Fortify Standalone Report Generator

OWASP Top 10 2021

G9_NF17027-2_898109_20230912_161654355928_JS

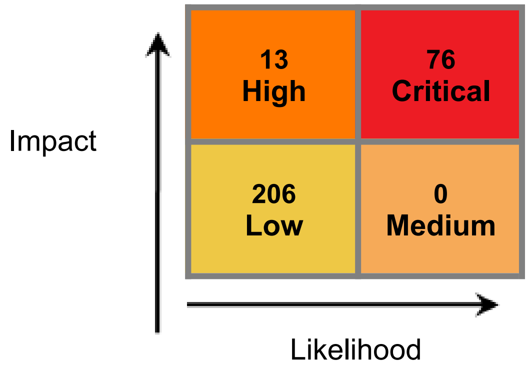
Table of Contents

Executive Summary

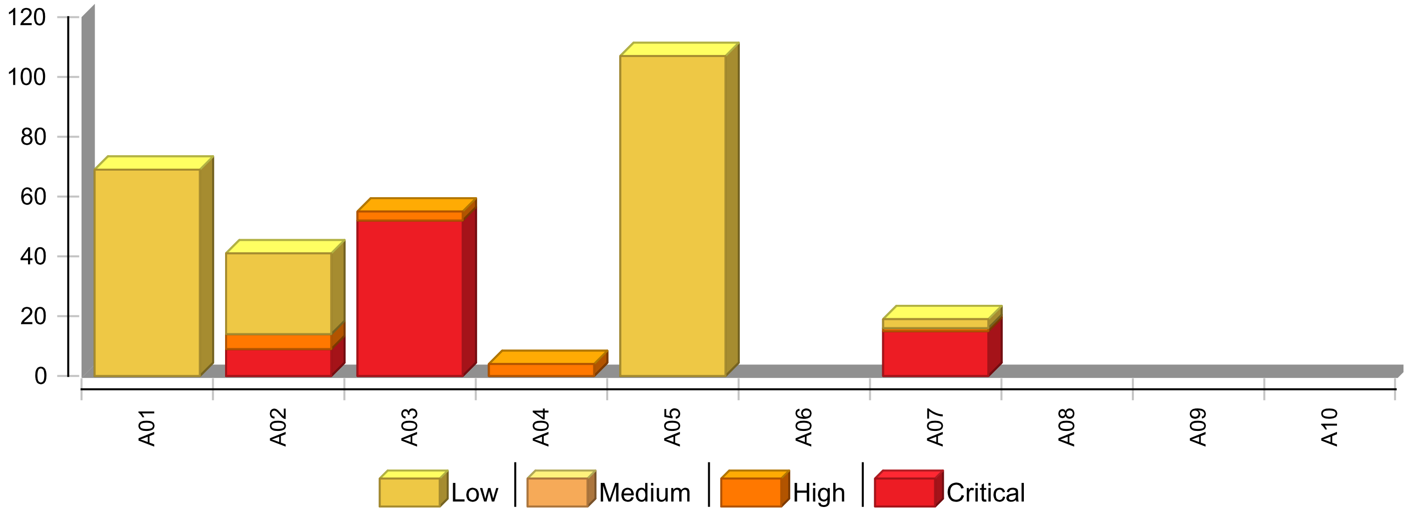
The OWASP Top 10 2021 provides a powerful awareness document for web application security focused on informing the community about the consequences of the most common and most important web application security weaknesses. The OWASP Top 10 represents a broad agreement about what the most critical web application security flaws are with consensus drawn from data collection and survey results. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Project Name:	G9_NF17027-2_898109
Project Version:	
SCA:	Results Present
WebInspect:	Results Not Present
WebInspect Agent:	Results Not Present
Other:	Results Not Present
Remediation Effort (Hrs):	23.6

Issues by Priority



Issues by OWASP Top 10 2021 Categories



* The detailed sections following the Executive Summary contain specifics.

Project Description

This section provides an overview of the Fortify scan engines used for this project, as well as the project meta-information.

SCA

Date of Last Analysis:	2023年9月12日 下午4:22	**Engine Version:**	22.2.2.0004
Host Name:	6F-812701-PC-02	**Certification:**	VALID
Number of Files:	572	**Lines of Code:**	38,473

Rulepack Name	Rulepack Version
Fortify Secure Coding Rules, Community, Cloud	2023.2.0.0007
Fortify Secure Coding Rules, Community, Universal	2023.2.0.0007
Fortify Secure Coding Rules, Core, Cloud	2023.2.0.0007
Fortify Secure Coding Rules, Core, JavaScript	2023.2.0.0007
Fortify Secure Coding Rules, Core, Universal	2023.2.0.0007
Fortify Secure Coding Rules, Extended, Configuration	2023.2.0.0007
Fortify Secure Coding Rules, Extended, Content	2023.2.0.0007
Fortify Secure Coding Rules, Extended, JavaScript	2023.2.0.0007

Issue Breakdown

The following table summarizes the number of issues identified across the different OWASP Top 10 2021 categories and broken down by Fortify Priority Order.

	Fortify Priority				Total Issues	Effort (hrs)
	Critical	High	Medium	Low		
A01 Broken Access Control	0	0	0	69	69	14.8
A02 Cryptographic Failures	9	5	0	27	41	2.7
A03 Injection	52	3	0	0	55	2.2
A04 Insecure Design	0	4	0	0	4	0.4
A05 Security Misconfiguration	0	0	0	107	107	3.8
A06 Vulnerable and Outdated Components	0	0	0	0	0	0.0
A07 Identification and Authentication Failures	15	1	0	3	19	1.6
A08 Software and Data Integrity Failures	0	0	0	0	0	0.0
A09 Security Logging and Monitoring Failures	0	0	0	0	0	0.0
A10 Server-Side Request Forgery	0	0	0	0	0	0.0

NOTE:
1. Reported issues in the above table may violate more than one OWASP Top 10 2021 category. As such, the same issue may appear in more than one row. The total number of unique vulnerabilities are reported in the Executive Summary table.
2. For the same reason, the Project-level remediation effort total shown in the Executive Summary removes the effect of any duplication and may be smaller than the sum of the remediation effort per individual category.
3. Similarly, the remediation effort per external category is not intended to equal the sum of the remediation effort from the issue details section since individual files may contain issues in multiple Fortify priorities or audit folders.

Issue Details

Below is an enumeration of all issues found in the project. The issues are organized by OWASP Top 10 2021, Fortify Priority Order, and vulnerability category. The issues are then further broken down by the package, namespace, or location in which they occur. Issues reported at the same line number with the same category originate from different taint sources.

A01 Broken Access Control

OWASP Top 10 Web Application Security Risks, A01:2021 states: "Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits."

Cross-Site Request Forgery ***Remediation Effort(Hrs): 14.8***	**Low**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD

Location	Analysis Info	Analyzer

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:251	`Sink: AssignmentStatement`
	`Enclosing Method: lambda()`
	`Source:`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:251	`Sink: AssignmentStatement`
	`Enclosing Method: lambda()`
	`Source:`
		SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.aws4

Location	Analysis Info	Analyzer

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/aws4/aws4.js:62	`Sink: AssignmentStatement`
	`Enclosing Method: RequestSigner()`
	`Source:`
		SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.form-data.lib

Location	Analysis Info	Analyzer

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/form-data/lib/form_data.js:392	`Sink: AssignmentStatement`
	`Enclosing Method: submit()`
	`Source:`
		SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.request

Location	Analysis Info	Analyzer

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:162	`Sink: AssignmentStatement`
	`Enclosing Method: init()`
	`Source:`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:728	`Sink: AssignmentStatement`
	`Enclosing Method: start()`
	`Source:`
		SCA

A01 Broken Access Control

OWASP Top 10 Web Application Security Risks, A01:2021 states: "Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits."

Cross-Site Request Forgery
Remediation Effort(Hrs): 14.8

Low

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.request.lib

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/redirect.js:119	**Sink:** `AssignmentStatement` **Enclosing Method:** `onResponse()` **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:152	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:312	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:452	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:602	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:835	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:870	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:886	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:914	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA

A01 Broken Access Control

OWASP Top 10 Web Application Security Risks, A01:2021 states: "Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits."

Cross-Site Request Forgery ***Remediation Effort(Hrs): 14.8***		**Low**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:924	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:934	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1010	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1103	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1118	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1134	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1150	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1175	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1198	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1232	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA

A01 Broken Access Control

OWASP Top 10 Web Application Security Risks, A01:2021 states: "Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits."

Cross-Site Request Forgery
Remediation Effort(Hrs): 14.8

Low

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1252	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1270	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1289	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1356	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1375	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1395	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1416	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1436	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1458	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1478	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA

A01 Broken Access Control

OWASP Top 10 Web Application Security Risks, A01:2021 states: "Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits."

Cross-Site Request Forgery
Remediation Effort(Hrs): 14.8

Low

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1493	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:142	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:169	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:301	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:434	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:461	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:581	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:814	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:849	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:865	**Sink:** AssignmentStatement **Enclosing Method:** lambda() **Source:**	SCA

A01 Broken Access Control

OWASP Top 10 Web Application Security Risks, A01:2021 states: "Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits."

Cross-Site Request Forgery ***Remediation Effort(Hrs): 14.8***		**Low**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:893	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:903	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:913	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:989	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1082	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1097	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1113	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1129	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1154	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1176	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA

A01 Broken Access Control

OWASP Top 10 Web Application Security Risks, A01:2021 states: "Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits."

Cross-Site Request Forgery ***Remediation Effort(Hrs): 14.8***		**Low**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1209	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1229	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1247	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1266	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1333	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1352	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1372	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1392	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1411	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1433	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA

A01 Broken Access Control

OWASP Top 10 Web Application Security Risks, A01:2021 states: "Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits."

Cross-Site Request Forgery ***Remediation Effort(Hrs): 14.8***	**Low**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1453	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1468	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.util

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/runtime.js:15	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/xrfile_delete_check.js:18	**Sink:** `AssignmentStatement` **Enclosing Method:** `lambda()` **Source:**	SCA

A02 Cryptographic Failures

OWASP Top 10 Web Application Security Risks, A02:2021 states: "The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS)."

Insecure Transport ***Remediation Effort(Hrs): 0.6***	**Critical**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/db_server.js:145	**Sink:** `FunctionPointerCall: listen` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js:119	**Sink:** `FunctionPointerCall: listen` **Enclosing Method:** `~file_function()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:356	**Sink:** `FunctionPointerCall: listen` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:356	**Sink:** `FunctionPointerCall: listen` **Enclosing Method:** `lambda()` **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.form-data.lib

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/form-data/lib/form_data.js:424	**Sink:** `FunctionPointerCall: request` **Enclosing Method:** `submit()` **Source:**	SCA

Weak Encryption ***Remediation Effort(Hrs): 0.2***	**Critical**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.jsbn

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsbn/index.js:1304	**Sink:** `FunctionCall: Arcfour` **Enclosing Method:** `init^()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsbn/index.js:1311	**Sink:** `FunctionCall: ARC4init` **Enclosing Method:** `init^()` **Source:**	SCA

A02 Cryptographic Failures

OWASP Top 10 Web Application Security Risks, A02:2021 states: "The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS)."

Weak Encryption
Remediation Effort(Hrs): 0.2

Critical

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.jsbn

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsbn/index.js:1326	**Sink:** `FunctionCall: ARC4next` **Enclosing Method:** `init^()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsbn/index.js:1341	**Sink:** `FunctionPointerCall: init^` **Enclosing Method:** `prng_newstate()` **Source:**	SCA

Insecure Randomness
Remediation Effort(Hrs): 0.5

High

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.form-data.lib

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/form-data/lib/form_data.js:321	**Sink:** `FunctionPointerCall: random` **Enclosing Method:** `_generateBoundary()` **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.jsbn

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsbn/index.js:1145	**Sink:** `FunctionPointerCall: random` **Enclosing Method:** `bnpMillerRabin()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsbn/index.js:1269	**Sink:** `FunctionPointerCall: random` **Enclosing Method:** `lambda()` **Source:**	SCA

A02 Cryptographic Failures

OWASP Top 10 Web Application Security Risks, A02:2021 states: "The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS)."

Insecure Randomness ***Remediation Effort(Hrs): 0.5***	**High**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.jsprim.lib

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsprim/lib/jsprim.js:570	**Sink:** `FunctionPointerCall: random` **Enclosing Method:** `randElt()` **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.rndm

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/rndm/index.js:22	**Sink:** `FunctionPointerCall: random` **Enclosing Method:** `rndm()` **Source:**	SCA

Weak Cryptographic Hash ***Remediation Effort(Hrs): 1.7***	**Low**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.aws-sign2

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/aws-sign2/index.js:71	**Sink:** `FunctionCall: hmacSha1` **Enclosing Method:** `init^()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/aws-sign2/index.js:87	**Sink:** `FunctionPointerCall: hmacSha1` **Enclosing Method:** `sign()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/aws-sign2/index.js:103	**Sink:** `FunctionPointerCall: hmacSha1` **Enclosing Method:** `signQuery()` **Source:**	SCA

A02 Cryptographic Failures

OWASP Top 10 Web Application Security Risks, A02:2021 states: "The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS)."

Weak Cryptographic Hash ***Remediation Effort(Hrs): 1.7***	**Low**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.cookie-signature

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/cookie-signature/index.js:42	**Sink:** `FunctionPointerCall: sha1` **Enclosing Method:** `unsign()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/cookie-signature/index.js:42	**Sink:** `FunctionPointerCall: sha1` **Enclosing Method:** `unsign()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/cookie-signature/index.js:49	**Sink:** `FunctionCall: sha1` **Enclosing Method:** `init^()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/cookie-signature/index.js:50	**Sink:** `FunctionPointerCall: createHash` **Enclosing Method:** `sha1()` **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.csrf

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/csrf/index.js:152	**Sink:** `FunctionPointerCall: createHash` **Enclosing Method:** `hash()` **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.express-session

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/express-session/index.js:608	**Sink:** `FunctionPointerCall: createHash` **Enclosing Method:** `hash()` **Source:**	SCA

A02 Cryptographic Failures

OWASP Top 10 Web Application Security Risks, A02:2021 states: "The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS)."

Weak Cryptographic Hash ***Remediation Effort(Hrs): 1.7***	**Low**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.oauth-sign

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/oauth-sign/index.js:3	**Sink:** `FunctionCall: sha` **Enclosing Method:** `init^()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/oauth-sign/index.js:86	**Sink:** `FunctionPointerCall: sha` **Enclosing Method:** `hmacsign()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/oauth-sign/index.js:96	**Sink:** `FunctionPointerCall: sha` **Enclosing Method:** `hmacsign256()` **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.request.lib

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js:82	**Sink:** `FunctionPointerCall: md5` **Enclosing Method:** `ha1Compute()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js:84	**Sink:** `FunctionPointerCall: md5` **Enclosing Method:** `ha1Compute()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js:94	**Sink:** `FunctionPointerCall: md5` **Enclosing Method:** `digest()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js:96	**Sink:** `FunctionPointerCall: md5` **Enclosing Method:** `digest()` **Source:**	SCA

A02 Cryptographic Failures

OWASP Top 10 Web Application Security Risks, A02:2021 states: "The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS)."

Weak Cryptographic Hash ***Remediation Effort(Hrs): 1.7***	**Low**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.request.lib

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js:97	**Sink:** FunctionPointerCall: md5 **Enclosing Method:** digest() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/helpers.js:30	**Sink:** FunctionCall: md5 **Enclosing Method:** init^() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/helpers.js:31	**Sink:** FunctionPointerCall: createHash **Enclosing Method:** md5() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/oauth.js:70	**Sink:** FunctionPointerCall: createHash **Enclosing Method:** buildBodyHash() **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.sshpk.lib

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/sshpk/lib/utils.js:117	**Sink:** FunctionPointerCall: createHash **Enclosing Method:** opensslKeyDeriv() **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.sshpk.lib.formats

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/sshpk/lib/formats/putty.js:143	**Sink:** FunctionPointerCall: createHash **Enclosing Method:** derivePPK2EncryptionKey() **Source:**	SCA

A02 Cryptographic Failures

OWASP Top 10 Web Application Security Risks, A02:2021 states: "The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS)."

Weak Cryptographic Hash ***Remediation Effort(Hrs): 1.7***		**Low**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.sshpk.lib.formats		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/sshpk/lib/formats/putty.js:147	**Sink:** `FunctionPointerCall: createHash` **Enclosing Method:** `derivePPK2EncryptionKey()` **Source:**	SCA
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.uuid.dist		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/uuid/dist/md5.js:12	**Sink:** `FunctionCall: md5` **Enclosing Method:** `init^()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/uuid/dist/md5.js:19	**Sink:** `FunctionPointerCall: createHash` **Enclosing Method:** `md5()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/uuid/dist/sha1.js:12	**Sink:** `FunctionCall: sha1` **Enclosing Method:** `init^()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/uuid/dist/sha1.js:19	**Sink:** `FunctionPointerCall: createHash` **Enclosing Method:** `sha1()` **Source:**	SCA

A03 Injection

OWASP Top 10 Web Application Security Risks, A03:2021 states: "An application is vulnerable to attack when: - User-supplied data is not validated, filtered, or sanitized by the application. - Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter. - Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records. - Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures. Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection."

Command Injection ***Remediation Effort(Hrs): 1.1***	**Critical**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.JSONStream

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/JSONStream/index.js:166	**Sink:** `FunctionPointerCall: exec` **Enclosing Method:** `check()` **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.node-windows.lib

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/binaries.js:44	**Sink:** `FunctionPointerCall: exec` **Enclosing Method:** `elevate()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/binaries.js:76	**Sink:** `FunctionPointerCall: exec` **Enclosing Method:** `sudo()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/cmd.js:17	**Sink:** `FunctionPointerCall: exec` **Enclosing Method:** `isAdminUser()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/cmd.js:52	**Sink:** `FunctionPointerCall: exec` **Enclosing Method:** `kill()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/cmd.js:65	**Sink:** `FunctionPointerCall: exec` **Enclosing Method:** `list()` **Source:**	SCA

A03 Injection

OWASP Top 10 Web Application Security Risks, A03:2021 states: "An application is vulnerable to attack when: - User-supplied data is not validated, filtered, or sanitized by the application. - Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter. - Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records. - Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures. Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection."

Command Injection ***Remediation Effort(Hrs): 1.1***	**Critical**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.node-windows.lib

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:774	**Sink:** `FunctionPointerCall: exec` **Enclosing Method:** `lambda()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/eventlog.js:67	**Sink:** `FunctionPointerCall: exec` **Enclosing Method:** `write()` **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.sybase.src

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/sybase/src/SybaseDB.js:41	**Sink:** `FunctionPointerCall: spawn` **Enclosing Method:** `connect()` **Source:**	SCA

Cross-Site Scripting: Reflected ***Remediation Effort(Hrs): 1***	**Critical**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js:110	**Sink:** `~JS_Generic.send()` **Enclosing Method:** `lambda()` **Source:** `lambda(0.body)` **from** `lambda()` **In** `D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js:108`	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:160	**Sink:** `~JS_Generic.send()` **Enclosing Method:** `lambda()` **Source:** `lambda(0.body)` **from** `lambda()` **In** `D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:151`	SCA

A03 Injection

OWASP Top 10 Web Application Security Risks, A03:2021 states: "An application is vulnerable to attack when: - User-supplied data is not validated, filtered, or sanitized by the application. - Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter. - Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records. - Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures. Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection."

Cross-Site Scripting: Reflected
Remediation Effort(Hrs): 1

Critical

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:257	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:247	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:344	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:317	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:376	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:353	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:408	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:385	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:438	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:417	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:465	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:417	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:531	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:477	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:679	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:661	SCA

A03 Injection

OWASP Top 10 Web Application Security Risks, A03:2021 states: "An application is vulnerable to attack when: - User-supplied data is not validated, filtered, or sanitized by the application. - Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter. - Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records. - Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures. Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection."

Cross-Site Scripting: Reflected
Remediation Effort(Hrs): 1

Critical

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:705	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:687	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:735	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:687	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:759	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:687	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:805	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:687	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:825	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:687	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:171	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:162	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:285	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:275	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:372	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:345	SCA

A03 Injection

OWASP Top 10 Web Application Security Risks, A03:2021 states: "An application is vulnerable to attack when: - User-supplied data is not validated, filtered, or sanitized by the application. - Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter. - Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records. - Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures. Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection."

Cross-Site Scripting: Reflected ***Remediation Effort(Hrs): 1***		**Critical**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:404	**Sink:** `~JS_Generic.send()` **Enclosing Method:** `lambda()` **Source:** `lambda(0.body)` **from** `lambda()` **In** `D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:381`	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:436	**Sink:** `~JS_Generic.send()` **Enclosing Method:** `lambda()` **Source:** `lambda(0.body)` **from** `lambda()` **In** `D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:413`	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:466	**Sink:** `~JS_Generic.send()` **Enclosing Method:** `lambda()` **Source:** `lambda(0.body)` **from** `lambda()` **In** `D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:445`	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:493	**Sink:** `~JS_Generic.send()` **Enclosing Method:** `lambda()` **Source:** `lambda(0.body)` **from** `lambda()` **In** `D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:445`	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:614	**Sink:** `~JS_Generic.send()` **Enclosing Method:** `lambda()` **Source:** `lambda(0.body)` **from** `lambda()` **In** `D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:534`	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:769	**Sink:** `~JS_Generic.send()` **Enclosing Method:** `lambda()` **Source:** `lambda(0.body)` **from** `lambda()` **In** `D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:751`	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:795	**Sink:** `~JS_Generic.send()` **Enclosing Method:** `lambda()` **Source:** `lambda(0.body)` **from** `lambda()` **In** `D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:777`	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:825	**Sink:** `~JS_Generic.send()` **Enclosing Method:** `lambda()` **Source:** `lambda(0.body)` **from** `lambda()` **In** `D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:777`	SCA

A03 Injection

OWASP Top 10 Web Application Security Risks, A03:2021 states: "An application is vulnerable to attack when: - User-supplied data is not validated, filtered, or sanitized by the application. - Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter. - Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records. - Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures. Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection."

Cross-Site Scripting: Reflected ***Remediation Effort(Hrs): 1***	**Critical**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:849	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:777	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:895	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:777	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:915	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:777	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1081	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1072	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1219	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1209	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1306	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1279	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1338	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1315	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1370	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1347	SCA

A03 Injection

OWASP Top 10 Web Application Security Risks, A03:2021 states: "An application is vulnerable to attack when: - User-supplied data is not validated, filtered, or sanitized by the application. - Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter. - Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records. - Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures. Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection."

Cross-Site Scripting: Reflected
Remediation Effort(Hrs): 1

Critical

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1400	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1379	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1427	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1379	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1493	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1439	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1669	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1651	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1695	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1677	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1725	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1677	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1749	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1677	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1795	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0.body) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1677	SCA

A03 Injection

OWASP Top 10 Web Application Security Risks, A03:2021 states: "An application is vulnerable to attack when: - User-supplied data is not validated, filtered, or sanitized by the application. - Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter. - Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records. - Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures. Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection."

Cross-Site Scripting: Reflected ***Remediation Effort(Hrs): 1***	**Critical**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1815	`Sink: ~JS_Generic.send()`
	`Enclosing Method: lambda()`
	`Source: lambda(0.body) from lambda() In D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1677`
		SCA

Header Manipulation ***Remediation Effort(Hrs): 0.2***	**High**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.request

Location	Analysis Info	Analyzer

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:1180	`Sink: ~JS_Generic.setHeader()`
	`Enclosing Method: pipeDest()`
	`Source: Read self.response from pipeDest() In D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:1174`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:1189	`Sink: ~JS_Generic.setHeader()`
	`Enclosing Method: pipeDest()`
	`Source: Read self.response from pipeDest() In D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:1174`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:1200	`Sink: ~JS_Generic.setHeader()`
	`Enclosing Method: pipeDest()`
	`Source: Read self.response from pipeDest() In D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:1174`
		SCA

A04 Insecure Design

OWASP Top 10 Web Application Security Risks, A04:2021 states: "Insecure design is a broad category representing different weaknesses, expressed as "missing or ineffective control design." Insecure design is not the source for all other Top 10 risk categories. There is a difference between insecure design and insecure implementation."

Race Condition ***Remediation Effort(Hrs): 0.4***		**High**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.request		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:888	**Sink:** `FunctionPointerCall: on` **Enclosing Method:** `onRequestResponse()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:888	**Sink:** `FunctionPointerCall: on` **Enclosing Method:** `onRequestResponse()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:888	**Sink:** `FunctionPointerCall: on` **Enclosing Method:** `onRequestResponse()` **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:1086	**Sink:** `FunctionPointerCall: on` **Enclosing Method:** `onRequestResponse()` **Source:**	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

Password Management: Password in Comment

Remediation Effort(Hrs): 1.4

Low

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.include.jquery@3.3.1

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/include/jquery@3.3.1/jquery.min.js:9312	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.include.jqueryui@1.13.0.external.jque

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/include/jqueryui@1.13.0/external/jquery/jquery.js:9368	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.debug.src

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/debug/src/node.js:203	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.hosted-git-info

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/hosted-git-info/index.js:117	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

Password Management: Password in Comment ***Remediation Effort(Hrs): 1.4***	**Low**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.jws.lib

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jws/lib/data-stream.js:25	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.node-windows.lib

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/binaries.js:19	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/binaries.js:47	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:339	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:378	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:433	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

Password Management: Password in Comment ***Remediation Effort(Hrs): 1.4***		**Low**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.node-windows.lib		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:776	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/winsw.js:3	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.pg.lib		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/pg/lib/connection-parameters.js:69	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/pg/lib/defaults.js:13	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.request.lib		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js:73	**Sink:** Comment **Enclosing Method:** () **Source:**	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

System Information Leak: External
Remediation Effort(Hrs): 1.1

Low

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:243	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:241	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:243	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:241	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:844	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:842	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:879	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:877	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:893	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:891	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1019	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1017	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1111	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1109	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

System Information Leak: External ***Remediation Effort(Hrs): 1.1***		**Low**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1126	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1124	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1143	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1141	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1157	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1155	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1184	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1182	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1207	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1205	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1224	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1222	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1241	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1239	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1281	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1279	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

System Information Leak: External ***Remediation Effort(Hrs): 1.1***		**Low**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1327	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1325	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1364	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1362	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1384	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1382	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1404	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1402	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1425	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1423	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1445	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1443	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1468	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1466	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:823	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:821	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

System Information Leak: External | **Low**
Remediation Effort(Hrs): 1.1

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:858	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:856	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:872	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:870	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:998	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:996	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1090	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1088	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1105	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1103	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1122	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1120	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1136	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1134	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1163	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1161	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

System Information Leak: External
Remediation Effort(Hrs): 1.1

Low

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1184	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1182	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1201	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1199	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1218	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1216	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1258	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1256	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1304	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1302	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1341	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1339	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1361	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1359	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1381	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1379	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

System Information Leak: External ***Remediation Effort(Hrs): 1.1***		**Low**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1400	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1398	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1420	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1418	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1443	**Sink:** ~JS_Generic.send() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1441	SCA

System Information Leak: Internal ***Remediation Effort(Hrs): 1.8***		**Low**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js:174	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js:164	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:204	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:203	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:205	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:203	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

System Information Leak: Internal ***Remediation Effort(Hrs): 1.8***	**Low**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:242	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:241	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:426	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:416	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js:20	**Sink:** ~JS_Generic.error() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js:19	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js:55	**Sink:** ~JS_Generic.error() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js:54	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js:92	**Sink:** ~JS_Generic.error() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js:91	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js:20	**Sink:** ~JS_Generic.error() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js:19	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js:72	**Sink:** ~JS_Generic.error() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js:71	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js:125	**Sink:** ~JS_Generic.error() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js:124	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

System Information Leak: Internal *Remediation Effort(Hrs): 1.8*	Low

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD

Location	Analysis Info	Analyzer

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:204	`Sink: ~JS_Generic.log()`
	`Enclosing Method: lambda()`
	`Source: lambda(0) from lambda() In D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:203`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:205	`Sink: ~JS_Generic.log()`
	`Enclosing Method: lambda()`
	`Source: lambda(0) from lambda() In D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:203`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:242	`Sink: ~JS_Generic.log()`
	`Enclosing Method: lambda()`
	`Source: lambda(0) from lambda() In D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:241`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:426	`Sink: ~JS_Generic.log()`
	`Enclosing Method: lambda()`
	`Source: lambda(0) from lambda() In D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:416`
		SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.node-windows.lib

Location	Analysis Info	Analyzer

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/winsw.js:77	`Sink: ~JS_Generic.log()`
	`Enclosing Method: generateXml()`
	`Source: Read process.execPath from generateXml() In D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/winsw.js:72`
		SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:162	`Sink: ~JS_Generic.log()`
	`Enclosing Method: lambda()`
	`Source: lambda(0) from lambda() In D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:161`
		SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

System Information Leak: Internal **Low**
Remediation Effort(Hrs): 1.8

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:321	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:320	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:462	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:461	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:612	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:611	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1018	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1017	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1260	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1259	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1280	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1279	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1326	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1325	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1346	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1345	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

System Information Leak: Internal *Remediation Effort(Hrs): 1.8*		Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1383	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1382	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1403	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1402	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1424	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1423	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1444	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1443	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1467	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1466	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:152	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:151	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:179	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:178	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:310	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:309	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

System Information Leak: Internal ***Remediation Effort(Hrs): 1.8***		**Low**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:444	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:443	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:471	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:470	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:591	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:590	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:997	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:996	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1237	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1236	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1257	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1256	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1303	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1302	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1323	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1322	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

System Information Leak: Internal ***Remediation Effort(Hrs): 1.8***	**Low**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1360	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1359	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1380	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1379	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1399	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1398	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1419	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1418	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1442	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1441	SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.util

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js:72	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js:71	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js:97	**Sink:** ~JS_Generic.log() **Enclosing Method:** lambda() **Source:** lambda(0) **from** lambda() **In** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js:96	SCA

A05 Security Misconfiguration

OWASP Top 10 Web Application Security Risks, A05:2021 states: "The application might be vulnerable if the application is: - Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services. - Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges). - Default accounts and their passwords are still enabled and unchanged. - Error handling reveals stack traces or other overly informative error messages to users. - For upgraded systems, the latest security features are disabled or not configured securely. - The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values. - The server does not send security headers or directives, or they are not set to secure values. - The software is out of date or vulnerable."

System Information Leak: Internal ***Remediation Effort(Hrs): 1.8***		**Low**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.util		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js:122	**Sink:** `~JS_Generic.log()` **Enclosing Method:** `lambda()` **Source:** `lambda(0)` **from** `lambda()` **In** `D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js:121`	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/runtime.js:23	**Sink:** `~JS_Generic.log()` **Enclosing Method:** `lambda()` **Source:** `lambda(0)` **from** `lambda()` **In** `D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/runtime.js:21`	SCA

A06 Vulnerable and Outdated Components

OWASP Top 10 Web Application Security Risks, A06:2021 states: "You are likely vulnerable: - If you do not know the versions of all components you use (both client-side and server-side). This includes components you directly use as well as nested dependencies. - If the software is vulnerable, unsupported, or out of date. This includes the OS, web/application server, database management system (DBMS), applications, APIs and all components, runtime environments, and libraries. - If you do not scan for vulnerabilities regularly and subscribe to security bulletins related to the components you use. - If you do not fix or upgrade the underlying platform, frameworks, and dependencies in a risk-based, timely fashion. This commonly happens in environments when patching is a monthly or quarterly task under change control, leaving organizations open to days or months of unnecessary exposure to fixed vulnerabilities. - If software developers do not test the compatibility of updated, upgraded, or patched libraries. - If you do not secure the components' configurations."

No Issues

A07 Identification and Authentication Failures

OWASP Top 10 Web Application Security Risks, A07:2021 states: "Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks. There may be authentication weaknesses if the application: - Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords. - Permits brute force or other automated attacks. - Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin". - Uses weak or ineffective credential recovery and forgot-password processes, such as "knowledge-based answers," which cannot be made safe. - Uses plain text, encrypted, or weakly hashed passwords data stores. - Has missing or ineffective multi-factor authentication. - Exposes session identifier in the URL. - Reuse session identifier after successful login. - Does not correctly invalidate Session IDs. User sessions or authentication tokens (mainly single sign-on (SSO) tokens) aren't properly invalidated during logout or a period of inactivity."

Credential Management: Hardcoded API Credentials
Remediation Effort(Hrs): 0.2

Critical

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.passport-jwt.test

Location	Analysis Info	Analyzer

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/passport-jwt/test/testdata.js:5	`Enclosing Method: ()`
	`Source:`
		SCA

Password Management: Hardcoded Password
Remediation Effort(Hrs): 1

Critical

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.hosted-git-info

Location	Analysis Info	Analyzer

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/hosted-git-info/index.js:118	`Enclosing Method: ()`
	`Source:`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/hosted-git-info/index.js:119	`Enclosing Method: ()`
	`Source:`
		SCA

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.pg-pool.test

Location	Analysis Info	Analyzer

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/pg-pool/test/connection-strings.js:8	`Enclosing Method: ()`
	`Source:`
		SCA

A07 Identification and Authentication Failures

OWASP Top 10 Web Application Security Risks, A07:2021 states: "Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks. There may be authentication weaknesses if the application: - Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords. - Permits brute force or other automated attacks. - Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin". - Uses weak or ineffective credential recovery and forgot-password processes, such as "knowledge-based answers," which cannot be made safe. - Uses plain text, encrypted, or weakly hashed passwords data stores. - Has missing or ineffective multi-factor authentication. - Exposes session identifier in the URL. - Reuse session identifier after successful login. - Does not correctly invalidate Session IDs. User sessions or authentication tokens (mainly single sign-on (SSO) tokens) aren't properly invalidated during logout or a period of inactivity."

Password Management: Hardcoded Password ***Remediation Effort(Hrs): 1***		**Critical**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.url		
Location	**Analysis Info**	**Analyzer**

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:436	`Enclosing Method: ()`
	`Source:`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:437	`Enclosing Method: ()`
	`Source:`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:651	`Enclosing Method: ()`
	`Source:`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:658	`Enclosing Method: ()`
	`Source:`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:857	`Enclosing Method: ()`
	`Source:`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:1049	`Enclosing Method: ()`
	`Source:`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:1050	`Enclosing Method: ()`
	`Source:`
		SCA

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:1202	`Enclosing Method: ()`
	`Source:`
		SCA

A07 Identification and Authentication Failures

OWASP Top 10 Web Application Security Risks, A07:2021 states: "Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks. There may be authentication weaknesses if the application: - Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords. - Permits brute force or other automated attacks. - Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin". - Uses weak or ineffective credential recovery and forgot-password processes, such as "knowledge-based answers," which cannot be made safe. - Uses plain text, encrypted, or weakly hashed passwords data stores. - Has missing or ineffective multi-factor authentication. - Exposes session identifier in the URL. - Reuse session identifier after successful login. - Does not correctly invalidate Session IDs. User sessions or authentication tokens (mainly single sign-on (SSO) tokens) aren't properly invalidated during logout or a period of inactivity."

Password Management: Hardcoded Password ***Remediation Effort(Hrs): 1***	**Critical**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.url

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:1203	**Enclosing Method:** () **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:1214	**Enclosing Method:** () **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:1215	**Enclosing Method:** () **Source:**	SCA

Password Management: Empty Password ***Remediation Effort(Hrs): 0.2***	**High**

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.node-windows.lib

Location	Analysis Info	Analyzer
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/binaries.js:73	**Sink:** VariableAccess: password **Enclosing Method:** sudo() **Source:**	SCA

A07 Identification and Authentication Failures

OWASP Top 10 Web Application Security Risks, A07:2021 states: "Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks. There may be authentication weaknesses if the application: - Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords. - Permits brute force or other automated attacks. - Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin". - Uses weak or ineffective credential recovery and forgot-password processes, such as "knowledge-based answers," which cannot be made safe. - Uses plain text, encrypted, or weakly hashed passwords data stores. - Has missing or ineffective multi-factor authentication. - Exposes session identifier in the URL. - Reuse session identifier after successful login. - Does not correctly invalidate Session IDs. User sessions or authentication tokens (mainly single sign-on (SSO) tokens) aren't properly invalidated during logout or a period of inactivity."

Password Management: Null Password ***Remediation Effort(Hrs): 0.3***		**Low**
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.node-windows.lib		
Location	**Analysis Info**	**Analyzer**
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:374	**Sink:** FieldAccess: password **Enclosing Method:** daemon() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:414	**Sink:** FieldAccess: password **Enclosing Method:** daemon() **Source:**	SCA
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:439	**Sink:** FieldAccess: password **Enclosing Method:** daemon() **Source:**	SCA

A08 Software and Data Integrity Failures

OWASP Top 10 Web Application Security Risks, A08:2021 states: "Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations. Another example is where objects or data are encoded or serialized into a structure that an attacker can see and modify is vulnerable to insecure deserialization."

No Issues

A09 Security Logging and Monitoring Failures

OWASP Top 10 Web Application Security Risks, A09:2021 states: "Help detect, escalate, and respond to active breaches. Without logging and monitoring, breaches cannot be detected. Insufficient logging, detection, monitoring, and active response occurs any time: - Auditable events, such as logins, failed logins, and high-value transactions, are not logged. - Warnings and errors generate no, inadequate, or unclear log messages. - Logs of applications and APIs are not monitored for suspicious activity. - Logs are only stored locally. - Appropriate alerting thresholds and response escalation processes are not in place or effective. - Penetration testing and scans by dynamic application security testing (DAST) tools do not trigger alerts. - The application cannot detect, escalate, or alert for active attacks in real-time or near real-time. You are vulnerable to information leakage by making logging and alerting events visible to a user or an attacker. "

No Issues

A10 Server-Side Request Forgery

OWASP Top 10 Web Application Security Risks, A10:2021 states: "SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL)."

No Issues

Description of Key Terminology

Likelihood and Impact

Likelihood
Likelihood is the probability that a vulnerability will be accurately identified and successfully exploited.

Impact
Impact is the potential damage an attacker could do to assets by successfully exploiting a vulnerability. This damage can be in the form of, but not limited to, financial loss, compliance violation, loss of brand reputation, and negative publicity.

Fortify Priority Order

Critical
Critical-priority issues have high impact and high likelihood. Critical-priority issues are easy to detect and exploit and result in large asset damage. These issues represent the highest security risk to the application. As such, they should be remediated immediately.

SQL Injection is an example of a critical issue.

High
High-priority issues have high impact and low likelihood. High-priority issues are often difficult to detect and exploit, but can result in large asset damage. These issues represent a high security risk to the application. High-priority issues should be remediated in the next scheduled patch release.

Password Management: Hardcoded Password is an example of a high issue.

Medium
Medium-priority issues have low impact and high likelihood. Medium-priority issues are easy to detect and exploit, but typically result in small asset damage. These issues represent a moderate security risk to the application. Medium-priority issues should be remediated in the next scheduled product update.

Path Manipulation is an example of a medium issue.

Low
Low-priority issues have low impact and low likelihood. Low-priority issues can be difficult to detect and exploit and typically result in small asset damage. These issues represent a minor security risk to the application. Low-priority issues should be remediated as time allows.

Dead Code is an example of a low issue.

Remediation Effort

The report provides remediation effort estimates. You can use these estimates to perform a relative comparison of projects and as a starting point for estimates specific to your organization. Remediation effort estimates are provided in the following report sections:

- Executive Summary
- Issue Breakdown
- Issue Details

To determine remediation effort for a collection of issues, Software Security Center weights each issue based on its category (“remediation constant”) and adds an overhead calculation based on the number of distinct files which contain the set of issues. The formula used at each report level is the same:

- Remediation Effort (in mins) = SUM(remediation constant for each issue in the set) + 6 * Number of distinct files in that set of issues.

At the lowest level of detail, issues are grouped based on Fortify category and Fortify priority OR Fortify category and folder name, depending on report options. So, for example, the Issue Details section of the report might show the remediation effort for “SQL Injection, Critical” or “SQL Injection, MyFolder”.

At the Issue Breakdown level, remediation effort is shown at the level of each external (non-Fortify) category (such as “AC-3 Access Enforcement” in the case of NIST, or “A1 Unvalidated Input” in the case of OWASP Top10). Remediation effort is calculated for the set of all issues that fall into that external category (irrespective of Fortify priority or folder name). As an example, if there are two SQL injection vulnerabilities, one critical and one medium, within the same file, the file overhead is only included once.

At the Executive Summary level, all issues of that project which are mapped to the specified external category list (such as NIST or CWE) are used in the remediation effort calculation.

Fortify recommends that you treat the different levels of remediation effort as information relevant at that level only. You cannot add up remediation effort at a lower level and expect it to match the remediation effort at a higher level.

About Fortify Solutions

Fortify is the leader in end-to-end application security solutions with the flexibility of testing on-premise and on-demand to cover the entire software development lifecycle. Learn more at www.microfocus.com/solutions/application-security.