IT8761 – Security Laboratory

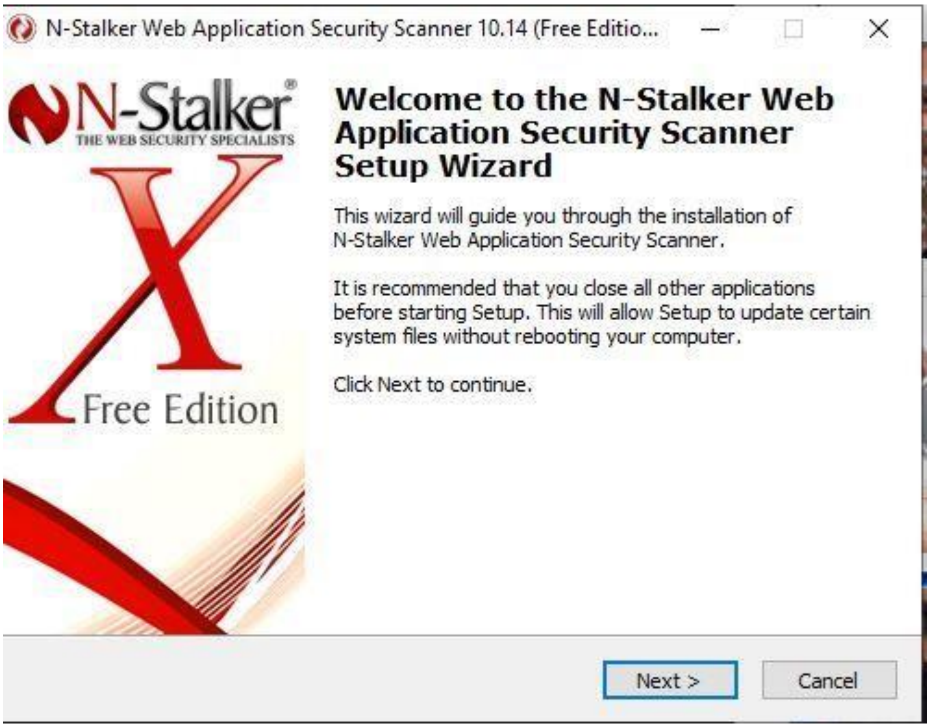
Reshma Ramesh Babu

312217104129

Exercise 11

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

Step 1: Install the free version of n-stalker



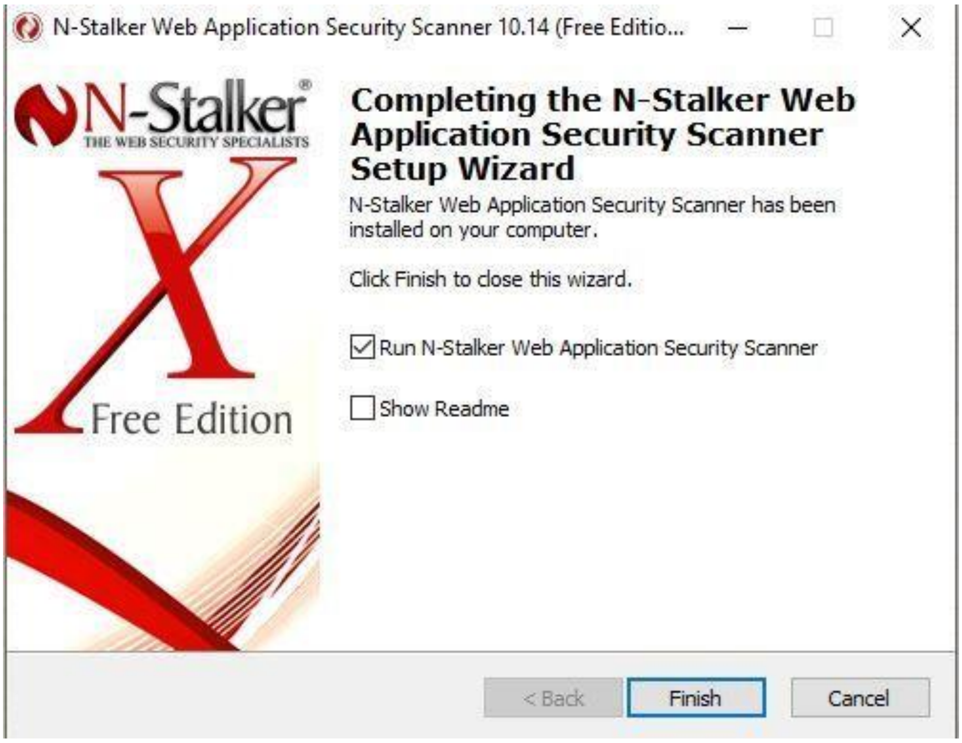
N-Stalker Web Application Security Scanner 10.14 (Free Editio...

Welcome to the N-Stalker Web Application Security Scanner Setup Wizard

This wizard will guide you through the installation of N-Stalker Web Application Security Scanner.

It is recommended that you close all other applications before starting Setup. This will allow Setup to update certain system files without rebooting your computer.

Click Next to continue.


N-Stalker Web Application Security Scanner 10.14 (Free Editio...
N-Stalker
THE WEB SECURITY SPECIALISTS
X
Free Edition
< Back
Finish
Cancel

Completing the N-Stalker Web Application Security Scanner Setup Wizard

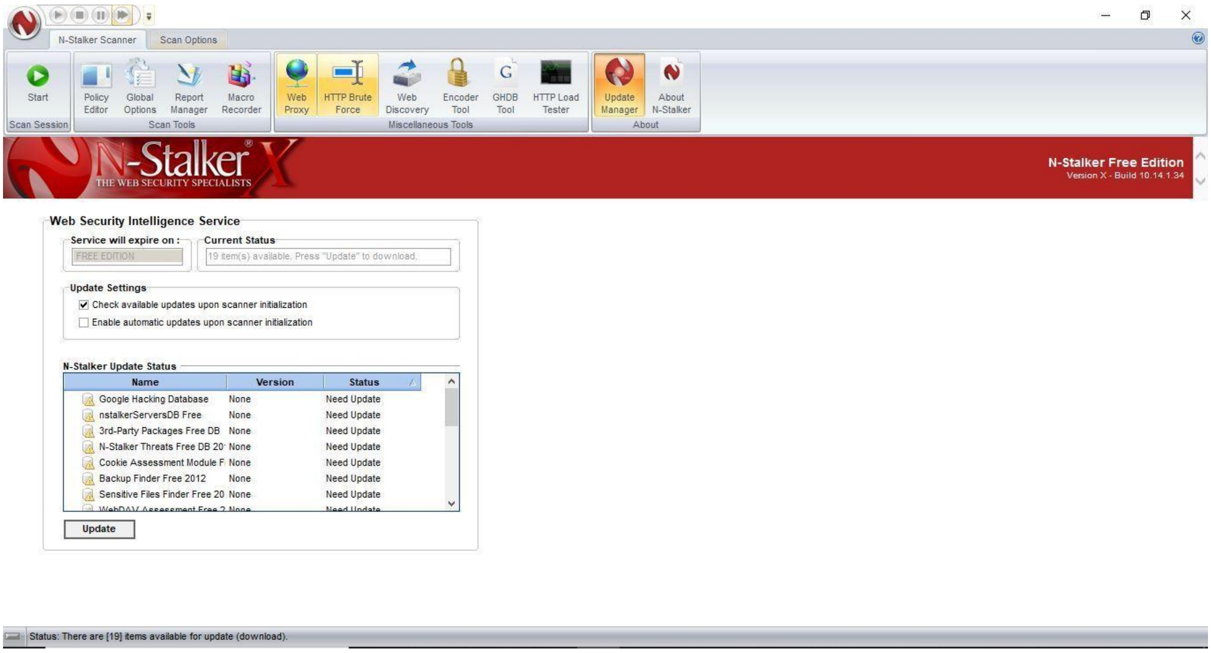
N-Stalker Web Application Security Scanner has been installed on your computer.

Click Finish to close this wizard.

☑ Run N-Stalker Web Application Security Scanner

☐ Show Readme

Step 2: Run and update n-stalker



Web Security Intelligence Service

Service will expire on : FREE EDITION

Current Status: 19 item(s) available. Press "Update" to download.

Update Settings

☑ Check available updates upon scanner initialization

☐ Enable automatic updates upon scanner initialization

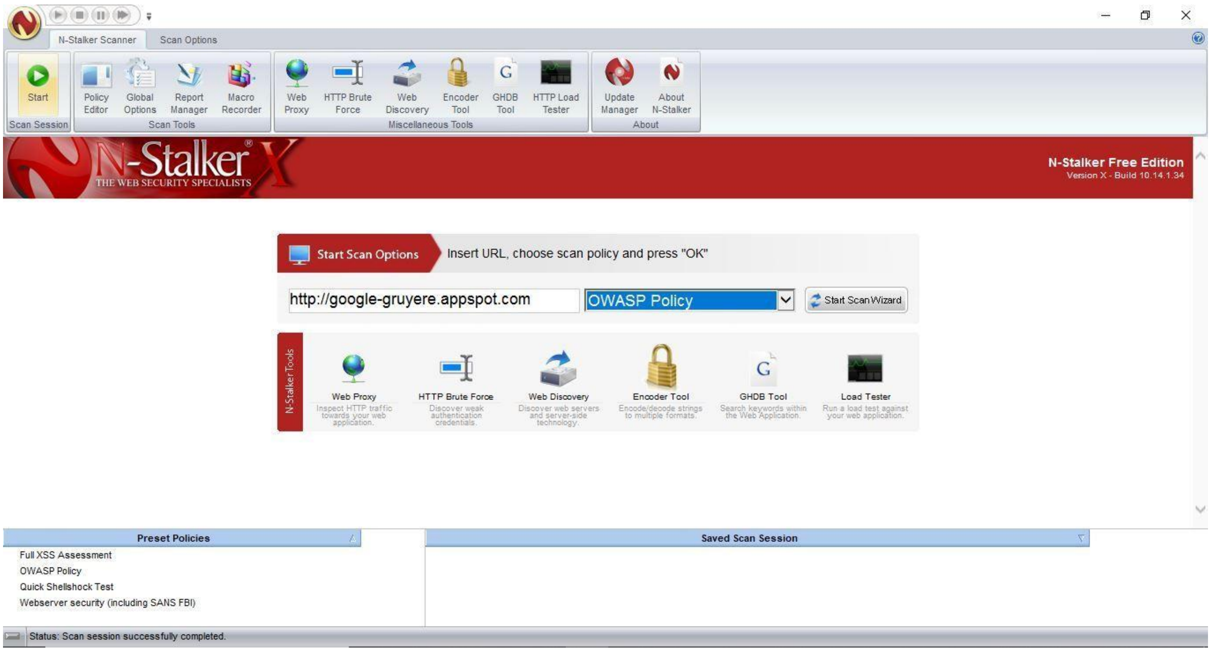
N-Stalker Update Status

Name	Version	Status
Google Hacking Database	None	Need Update
nstalkerServersDB Free	None	Need Update
3rd-Party Packages Free DB	None	Need Update
N-Stalker Threats Free DB 20	None	Need Update
Cookie Assessment Module F	None	Need Update
Backup Finder Free 2012	None	Need Update
Sensitive Files Finder Free 20	None	Need Update
WebDAV Assessment Free 2	None	Need Update

Update

Status: There are [19] items available for update (download).

Step 3: Enter a host address or a range of addresses to scan and click “start ScanWizard”



Start Scan Options — Insert URL, choose scan policy and press "OK"

http://google-gruyere.appspot.com | OWASP Policy | Start Scan Wizard

Preset Policies

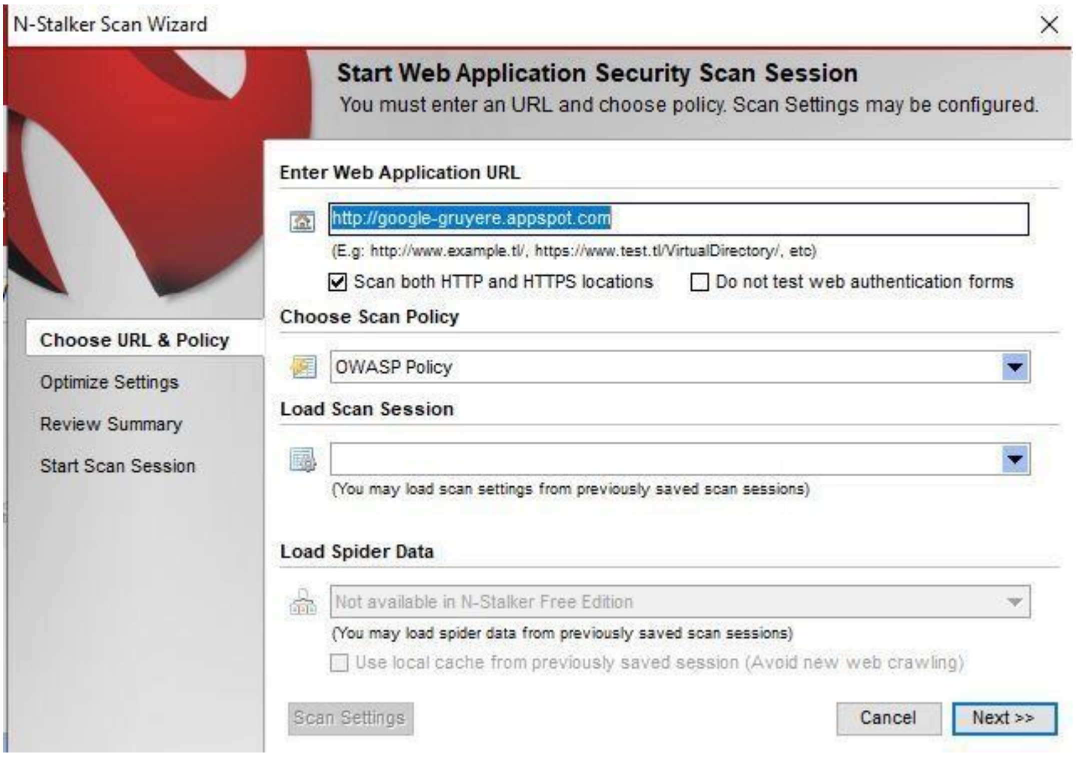
- Full XSS Assessment
- OWASP Policy
- Quick Shellshock Test
- Webserver security (including SANS FBI)

Saved Scan Session

Status: Scan session successfully completed.

Step 4: A prompt appears. 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.


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

http://google-gruyere.appspot.com

(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)

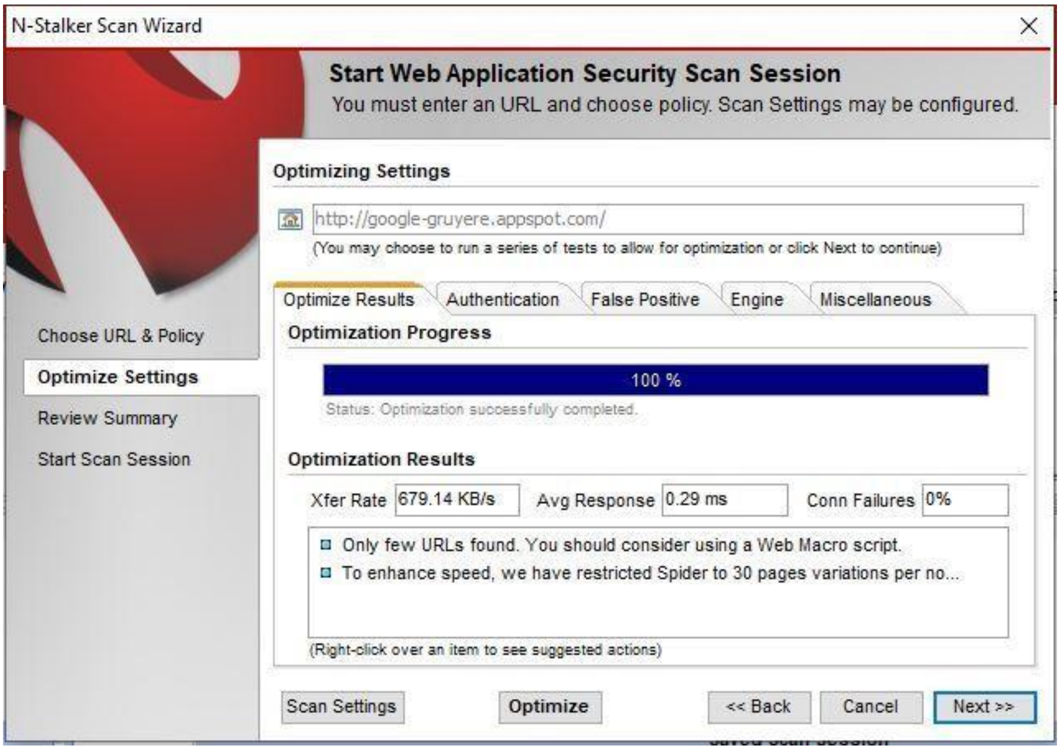
Load Spider Data

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)

Step 5: Once, the option has been selected, next step is “Optimize settings” which will crawl the whole website for further analysis.


N-Stalker Scan Wizard

Start Web Application Security Scan Session

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

Optimizing Settings

http://google-gruyere.appspot.com/

(You may choose to run a series of tests to allow for optimization or click Next to continue)

Optimization Progress

100 %

Status: Optimization successfully completed.

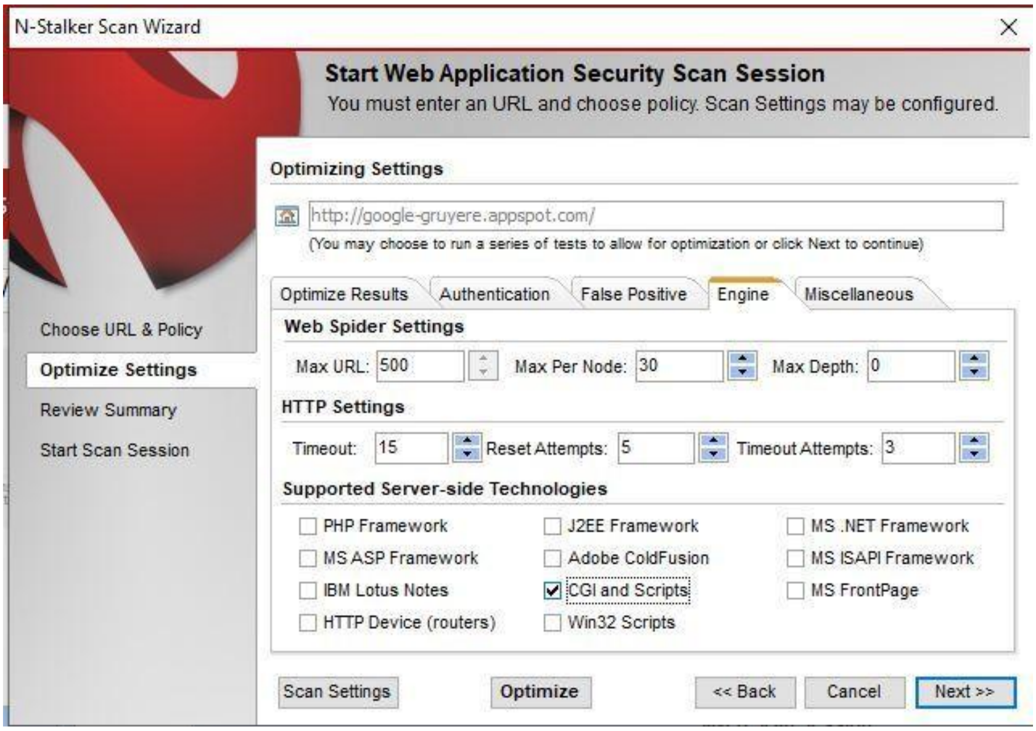
Optimization Results

Xfer Rate 679.14 KB/s Avg Response 0.29 ms Conn Failures 0%

- Only few URLs found. You should consider using a Web Macro script.
- To enhance speed, we have restricted Spider to 30 pages variations per no...

(Right-click over an item to see suggested actions)

Step 6: In the engine option, you can choose certain supported server side technologies, if you know the backend of the server.



Start Web Application Security Scan Session

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

Optimizing Settings

http://google-gruyere.appspot.com/

(You may choose to run a series of tests to allow for optimization or click Next to continue)

Web Spider Settings

Max URL: 500 Max Per Node: 30 Max Depth: 0

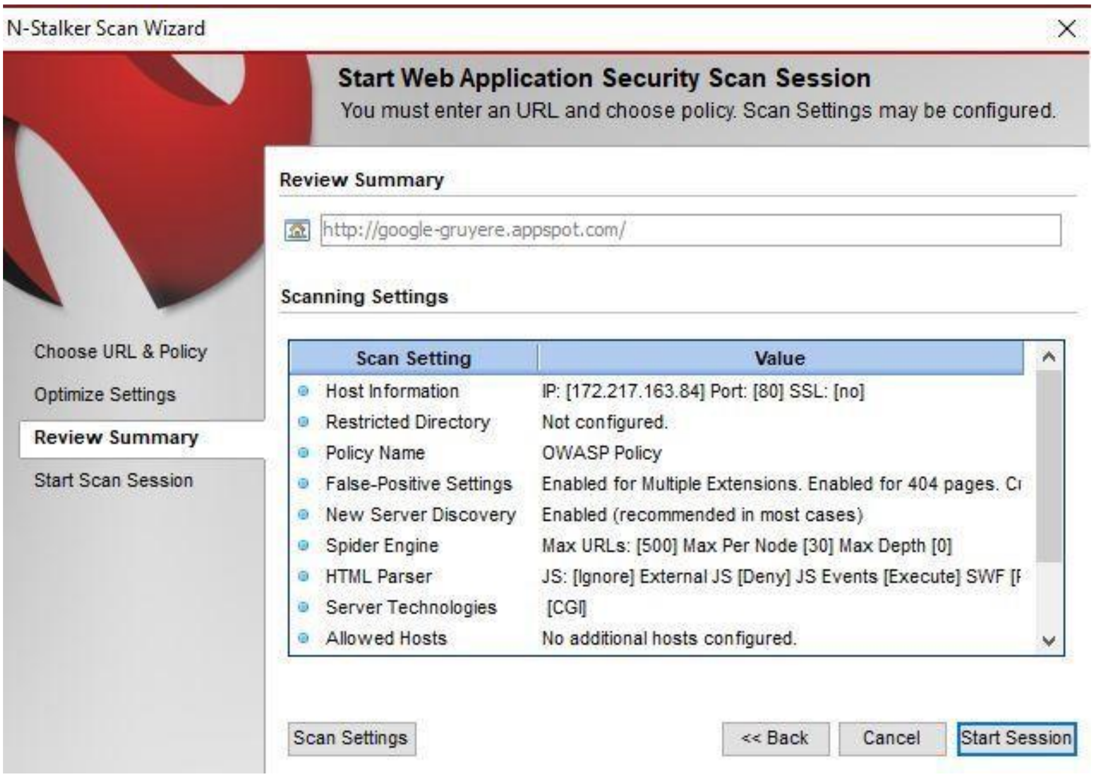
HTTP Settings

Timeout: 15 Reset Attempts: 5 Timeout Attempts: 3

Supported Server-side Technologies

- ☐ PHP Framework
- ☐ MS ASP Framework
- ☐ IBM Lotus Notes
- ☐ HTTP Device (routers)
- ☐ J2EE Framework
- ☐ Adobe ColdFusion
- ☑ CGI and Scripts
- ☐ Win32 Scripts
- ☐ MS .NET Framework
- ☐ MS ISAPI Framework
- ☐ MS FrontPage

Step 7: In review option, you can get all the information like host information, technologies used, policy name, etc.



Start Web Application Security Scan Session

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

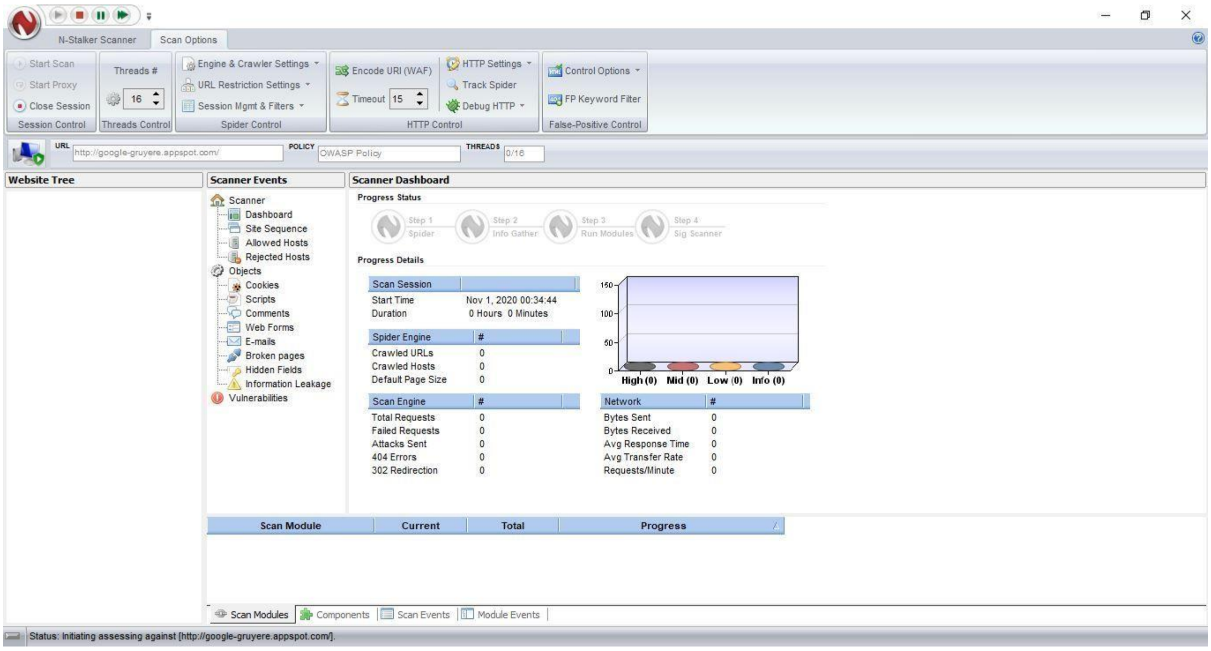
Review Summary

http://google-gruyere.appspot.com/

Scanning Settings

Scan Setting	Value
Host Information	IP: [172.217.163.84] 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	[CGI]
Allowed Hosts	No additional hosts configured.

Step 8: 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.



Threads # 16

Timeout 15

URL http://google-gruyere.appspot.com/ POLICY OWASP Policy THREADS 0/16

Progress Details

Scan Session	
Start Time	Nov 1, 2020 00:34:44
Duration	0 Hours 0 Minutes

Spider Engine	#
Crawled URLs	0
Crawled Hosts	0
Default Page Size	0

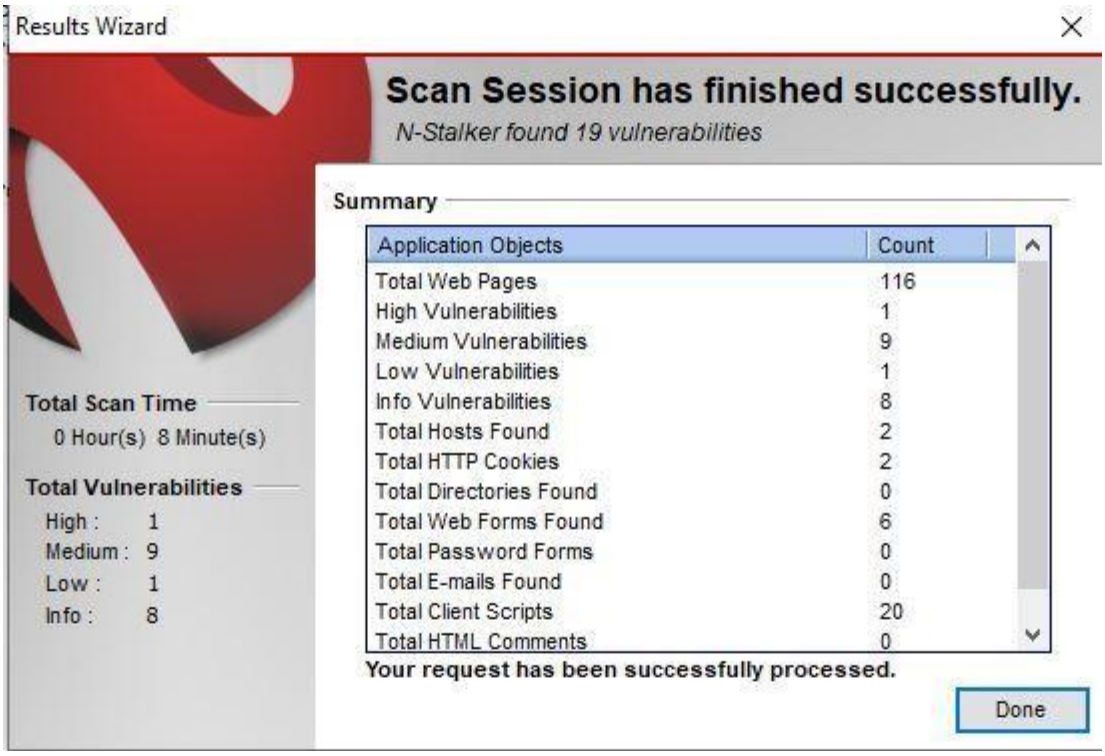
Scan Engine	#
Total Requests	0
Failed Requests	0
Attacks Sent	0
404 Errors	0
302 Redirection	0

Network	#
Bytes Sent	0
Bytes Received	0
Avg Response Time	0
Avg Transfer Rate	0
Requests/Minute	0

Scan Module	Current	Total	Progress

Status: Initiating assessing against [http://google-gruyere.appspot.com/].

Step 9: 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.



Scan Session has finished successfully.

N-Stalker found 19 vulnerabilities

Summary

Application Objects	Count
Total Web Pages	116
High Vulnerabilities	1
Medium Vulnerabilities	9
Low Vulnerabilities	1
Info Vulnerabilities	8
Total Hosts Found	2
Total HTTP Cookies	2
Total Directories Found	0
Total Web Forms Found	6
Total Password Forms	0
Total E-mails Found	0
Total Client Scripts	20
Total HTML Comments	0

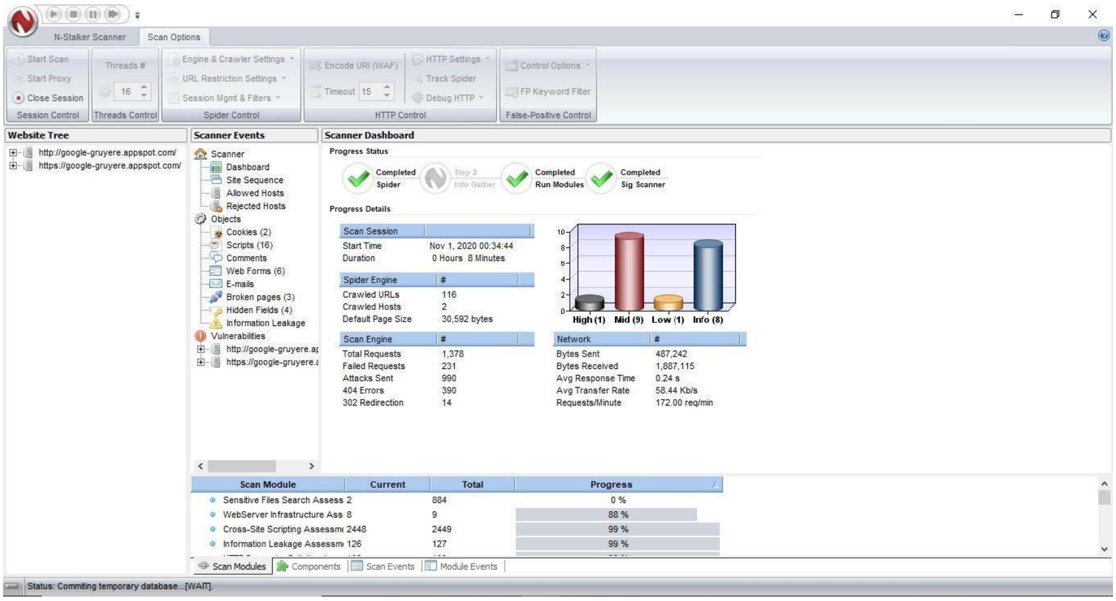
Total Scan Time

0 Hour(s) 8 Minute(s)

Total Vulnerabilities

High :	1
Medium :	9
Low :	1
Info :	8

Your request has been successfully processed.



Website Tree

http://google-gruyere.appspot.com/
https://google-gruyere.appspot.com/

Scanner Events

Scanner
Dashboard
Site Sequence
Allowed Hosts
Rejected Hosts
Objects
Cookies (2)
Scripts (16)
Comments
Web Forms (6)
E-mails
Broken pages (3)
Hidden Fields (4)
Information Leakage
Vulnerabilities
http://google-gruyere.ap
https://google-gruyere.a

Scanner Dashboard

Progress Status

Completed Spider — Step 2 Info Gather — Completed Run Modules — Completed Sig Scanner

Progress Details

Scan Session	
Start Time	Nov 1, 2020 00:34:44
Duration	0 Hours 8 Minutes

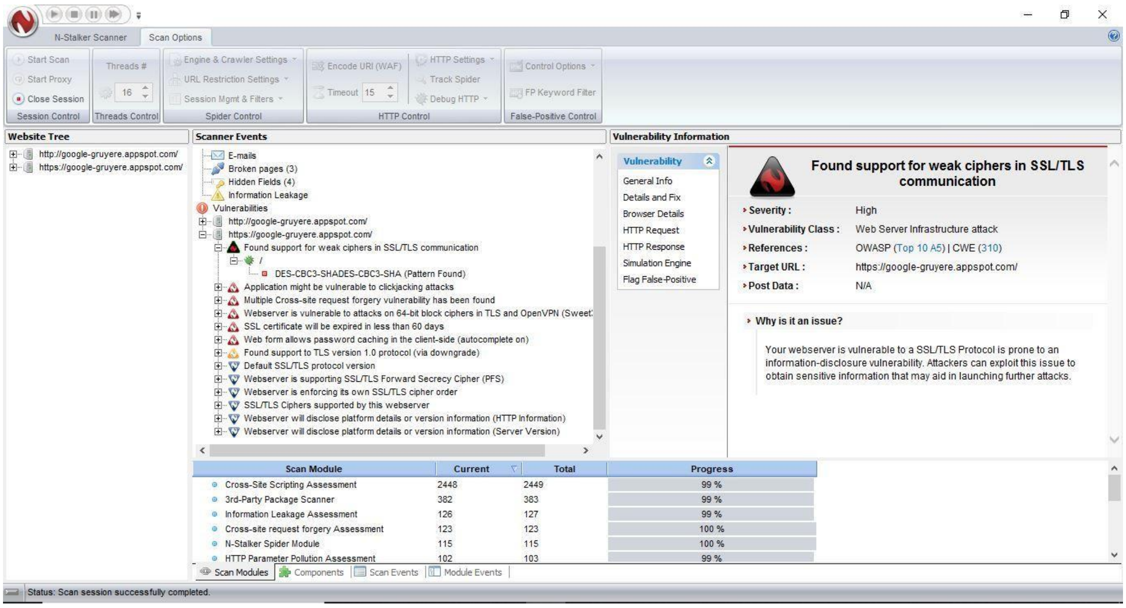
Spider Engine	#
Crawled URLs	116
Crawled Hosts	2
Default Page Size	30,592 bytes

Scan Engine	#
Total Requests	1,378
Failed Requests	231
Attacks Sent	990
404 Errors	390
302 Redirection	14

Network	#
Bytes Sent	487,242
Bytes Received	1,887,115
Avg Response Time	0.24 s
Avg Transfer Rate	58.44 Kb/s
Requests/Minute	172.00 req/min

Scan Module	Current	Total	Progress
Sensitive Files Search Assess	2	884	0 %
WebServer Infrastructure Ass	8	9	88 %
Cross-Site Scripting Assessm	2448	2449	99 %
Information Leakage Assessm	126	127	99 %

Status: Commiting temporary database...[WAIT].



Website Tree

http://google-gruyere.appspot.com/
https://google-gruyere.appspot.com/

Scanner Events

E-mails
Broken pages (3)
Hidden Fields (4)
Information Leakage
Vulnerabilities
http://google-gruyere.appspot.com/
https://google-gruyere.appspot.com/
Found support for weak ciphers in SSL/TLS communication
/
DES-CBC3-SHADES-CBC3-SHA (Pattern Found)
Application might be vulnerable to clickjacking attacks
Multiple Cross-site request forgery vulnerability has been found
Webserver is vulnerable to attacks on 64-bit block ciphers in TLS and OpenVPN (Sweet
SSL certificate will be expired in less than 60 days
Web form allows password caching in the client-side (autocomplete on)
Found support to TLS version 1.0 protocol (via downgrade)
Default SSL/TLS protocol version
Webserver is supporting SSL/TLS Forward Secrecy Cipher (PFS)
Webserver is enforcing its own SSL/TLS cipher order
SSL/TLS Ciphers supported by this webserver
Webserver will disclose platform details or version information (HTTP Information)
Webserver will disclose platform details or version information (Server Version)

Vulnerability Information

Found support for weak ciphers in SSL/TLS communication

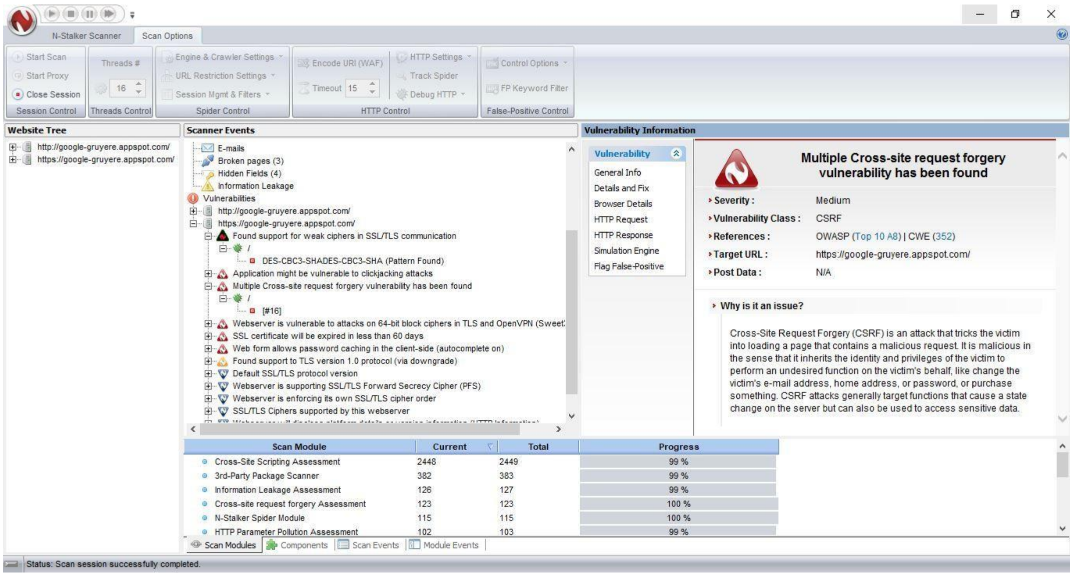
- Severity : High
- Vulnerability Class : Web Server Infrastructure attack
- References : OWASP (Top 10 A5) | CWE (310)
- Target URL : https://google-gruyere.appspot.com/
- Post Data : N/A

Why is it an issue?

Your webserver is vulnerable to a SSL/TLS Protocol is prone to an information-disclosure vulnerability. Attackers can exploit this issue to obtain sensitive information that may aid in launching further attacks.

Scan Module	Current	Total	Progress
Cross-Site Scripting Assessment	2448	2449	99 %
3rd-Party Package Scanner	382	383	99 %
Information Leakage Assessment	126	127	99 %
Cross-site request forgery Assessment	123	123	100 %
N-Stalker Spider Module	115	115	100 %
HTTP Parameter Pollution Assessment	102	103	99 %

Status: Scan session successfully completed.



Website Tree

http://google-gruyere.appspot.com/
https://google-gruyere.appspot.com/

Scanner Events

E-mails
Broken pages (3)
Hidden Fields (4)
Information Leakage
Vulnerabilities
http://google-gruyere.appspot.com/
https://google-gruyere.appspot.com/
Found support for weak ciphers in SSL/TLS communication
/
DES-CBC3-SHADES-CBC3-SHA (Pattern Found)
Application might be vulnerable to clickjacking attacks
Multiple Cross-site request forgery vulnerability has been found
/
[#16]
Webserver is vulnerable to attacks on 64-bit block ciphers in TLS and OpenVPN (Sweet
SSL certificate will be expired in less than 60 days
Web form allows password caching in the client-side (autocomplete on)
Found support to TLS version 1.0 protocol (via downgrade)
Default SSL/TLS protocol version
Webserver is supporting SSL/TLS Forward Secrecy Cipher (PFS)
Webserver is enforcing its own SSL/TLS cipher order
SSL/TLS Ciphers supported by this webserver

Vulnerability Information

Multiple Cross-site request forgery vulnerability has been found

- Severity : Medium
- Vulnerability Class : CSRF
- References : OWASP (Top 10 A8) | CWE (352)
- Target URL : https://google-gruyere.appspot.com/
- Post Data : N/A

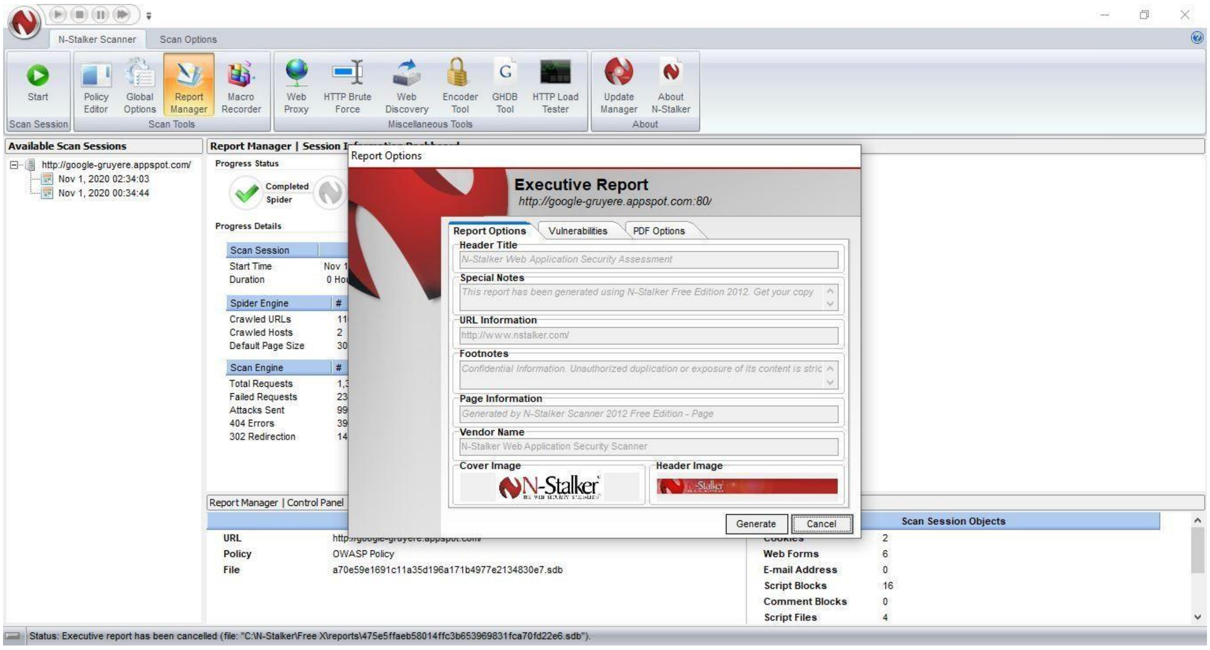
Why is it an issue?

Cross-Site Request Forgery (CSRF) is an attack that tricks the victim into loading a page that contains a malicious request. It is malicious in the sense that it inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf, like change the victim's e-mail address, home address, or password, or purchase something. CSRF attacks generally target functions that cause a state change on the server but can also be used to access sensitive data.

Scan Module	Current	Total	Progress
Cross-Site Scripting Assessment	2448	2449	99 %
3rd-Party Package Scanner	382	383	99 %
Information Leakage Assessment	126	127	99 %
Cross-site request forgery Assessment	123	123	100 %
N-Stalker Spider Module	115	115	100 %
HTTP Parameter Pollution Assessment	102	103	99 %

Status: Scan session successfully completed.

Step 10: Go to Report Manager, click on saved scan, generate either an executive/technical report



Available Scan Sessions

- http://google-gruyere.appspot.com/
  - Nov 1, 2020 02:34:03
  - Nov 1, 2020 00:34:44

Scan Session	
Start Time	Nov 1
Duration	0 Ho

Spider Engine	#
Crawled URLs	11
Crawled Hosts	2
Default Page Size	30

Scan Engine	#
Total Requests	1,3
Failed Requests	23
Attacks Sent	99
404 Errors	39
302 Redirection	14

Executive Report
http://google-gruyere.appspot.com:80/

Header Title: N-Stalker Web Application Security Assessment

Special Notes: This report has been generated using N-Stalker Free Edition 2012. Get your copy

URL Information: http://www.nstalker.com/

Footnotes: Confidential Information. Unauthorized duplication or exposure of its content is stric

Page Information: Generated by N-Stalker Scanner 2012 Free Edition - Page

Vendor Name: N-Stalker Web Application Security Scanner

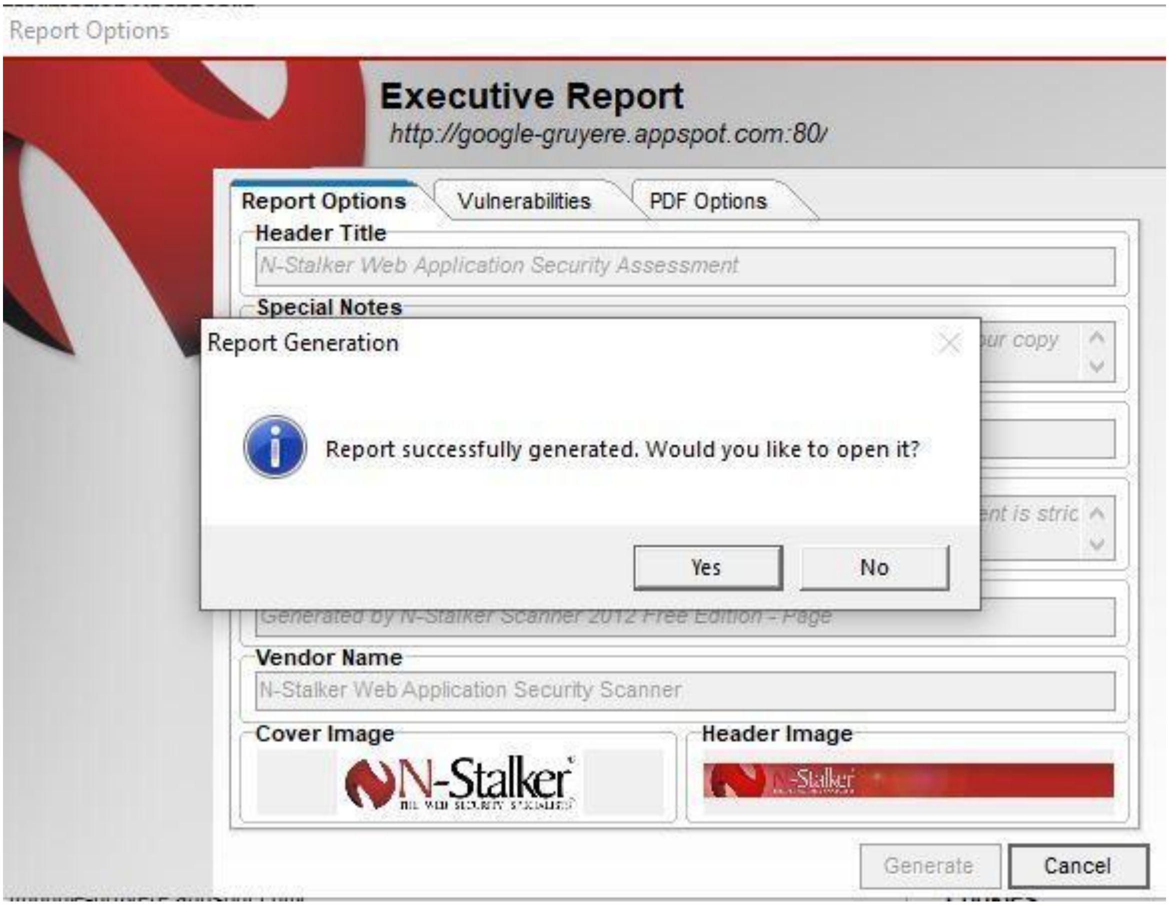
Cover Image

Header Image

URL	http://google-gruyere.appspot.com/
Policy	OWASP Policy
File	a70e59e1691c11a35d196a171b4977e2134830e7.sdb

Scan Session Objects	
Cookies	2
Web Forms	6
E-mail Address	0
Script Blocks	16
Comment Blocks	0
Script Files	4

Status: Executive report has been cancelled (file: "C:\N-Stalker\Free X\reports\475e5ffaeb58014ffc3b653969831fca70fd22e6.sdb").



Executive Report
http://google-gruyere.appspot.com:80/

Header Title: N-Stalker Web Application Security Assessment

Special Notes

Report successfully generated. Would you like to open it?

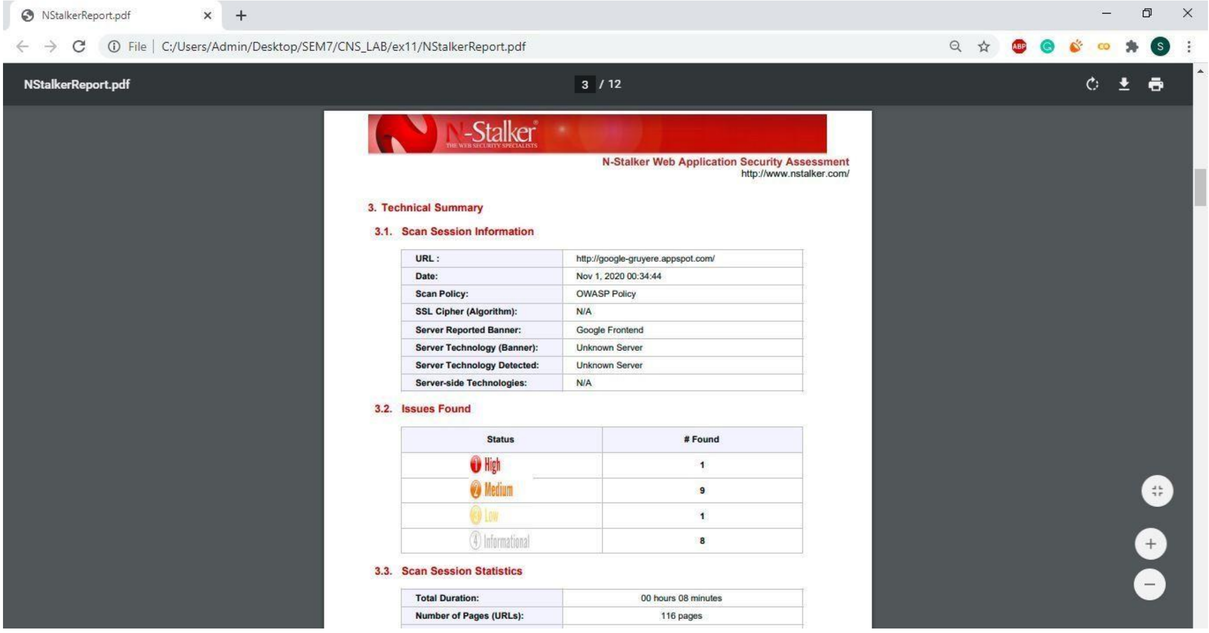
Generated by N-Stalker Scanner 2012 Free Edition - Page

Vendor Name: N-Stalker Web Application Security Scanner

Cover Image

Header Image

Step 11:View the saved report.



NStalkerReport.pdf
File | C:/Users/Admin/Desktop/SEM7/CNS_LAB/ex11/NStalkerReport.pdf
NStalkerReport.pdf
3 / 12
N-Stalker
THE WEB SECURITY SPECIALISTS

N-Stalker Web Application Security Assessment
http://www.nstalker.com/

3. Technical Summary

3.1. Scan Session Information

URL :	http://google-gruyere.appspot.com/
Date:	Nov 1, 2020 00:34:44
Scan Policy:	OWASP Policy
SSL Cipher (Algorithm):	N/A
Server Reported Banner:	Google Frontend
Server Technology (Banner):	Unknown Server
Server Technology Detected:	Unknown Server
Server-side Technologies:	N/A

3.2. Issues Found

Status	# Found
① High	1
② Medium	9
③ Low	1
④ Informational	8

3.3. Scan Session Statistics

Total Duration:	00 hours 08 minutes
Number of Pages (URLs):	116 pages