

Ex. No : 10 Date:27/10/2020	Exploring N-Stalker, a Vulnerability Assessment Tool
--	---

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.
-
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.



Web Security Intelligence Service

Service will expire on : FREE EDITION **Current Status** All components are updated.

Update Settings

☒ Check available updates upon scanner initialization
☐ Enable automatic updates upon scanner initialization

N-Stalker Update Status

Name	Version	Status
XSS Assessment Free DB	11012501	Up to date
Backup Finder Free 2012	11011901	Up to date
Sensitive Files Finder Free 20	11110901	Up to date
WebDAV Assessment Free 2	10102501	Up to date
Info Leak Assessment Free 2i	11052401	Up to date
HTTP Method Finder Free 201	10091601	Up to date
Webserver Infrastructure Fre	11110905	Up to date
Cross Domain Policy Inspecti	11032901	Up to date

Update

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.

Choose URL & Policy

Optimize Settings

Review Summary

Start Scan Session

Enter Web Application URL

www.target.com

(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

Not available in N-Stalker Free Edition

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

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

Scan Settings

Cancel

Next >>

N-Stalker Scan Wizard

Start Web Application Security Scan Session

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

Choose URL & Policy

Optimize Settings

Review Summary

Start Scan Session

Review Summary

http://www.target.com/

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. Nk
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.

Scan Settings

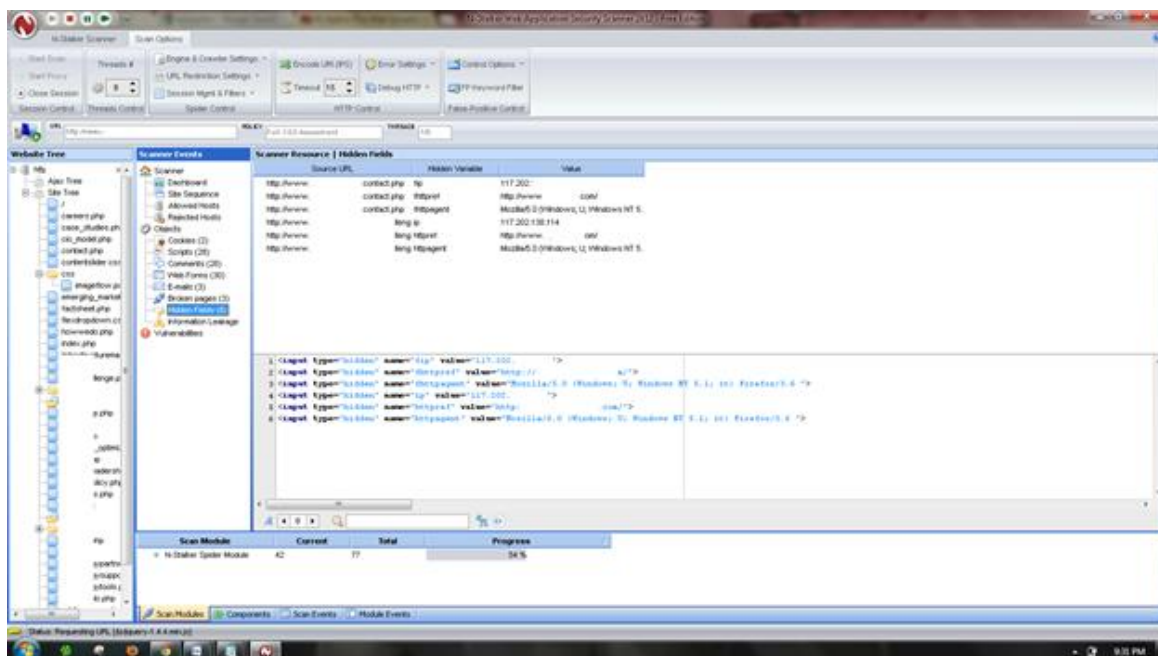
<< Back

Cancel

Start 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?

Web Application Security Scanner 2012 (Free Edition)

Start Scan | Start Process | Close Session | Session Control | Scan Options | Engine & Crawler Settings | URL Restriction Settings | Session Agent & Filters | Spider Control | Exclude URL (PFI) | Error Settings | Control Options | Timeout | Delay HTTP | HTTP Control | HTTP Keyword Filter

Website Tree | Scanner Events | Vulnerability Information

Possible Cross-site Scripting and/or HTML Injection found

Severity: Medium
Vulnerability Class: Cross-Site Scripting
Target URL: http://www.../contact.php
Post Data: N/A

Why is it an issue?

Cross-site Scripting (XSS) is the most common security problem that affects Web Application all over the Internet. According to OIVADP Top 10 Standard, XSS is categorized as one of the most frequent attacks in place over the web protocol. It is relatively easy to exploit and sometimes difficult to detect and avoid its presence on target/complex applications.

Since 2000 when first reported by US CERT, XSS have not been taken seriously by organizations as a security threat. This is specially due to its common exploitation procedure that aims to affect legitimate users of the application instead of application infrastructure itself.

Consequences of that particular attack includes:

- Web Application defacement
- Secret Engineering (against legitimate users)
- Malware/Virus spreading

According to OIVADP Top 10 version 2010:

"Cross site scripting, better known as XSS, is in fact a subset of HTML injection. XSS is the most prevalent and pernicious web application security issue. XSS first occur whenever an application fetches data that originated from a user and sends it to a web browser without that validation or escaping that content."

Scan Module	Current	Total	Progress
Cross-Site Scripting Assessment	6573	10244	95 %
MS-SQL Spider Module	87	87	100 %
File Extensions Finder	96	96	100 %
WebServer Infrastructure App-2	2	2	100 %

Scan Modules | Components | Scan Events | Module Events

Status: Testing XSS injection attack against (spiderchallenge_index.php)