Experiment - 10

Date: 15/10/2025

N-STALKER

Aim:

To evaluate the web application security posture using the N-Stalker web application security scanner.

Algorithm / Procedure (Step-by-step):

1. Step-1: Open the N-Stalker application on your system.
2. Step-2: Click 'New Scan' to create a new scanning session.
3. Step-3: Enter the target web application URL (e.g., https://www.rajalakshmi.org) in the target field.
4. Step-4: Choose a scan policy (e.g., 'Manual Test' or a predefined policy) and click 'Next'.
5. Step-5: Optionally click 'Optimize' to tune crawling and scanning parameters for speed/coverage.
6. Step-6: Click 'Start Session' to initialize the scanner session and prepare the crawler.
7. Step-7: Press 'Start Scan' to begin automated crawling and vulnerability scanning of the target application.
8. Step-8: Monitor progress and review intermediate results in the scan console (issues, hosts, requests).
9. Step-9: When the scan completes (or after sufficient coverage), click 'Save' to export the scan results (report formats such as HTML, PDF, XML may be available).
10. Step-10: Analyze the generated report to prioritize and remediate identified vulnerabilities.

Output:

The scanner will produce a report containing discovered vulnerabilities, including severity levels, proof-of-concept requests/responses, affected URLs, parameter names, and remediation suggestions. Typical outputs include:

- List of discovered issues (e.g., SQL Injection, XSS, CSRF, Sensitive Data Exposure)
- HTTP request/response examples showing the evidence
- Scan statistics (number of requests, duration, pages crawled)
- Exportable report files (HTML/PDF/XML)

Result:

N-Stalker successfully scanned the target web application and produced a vulnerability report. The findings should be reviewed, validated to remove any false positives, and prioritized for remediation based on severity and impact.