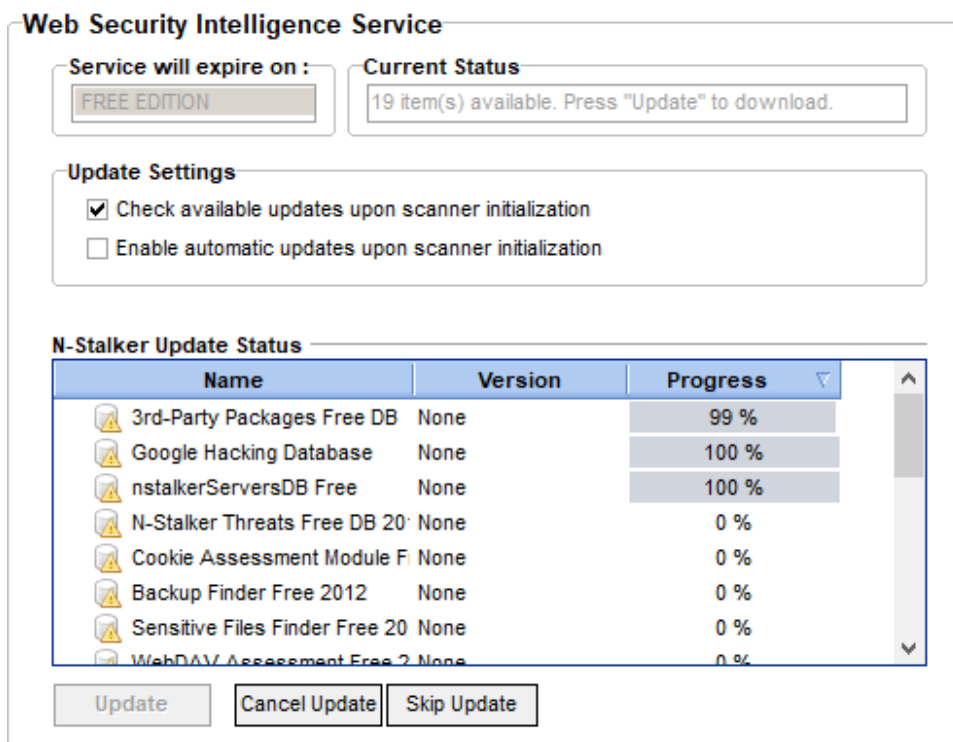


OUTPUT

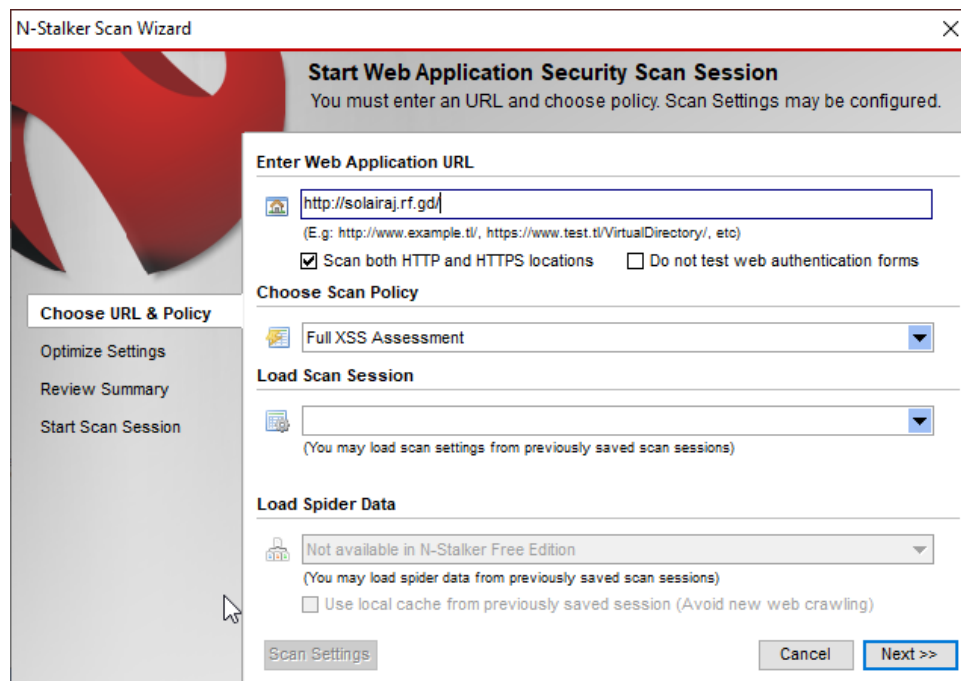
Download and Install N-Stalker Application in your Localmachine.



Before Trying to Scan for Vulnerabilities it is a better option to update the database.



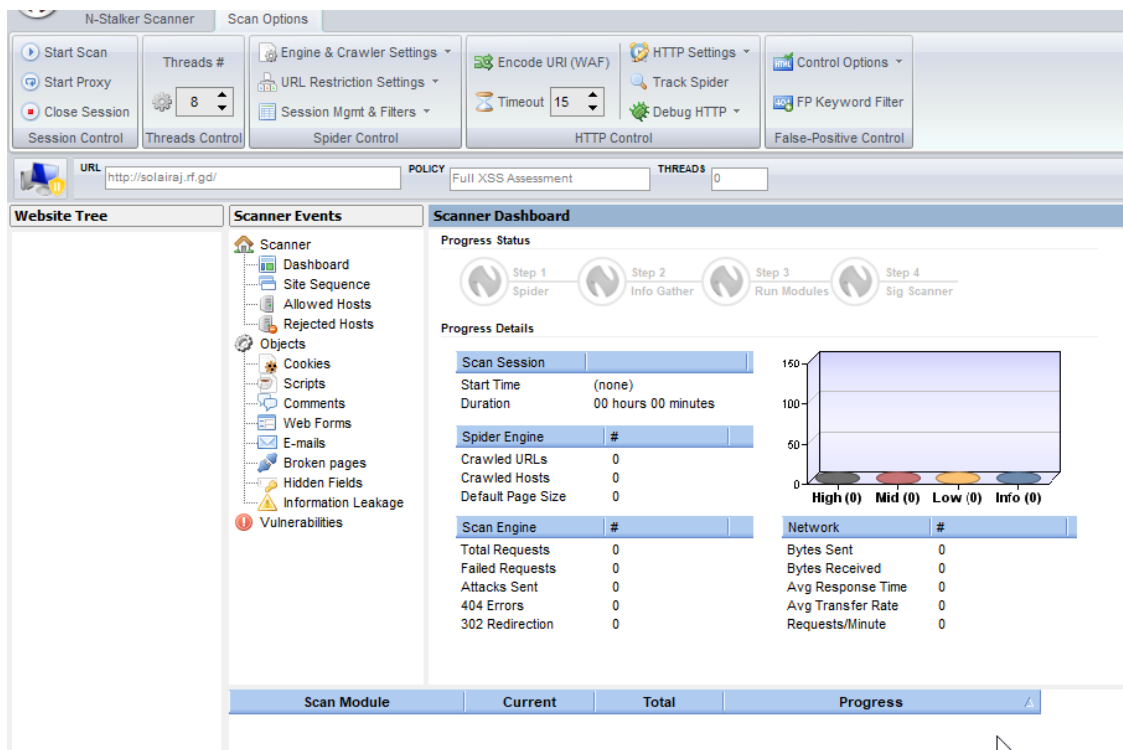
Enter the Url of the web application to be scanned and Scan type



The N-Stalker Scan Wizard dialog box is titled "Start Web Application Security Scan Session". It contains the following sections:

- Enter Web Application URL:** A text box with "http://solairaj.rf.gd/" entered. Below it, a note says "(E.g: http://www.example.tv/, https://www.test.tl/VirtualDirectory/, etc)". There are two checkboxes: "Scan both HTTP and HTTPS locations" (checked) and "Do not test web authentication forms" (unchecked).
- Choose Scan Policy:** A dropdown menu showing "Full XSS Assessment".
- Load Scan Session:** A dropdown menu with a note "(You may load scan settings from previously saved scan sessions)".
- Load Spider Data:** A dropdown menu showing "Not available in N-Stalker Free Edition" with a note "(You may load spider data from previously saved scan sessions)". Below it is a checkbox "Use local cache from previously saved session (Avoid new web crawling)" which is unchecked.
- Buttons at the bottom: "Scan Settings", "Cancel", and "Next >>".

Select the Start Scan option to start the vulnerability scanning.



The N-Stalker Scanner main interface is divided into several sections:

- Top Bar:** "N-Stalker Scanner" and "Scan Options".
- Left Panel:** "Website Tree" showing a hierarchy of items: Scanner, Dashboard, Site Sequence, Allowed Hosts, Rejected Hosts, Objects (Cookies, Scripts, Comments, Web Forms, Broken pages, Hidden Fields, Information Leakage, Vulnerabilities).
- Top Right Panel:** "Scan Options" with various settings: "Start Scan", "Start Proxy", "Close Session", "Session Control", "Threads # 8", "Engine & Crawler Settings", "URL Restriction Settings", "Session Mgmt & Filters", "Spider Control", "Encode URI (WAF)", "Timeout 15", "HTTP Settings", "Track Spider", "Debug HTTP", "Control Options", "FP Keyword Filter", "False-Positive Control".
- URL and Policy:** "URL" field with "http://solairaj.rf.gd/" and "POLICY" dropdown with "Full XSS Assessment". "THREADS" field with "0".
- Scanner Dashboard:** "Progress Status" showing a 4-step process: Step 1 Spider, Step 2 Info Gather, Step 3 Run Modules, Step 4 Sig Scanner. "Progress Details" table showing scan session and spider engine statistics. A bar chart showing progress for High, Mid, Low, and Info categories. A table showing network statistics.
- Bottom Panel:** A table with columns: Scan Module, Current, Total, Progress.

Scan Results are viewed after a successful scan, Here the webapplication contains no vulnerabilities.

Results Wizard

✕

Scan Session has finished successfully.

N-Stalker did not found any vulnerabilities.

Summary

Application Objects	Count
Total Web Pages	3
High Vulnerabilities	0
Medium Vulnerabilities	0
Low Vulnerabilities	0
Info Vulnerabilities	0
Total Hosts Found	1
Total HTTP Cookies	0
Total Directories Found	0
Total Web Forms Found	0
Total Password Forms	0
Total E-mails Found	0
Total Client Scripts	2
Total HTML Comments	0

Total Scan Time

0 Hour(s) 0 Minute(s)

Total Vulnerabilities

High : 0

Medium : 0

Low : 0

Info : 0

Your request has been successfully processed.

Done