

SQL Injection

Lab Assignment (Module 15)

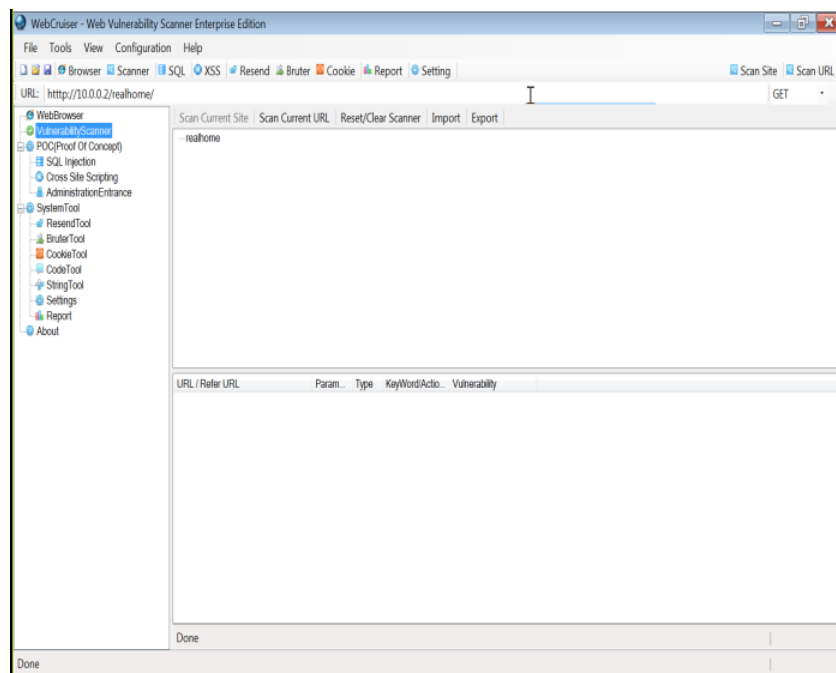
Name: Sachin Saj T K

Roll No: CB.EN.P2CEN18012

Date of Submission: 22/06/2019

Testing for SQL Injection Using WebCruiser Tool

1. Open WebCruiser tool, and type <http://10.0.0.2/realhome>

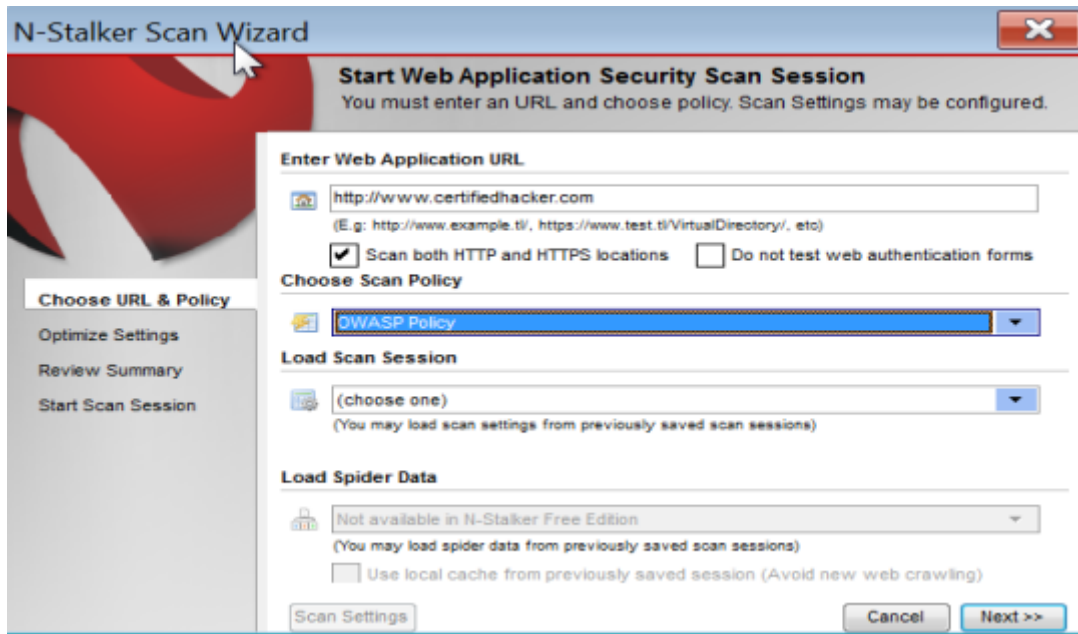


Note: As you can see there is no vulnerability in the site, so SQL injection can't be done.

Tool/Utility	Information Collected/Objective Achieved
WebCruiser	SQL Injection can't be done, since there were no vulnerabilities.

Testing for SQL Injection Using N-Stalker Tool

1. After updating the software, start web application security scan session. The web application URL – <http://www.certifiedhacker.com>



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.tv/, https://www.test.tv/VirtualDirectory/, etc)

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

Choose Scan Policy

Load Scan Session

(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)



N-Stalker Scan Wizard

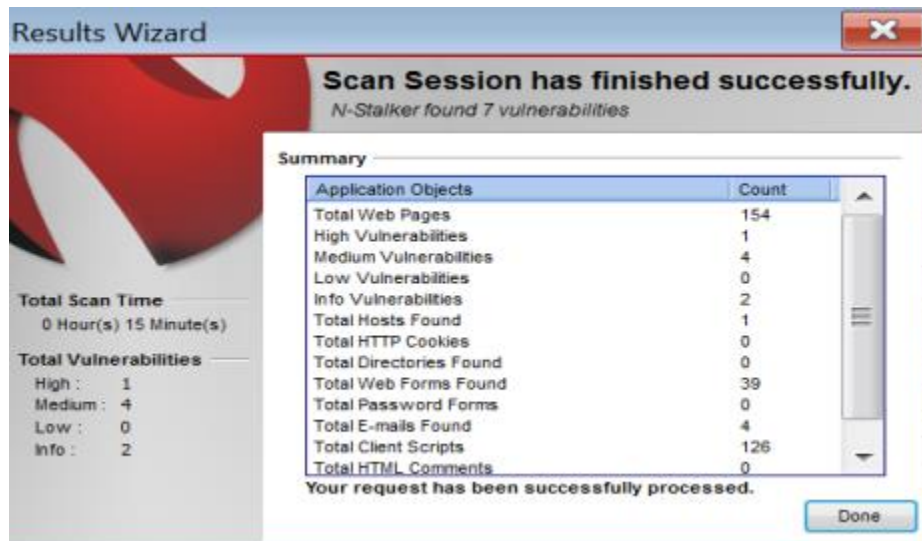
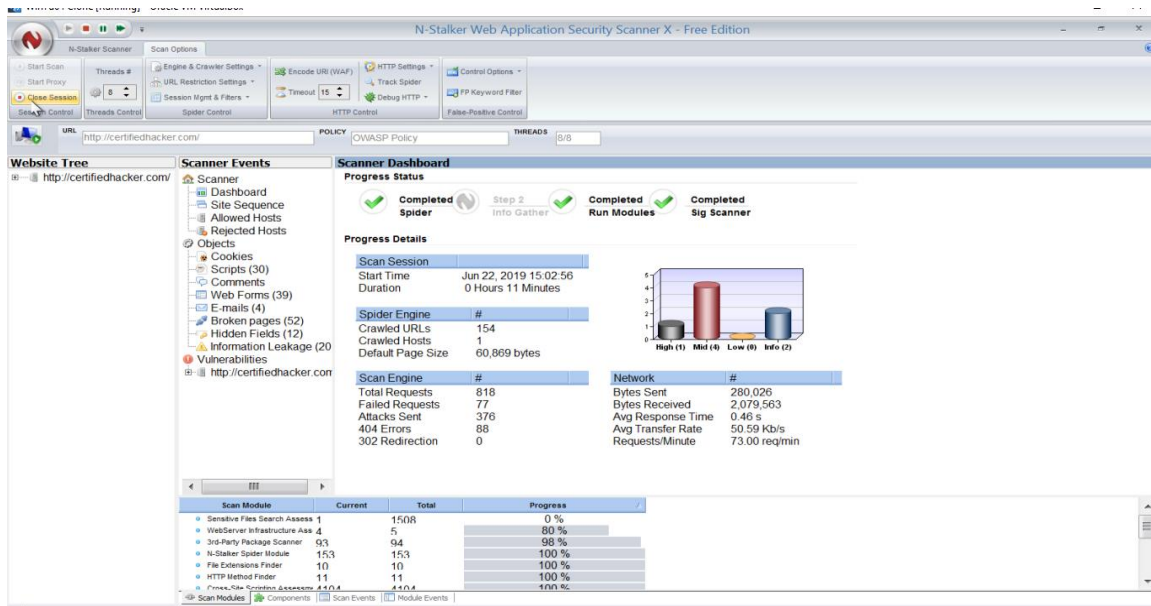
Start Web Application Security Scan Session
You must enter an URL and choose policy. Scan Settings may be configured.

Review Summary

Scanning Settings

Scan Setting	Value
Host Information	IP: [10.0.0.2] Port: [80] SSL: [no]
Restricted Directory	/realhome/
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 [I
Server Technologies	N/A

2. Scan results



Lab Analysis

Tool/Utility	Information Collected/Objective Achieved
N-Stalker	Scan session successfully processed with 7 vulnerabilities detected.