

Scanning web applications using Nstalker

Scanning web applications using Nstalker

N-Stalker Web Application Security Scanner is a Web security assessment tool.

Download the N-Stalker from their official [website](#)



Conviso Platform

About Conviso

Contact Us

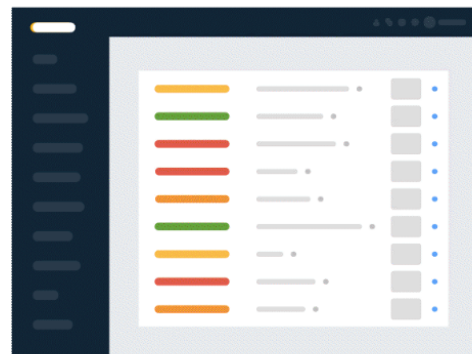


N-Stalker is now part of Conviso Platform

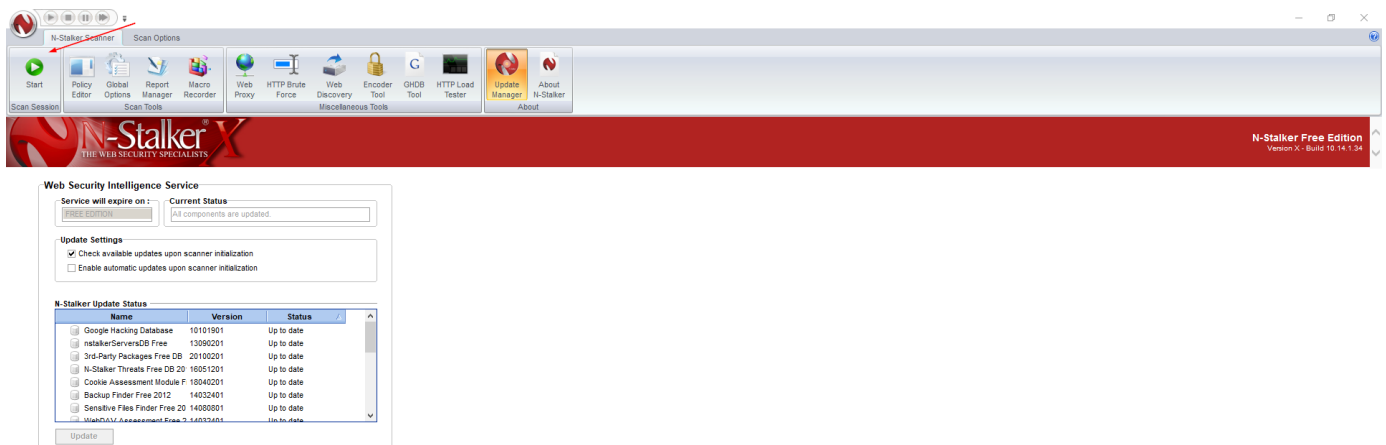
N-Stalker technology is now offered as part of Conviso Platform – our DevSecOps solution created to support the entire secure software development cycle.

See for yourself

Try the free edition



Update the database and press Start



Activate Windows
Go to Settings to activate Windows.


Define the target URL and choose scan policy

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


 192.168.0.115
(E.g: http://www.example.tl/, https://www.test.tl/VirtualDirectory/, etc)

☒ Scan both HTTP and HTTPS locations ☐ Do not test web authentication forms


Choose Scan Policy

 OWASP Policy

Load Scan Session


(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 >>](#)


Press Start 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

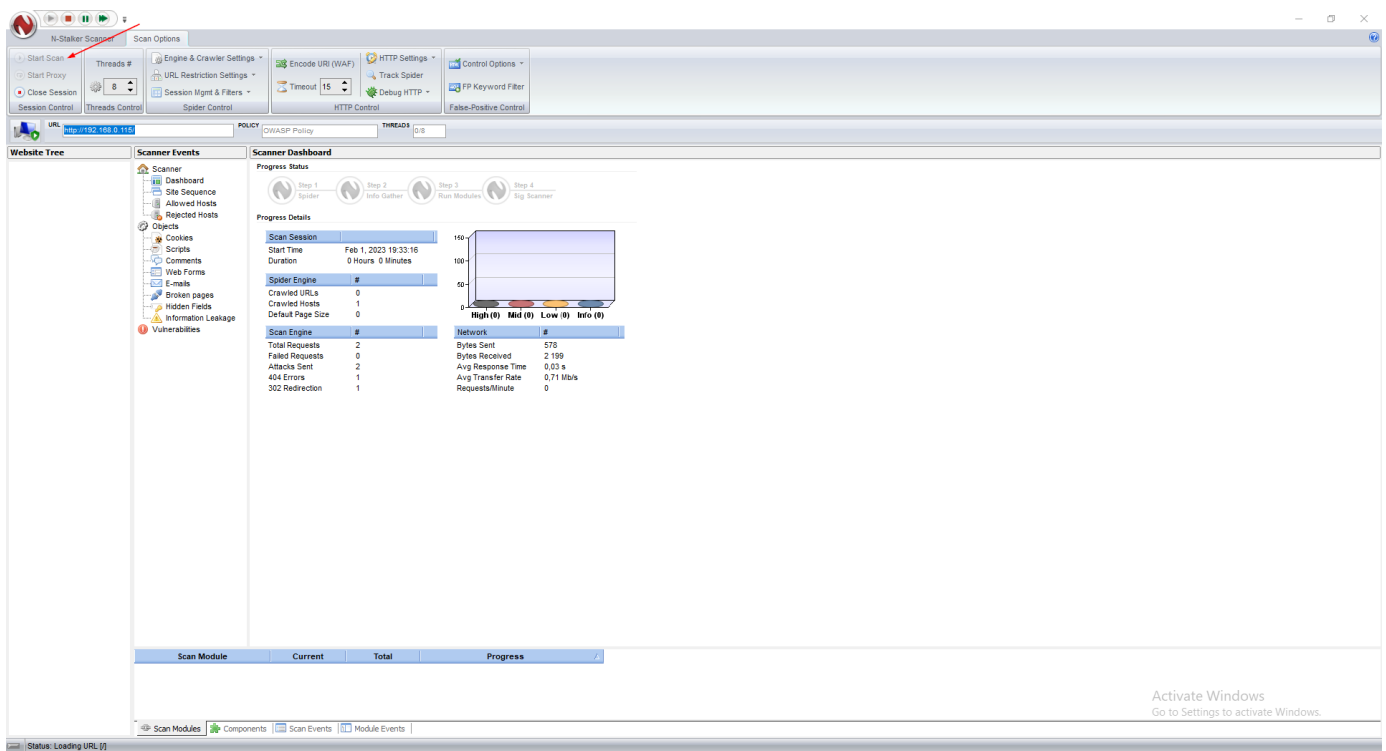
 http://192.168.0.115/

Scanning Settings

Scan Setting	Value
Host Information	IP: [192.168.0.115] Port: [80] SSL: [no]
Restricted Directory	Not configured.
Policy Name	OWASP Policy
False-Positive Settings	Enabled for Multiple Extensions. Enabled for 404 pages. C...
New Server Discovery	Enabled (recommended in most cases)
Spider Engine	Max URLs: [500] Max Per Node [30] Max Depth [0]
HTML Parser	JS: [Ignore] External JS [Deny] JS Events [Execute] SWF [F...
Server Technologies	N/A
Allowed Hosts	No additional hosts configured.

[Scan Settings](#) [<< Back](#) [Cancel](#) [Start Session](#)

Press Start Scan button



You will this window after the scan is completed:

Results Wizard

Scan Session has finished successfully.
N-Stalker found 199 vulnerabilities

Summary

Application Objects	Count
Total Web Pages	5
High Vulnerabilities	131
Medium Vulnerabilities	63
Low Vulnerabilities	2
Info Vulnerabilities	3
Total Hosts Found	1
Total HTTP Cookies	2
Total Directories Found	0
Total Web Forms Found	1
Total Password Forms	0
Total E-mails Found	0
Total Client Scripts	0
Total HTML Comments	0

Your request has been successfully processed.

Done

Total Scan Time
0 Hour(s) 3 Minute(s)

Total Vulnerabilities


High : 131
Medium : 63
Low : 2
Info : 3

Observe the results:

Scanner Events

- PHP CVE-2018-9933 Denial of Service
- PHP CVE-2018-9934 NULL Pointer Dereference
- PHP CVE-2018-9935 Out-of-Bounds Read
- PHP CVE-2017-11142 Resource Exhaustion
- PHP CVE-2017-11143 Denial of Service
- PHP CVE-2017-11144 Buffer Overflow
- PHP CVE-2017-11145 Information Exposure
- PHP CVE-2017-11147 Memory Corruption
- PHP CVE-2017-11628 Stack Buffer Overflow
- PHP CVE-2017-12933 Heap Buffer Overflow
- PHP CVE-2018-5711 Denial of Service
- PHP CVE-2018-5712 Cross-Site Scripting
- PHP CVE-2018-7584 Stack Buffer Overflow
- PHP CVE-2018-10545 Security Bypass
- PHP CVE-2018-19518 Remote Code Execution

Vulnerability Information



PHP CVE-2018-19518 Remote Code Execution

Severity: High

Vulnerability Class: Web Server Infrastructure attack

References: OWASP (Top 10 A5) | CVE (78)

Target URL: http://192.168.0.115/

Post Data: N/A

Why is it an issue?

N-Stalker has detected a vulnerable PHP server installed within your URL.

University of Washington IMAP Toolkit 20071 on UNIX, as used in imap_open() in PHP and other products, launches an rsh command (by means of the imap_rimap function in c-client/imap4r.c and the tgz_ropen function in osdespatch.c, unix.c) without preventing argument injection, which might allow remote attackers to execute arbitrary OS commands if the IMAP server name is untrusted input (e.g., entered by a user of a web application) and if rsh has been replaced by a program with different argument semantics. For example, if rsh is a link to ssh (as seen on Debian and Ubuntu systems), then the attack can use an IMAP server name containing a "-oProxyCommand=" argument.