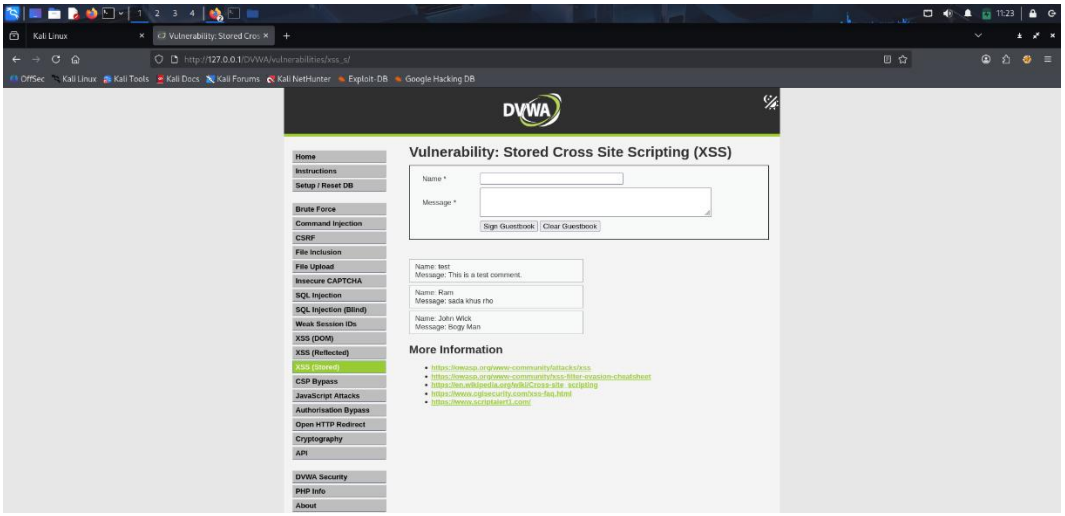
```
            // Bind parameters
            $stmt->bindValue(':id', $id, SQLITE3_INTEGER);

            // Execute the query
            $results = $stmt->execute();

            // Fetch results
            while ($row = $results->fetchArray()) {
              $first = $row["first_name"];
              $last = $row["last_name"];
              echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
            }

        } catch (Exception $e) {
            echo 'Caught exception: ' . $e->getMessage();
        }
        break;
    }
}
?>
```

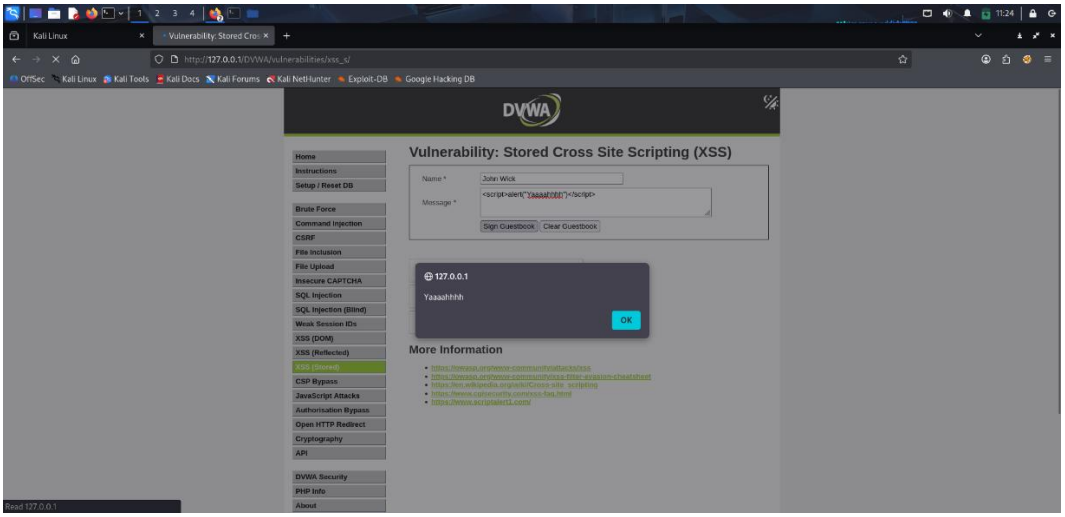
2. Cross-Site Scripting (XSS):-

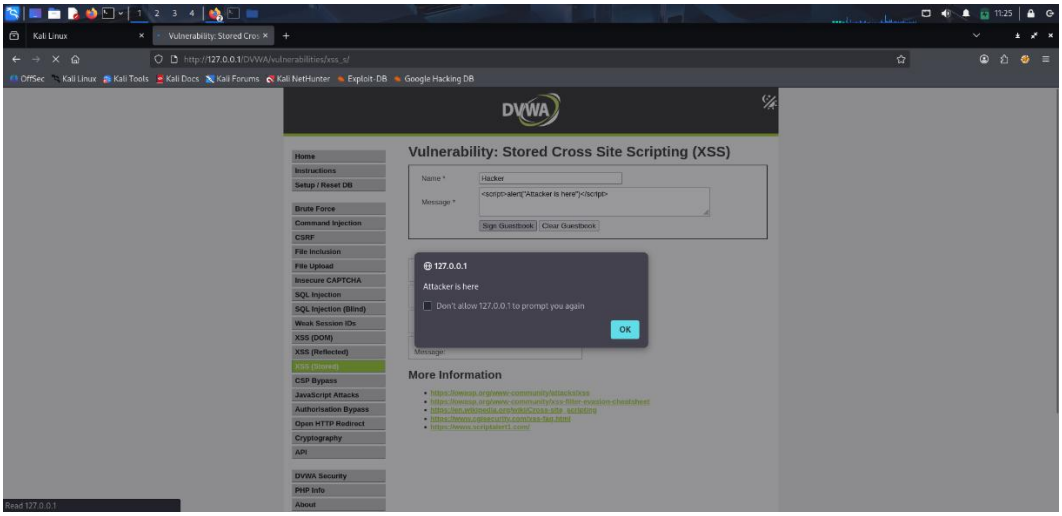


Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**

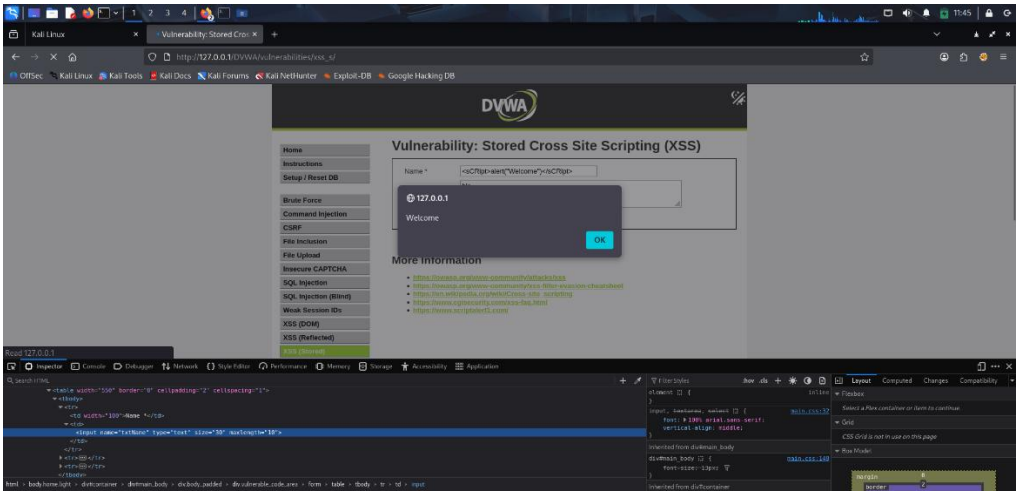


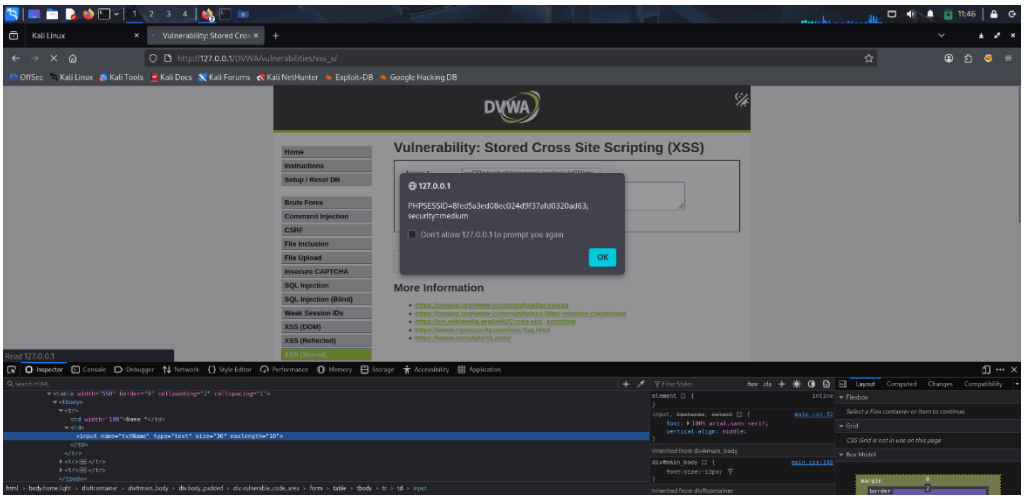




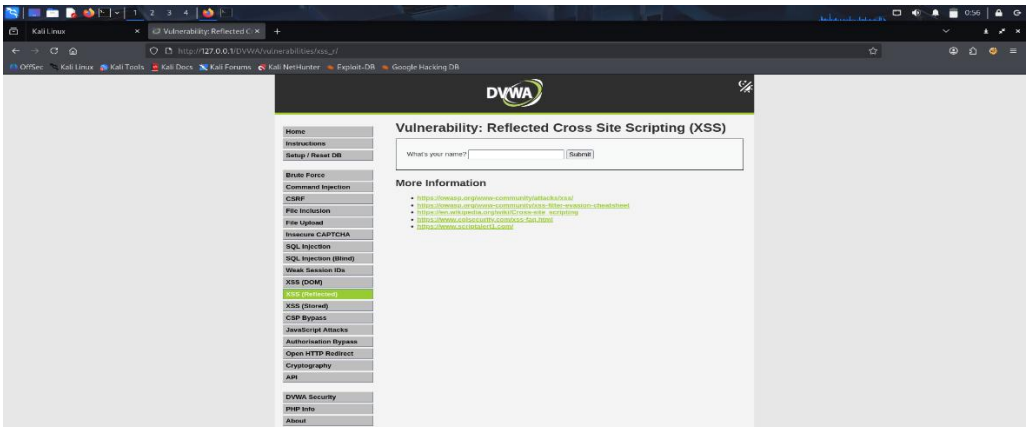
Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**



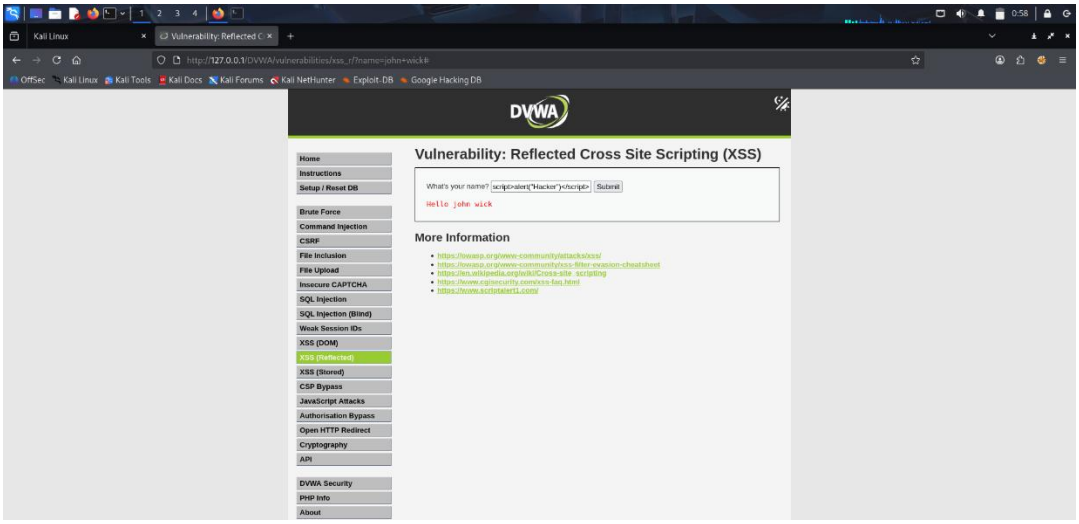


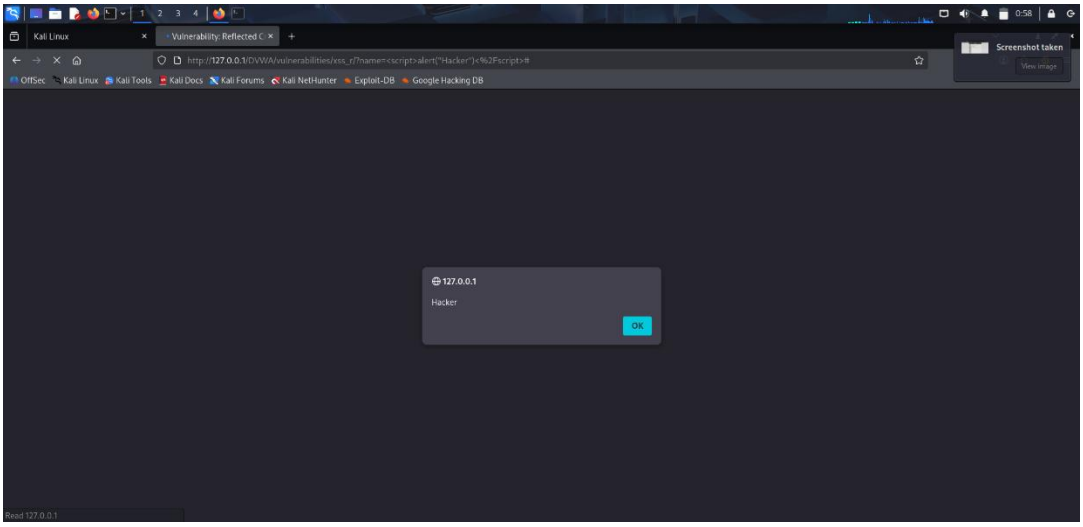
Reflected XSS using query parameters:-

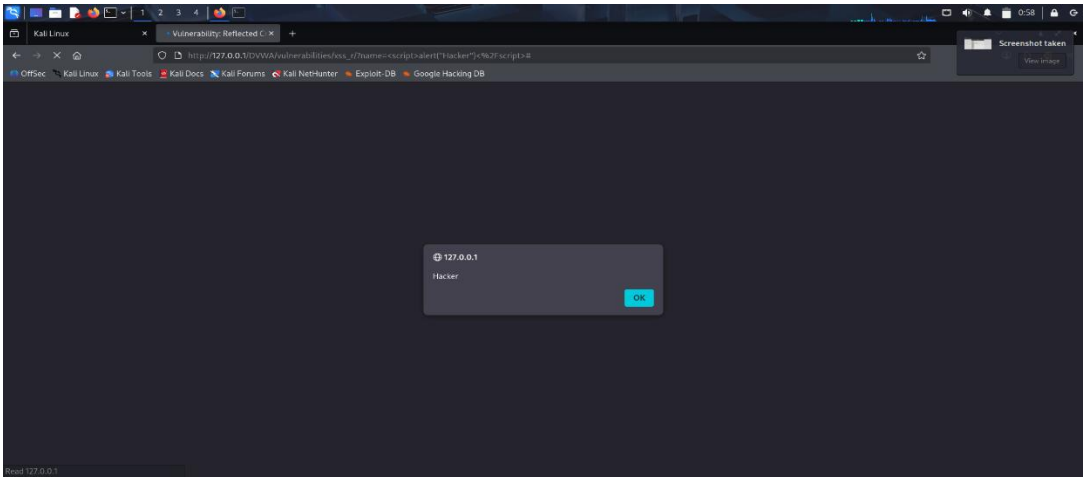


Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**

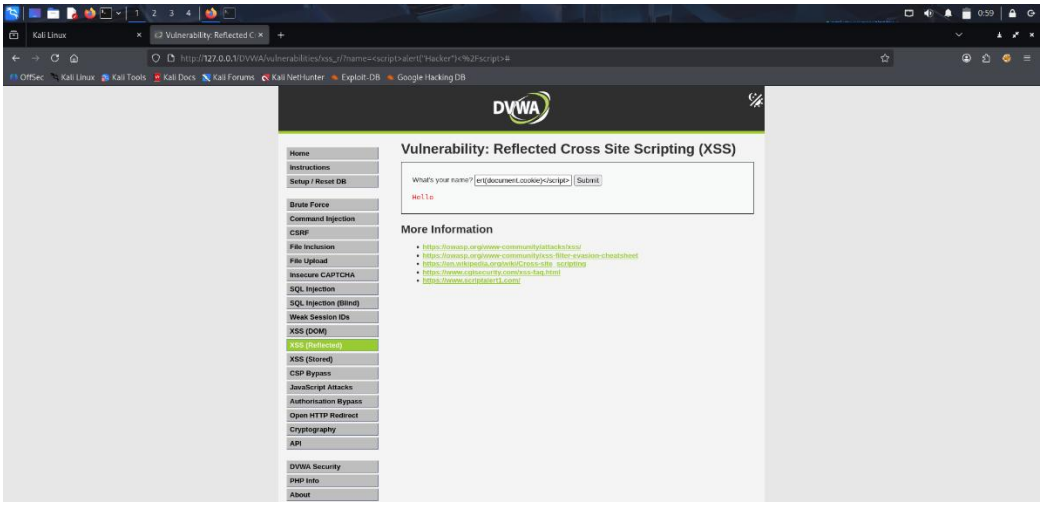


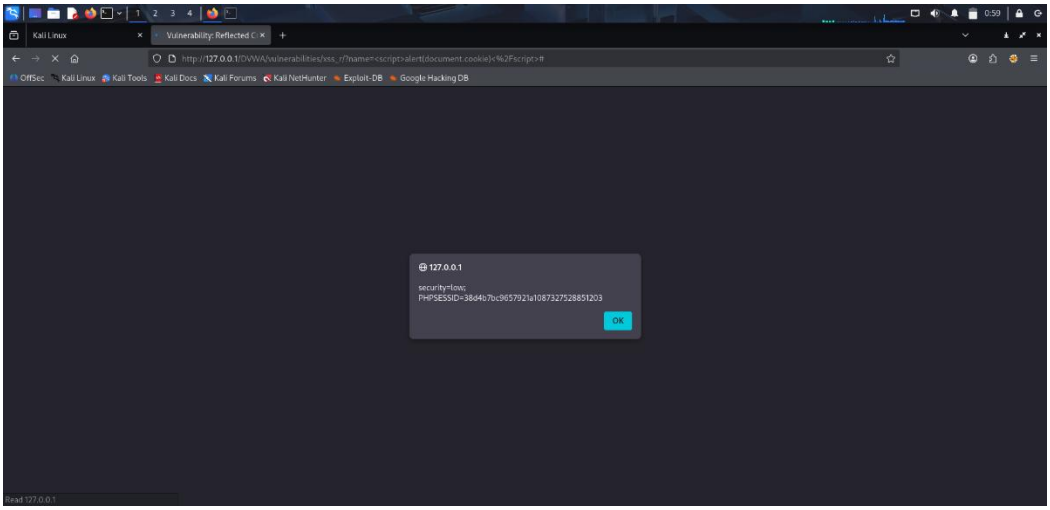


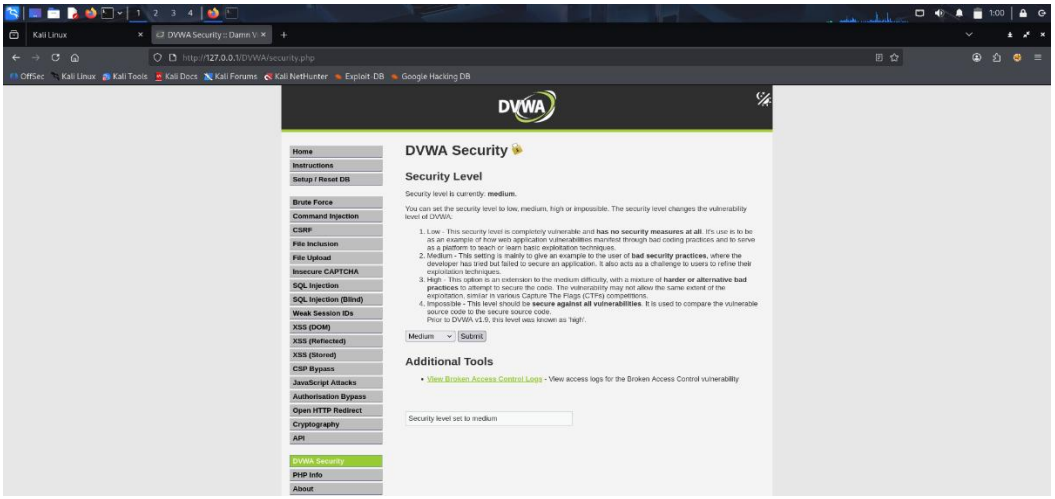


Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**

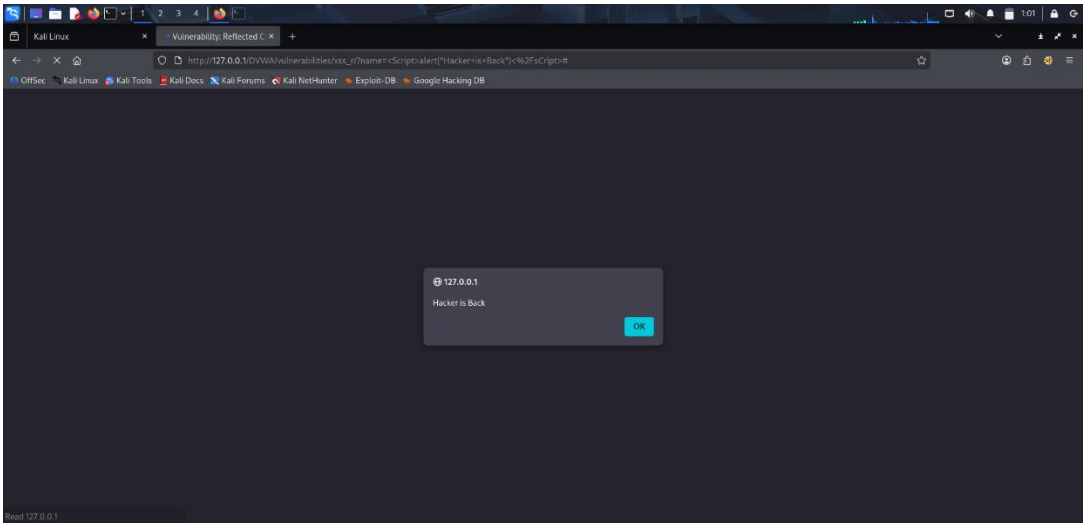


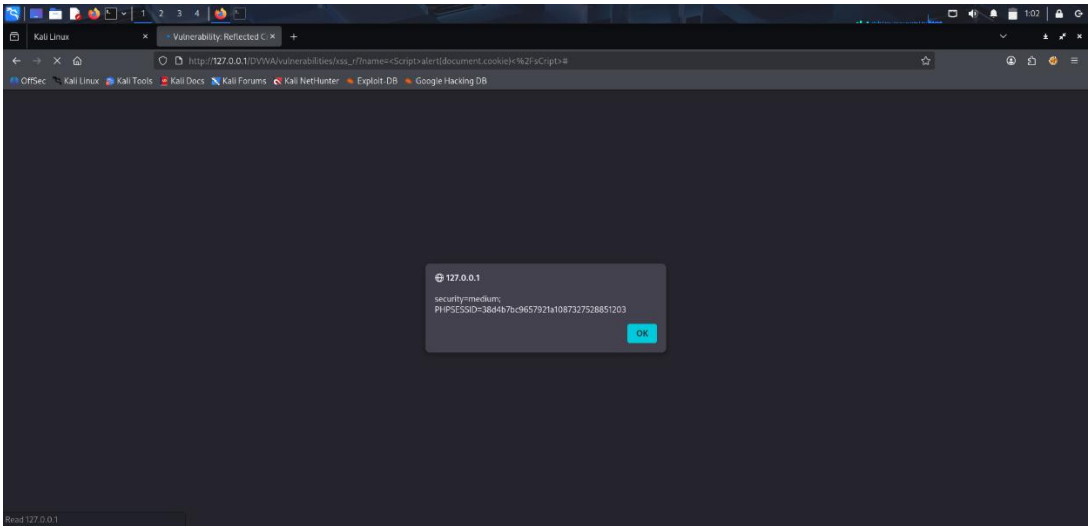




Task 3 — Web Application Security

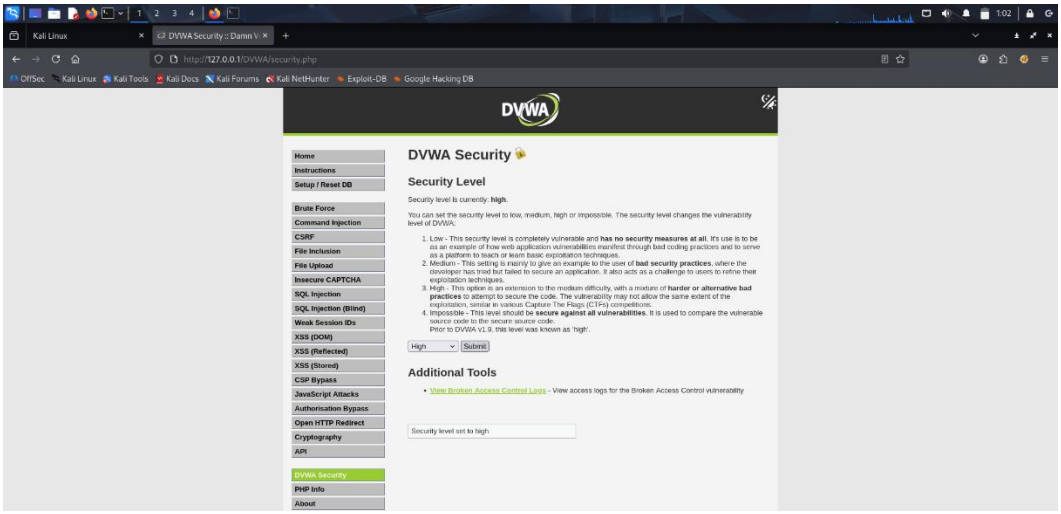
Intern Name: **Nitesh Sharma** Date: **05/10/2025**

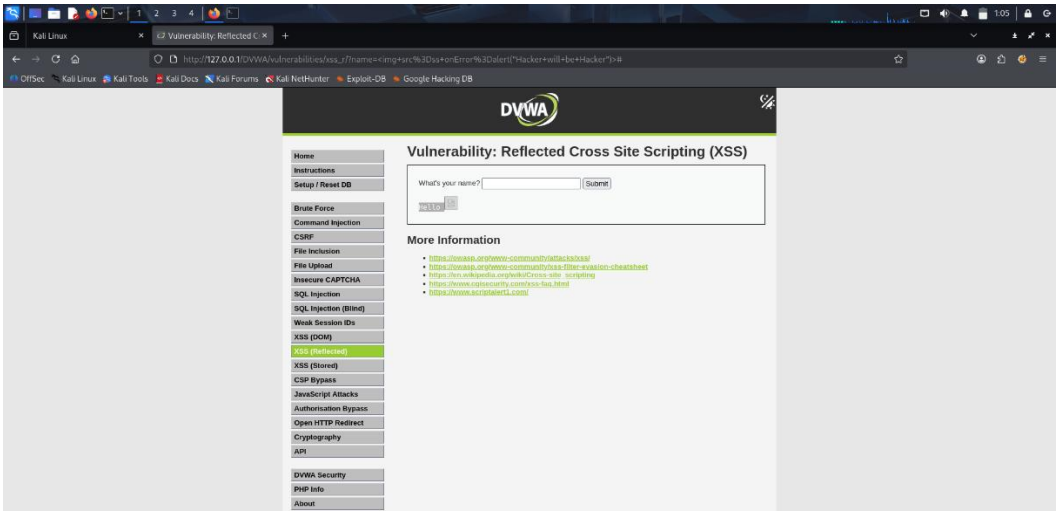


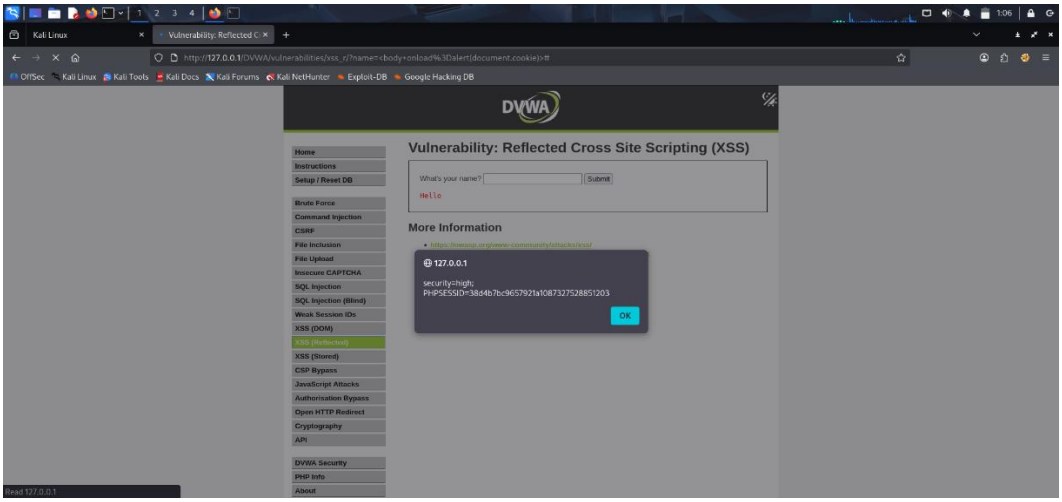


Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**



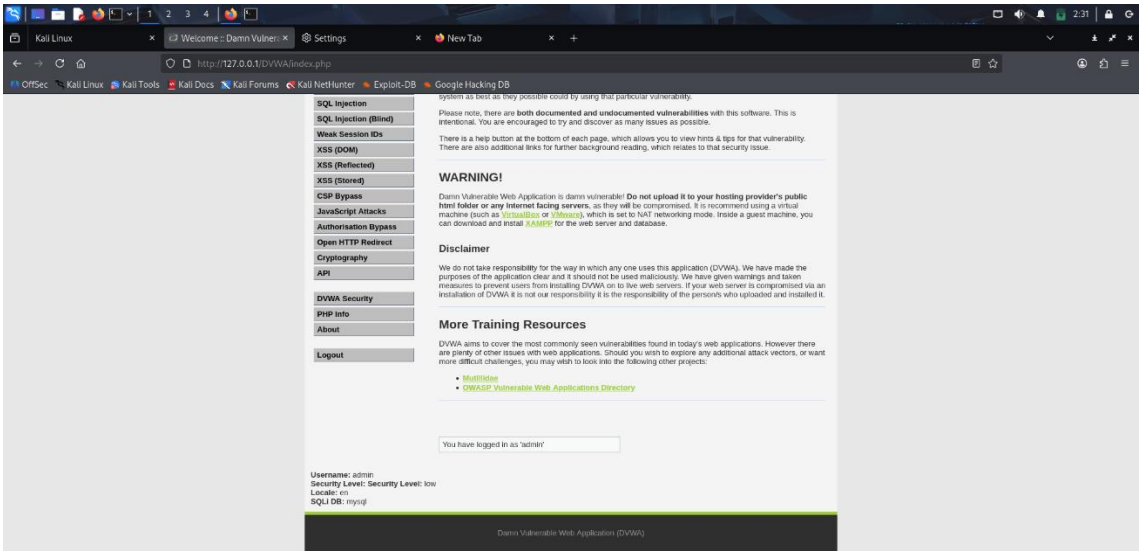


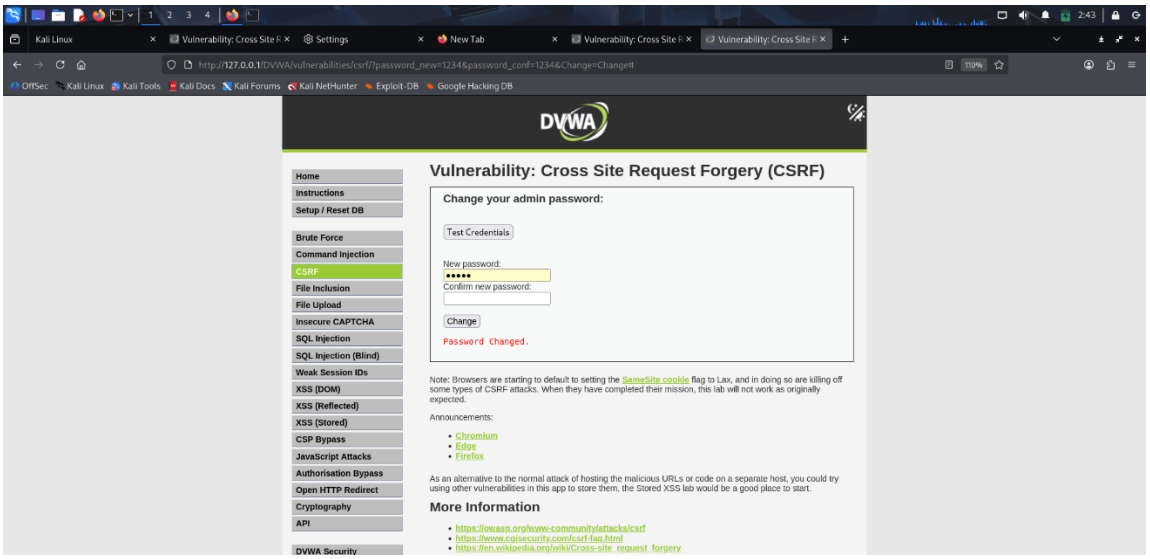


Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**

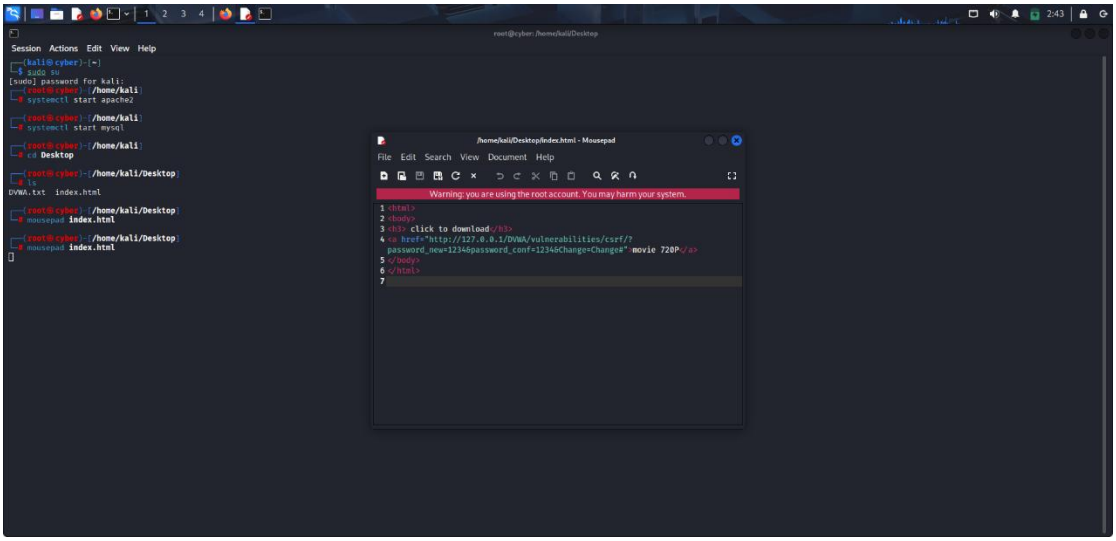
3. Cross-Site Request Forgery (CSRF):-

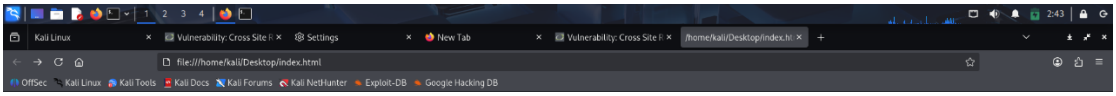




Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**



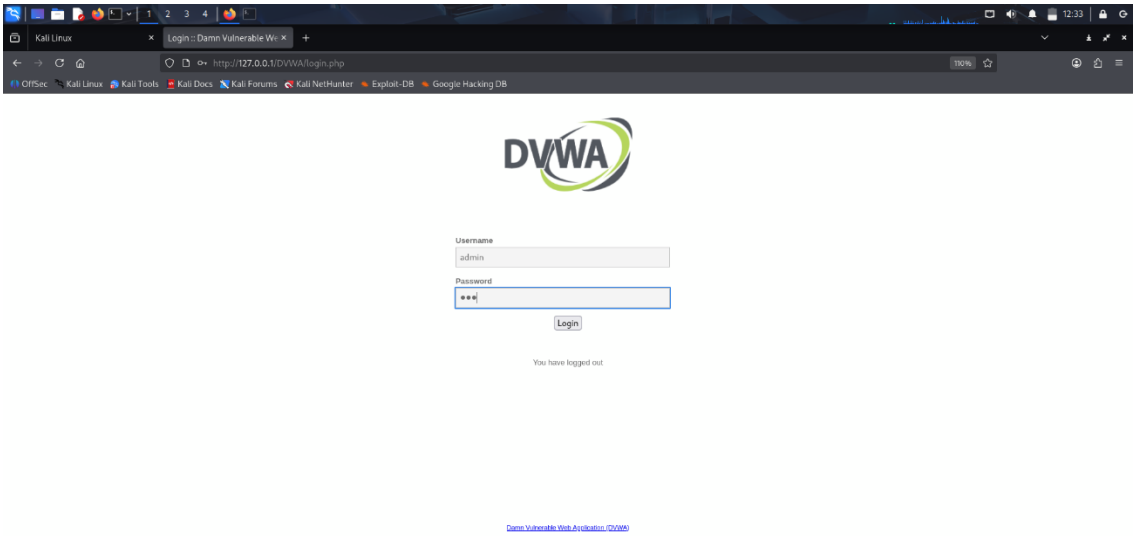


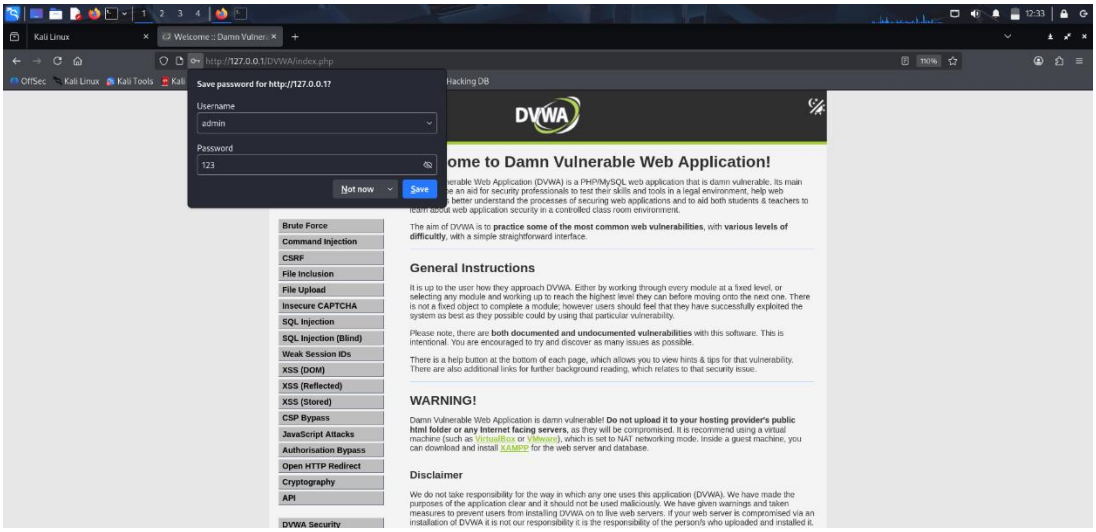
click to download

movie 720P

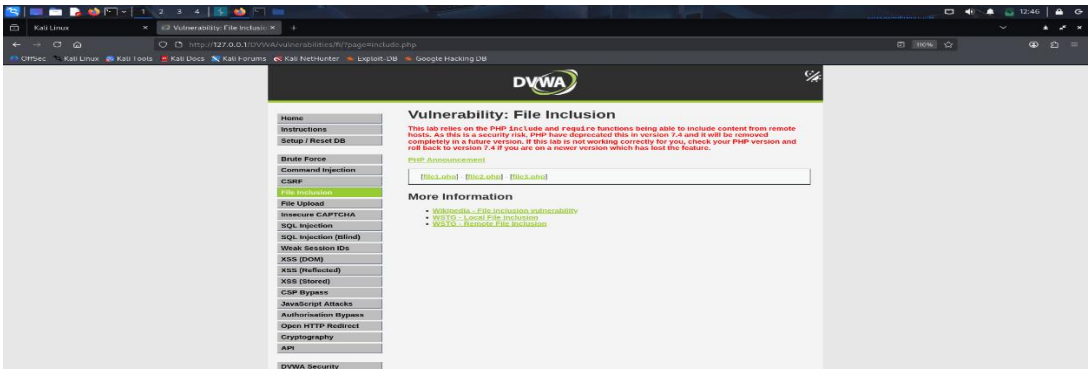
Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**



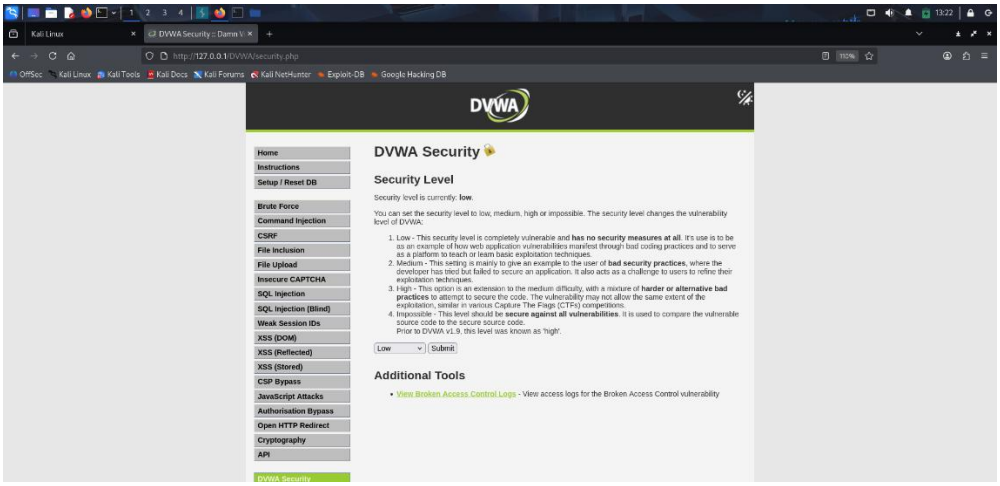


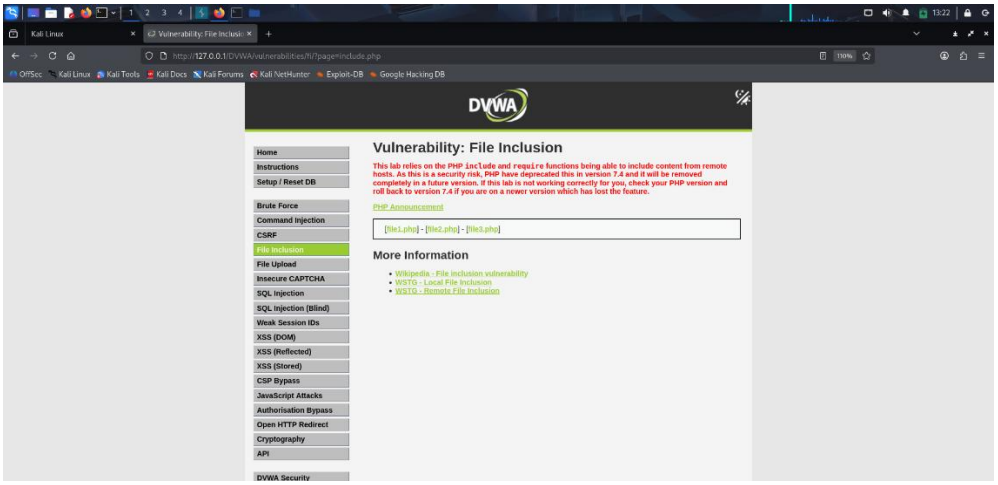
4. File inclusion attack:-

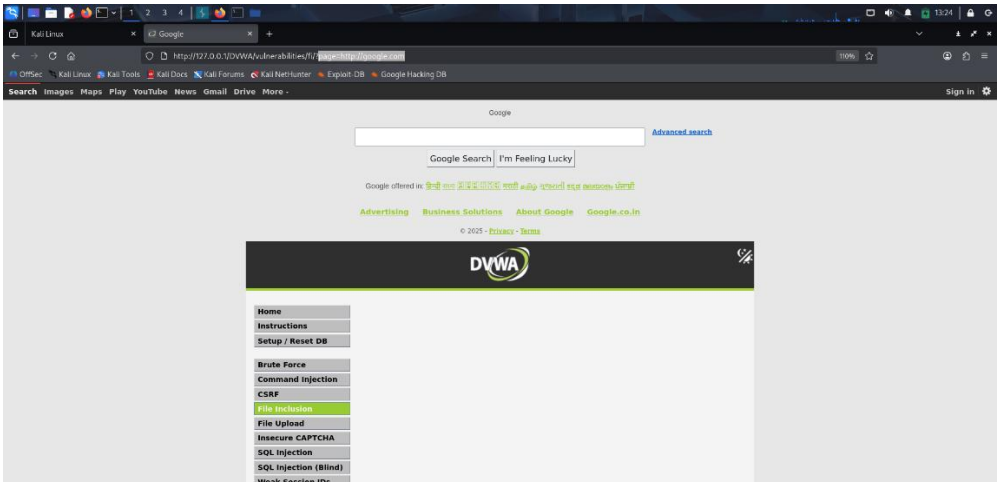


Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**

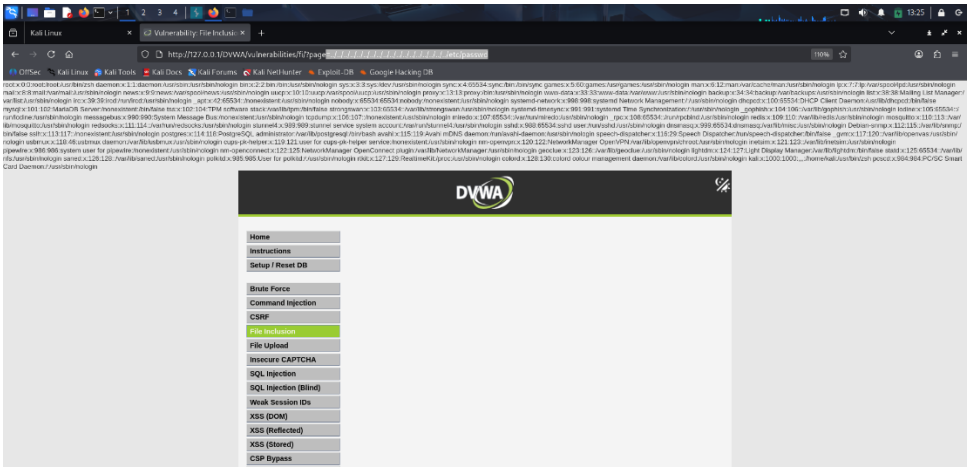


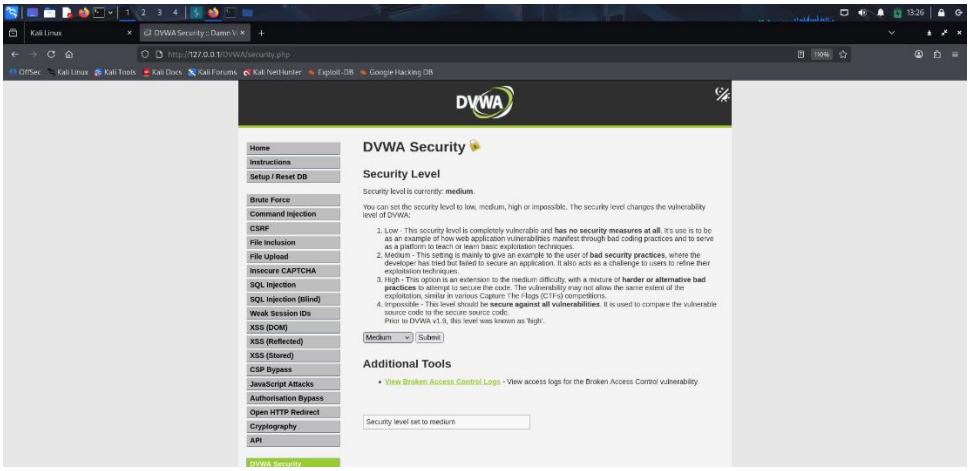


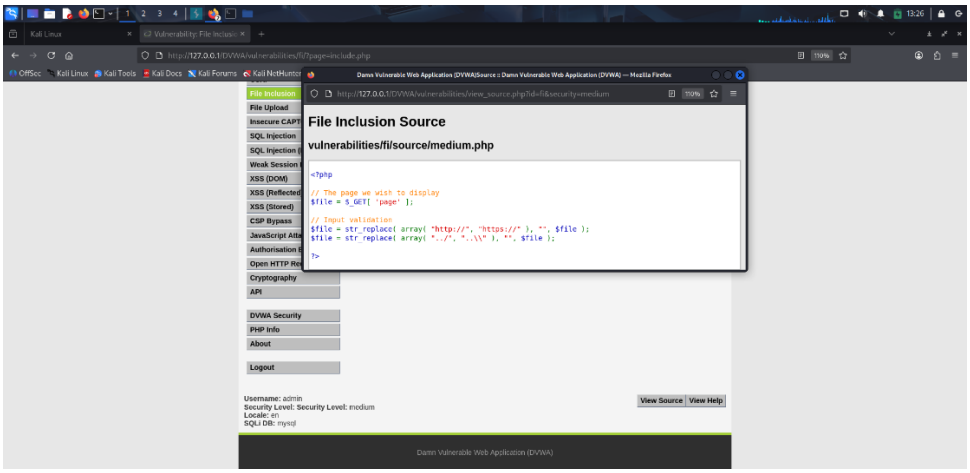


Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**

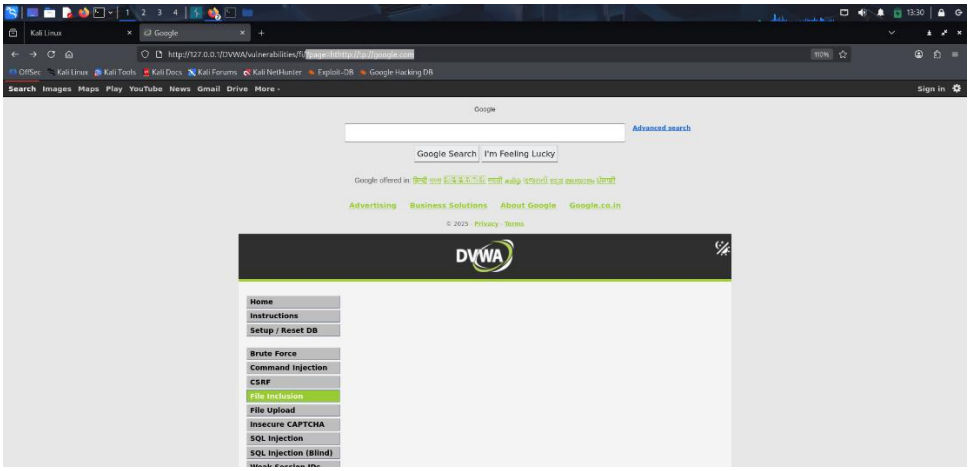


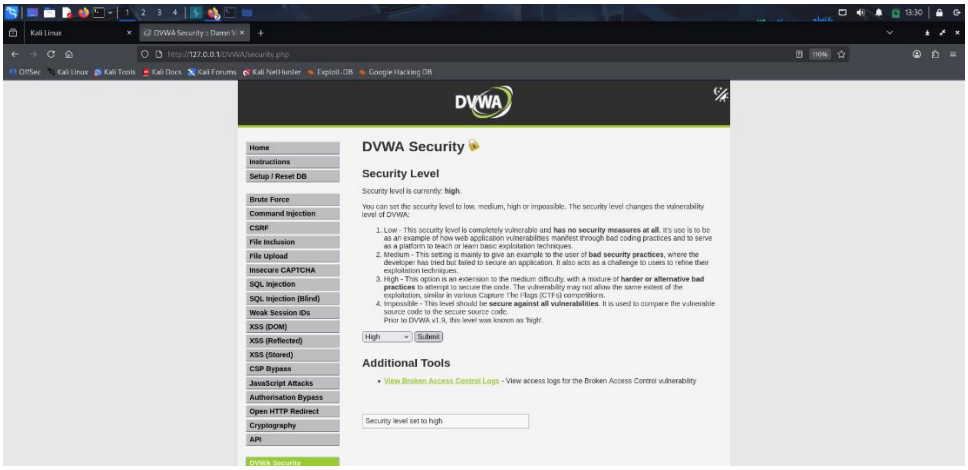


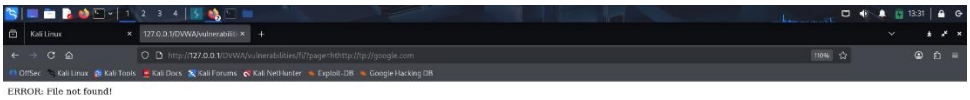


Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**

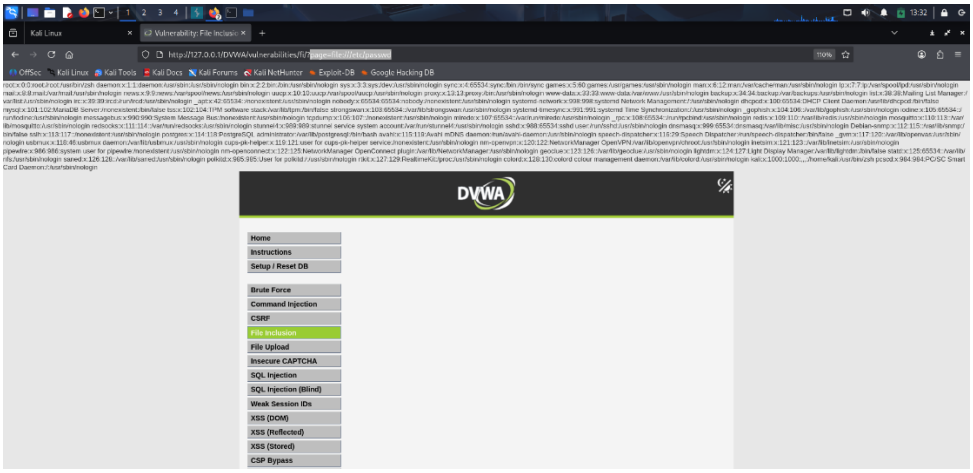


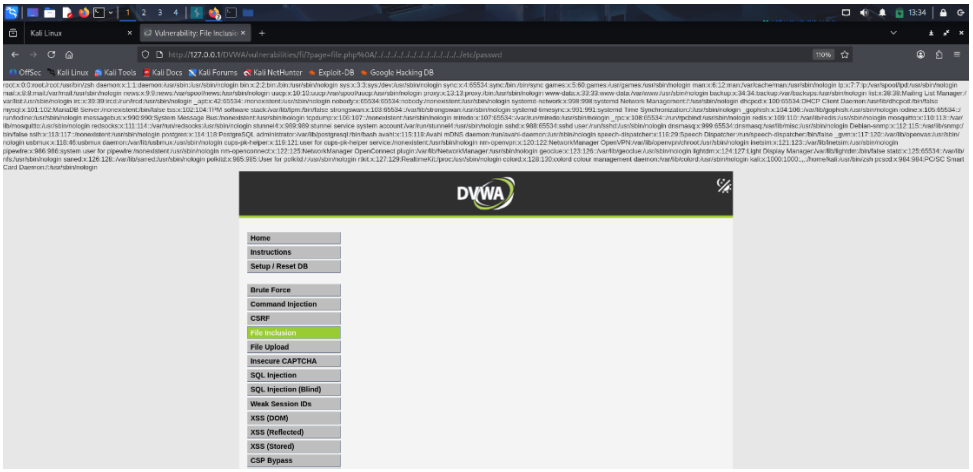




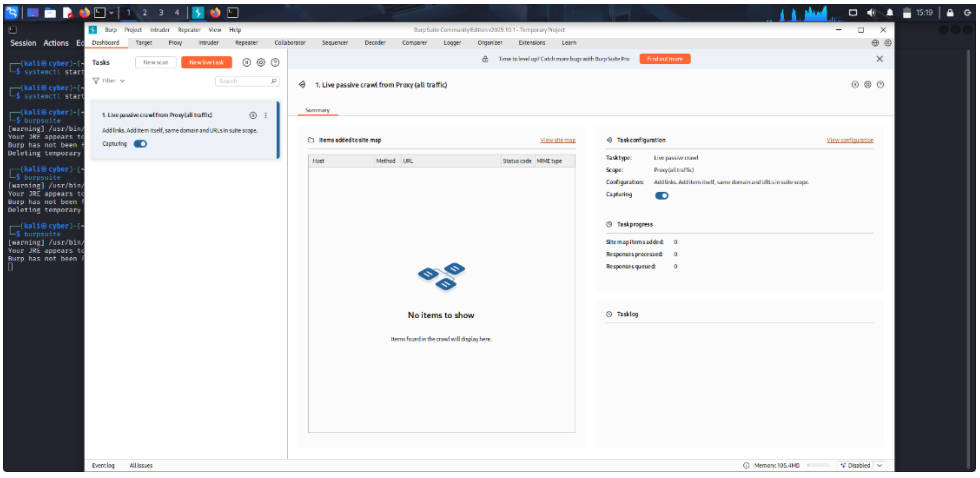
Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**



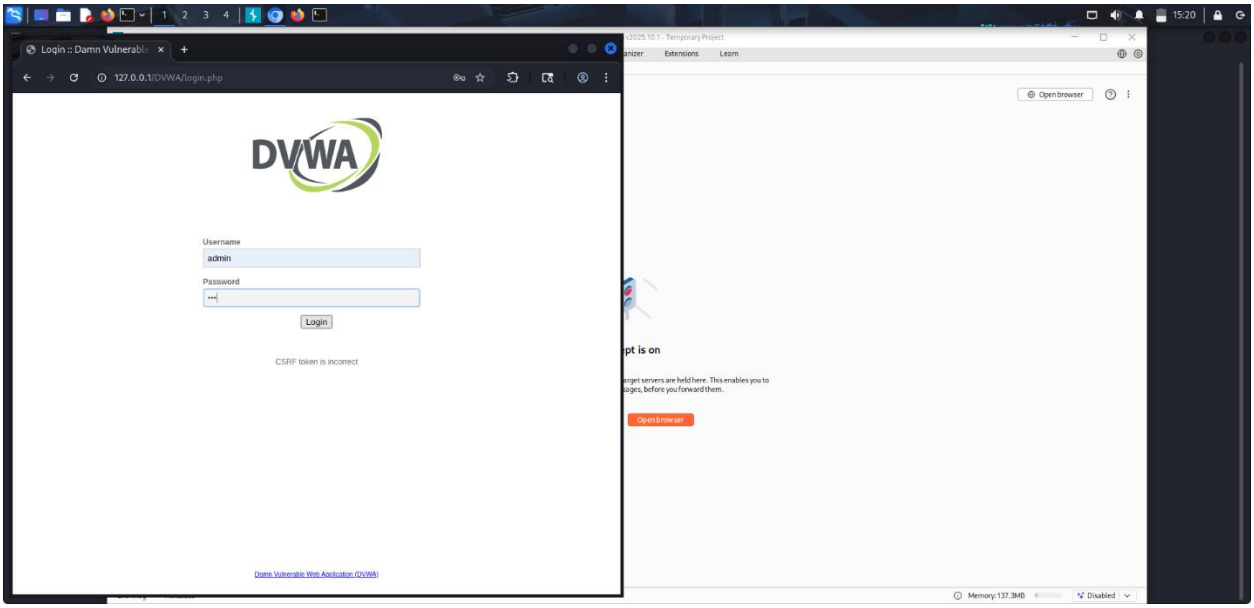


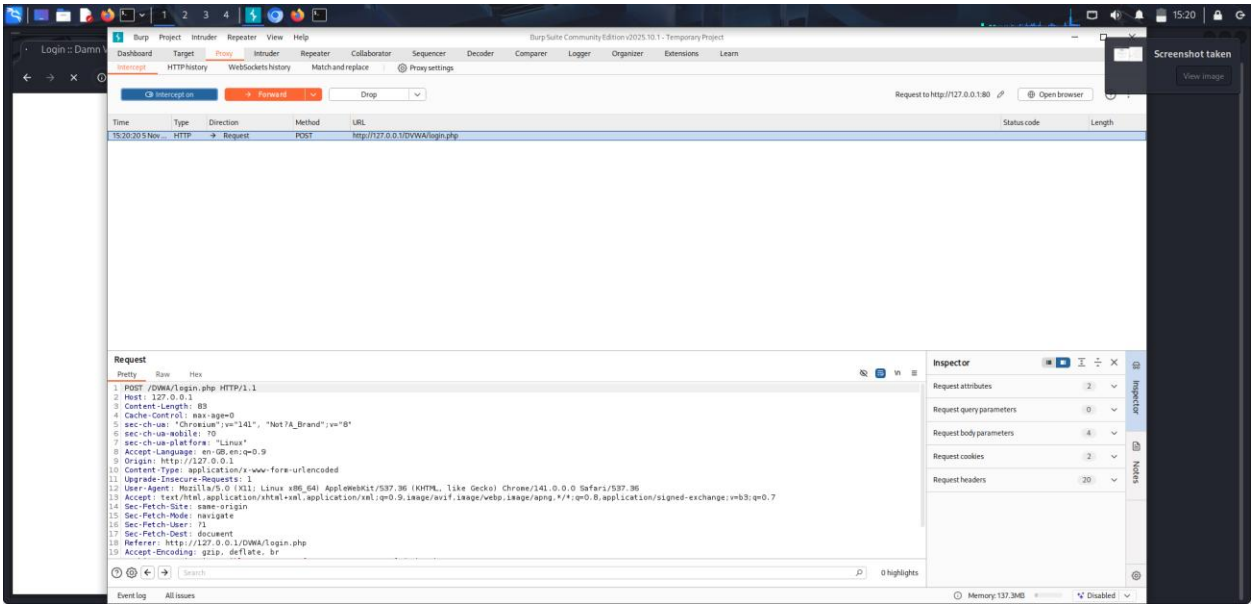
5. Burp-Suite Advanced:-



Task 3 — Web Application Security

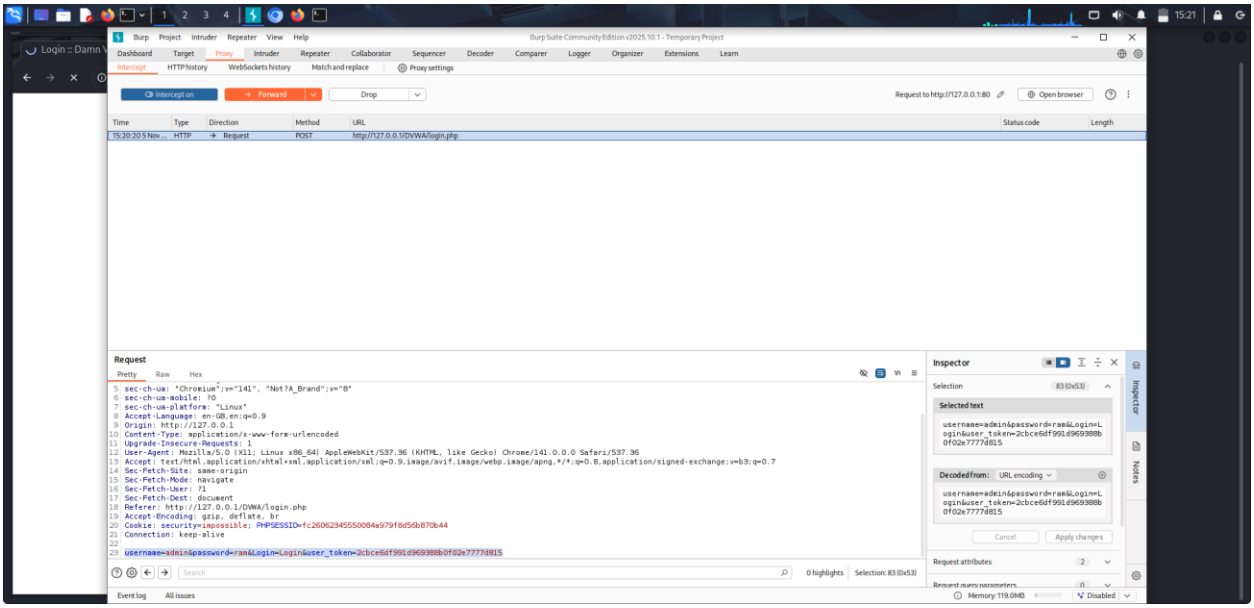
Intern Name: **Nitesh Sharma** Date: **05/10/2025**

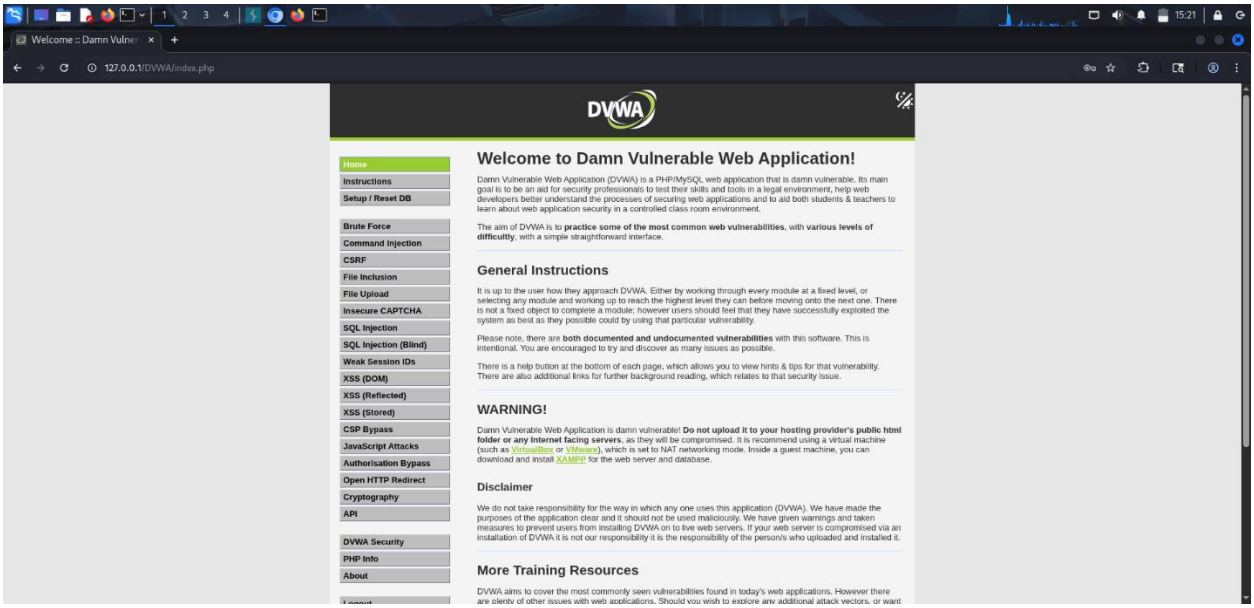




Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**

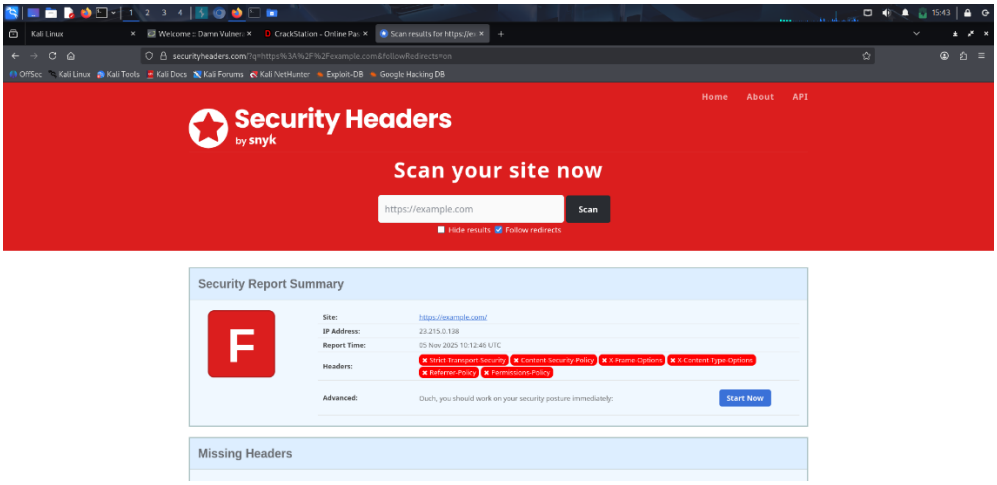


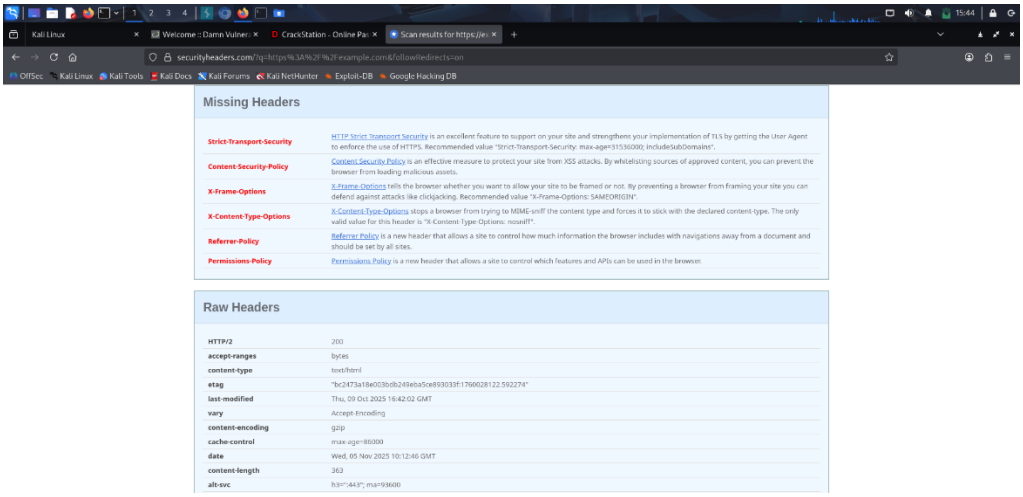


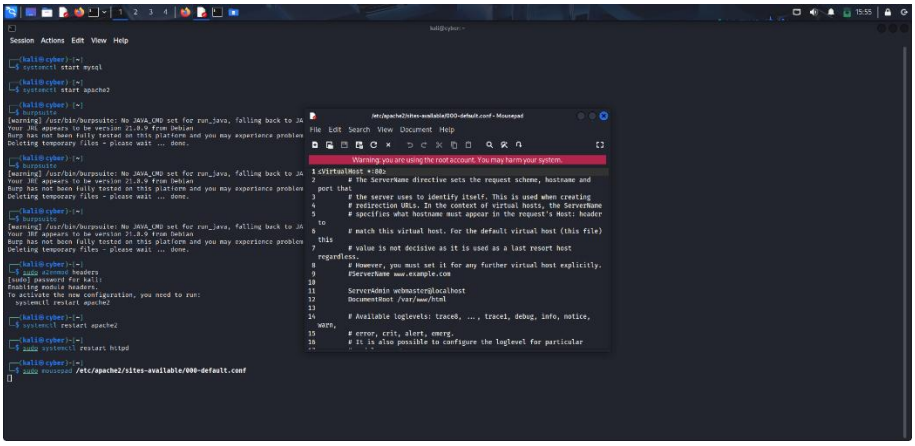
Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**

6. Web-Security Headers:-







Task 3 — Web Application Security

Intern Name: **Nitesh Sharma** Date: **05/10/2025**