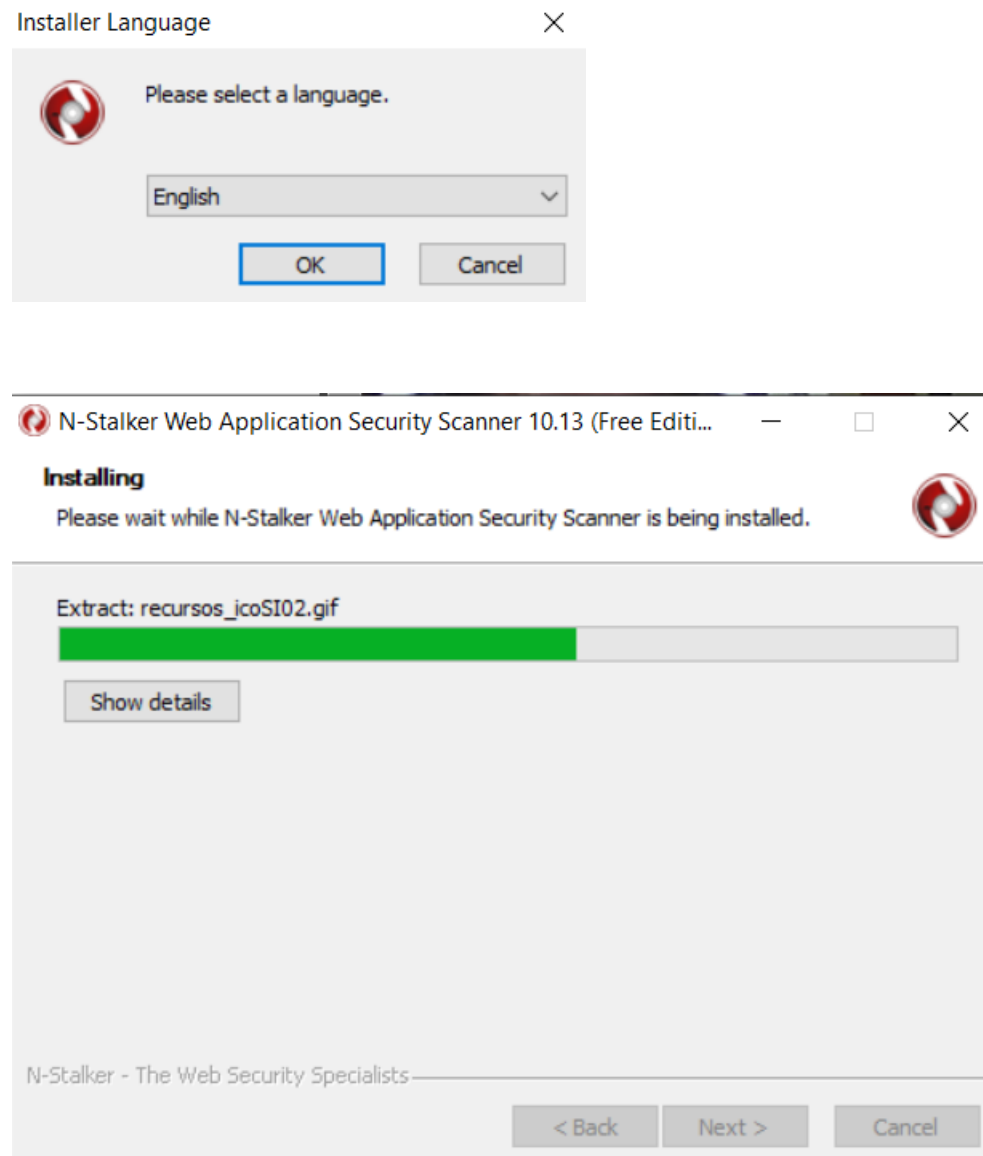


## Exercise 11:

### AIM:

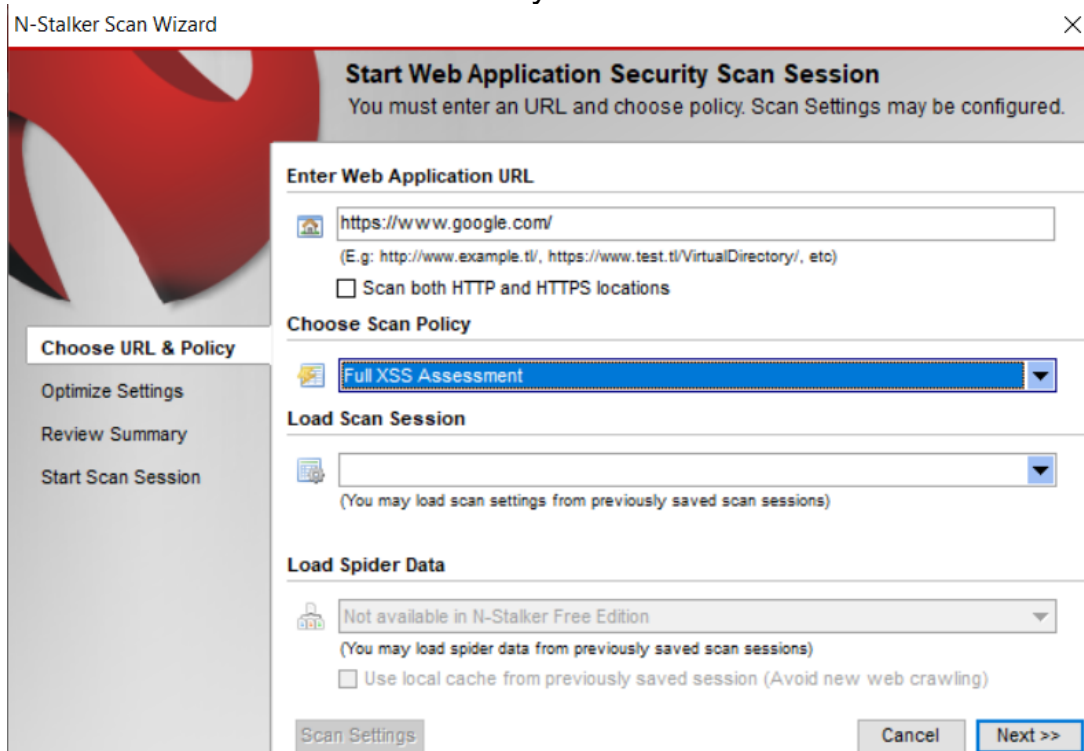
To download the N-Stalker Vulnerability Assessment Tool and exploring the features.

#### 1) Download and install N-Stalker





- 2) Click on “Scan ” and 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.




- 3) 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



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

Optimize Results | Authentication | False Positive | Engine | Miscellaneous

#### Optimization Progress

Press "Optimize" to optimize scan settings.

#### Optimization Results

Xfer Rate  Avg Response  Conn Failures


- 4) In review summary, 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.

#### Review Summary



#### Scanning Settings

Scan Setting	Value
• Host Information	IP: [172.217.167.132] Port: [443] SSL: [yes]
• Restricted Directory	Not configured.
• Policy Name	Full XSS Assessment
• 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] External JS [Deny] JS Events [Execute] SWF
• Server Technologies	N/A
• Allowed Hosts	No additional hosts configured.

5) 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.

Dashboard:

The screenshot displays the N-Stalker Scanner interface. The top section includes controls for starting the scan, setting threads (8), and configuring various settings like Engine & Crawler, URL Restrictions, Session Management, Encode URI, Error Settings, and Control Options. The main dashboard area shows the progress of a scan on <https://www.google.com/> using a Full XSS Assessment policy with 8 threads. The progress status indicates that the Spider is completed, while Info Gather, Run Modules, and Sig Scanner are not tested. The progress details table shows the scan session started on Nov 3, 2020, at 14:03:12, with a duration of 1 hour and 17 minutes. The Spider Engine has crawled 502 URLs, 1 host, and 556,296 bytes. The Scan Engine statistics show 2,725 total requests, 0 failed requests, 246 attacks sent, 1,492 errors, and 207 302 redirections. The Network statistics show 1,465,577 bytes sent, 44,733,046 bytes received, an average response time of 0.93 s, an average transfer rate of 134.03 KB/s, and 35.00 requests per minute. A bar chart shows the distribution of vulnerabilities: High (0), Mid (0), Low (0), and Info (0). The log at the bottom shows the scanner reaching the URL limit imposed by the N-Stalker Free Edition (500 pages) and successfully executing the Main() and HttpPipeline() modules.

**Website Tree**

- <https://www.google.com/>
  - Ajax Tree
  - fbx
  - Site Tree

**Scanner Events**

- Scanner
  - Dashboard
  - Site Sequence
  - Allowed Hosts
  - Rejected Hosts
  - Objects
    - Cookies (7)
    - Scripts (303)
    - Comments
    - Web Forms (198)
    - E-mails
    - Broken pages (232)
    - Hidden Fields (984)
    - Information Leakage
    - Vulnerabilities

**Scanner Dashboard**

**Progress Status**

- Completed Spider
- Not Tested Info Gather
- Step 3 Run Modules
- Not Tested Sig Scanner

**Progress Details**

Scan Session	#
Start Time	Nov 3, 2020 14:03:12
Duration	1 Hours 17 Minutes

Spider Engine	#
Crawled URLs	502
Crawled Hosts	1
Default Page Size	556,296 bytes

Scan Engine	#
Total Requests	2,725
Failed Requests	0
Attacks Sent	246
404 Errors	1,492
302 Redirection	207

Network	#
Bytes Sent	1,465,577
Bytes Received	44,733,046
Avg Response Time	0.93 s
Avg Transfer Rate	134.03 KB/s
Requests/Minute	35.00 req/min

**Log**

```
[11/03/2020 15:19:15] ZSpider(): N-Stalker has reached an URL limit imposed by N-Stalker Free Edition (500 pages)
[11/03/2020 15:19:16] Main(): N-Stalker Spider Module has been successfully executed.
[11/03/2020 15:19:16] HttpPipeline(): HttpPipeline has been successfully completed.
[11/03/2020 15:19:27] HttpPipeline(): All pipes have been successfully terminated.
[11/03/2020 15:19:28] ModuleLoader(): Loading Attack Module [File Extensions Finder] version [17102702] (open script).
[11/03/2020 15:19:28] ModuleLoader(): Module [File Extensions Finder] has finished [Total: 1 servers].
[11/03/2020 15:19:28] LuaScript(): [string "-- nsmod10..."]:292: attempt to call method 'getNoPostForm' (a string value)
[11/03/2020 15:19:28] ModuleLoader(): Loading Attack Module [WebServer Infrastructure Assessment] version [20082101] (open script).
[11/03/2020 15:19:28] ModuleLoader(): Module [WebServer Infrastructure Assessment] has finished [Total: 1 servers].
[11/03/2020 15:19:28] ModuleLoader(): Loading Attack Module [HTTP Method Finder] version [13091701] (open script).
[11/03/2020 15:19:28] ModuleLoader(): Module [HTTP Method Finder] has finished [Total: 1 servers].
[11/03/2020 15:19:28] LuaScript(): Skipping checks for webserver vulnerabilities on [https://www.google.com/] (user policy)
[11/03/2020 15:19:28] LuaScript(): Skipping checks for SSL/TLS vulnerabilities on [https://www.google.com/] (due to user policy)
[11/03/2020 15:19:32] ModuleLoader(): Loading Attack Module [Cross-Site Scripting Assessment] version [16061401] (by URI).
```

**Scan Modules** **Components** **Scan Events** **Module Events**

## Site sequence:

The screenshot shows the N-Stalker Scanner interface with the 'Site Sequence' tab selected. The URL is 'https://www.google.com/' and the policy is 'Full XSS Assessment'. The threads are set to 8. The 'Site Sequence' table lists 21 requests, all GET methods, to various Google URLs. The 'Post Data' column shows 'N/A' for all requests. Below the table, the HTTP response details are displayed, including status '200 OK', date, expires, cache-control, content-type, p3p, content-encoding, server, x-xss-protection, and x-frame-options.

#	Method	URL	Post Data
1	GET	https://www.google.com/	N/A
3	GET	https://www.google.com/robots.txt	N/A
5	GET	https://www.google.com/search?hl=en-IN&source=	N/A
7	GET	https://www.google.com/doodles/	N/A
9	GET	https://www.google.com/advanced_search?hl=en-	N/A
11	GET	https://www.google.com/setprefs?sig=0_5g07z2Z	N/A
13	GET	https://www.google.com/setprefs?sig=0_5g07z2Z	N/A
15	GET	https://www.google.com/setprefs?sig=0_5g07z2Z	N/A
17	GET	https://www.google.com/setprefs?sig=0_5g07z2Z	N/A
19	GET	https://www.google.com/setprefs?sig=0_5g07z2Z	N/A
21	GET	https://www.google.com/setprefs?sig=0_5g07z2Z	N/A

```
1 HTTP/1.1 200 OK
2 Date: Tue, 03 Nov 2020 08:33:21 GMT
3 Expires: -1
4 Cache-Control: private, max-age=0
5 Content-Type: text/html; charset=UTF-8
6 P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
7 Content-Encoding: gzip
8 Server: gws
9 X-XSS-Protection: 0
10 X-Frame-Options: SAMEORIGIN
```

## Cookies:

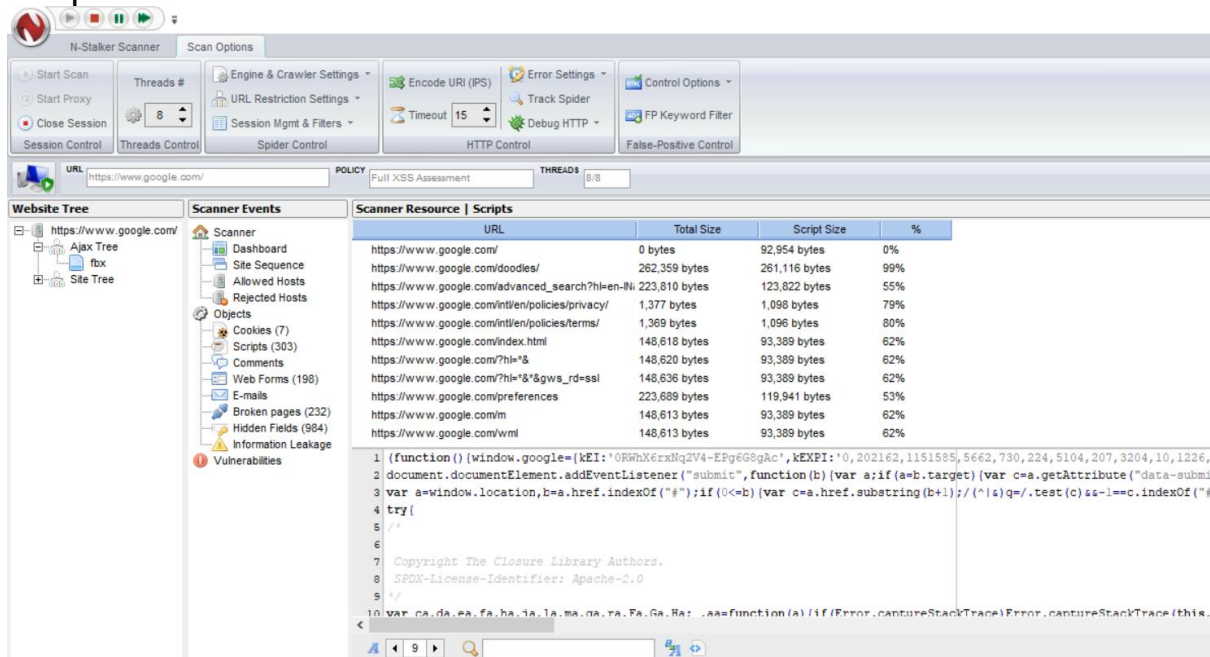
The screenshot shows the N-Stalker Scanner interface with the 'Cookies' tab selected. The URL is 'https://www.google.com/' and the policy is 'Full XSS Assessment'. The threads are set to 8. The 'Scanner Resource | Cookies' table lists 6 cookies from various Google URLs. The 'Cookie Value' column shows the value of each cookie. Below the table, the cookie details are displayed, including name, value, expires, domain, path, session, secure, httpOnly, and N-Stalker Decoded Value.

Source URL	Cookie Name	Cookie Value	Cookie Type	Visibility	Domain
https://www.google.com/	1P_JAR	2020-11-03-09	DISK	ALL	google.com
https://www.google.com/	NID	204=Vm0zzk5cumbYLHcPnDk	DISK	BROWSER-ONL	google.com
https://www.google.com/s	CGIC	IgMqLyO	DISK	BROWSER-ONL	google.com
https://www.google.com/s	CGIC	IgMqLyO	DISK	BROWSER-ONL	google.com
https://www.google.com/d	hl	en	DISK	ALL	www.google.com
https://www.google.com/d	xid	535534178	DISK	BROWSER-ONL	www.google.com
https://www.google.com/r	PAIDCONTENT	mo3fzqhi7wslmmg55ti	DISK	BROWSER-ONL	www.google.com

```
1 Cookie = {
2   Name = "1P_JAR",
3   Value = "2020-11-03-09",
4   Expires = "Thu, 03-Dec-2020 08:33:21 GMT",
5   Domain = ".google.com",
6   Path = "/",
7   Session = false,
8   Secure = true,
9   httpOnly = false,
10  N-Stalker Decoded Value = "N/A"
```



## Scripts:



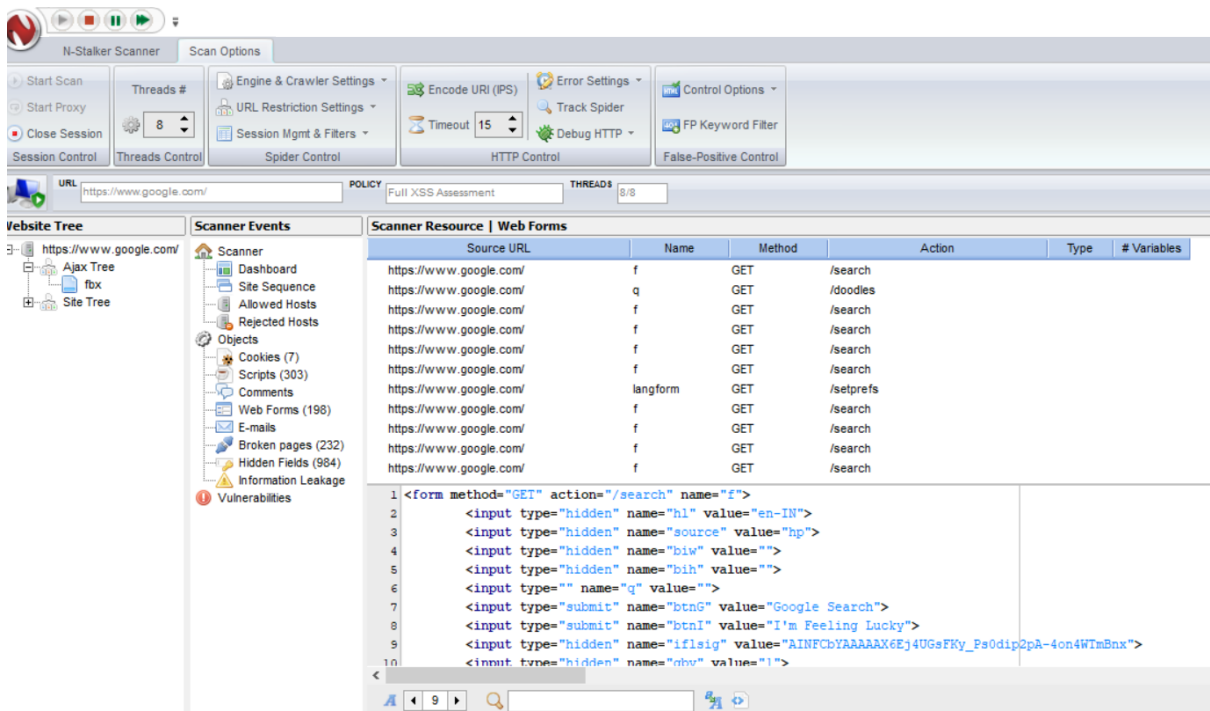
The N-Stalker Scanner interface displays the results of a scan for scripts on the website https://www.google.com/. The main window is titled "Scripts" and shows a table of resources found. The table has columns for URL, Total Size, Script Size, and %.

URL	Total Size	Script Size	%
https://www.google.com/	0 bytes	92,954 bytes	0%
https://www.google.com/doodles/	262,359 bytes	261,116 bytes	99%
https://www.google.com/advanced_search?hl=en-IN	223,810 bytes	123,822 bytes	55%
https://www.google.com/intl/en/policies/privacy/	1,377 bytes	1,096 bytes	79%
https://www.google.com/intl/en/policies/terms/	1,369 bytes	1,096 bytes	80%
https://www.google.com/index.html	148,618 bytes	93,389 bytes	62%
https://www.google.com/?hl=&	148,620 bytes	93,389 bytes	62%
https://www.google.com/?hl=&&gws_rd=ssl	148,636 bytes	93,389 bytes	62%
https://www.google.com/preferences	223,689 bytes	119,941 bytes	53%
https://www.google.com/vm	148,613 bytes	93,389 bytes	62%
https://www.google.com/vml	148,613 bytes	93,389 bytes	62%

Below the table, there is a code editor showing the JavaScript code for the first script (https://www.google.com/). The code is a function that initializes the Google search interface.

```
1 (function () {window.google={kEI:'ORWhX6rxMq2V4-EPg6G8gAc',kEXPI:'0,202162,1151585,5662,730,224,5104,207,3204,10,1226,
2 document.documentElement.addEventListener("submit",function(b){var a;if(a=b.target){var c=a.getAttribute("data-submit")
3 var a=window.location,b=a.href.indexOf("#");if(0<=b){var c=a.href.substring(b+1);/^([a-z0-9-])+$/.test(c)&&1==c.indexOf("#")
4 try{
5 }
6
7 Copyright The Closure Library Authors.
8 SPDX-License-Identifier: Apache-2.0
9
10 var ca,da,ea,fa,ha,ia,la,ma,na,pa,ra,sa,ta,ua,va,wa,xa,ya,za;aa=function(a){if(Error.captureStackTrace)Error.captureStackTrace(this,
```

## Web forms:



The N-Stalker Scanner interface displays the results of a scan for web forms on the website https://www.google.com/. The main window is titled "Web Forms" and shows a table of resources found. The table has columns for Source URL, Name, Method, Action, Type, and # Variables.

Source URL	Name	Method	Action	Type	# Variables
https://www.google.com/	f	GET	/search		
https://www.google.com/	q	GET	/doodles		
https://www.google.com/	f	GET	/search		
https://www.google.com/	f	GET	/search		
https://www.google.com/	f	GET	/search		
https://www.google.com/	f	GET	/search		
https://www.google.com/	langform	GET	/setprefs		
https://www.google.com/	f	GET	/search		
https://www.google.com/	f	GET	/search		
https://www.google.com/	f	GET	/search		
https://www.google.com/	f	GET	/search		

Below the table, there is a code editor showing the HTML code for the first web form (https://www.google.com/). The code is an HTML form for searching on Google.

```
1 <form method="GET" action="/search" name="f">
2   <input type="hidden" name="hl" value="en-IN">
3   <input type="hidden" name="source" value="hp">
4   <input type="hidden" name="biw" value="">
5   <input type="hidden" name="bih" value="">
6   <input type="text" name="q" value="">
7   <input type="submit" name="btnG" value="Google Search">
8   <input type="submit" name="btnI" value="I'm Feeling Lucky">
9   <input type="hidden" name="ifsig" value="AINFCbYAAAAAX6Ej4UGsFKy_Ps0dip2pA-4on4WImBnx">
10  <input type="hidden" name="nbt" value="1">
```

The screenshot displays the N-Stalker Scanner application interface. The top bar includes navigation icons and the application name. The main window is divided into several sections:

- Top Bar:** Contains icons for Start Scan, Start Proxy, Close Session, Session Control, Threads Control, Engine & Crawler Settings, URL Restriction Settings, Session Mgmt & Filters, Spider Control, Encode URI (IPS), Error Settings, Control Options, FP Keyword Filter, Timeout (set to 15), Track Spider, Debug HTTP, HTTP Control, and False-Positive Control.
- URL Bar:** Shows the target URL as `https://www.google.com/` and the scan type as `Full XSS Assessment`. The thread count is `8/8`.
- Website Tree:** A hierarchical view of the scanned website structure, including `https://www.google.com/`, `Ajax Tree`, `fbx`, `Site Tree`, `Scanner`, `Dashboard`, `Site Sequence`, `Allowed Hosts`, `Rejected Hosts`, `Objects`, `Cookies (7)`, `Scripts (303)`, `Comments`, `Web Forms (198)`, `E-mails`, `Broken pages (232)`, `Hidden Fields (984)`, and `Information Leakage`.
- Scanner Events:** A list of events related to the scan, including `Scanner`, `Dashboard`, `Site Sequence`, `Allowed Hosts`, `Rejected Hosts`, `Objects`, `Cookies (7)`, `Scripts (303)`, `Comments`, `Web Forms (198)`, `E-mails`, `Broken pages (232)`, `Hidden Fields (984)`, and `Information Leakage`.
- Scanner Resource | Broken Pages:** A table showing the results of the scan, listing the source URL, the broken page, and the number of repetitions.

Source URL	Broken Page	# Repetitions
<code>https://www.google.com/robots.txt</code>	<code>https://www.google.com/sdch</code>	1
<code>https://www.google.com/robots.txt</code>	<code>https://www.google.com/u/</code>	1
<code>https://www.google.com/robots.txt</code>	<code>https://www.google.com/default</code>	1
<code>https://www.google.com/robots.txt</code>	<code>https://www.google.com/m/</code>	1
<code>https://www.google.com/robots.txt</code>	<code>https://www.google.com/wml/</code>	1
<code>https://www.google.com/robots.txt</code>	<code>https://www.google.com/xhtml/</code>	1
<code>https://www.google.com/robots.txt</code>	<code>https://www.google.com/xml</code>	1
<code>https://www.google.com/robots.txt</code>	<code>https://www.google.com/imode/</code>	1
<code>https://www.google.com/robots.txt</code>	<code>https://www.google.com/imode/search</code>	1
<code>https://www.google.com/robots.txt</code>	<code>https://www.google.com/jsky</code>	1
<code>https://www.google.com/robots.txt</code>	<code>https://www.google.com/jsky/</code>	1

Below the table, a list of broken pages is shown, including `https://www.google.com/sdch`, `https://www.google.com/u/`, `https://www.google.com/default`, `https://www.google.com/m/`, `https://www.google.com/wml/`, `https://www.google.com/xhtml/`, `https://www.google.com/xml`, `https://www.google.com/imode/`, `https://www.google.com/imode/search`, and `https://www.google.com/jsky`.

The screenshot displays the N-Stalker Scanner application interface. At the top, there's a navigation bar with 'N-Stalker Scanner' and 'Scan Options'. Below this, a control panel includes buttons for 'Start Scan', 'Start Proxy', 'Close Session', and 'Session Control', along with 'Threads #' (set to 8), 'Engine & Crawler Settings', 'URL Restriction Settings', 'Session Mgmt & Filters', 'Spider Control', 'Encode URI (IPS)', 'Error Settings', 'Track Spider', 'Debug HTTP', 'HTTP Control', 'Control Options', and 'FP Keyword Filter'. The main area shows the 'URL' as 'https://www.google.com/' and 'THREADS' as '8/8'. The 'Website Tree' on the left lists various scanned elements like 'Ajax Tree', 'fbx', 'Site Tree', 'Scanner', 'Dashboard', 'Site Sequence', 'Allowed Hosts', 'Rejected Hosts', 'Objects', 'Cookies (7)', 'Scripts (303)', 'Comments', 'Web Forms (198)', 'E-mails', 'Broken pages (232)', 'Hidden Fields (984)', and 'Vulnerabilities'. The 'Scanner Resource | Hidden Fields' table is the central focus, listing source URLs and their hidden variables. The table has three columns: 'Source URL', 'Hidden Variable', and 'Value'. It lists several URLs from 'https://www.google.com/' and their hidden variables, all with values like 'en-IN'. Below the table, a list of hidden fields is shown, each starting with '<input type="hidden" name="hl" value="en-IN">'. The bottom status bar shows '4' and navigation icons.

**Scanner Resource | Hidden Fields**

Source URL	Hidden Variable	Value
https://www.google.com/	hl	en-IN
https://www.google.com/advanced_search	hl	en-IN
https://www.google.com/index.html	hl	en-IN
https://www.google.com/?hl=*%&	hl	en-IN
https://www.google.com/?hl=*%&*gws_r	hl	en-IN
https://www.google.com/m	hl	en-IN
https://www.google.com/vml	hl	en-IN
https://www.google.com/vml/search	hl	en-IN
https://www.google.com/xhtml	hl	en-IN
https://www.google.com/imode	hl	en-IN
https://www.google.com/pda	hl	en-IN

Below the table, a list of hidden fields is displayed:

```

1 <input type="hidden" name="hl" value="en-IN">
2 <input type="hidden" name="hl" value="en-IN">
3 <input type="hidden" name="hl" value="en-IN">
4 <input type="hidden" name="hl" value="en-IN">
5 <input type="hidden" name="hl" value="en-IN">
6 <input type="hidden" name="hl" value="en-IN">
7 <input type="hidden" name="hl" value="en-IN">
8 <input type="hidden" name="hl" value="en-IN">
9 <input type="hidden" name="hl" value="en-IN">
10 <input type="hidden" name="hl" value="en-IN">

```

5) Scan completed successfully

Results Wizard

**Scan Session has finished successfully.**  
*N-Stalker did not found any vulnerabilities.*

**Session Management Options**

☒ Save scan results  
☐ Discard scan results

**Next Steps**

☒ Close scan session and return to main screen  
☐ Open N-Stalker Report Manager  
☐ Keep scan session for further analysis

**Total Scan Time**  
2 Hour(s) 49 Minute(s)

**Total Vulnerabilities**

High : 0  
Medium : 0  
Low : 0  
Info : 0

Cancel Next >>

Results Wizard

**Scan Session has finished successfully.**  
*N-Stalker did not found any vulnerabilities.*

**Summary**

Application Objects	Count
Total Web Pages	502
High Vulnerabilities	0
Medium Vulnerabilities	0
Low Vulnerabilities	0
Info Vulnerabilities	0
Total Hosts Found	1
Total HTTP Cookies	7
Total Directories Found	0
Total Web Forms Found	198
Total Password Forms	0
Total E-mails Found	0
Total Client Scripts	335
Total HTML Comments	0

Your request has been successfully processed.

Done



## 6) Report generation

The screenshot displays the N-Stalker Scanner interface. The top menu bar includes options like Start, Policy Editor, Global Options, Report Manager, Macro Recorder, Web Proxy, HTTP Brute Force, Web Discovery, Encoder Tool, GHDB Tool, HTTP Load Tester, Update Manager, and About N-Stalker. The main window is titled 'Report Manager | Session Information Dashboard'. It shows a progress status for a scan session on 'https://www.google.com/' starting on Nov 3, 2020, at 14:03:12. The session duration is 2 hours and 49 minutes. The Spider Engine has crawled 502 URLs, 1 host, and 556,296 bytes. The Scan Engine has processed 13,740 total requests, 0 failed requests, 11,261 attacks sent, 1,635 404 errors, and 2,234 302 redirections. A network statistics table shows 9,638,751 bytes sent, 524,133,200 bytes received, a 2.00s average response time, 0.00 B/s average transfer rate, and 81.00 requests per minute. A bar chart shows the distribution of issues by severity: High (8), Mid (0), Low (0), and Info (0). The bottom section, 'Report Manager | Control Panel', displays scan session details (URL, Policy, File) and scan session objects (Cookies, Web Forms, E-mail Address, Script Blocks, Comment Blocks, Script Files).

Scan Session	
Start Time	Nov 3, 2020 14:03:12
Duration	2 Hours 49 Minutes
Spider Engine	
Crawled URLs	502
Crawled Hosts	1
Default Page Size	556,296 bytes
Scan Engine	
Total Requests	13,740
Failed Requests	0
Attacks Sent	11,261
404 Errors	1,635
302 Redirection	2,234

Network	
Bytes Sent	9,638,751
Bytes Received	524,133,200
Avg Response Time	2.00 s
Avg Transfer Rate	0.00 B/s
Requests/Minute	81.00 req/min

Scan Session Objects	
Cookies	7
Web Forms	198
E-mail Address	0
Script Blocks	303
Comment Blocks	0
Script Files	32

### Report Options

The screenshot shows the 'Technical Report' generation options dialog box for the URL 'https://www.google.com:443/'. The dialog has four tabs: Section Configuration, Report Options, Vulnerabilities, and PDF Options. The 'Section Configuration' tab is active, showing various checkboxes for report content. The 'Generate' button is highlighted.

**Technical Report**  
*https://www.google.com:443/*

**Section Configuration** | Report Options | Vulnerabilities | PDF Options

**Technical Summary**

- ☒ Show Scan Session Statistics
- ☒ Show Scan Policy Details

**Graphic Details**

- ☒ Show Graphical Statistics of Scan Session

**Items that Require your attention**

- ☒ Show Infrastructure Issues
- ☒ Show Confidentiality Issues
- ☒ Show Application Issues

**Object Technical Details**

- ☒ Show Objects Summary
- ☒ Show Hidden Directories
- ☐ Show HTML Hidden Fields
- ☐ Show Web Forms Structure
- ☒ Show HTTP Cookies
- ☒ Show E-mail Address
- ☒ Show Information Exposure

**Vulnerability Technical Details**

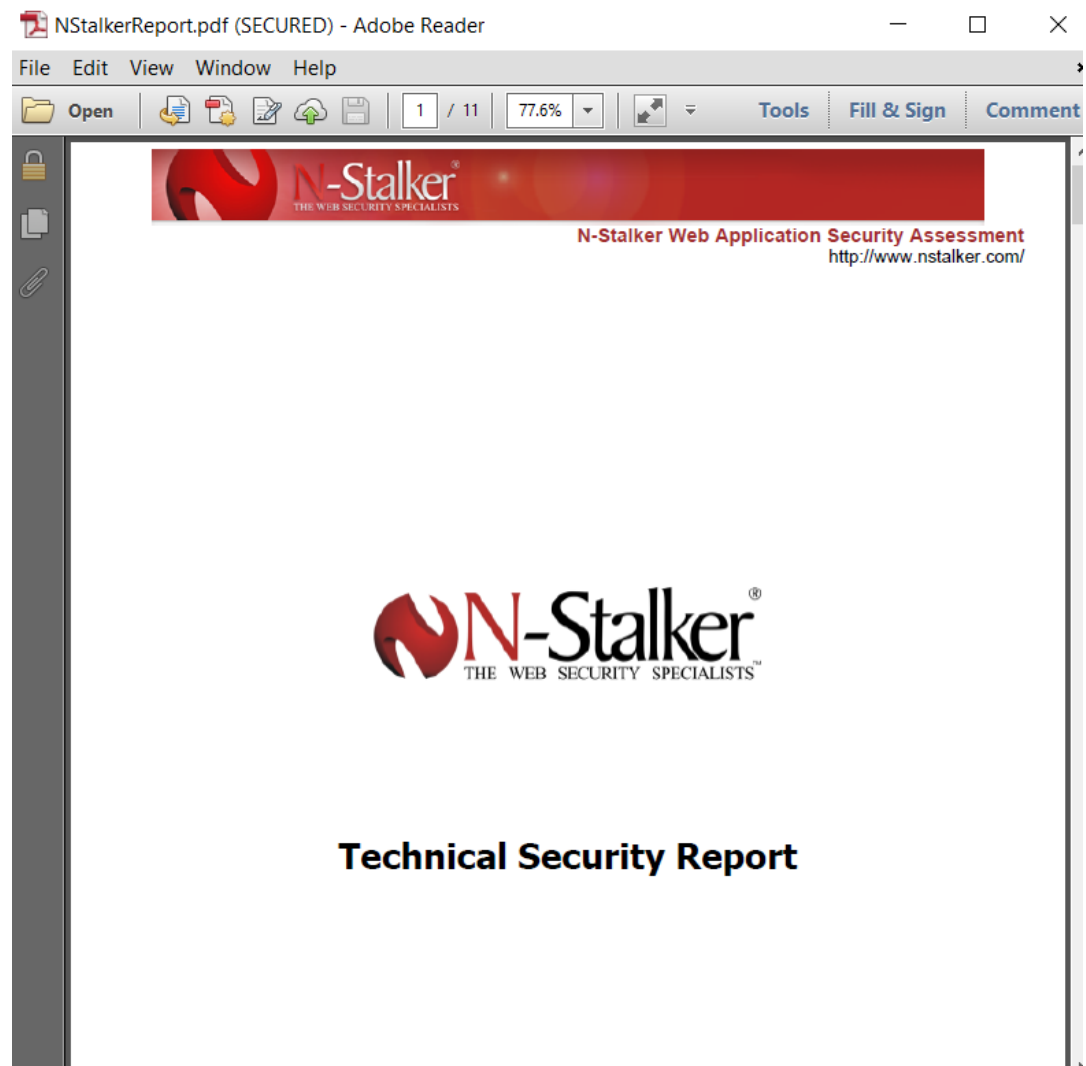
- ☒ Show Infrastructure Issues
- ☒ Show Confidentiality Issues
- ☒ Show Application Issues
- ☒ Aggregate similar vulnerabilities

**HTTP Evidence Details**

- ☒ Show HTTP Request & Response
- ☐ Show Header Only
- ☒ Show Header/Body
- Restrict to: (0 none) 3000 bytes

**Generate** **Cancel**

## NSTALKER REPORT:







### 3. Technical Summary

#### 3.1. Scan Session Information

URL :	https://www.google.com/
Date:	Nov 3, 2020 14:03:12
Scan Policy:	Full XSS Assessment
SSL Cipher (Algorithm):	N/A
Server Reported Banner:	gws
Server Technology (Banner):	Unknown Server
Server Technology Detected:	Unknown Server
Server-side Technologies:	N/A

#### 3.2. Issues Found

Status	# Found
 High	0
 Medium	0
 Low	0
 Informational	0

#### 3.3. Scan Session Statistics

Total Duration:	02 hours 49 minutes
Number of Pages (URLs):	502 pages
Total Requests:	13,740 requests
Total Bytes In:	524,133,200 bytes
Total Bytes Out:	9,638,751 bytes
Average Response Time:	2 ms
Average Transfer Rate:	15,382.00 KB/s
Average Page Size:	556,296 bytes

## 6. Object Technical Details

### 6.1. Objects Summary

Cookies	7
Javascript (# of Script Blocks)	303
Javascript (# of Script Files)	32
HTML Comments (# of Blocks)	0
E-mail Address	0
Broken Pages	232
Web Forms	198
Hidden Fields (Forms)	984
Information Exposure (Tags)	0

### 6.2. HTTP Cookies

Cookie Name	1P_JAR
Cookie Value	2020-11-03-09
Cookie Domain	.google.com
Cookie Path	/
Cookie Attributes	Disk Cookie; SSL; Protected from script
Source URL	<a href="https://www.google.com/?tbn=pts&amp;hl=en-IN&amp;source=hp&amp;biw=&amp;bih=&amp;q=&amp;btnG=Google%20Search&amp;btnI=I'm%20Feeling%20Lucky&amp;fbsig=AINFcbYAAAAAX6EndrCqwoLHr0li8jjWzScUQkKV_D&amp;gbv=1">https://www.google.com/?tbn=pts&amp;hl=en-IN&amp;source=hp&amp;biw=&amp;bih=&amp;q=&amp;btnG=Google%20Search&amp;btnI=I'm%20Feeling%20Lucky&amp;fbsig=AINFcbYAAAAAX6EndrCqwoLHr0li8jjWzScUQkKV_D&amp;gbv=1</a>

Cookie Name	NID
Cookie Value	204=Vm0zzk5cumbYLHcPnDKIHNVicgyffDqtF9NPF-CztEs7iDt8NQI3x6xtnK_PnQyDpMXIVRVooknEn14_fN1J0bMAJ OzO_XA8TI0q2lwk9kXm2cXIFU8jOLM1mBXLhPrs3gKfC3L1RUd 84rFJtFU66cE-EL2oKfb_nJpucsg3rGo
Cookie Domain	.google.com
Cookie Path	/
Cookie Attributes	Disk Cookie; SSL; Exposed to script
Source URL	<a href="https://www.google.com/?hl=en-IN&amp;source=hp&amp;biw=&amp;bih=&amp;q=&amp;btnG=Google%20Search&amp;btnI=I'm%20Feeling%20Lucky&amp;fbsig=AINFcbYAAAAAX6EIDVQpOOrWUUsZ1sRB-AX1W9yX64A&amp;gbv=1">https://www.google.com/?hl=en-IN&amp;source=hp&amp;biw=&amp;bih=&amp;q=&amp;btnG=Google%20Search&amp;btnI=I'm%20Feeling%20Lucky&amp;fbsig=AINFcbYAAAAAX6EIDVQpOOrWUUsZ1sRB-AX1W9yX64A&amp;gbv=1</a>

Cookie Name	CGIC
-------------	------

Confidential Information. Unauthorized duplication or exposure of its content is strictly forbidden.