

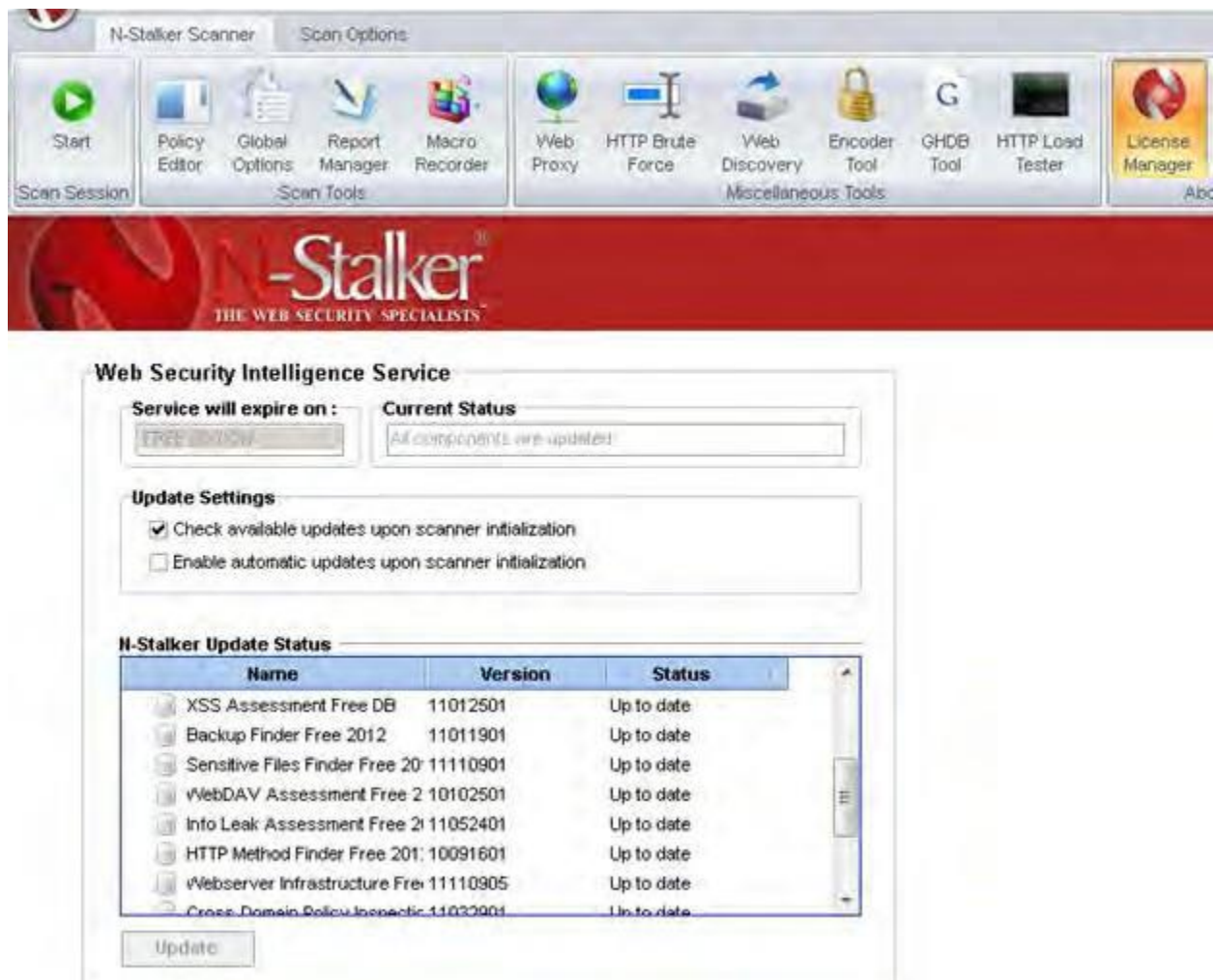
<b>Ex. No : 10</b> <b>Date :</b>	<b>Exploring N-Stalker, a Vulnerability Assessment Tool</b>
-------------------------------------	---

**AIM:**

To download the N-Stalker Vulnerability Assessment Tool and exploring the features.

**EXPLORING N-STALKER:**

- N-Stalker Web Application Security Scanner is a Web security assessment tool.
  - It incorporates with a well-known N-Stealth HTTP Security Scanner and 35,000 Web attack signature database.
  - This tool also comes in both free and paid version.
  - Before scanning the target, go to “License Manager” tab, perform the update.
  - Once update, you will note the status as up to date.
  - You need to download and install N-Stalker from [www.nstalker.com](http://www.nstalker.com).
- 
1. Start N-Stalker from a Windows computer. The program is installed under Start ⇨ Programs ⇨ N-Stalker ⇨ N-Stalker Free Edition.
  2. Enter a host address or a range of addresses to scan.
  3. Click Start Scan.
  4. After the scan completes, the N-Stalker Report Manager will prompt
  5. you to select a format for the resulting report as choose Generate HTML.
  6. Review the HTML report for vulnerabilities.



Now goto “Scan Session”, enter the target URL.

In scan policy, you can select from the four options,

- Manual test which will crawl the website and will be waiting for manual attacks.
- full xss assessment
- owasp policy
- Web server infrastructure analysis.

Once, the option has been selected, next step is “Optimize settings” which will crawl the whole website for further analysis.


In review option, you can get all the information like host information, technologies used, policy name, etc.

N-Stalker Scan Wizard

## Start Web Application Security Scan Session


You must enter an URL and choose policy. Scan Settings may be configured.

**Enter Web Application URL**



(E.g: <http://www.example.tl/>, <https://www.test.tl/VirtualDirectory/>, etc)

**Choose Scan Policy**


 (choose one) ▼

**Load Scan Session**

 (choose one) ▼

(You may load scan settings from previously saved scan sessions)

**Load Spider Data**



(You may load spider data from previously saved scan sessions)

☐ Use local cache from previously saved session (Avoid new web crawling)

**Choose URL & Policy**

Optimize Settings

Review Summary


Start Scan Session

N-Stalker Scan Wizard

## Start Web Application Security Scan Session

You must enter an URL and choose policy. Scan Settings may be configured.

**Review Summary**



**Scanning Settings**

Scan Setting	Value
Host information	IP: [125.56.222.19] Port: [80] SSL: [no]
Restricted Directory	Not configured.
Policy Name	Spider Only
False-Positive Settings	Enabled for Multiple Extensions. Enabled for 404 pages. N
New Server Discovery	Enabled (recommended in most cases)
Spider Engine	Max URLs: [500] Max Per Node [30] Max Depth [0]
HTML Parser	JS: [Execute/Parse] External JS [Deny] JS Events [Execute]
Server Technologies	N/A
Allowed Hosts	No additional hosts configured.

**Choose URL & Policy**

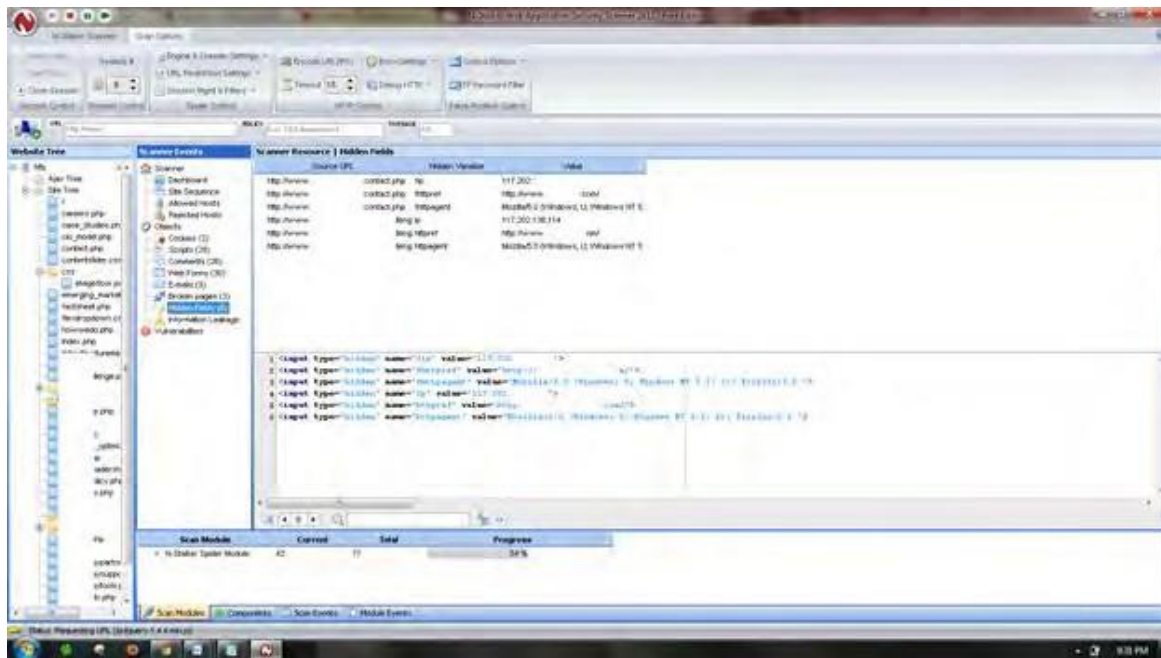
Optimize Settings

**Review Summary**

Start Scan Session

Once done, start the session and start the scan.

The scanner will crawl the whole website and will show the scripts, broken pages, hidden fields, information leakage, web forms related information which helps to analyze further.



Once the scan is completed, the NStalker scanner will show details like severity level, vulnerability class, why is it an issue, the fix for the issue and the URL which is vulnerable to the particular vulnerability?

