Fortify Standalone Report Generator

Developer Workbook

G9_NF17027-2_898109_20230912_161654355928_JS
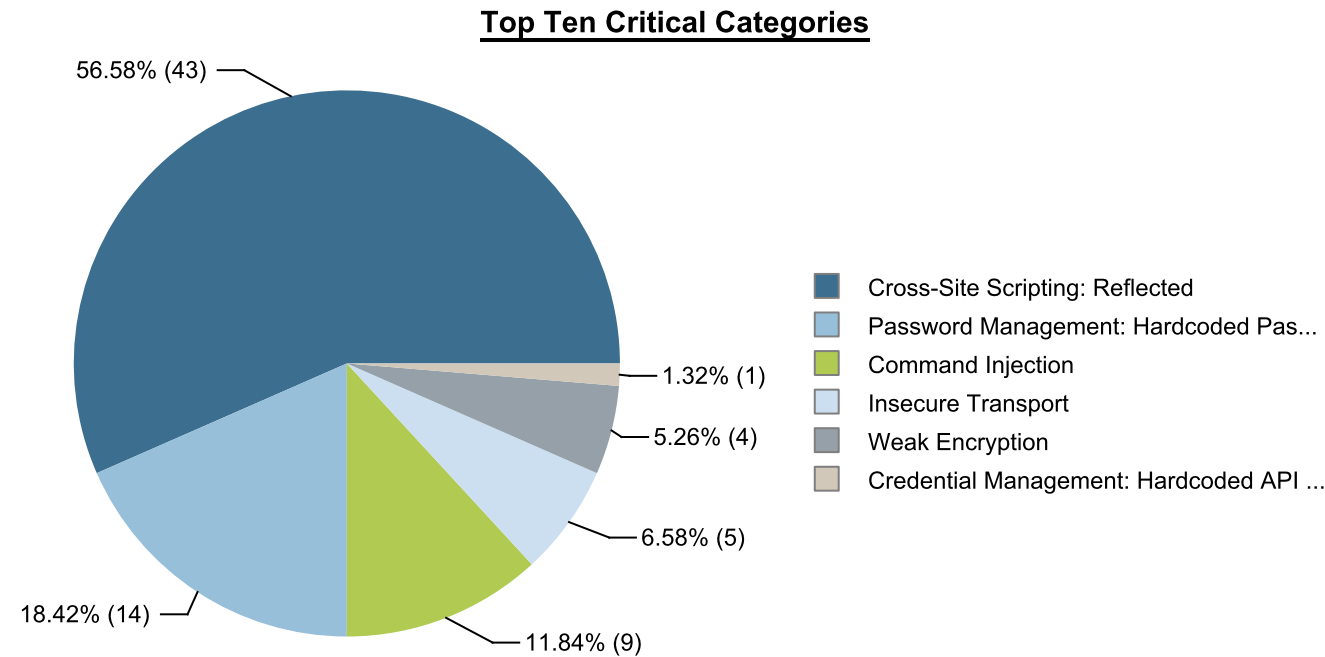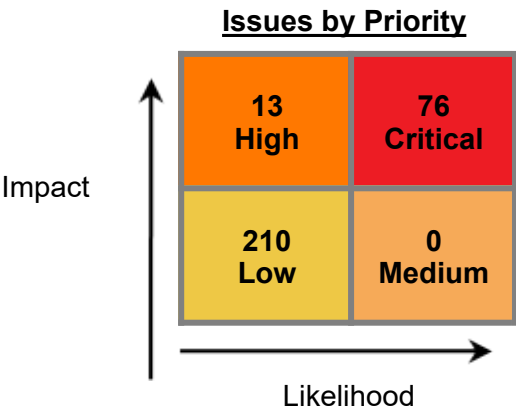
Table of Contents

Executive Summary

This workbook is intended to provide all necessary details and information for a developer to understand and remediate the different issues discovered during the G9_NF17027-2_898109_20230912_161654355928_JS project audit. The information contained in this workbook is targeted at project managers and developers.

This section provides an overview of the issues uncovered during analysis.

Project Name: G9_NF17027-2_898109

Project Version:

SCA: Results Present

WebInspect: Results Not Present

WebInspect Agent: Results Not Present

Other: Results Not Present

Issues by Priority

Impact ↑		
	13 High	**76 Critical**
	210 Low	**0 Medium**

Likelihood →

Top Ten Critical Categories

- 56.58% (43)
- 18.42% (14)
- 11.84% (9)
- 6.58% (5)
- 5.26% (4)
- 1.32% (1)

Legend:
- Cross-Site Scripting: Reflected
- Password Management: Hardcoded Pas...
- Command Injection
- Insecure Transport
- Weak Encryption
- Credential Management: Hardcoded API ...

Project Description

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

<u>**SCA**</u>

Date of Last Analysis:	2023 9 12 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 by Fortify Categories

The following table depicts a summary of all issues grouped vertically by Fortify Category. For each category, the total number of issues is shown by Fortify Priority Order, including information about the number of audited issues.

Category	Fortify Priority (audited/total)				Total Issues
	Critical	High	Medium	Low	
Command Injection	0 / 9	0	0	0	0 / 9
Credential Management: Hardcoded API Credentials	0 / 1	0	0	0	0 / 1
Cross-Site Request Forgery	0	0	0	0 / 69	0 / 69
Cross-Site Scripting: Reflected	0 / 43	0	0	0	0 / 43
Denial of Service	0	0	0	0 / 2	0 / 2
Header Manipulation	0	0 / 3	0	0	0 / 3
Insecure Randomness	0	0 / 5	0	0	0 / 5
Insecure Transport	0 / 5	0	0	0	0 / 5
Password Management: Empty Password	0	0 / 1	0	0	0 / 1
Password Management: Hardcoded Password	0 / 14	0	0	0	0 / 14
Password Management: Null Password	0	0	0	0 / 3	0 / 3
Password Management: Password in Comment	0	0	0	0 / 15	0 / 15
Poor Logging Practice: Use of a System Output Stream	0	0	0	0 / 2	0 / 2
Race Condition	0	0 / 4	0	0	0 / 4
System Information Leak: External	0	0	0	0 / 42	0 / 42
System Information Leak: Internal	0	0	0	0 / 50	0 / 50
Weak Cryptographic Hash	0	0	0	0 / 27	0 / 27
Weak Encryption	0 / 4	0	0	0	0 / 4

Results Outline

Command Injection (9 issues)

Abstract

Executing commands that include unvalidated user input can cause an application to execute malicious commands on behalf of an attacker.

Explanation

Command injection vulnerabilities take two forms: - An attacker can change the command that the program executes: the attacker explicitly controls what the command is. - An attacker can change the environment in which the command executes: the attacker implicitly controls what the command means. In this case, we are primarily concerned with the second scenario, the possibility that an attacker may be able to change the meaning of the command by changing an environment variable or by putting a malicious executable early in the search path. Command injection vulnerabilities of this type occur when: 1. An attacker modifies an application's environment. 2. The application executes a command without specifying an absolute path or verifying the binary being executed. 3. By executing the command, the application gives an attacker a privilege or capability that the attacker would not otherwise have. **Example:** The following code is from a web application that provides an interface through which users can update their password on the system. Part of the process for updating passwords in certain network environments is to run a `make` command in the `/var/yp` directory.

```
...
require('child_process').exec("make", function(error, stdout, stderr){
  ...
});
...
```

The problem here is that the program does not specify an absolute path for `make` and fails to clean its environment prior to executing the call to `child_process.exec()`. If an attacker can modify the `$PATH` variable to point to a malicious binary called `make` and then execute the application in their environment, the malicious binary will be loaded instead of the one intended. Because of the nature of the application, it runs with the privileges necessary to perform system operations, which means the attacker's `make` will now be run with these privileges, possibly giving them complete control of the system.

Recommendation

An attacker may indirectly control commands executed by a program by modifying the environment in which they are executed. The environment should not be trusted and precautions should be taken to prevent an attacker from using some manipulation of the environment to perform an attack. Whenever possible, commands should be controlled by the application and executed using an absolute path. In cases where the path is not known at compile time, such as for cross-platform applications, an absolute path should be constructed from trusted values during execution. Command values and paths read from configuration files or the environment should be sanity-checked against a set of invariants that define valid values. Other checks can sometimes be performed to detect if these sources may have been tampered with. For example, if a configuration file is world-writable, the program might refuse to run. In cases where information about the binary to be executed is known in advance, the program may perform checks to verify the identity of the binary. If a binary should always be owned by a particular user or have a particular set of access permissions assigned to it, these properties can be verified programmatically before the binary is executed. In the end it may be impossible for a program to fully protect itself from an imaginative attacker bent on controlling the commands the program executes. You should strive to identify and protect against every conceivable manipulation of input values and the environment. The goal should be to shut down as many attack vectors as possible.

Issue Summary
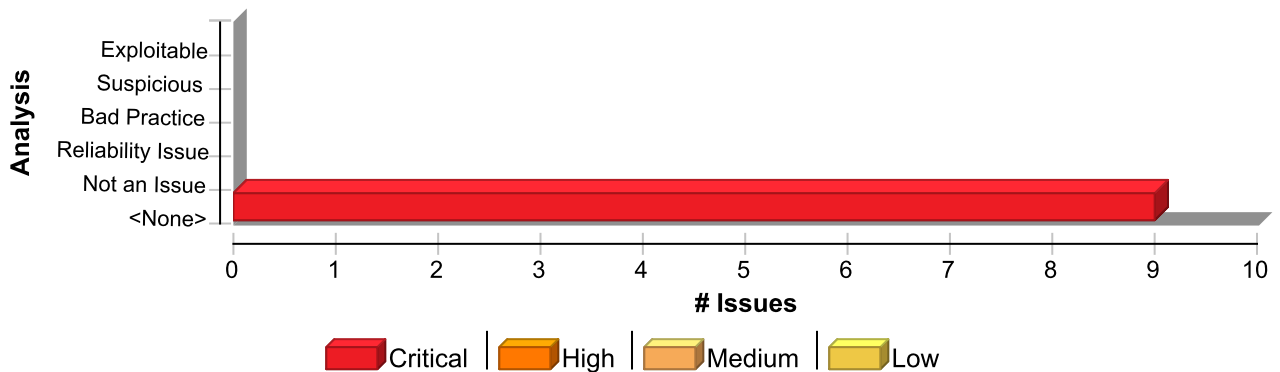
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Command Injection	9	0	0	9
Total	**9**	**0**	**0**	**9**

Command Injection	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ JSONStream/index.js, line 166 (Command Injection)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: exec
Enclosing Method: check()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/JSONStream/
index.js:166
Taint Flags:

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/binaries.js, line 44 (Command Injection)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Structural)

Sink Details

Command Injection	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/binaries.js, line 44 (Command Injection)	Critical

Sink: FunctionPointerCall: exec
Enclosing Method: elevate()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/binaries.js:44
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/eventlog.js, line 67 (Command Injection)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: exec
Enclosing Method: write()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/eventlog.js:67
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/binaries.js, line 76 (Command Injection)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: exec
Enclosing Method: sudo()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/binaries.js:76
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/cmd.js, line 52 (Command Injection)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Structural)

Sink Details

Command Injection	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/cmd.js, line 52 (Command Injection)	Critical

Sink: FunctionPointerCall: exec
Enclosing Method: kill()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/cmd.js:52
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/cmd.js, line 17 (Command Injection)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: exec
Enclosing Method: isAdminUser()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/cmd.js:17
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/daemon.js, line 774 (Command Injection)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: exec
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:774
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/cmd.js, line 65 (Command Injection)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Structural)

Sink Details

Command Injection	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/cmd.js, line 65 (Command Injection)	Critical

Sink: FunctionPointerCall: exec
Enclosing Method: list()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/cmd.js:65
Taint Flags:

```
No snippet available
```

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ sybase/src/SybaseDB.js, line 41 (Command Injection)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: spawn
Enclosing Method: connect()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/sybase/src/SybaseDB.js:41
Taint Flags:

```
No snippet available
```

Credential Management: Hardcoded API Credentials (1 issue)

Abstract

Hardcoded API credentials can compromise system security in a way that is not easy to remedy.

Explanation

Never hardcode credentials, including usernames, passwords, API keys, API secrets, and API Tokens. Not only are hardcoded credentials visible to all of the project developers, they are extremely difficult to update. After the code is in production, the credentials cannot be changed without patching the software. If the credentials are compromised, the organization must choose between security and system availability.

Recommendation

Make sure that API credentials are either loaded from a configuration file that is only available in the runtime environment or from environment variables.

Issue Summary
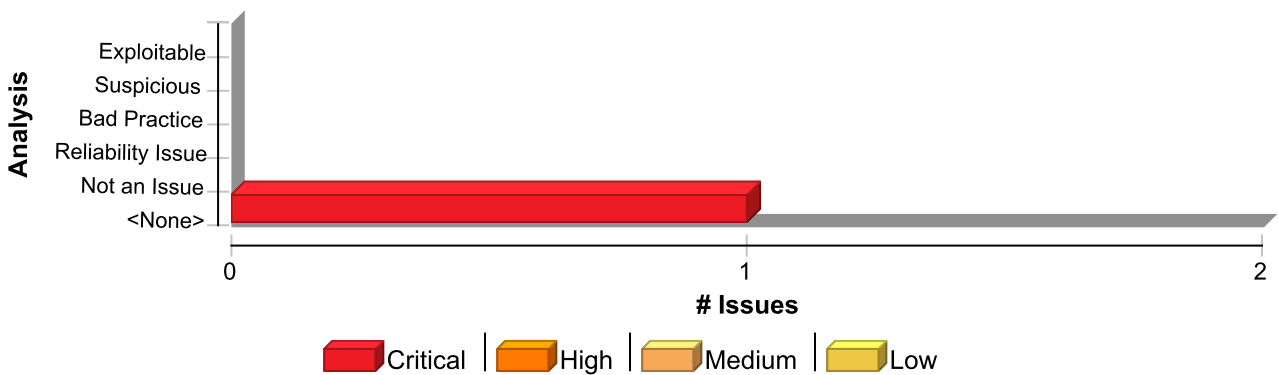
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Credential Management: Hardcoded API Credentials	1	0	0	1
Total	**1**	**0**	**0**	**1**

Credential Management: Hardcoded API Credentials	Critical
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.passport-jwt.test	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ passport-jwt/test/testdata.js, line 5 (Credential Management: Hardcoded API Credentials)	Critical
Issue Details	

> **Kingdom:** Security Features
> **Scan Engine:** SCA (Configuration)

Sink Details

Credential Management: Hardcoded API Credentials	Critical
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.passport-jwt.test	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ passport-jwt/test/testdata.js, line 5 (Credential Management: Hardcoded API Credentials)	**Critical**

> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/passport-jwt/test/testdata.js:5
> **Taint Flags:**

`No snippet available`

Cross-Site Request Forgery (69 issues)

Abstract

HTTP requests must contain a user-specific secret to prevent an attacker from making unauthorized requests.

Explanation

A cross-site request forgery (CSRF) vulnerability occurs when: 1. A web application uses session cookies. 2. The application acts on an HTTP request without verifying that the request was made with the user's consent. A nonce is a cryptographic random value that is sent with a message to prevent replay attacks. If the request does not contain a nonce that proves its provenance, the code that handles the request is vulnerable to a CSRF attack (unless it does not change the state of the application). This means a web application that uses session cookies has to take special precautions to ensure that an attacker can't trick users into submitting bogus requests. Imagine a web application that allows administrators to create new accounts as follows:

```
var req = new XMLHttpRequest();
req.open("POST", "/new_user", true);
body = addToPost(body, new_username);
body = addToPost(body, new_passwd);
req.send(body);
```

An attacker might set up a malicious web site that contains the following code.

```
var req = new XMLHttpRequest();
req.open("POST", "http://www.example.com/new_user", true);
body = addToPost(body, "attacker");
body = addToPost(body, "haha");
req.send(body);
```

If an administrator for `example.com` visits the malicious page while she has an active session on the site, she will unwittingly create an account for the attacker. This is a CSRF attack. It is possible because the application does not have a way to determine the provenance of the request. Any request could be a legitimate action chosen by the user or a faked action set up by an attacker. The attacker does not get to see the Web page that the bogus request generates, so the attack technique is only useful for requests that alter the state of the application. Applications that pass the session identifier in the URL rather than as a cookie do not have CSRF problems because there is no way for the attacker to access the session identifier and include it as part of the bogus request. CSRF is entry number five on the 2007 OWASP Top 10 list.

Recommendation

Applications that use session cookies must include some piece of information in every form post that the back-end code can use to validate the provenance of the request. One way to do that is to include a random request identifier or nonce, as follows:

```
RequestBuilder rb = new RequestBuilder(RequestBuilder.POST, "/new_user");
body = addToPost(body, new_username);
body = addToPost(body, new_passwd);
body = addToPost(body, request_id);
rb.sendRequest(body, new NewAccountCallback(callback));
```

Then the back-end logic can validate the request identifier before processing the rest of the form data. When possible, the request identifier should be unique to each server request rather than shared across every request for a particular session. As with session identifiers, the harder it is for an attacker to guess the request identifier, the harder it is to conduct a successful CSRF attack. The token should not be easily guessed and it should be protected in the same way that session tokens are protected, such as using SSLv3. Additional mitigation techniques include: **Framework protection:** Most modern web application frameworks embed CSRF protection and they will automatically include and verify CSRF tokens. **Use a Challenge-Response control:** Forcing the customer to respond to a challenge sent by the server is a strong defense against CSRF. Some of the challenges that can be used for this purpose are: CAPTCHAs, password re-authentication and one-time tokens. **Check HTTP Referer/Origin headers:** An attacker won't be able to spoof these headers while performing a CSRF attack. This makes these headers a useful method to prevent CSRF attacks. **Double-submit Session Cookie:** Sending the session ID Cookie as a hidden form value in addition to the actual session ID Cookie is a good protection against CSRF attacks. The server will check both values and make sure they are identical before processing the rest of the form data. If an attacker submits a form in behalf of a user, he won't be able to modify the session ID cookie value as per the same-origin-policy. **Limit Session Lifetime:** When accessing protected resources using a CSRF attack, the attack will only be valid as long as the session ID sent as part of the attack is still valid on the server. Limiting the Session lifetime will reduce the probability of a successful attack. The techniques described here can be defeated with XSS attacks. Effective CSRF mitigation includes XSS mitigation techniques.

Issue Summary
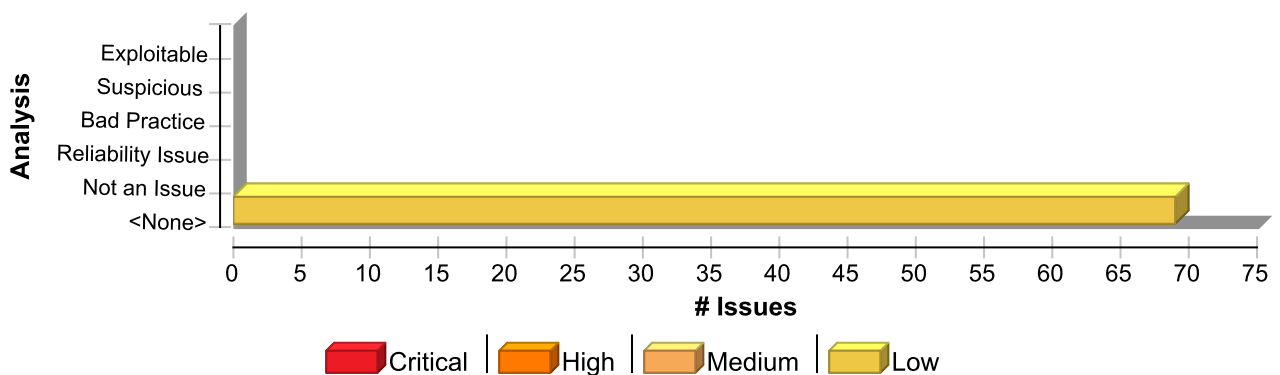
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Cross-Site Request Forgery	69	0	0	69
Total	**69**	**0**	**0**	**69**

Cross-Site Request Forgery	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js, line 251 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

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

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js, line 251 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

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

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ aws4/aws4.js, line 62 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

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

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ form-data/lib/form_data.js, line 392 (Cross-Site Request Forgery)	Low

Issue Details

Cross-Site Request Forgery	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ form-data/lib/form_data.js, line 392 (Cross-Site Request Forgery)	Low

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

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

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/request.js, line 728 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

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

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/request.js, line 162 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

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

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/lib/redirect.js, line 119 (Cross-Site Request Forgery)	Low

Issue Details

Cross-Site Request Forgery	Low

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.request.lib	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/lib/redirect.js, line 119 (Cross-Site Request Forgery)	**Low**

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: onResponse()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/redirect.js:119
Taint Flags:

`No snippet available`

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 152 (Cross-Site Request Forgery)	**Low**

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:152
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 312 (Cross-Site Request Forgery)	**Low**

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:312
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 452 (Cross-Site Request Forgery)	**Low**

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Cross-Site Request Forgery	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 452 (Cross-Site Request Forgery)	**Low**

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:452
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 602 (Cross-Site Request Forgery)	**Low**

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:602
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 914 (Cross-Site Request Forgery)	**Low**

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:914
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 924 (Cross-Site Request Forgery)	**Low**

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:924
Taint Flags:

Cross-Site Request Forgery	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 924 (Cross-Site Request Forgery)	**Low**

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 934 (Cross-Site Request Forgery)	**Low**

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:934
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1010 (Cross-Site Request Forgery)	**Low**

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1010
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1175 (Cross-Site Request Forgery)	**Low**

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1175
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 142 (Cross-Site Request Forgery)	**Low**

Issue Details

Cross-Site Request Forgery	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 142 (Cross-Site Request Forgery)	Low

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:142
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 301 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:301
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 434 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:434
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 581 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Cross-Site Request Forgery	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 581 (Cross-Site Request Forgery)	Low

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:581
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 893 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:893
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 903 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:903
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 913 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:913
Taint Flags:

`No snippet available`

Cross-Site Request Forgery	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 989 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:989
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1154 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1154
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 835 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:835
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 870 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Cross-Site Request Forgery	Low

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 870 (Cross-Site Request Forgery)	Low

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:870
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 886 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:886
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1103 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1103
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1118 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1118
Taint Flags:

`No snippet available`

Cross-Site Request Forgery	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1134 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1134
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1150 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1150
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1198 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1198
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1232 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Cross-Site Request Forgery	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1232 (Cross-Site Request Forgery)	Low

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1232
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1252 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1252
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1270 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1270
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1289 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1289
Taint Flags:

`No snippet available`

Cross-Site Request Forgery	Low

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1356 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1356
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1375 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1375
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1395 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1395
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1416 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Cross-Site Request Forgery	Low

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1416 (Cross-Site Request Forgery)	Low

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1416
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1436 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1436
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1458 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1458
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1478 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1478
Taint Flags:

`No snippet available`

Cross-Site Request Forgery	Low

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1493 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1493
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 814 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:814
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 849 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:849
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 865 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Cross-Site Request Forgery	Low

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 865 (Cross-Site Request Forgery)	Low

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:865
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1082 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1082
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1097 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1097
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1113 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1113
Taint Flags:

`No snippet available`

Cross-Site Request Forgery	Low

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1129 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1129
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1176 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1176
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1209 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1209
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1229 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Cross-Site Request Forgery	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js, line 1229 (Cross-Site Request Forgery)	Low

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1229
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js, line 1247 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1247
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js, line 1266 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1266
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js, line 1333 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1333
Taint Flags:

`No snippet available`

Cross-Site Request Forgery	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1352 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1352
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1372 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1372
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1392 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1392
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1411 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Cross-Site Request Forgery	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1411 (Cross-Site Request Forgery)	Low

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1411
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1433 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1433
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1453 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1453
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1468 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1468
Taint Flags:

`No snippet available`

Cross-Site Request Forgery	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 169 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:169
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 461 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:461
Taint Flags:

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ xrfile_delete_check.js, line 18 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/xrfile_delete_check.js:18
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/runtime.js, line 15 (Cross-Site Request Forgery)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Cross-Site Request Forgery	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.util	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/runtime.js, line 15 (Cross-Site Request Forgery)	Low

Sink Details

Sink: AssignmentStatement
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/runtime.js:15
Taint Flags:

```
No snippet available
```

Cross-Site Scripting: Reflected (43 issues)

Abstract

Sending unvalidated data to a web browser can result in the browser executing malicious code.

<u>Explanation</u>

Cross-site scripting (XSS) vulnerabilities occur when: 1. Data enters a web application through an untrusted source. In the case of reflected XSS, the untrusted source is typically a web request, while in the case of persisted (also known as stored) XSS it is typically a database or other back-end data store. 2. The data is included in dynamic content that is sent to a web user without validation. The malicious content sent to the web browser often takes the form of a JavaScript segment, but can also include HTML, Flash or any other type of code that the browser executes. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data such as cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site. **Example 1:** The following Node.js code segment reads an employee ID, `eid`, from an HTTP request and displays it to the user.

```
var http = require('http');
var url = require('url');

...

function listener(request, response){
  var eid = url.parse(request.url, true)['query']['eid'];
  if (eid !== undefined){
    response.write('<p>Welcome, ' + eid + '!</p>');
  }
  ...
}
...
http.createServer(listener).listen(8080);
```

The code in this example operates correctly if `eid` contains only standard alphanumeric text. If `eid` has a value that includes metacharacters or source code, then the code is executed by the web browser as it displays the HTTP response. Initially this might not appear to be much of a vulnerability. After all, why would someone enter a URL that causes malicious code to run on their own computer? The real danger is that an attacker will create the malicious URL, then use email or social engineering tricks to lure victims into visiting a link to the URL. When victims click the link, they unwittingly reflect the malicious content through the vulnerable web application back to their own computers. This mechanism of exploiting vulnerable web applications is known as Reflected XSS. **Example 2:** The following Node.js code segment queries a database for an employee with a given ID and prints the corresponding employee's name.

```
var http = require('http');
...

function listener(request, response){
  connection.query('SELECT * FROM emp WHERE eid="' + eid + '"', function(err,
rows){
    if (!err && rows.length > 0){
      response.write('<p>Welcome, ' + rows[0].name + '!</p>');
    }
    ...
  });
  ...
}
...
http.createServer(listener).listen(8080);
```

As in `Example 1`, this code functions correctly when the values of `name` are well-behaved, but it does nothing to prevent exploits if they are not. Again, this code can appear less dangerous because the value of `name` is read from a database, whose contents are apparently managed by the application. However, if the value of `name` originates from user-supplied data, then the database can be a conduit for malicious content. Without proper input validation on all data stored in the database, an attacker may execute malicious commands in the user's web browser. This type of exploit, known as Persistent (or Stored) XSS, is particularly insidious because the indirection caused by the data store makes it difficult to identify the threat and increases the possibility that the attack might affect multiple users. XSS got its start in this form with web sites that offered a "guestbook" to visitors. Attackers would include JavaScript in their guestbook

entries, and all subsequent visitors to the guestbook page would execute the malicious code. As the examples demonstrate, XSS vulnerabilities are caused by code that includes unvalidated data in an HTTP response. There are three vectors by which an XSS attack can reach a victim: - As in `Example 1`, data is read directly from the HTTP request and reflected back in the HTTP response. Reflected XSS exploits occur when an attacker causes a user to supply dangerous content to a vulnerable web application, which is then reflected back to the user and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or emailed directly to victims. URLs constructed in this manner constitute the core of many phishing schemes, whereby an attacker convinces victims to visit a URL that refers to a vulnerable site. After the site reflects the attacker's content back to the user, the content is executed and proceeds to transfer private information, such as cookies that might include session information, from the user's machine to the attacker or perform other nefarious activities. - As in `Example 2`, the application stores dangerous data in a database or other trusted data store. The dangerous data is subsequently read back into the application and included in dynamic content. Persistent XSS exploits occur when an attacker injects dangerous content into a data store that is later read and included in dynamic content. From an attacker's perspective, the optimal place to inject malicious content is in an area that is displayed to either many users or particularly interesting users. Interesting users typically have elevated privileges in the application or interact with sensitive data that is valuable to the attacker. If one of these users executes malicious content, the attacker may be able to perform privileged operations on behalf of the user or gain access to sensitive data belonging to the user. - A source outside the application stores dangerous data in a database or other data store, and the dangerous data is subsequently read back into the application as trusted data and included in dynamic content.

<u>Recommendation</u>

The solution to prevent XSS is to ensure that validation occurs in the required places and that relevant properties are set to prevent vulnerabilities. Because XSS vulnerabilities occur when an application includes malicious data in its output, one logical approach is to validate data immediately before it leaves the application. However, because web applications often have complex and intricate code for generating dynamic content, this method is prone to errors of omission (missing validation). An effective way to mitigate this risk is to also perform input validation for XSS. Web applications must validate all input to prevent other vulnerabilities, such as SQL injection, so augmenting an application's existing input validation mechanism to include checks for XSS is generally relatively easy. Despite its value, input validation for XSS does not take the place of rigorous output validation. An application might accept input through a shared data store or other trusted source, and that data store might accept input from a source that does not perform adequate input validation. Therefore, the application cannot implicitly rely on the safety of this or any other data. This means that the best way to prevent XSS vulnerabilities is to validate everything that enters the application and leaves the application destined for the user. The most secure approach to validation for XSS is to create an allow list of safe characters that can appear in HTTP content and accept input composed exclusively of characters in the approved set. For example, a valid username might only include alphanumeric characters or a phone number might only include digits 0-9. However, this solution is often infeasible in web applications because many characters that have special meaning to the browser must be considered valid input after they are encoded, such as a web design bulletin board that must accept HTML fragments from its users. A more flexible, but less secure approach is to implement a deny list, which selectively rejects or escapes potentially dangerous characters before using the input. To form such a list, you first need to understand the set of characters that hold special meaning for web browsers. Although the HTML standard defines which characters have special meaning, many web browsers try to correct common mistakes in HTML and might treat other characters as special in certain contexts. This is why we do not recommend the use of deny lists as a means to prevent XSS. The CERT(R) Coordination Center at the Software Engineering Institute at Carnegie Mellon University provides the following details about special characters in various contexts [1]: In the content of a block-level element (in the middle of a paragraph of text): - "<" is special because it introduces a tag. - "&" is special because it introduces a character entity. - ">" is special because some browsers treat it as special, on the assumption that the author of the page intended to include an opening "<", but omitted it in error. The following principles apply to attribute values: - In attribute values enclosed in double quotes, the double quotes are special because they mark the end of the attribute value. - In attribute values enclosed in single quote, the single quotes are special because they mark the end of the attribute value. - In attribute values without any quotes, white-space characters, such as space and tab, are special. - "&" is special when used with certain attributes, because it introduces a character entity. In URLs, for example, a search engine might provide a link within the results page that the user can click to re-run the search. This can be implemented by encoding the search query inside the URL, which introduces additional special characters: - Space, tab, and new line are special because they mark the end of the URL. - "&" is special because it either introduces a character entity or separates CGI parameters. - Non-ASCII characters (that is, everything greater than 127 in the ISO-8859-1 encoding) are not allowed in URLs, so they are considered to be special in this context. - The "%" symbol must be filtered from input anywhere parameters encoded with HTTP escape sequences are decoded by server-side code. For example, "%" must be filtered if input such as "%68%65%6C%6C%6F" becomes "hello" when it appears on the web page. Within the body of a : - Semicolons, parentheses, curly braces, and new line characters must be filtered out in situations where text could be inserted directly into a pre-existing script tag. Server-side scripts: - Server-side scripts that convert any exclamation characters (!) in input to double-quote characters (") on output might require additional filtering. Other possibilities: - If an attacker submits a request in UTF-7, the special character '<' appears as '+ADw-' and might bypass filtering. If the output is included in a page that does not explicitly specify an encoding format, then some browsers try to intelligently identify the encoding based on the content (in this case, UTF-7). After you identify the correct points in an application to perform validation for XSS attacks and what special characters the validation should consider, the next challenge is to identify how your validation handles special characters. If special characters are not considered valid input to the application, then you can reject any input that contains special characters as invalid. A second option is to remove special characters with filtering. However, filtering has the side effect of changing any visual representation of the filtered content and might be unacceptable in circumstances where the integrity of the input must be preserved for display. If input containing special characters must be accepted and displayed accurately, validation must

encode any special characters to remove their significance. A complete list of ISO 8859-1 encoded values for special characters is provided as part of the official HTML specification [2]. Many application servers attempt to limit an application's exposure to cross-site scripting vulnerabilities by providing implementations for the functions responsible for setting certain specific HTTP response content that perform validation for the characters essential to a cross-site scripting attack. Do not rely on the server running your application to make it secure. For any developed application, there are no guarantees about which application servers it will run on during its lifetime. As standards and known exploits evolve, there are no guarantees that application servers will continue to stay in sync.

Issue Summary
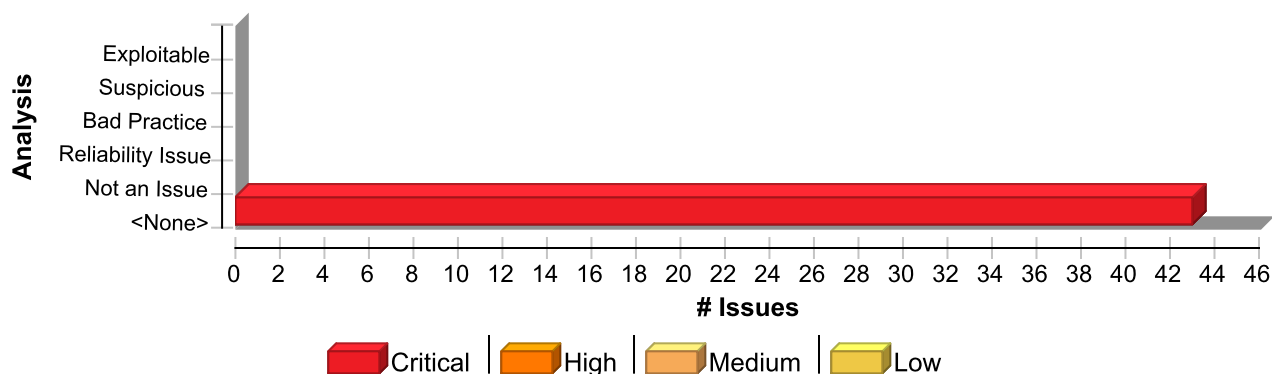
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Cross-Site Scripting: Reflected	43	0	0	43
Total	**43**	**0**	**0**	**43**

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js, line 110 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js:108

```
105
106
107
108 app.post('/log', function (req, res) {
109   console.log(req.body);
110   res.send(req.body);
111
```

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js, line 110 (Cross-Site Scripting: Reflected)	Critical

Sink Details

> **Sink:** ~JS_Generic.send()
> **Enclosing Method:** lambda()
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js:110
> **Taint Flags:** WEB, XSS

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js, line 160 (Cross-Site Scripting: Reflected)	Critical

Issue Details

> **Kingdom:** Input Validation and Representation
> **Scan Engine:** SCA (Data Flow)

Source Details

> **Source:** lambda(0.body)
> **From:** lambda
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
> 151

```
148  })
149  })
150
151  router.post('/typeform_insert', function (req, res) {
152
153   var data = req.body
154   data.uuid = uuidv4()
```

Sink Details

> **Sink:** ~JS_Generic.send()
> **Enclosing Method:** lambda()
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:160
> **Taint Flags:** WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js, line 257 (Cross-Site Scripting: Reflected)	Critical

Issue Details

> **Kingdom:** Input Validation and Representation
> **Scan Engine:** SCA (Data Flow)

Source Details

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 257 (Cross-Site Scripting: Reflected)	Critical

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
247

```
244
245 })
246
247 router.post('/npc_insert', function (req, res) {
248
249  var data = req.body
250  data.name = string_to_unicode(data.name)
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:257
Taint Flags: WEB, XSS

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 344 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
317

```
314  })
315 })
316
317 router.post('/trainrecord_insert', function (req, res) {
318
319  var data = req.body
320  // console.log("trainrecord_insert req.body");
```

Sink Details

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 344 (Cross-Site Scripting: Reflected)	Critical

> **Sink:** ~JS_Generic.send()
> **Enclosing Method:** lambda()
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:344
> **Taint Flags:** WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 376 (Cross-Site Scripting: Reflected)	Critical

Issue Details

> **Kingdom:** Input Validation and Representation
> **Scan Engine:** SCA (Data Flow)

Source Details

> **Source:** lambda(0.body)
> **From:** lambda
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
> 353

```
350  })
351  })
352
353  router.post('/trainrecord_insert2', function (req, res) {
354
355    var data = req.body
356    data.uuid = string_to_unicode(data.uuid)
```

Sink Details

> **Sink:** ~JS_Generic.send()
> **Enclosing Method:** lambda()
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:376
> **Taint Flags:** WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 408 (Cross-Site Scripting: Reflected)	Critical

Issue Details

> **Kingdom:** Input Validation and Representation
> **Scan Engine:** SCA (Data Flow)

Source Details

> **Source:** lambda(0.body)
> **From:** lambda
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
> 385

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 408 (Cross-Site Scripting: Reflected)	Critical

```
382  })
383  })
384
385  router.post('/trainrecord_insert3', function (req, res) {
386
387    var data = req.body
388    data.uuid = string_to_unicode(data.uuid)
```

Sink Details

> **Sink:** ~JS_Generic.send()
> **Enclosing Method:** lambda()
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:408
> **Taint Flags:** WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 438 (Cross-Site Scripting: Reflected)	Critical

Issue Details

> **Kingdom:** Input Validation and Representation
> **Scan Engine:** SCA (Data Flow)

Source Details

> **Source:** lambda(0.body)
> **From:** lambda
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
> 417

```
414  })
415  })
416
417  router.post('/trainrecord_insert4', function (req, res) {
418    var data = req.body
419    data.name = string_to_unicode(data.name)
420    data.coursename = string_to_unicode(data.coursename)
```

Sink Details

> **Sink:** ~JS_Generic.send()
> **Enclosing Method:** lambda()
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:438
> **Taint Flags:** WEB, XSS

`No snippet available`

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 465 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
417

```
414  })
415  })
416
417  router.post('/trainrecord_insert4', function (req, res) {
418   var data = req.body
419   data.name = string_to_unicode(data.name)
420   data.coursename = string_to_unicode(data.coursename)
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:465
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 531 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
477

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 531 (Cross-Site Scripting: Reflected)	Critical

474	`})`
475	`})`
476	
477	`router.post('/trainrecord_insertv2', function (req, res) {`
478	`var data = req.body`
479	`data.OK_NAME = string_to_unicode(data.OK_NAME)`
480	`data.OK_COURSENAME = string_to_unicode(data.OK_COURSENAME)`

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:531
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 679 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
661

658	
659	`})`
660	
661	`router.post('/check_files_version', function (req, res) {`
662	`var data = req.body`
663	
664	`if (data.checktype == 1) {`

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:679
Taint Flags: WEB, XSS

`No snippet available`

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 705 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
687

```
684  })
685  })
686
687  router.post('/file_delete', async function (req, res) {
688   var data = req.body.data
689
690   switch (data.datatype) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:705
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 735 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
687

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 735 (Cross-Site Scripting: Reflected)	**Critical**

```
684   })
685 })
686
687 router.post('/file_delete', async function (req, res) {
688   var data = req.body.data
689
690   switch (data.datatype) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:735
Taint Flags: WEB, XSS

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 759 (Cross-Site Scripting: Reflected)	**Critical**

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
687

```
684   })
685 })
686
687 router.post('/file_delete', async function (req, res) {
688   var data = req.body.data
689
690   switch (data.datatype) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:759
Taint Flags: WEB, XSS

No snippet available

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 805 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
687

```
684  })
685  })
686
687  router.post('/file_delete', async function (req, res) {
688    var data = req.body.data
689
690    switch (data.datatype) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:805
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 825 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:
687

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.xr.router.js, line 825 (Cross-Site Scripting: Reflected)	Critical

```
684  })
685  })
686
687  router.post('/file_delete', async function (req, res) {
688    var data = req.body.data
689
690    switch (data.datatype) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.xr.router.js:825
Taint Flags: WEB, XSS

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 171 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:162

```
159  })
160  })
161
162  router.post('/typeform_insert', function (req, res) {
163
164    var data = req.body
165    data.uuid = uuidv4()
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:171
Taint Flags: WEB, XSS

No snippet available

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 285 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:275

```
272
273 })
274
275 router.post('/npc_insert', function (req, res) {
276
277   var data = req.body
278   data.name = string_to_unicode(data.name)
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:285
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 372 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:345

```
342   })
343 })
344
345 router.post('/trainrecord_insert', function (req, res) {
346
347   var data = req.body
348   // console.log("trainrecord_insert req.body");
```

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 372 (Cross-Site Scripting: Reflected)	Critical

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:372
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 404 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:381

```
378  })
379 })
380
381 router.post('/trainrecord_insert2', function (req, res) {
382
383  var data = req.body
384  data.uuid = string_to_unicode(data.uuid)
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:404
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 436 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:413

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 436 (Cross-Site Scripting: Reflected)	Critical

```
410  })
411  })
412
413  router.post('/trainrecord_insert3', function (req, res) {
414
415  var data = req.body
416  data.uuid = string_to_unicode(data.uuid)
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:436
Taint Flags: WEB, XSS

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 466 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:445

```
442  })
443  })
444
445  router.post('/trainrecord_insert4', function (req, res) {
446  var data = req.body
447  data.name = string_to_unicode(data.name)
448  data.coursename = string_to_unicode(data.coursename)
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:466
Taint Flags: WEB, XSS

No snippet available

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 493 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:445

```
442  })
443  })
444
445  router.post('/trainrecord_insert4', function (req, res) {
446  var data = req.body
447  data.name = string_to_unicode(data.name)
448  data.coursename = string_to_unicode(data.coursename)
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:493
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 614 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:534

```
531  }
532  })
533  })
534  router.post('/trainrecord_insertv2', function (req, res) {
535  var data = req.body
536  if (data.OK_NAME != '') {
537  data.OK_NAME = string_to_unicode(data.OK_NAME)
```

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 614 (Cross-Site Scripting: Reflected)	Critical

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:614
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 769 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:751

```
748
749 })
750
751 router.post('/check_files_version', function (req, res) {
752   var data = req.body
753
754   if (data.checktype == 1) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:769
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 795 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:777

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 795 (Cross-Site Scripting: Reflected)	Critical

```
774  })
775 })
776
777 router.post('/file_delete', async function (req, res) {
778   var data = req.body.data
779
780   switch (data.datatype) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:795
Taint Flags: WEB, XSS

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 825 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:777

```
774  })
775 })
776
777 router.post('/file_delete', async function (req, res) {
778  var data = req.body.data
779
780  switch (data.datatype) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:825
Taint Flags: WEB, XSS

No snippet available

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 849 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:777

```
774  })
775 })
776
777 router.post('/file_delete', async function (req, res) {
778  var data = req.body.data
779
780  switch (data.datatype) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:849
Taint Flags: WEB, XSS

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 895 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:777

```
774  })
775 })
776
777 router.post('/file_delete', async function (req, res) {
778  var data = req.body.data
779
780  switch (data.datatype) {
```

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 895 (Cross-Site Scripting: Reflected)	Critical

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:895
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 915 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:777

```
774  })
775  })
776
777  router.post('/file_delete', async function (req, res) {
778   var data = req.body.data
779
780   switch (data.datatype) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:915
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1081 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1072

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1081 (Cross-Site Scripting: Reflected)	Critical

```
1069  })
1070  })
1071
1072  router.post('/temp/typeform_insert', function (req, res) {
1073
1074   var data = req.body
1075   data.uuid = uuidv4()
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1081
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1219 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1209

```
1206
1207  })
1208
1209  router.post('/temp/npc_insert', function (req, res) {
1210
1211   var data = req.body
1212   data.name = string_to_unicode(data.name)
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1219
Taint Flags: WEB, XSS

`No snippet available`

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1306 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1279

```
1276  })
1277 })
1278
1279 router.post('/temp/trainrecord_insert', function (req, res) {
1280
1281  var data = req.body
1282  // console.log("trainrecord_insert req.body");
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1306
Taint Flags: WEB, XSS

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1338 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1315

```
1312  })
1313 })
1314
1315 router.post('/temp/trainrecord_insert2', function (req, res) {
1316
1317  var data = req.body
1318  data.uuid = string_to_unicode(data.uuid)
```

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1338 (Cross-Site Scripting: Reflected)	Critical

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1338
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1370 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1347

```
1344  })
1345 })
1346
1347 router.post('/temp/trainrecord_insert3', function (req, res) {
1348
1349  var data = req.body
1350  data.uuid = string_to_unicode(data.uuid)
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1370
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1400 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1379

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1400 (Cross-Site Scripting: Reflected)	Critical

```
1376  })
1377 })
1378
1379 router.post('/temp/trainrecord_insert4', function (req, res) {
1380  var data = req.body
1381  data.name = string_to_unicode(data.name)
1382  data.coursename = string_to_unicode(data.coursename)
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1400
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1427 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1379

```
1376  })
1377 })
1378
1379 router.post('/temp/trainrecord_insert4', function (req, res) {
1380  var data = req.body
1381  data.name = string_to_unicode(data.name)
1382  data.coursename = string_to_unicode(data.coursename)
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1427
Taint Flags: WEB, XSS

`No snippet available`

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1493 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1439

1436	`})`
1437	`})`
1438	
1439	`router.post('/temp/trainrecord_insertv2', function (req, res) {`
1440	`var data = req.body`
1441	`data.OK_NAME = string_to_unicode(data.OK_NAME)`
1442	`data.OK_COURSENAME = string_to_unicode(data.OK_COURSENAME)`

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1493
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1669 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1651

1648	
1649	`})`
1650	
1651	`router.post('/temp/check_files_version', function (req, res) {`
1652	`var data = req.body`
1653	
1654	`if (data.checktype == 1) {`

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1669 (Cross-Site Scripting: Reflected)	Critical

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1669
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1695 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1677

```
1674  })
1675 })
1676
1677 router.post('/temp/file_delete', async function (req, res) {
1678  var data = req.body.data
1679
1680  switch (data.datatype) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1695
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1725 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1677

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1725 (Cross-Site Scripting: Reflected)	Critical

```
1674  })
1675 })
1676
1677 router.post('/temp/file_delete', async function (req, res) {
1678  var data = req.body.data
1679
1680  switch (data.datatype) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1725
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1749 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1677

```
1674  })
1675 })
1676
1677 router.post('/temp/file_delete', async function (req, res) {
1678  var data = req.body.data
1679
1680  switch (data.datatype) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1749
Taint Flags: WEB, XSS

`No snippet available`

Cross-Site Scripting: Reflected	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1795 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1677

```
1674  })
1675  })
1676
1677  router.post('/temp/file_delete', async function (req, res) {
1678    var data = req.body.data
1679
1680    switch (data.datatype) {
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1795
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1815 (Cross-Site Scripting: Reflected)	Critical

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0.body)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1677

```
1674  })
1675  })
1676
1677  router.post('/temp/file_delete', async function (req, res) {
1678    var data = req.body.data
1679
1680    switch (data.datatype) {
```

Cross-Site Scripting: Reflected	Critical
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js, line 1815 (Cross-Site Scripting: Reflected)	**Critical**

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/xr.router.js:1815
Taint Flags: WEB, XSS

`No snippet available`

Denial of Service (2 issues)

Abstract

An attacker could cause the program to crash or otherwise become unavailable to legitimate users.

Explanation

Attackers may be able to deny service to legitimate users by flooding the application with requests, but flooding attacks can often be defused at the network layer. More problematic are bugs that allow an attacker to overload the application using a small number of requests. Such bugs allow the attacker to specify the quantity of system resources their requests will consume or the duration for which they will use them. **Example 1:** The following code allows a user to specify the size of the file system to be used. By specifying a large number, an attacker may deplete file system resources.

```
var fsync = requestFileSystemSync(0, userInput);
```

Example 2: The following code writes to a file. Because the file may be continuously written and rewritten until it is deemed closed by the user agent, disk quota, IO bandwidth, and processes that may require analyzing the content of the file are impacted.

```
function oninit(fs) {
  fs.root.getFile('applog.txt', {create: false}, function(fileEntry) {
    fileEntry.createWriter(function(fileWriter) {
      fileWriter.seek(fileWriter.length);
      var bb = new BlobBuilder();
      bb.append('Appending to a file');
      fileWriter.write(bb.getBlob('text/plain'));
    }, errorHandler);
  }, errorHandler);
}

window.requestFileSystem(window.TEMPORARY, 1024*1024, oninit, errorHandler);
```

Recommendation

Validate user input to ensure that it will not cause inappropriate resource utilization. **Example 3:** The following code allows a user to specify the size of the file system just as in `Example 1`, but only if the value is within reasonable bounds.

```
if (userInput >= SIZE_MIN &&
    userInput <= SIZE_MAX) {
  var fsync = requestFileSystemSync(0, userInput);
} else {
  throw "Invalid file system size";
}
}
```

Example 4: The following code writes to a file just as in `Example 2`, but the maximum file size is `MAX_FILE_LEN`.

```
function oninit(fs) {
  fs.root.getFile('applog.txt', {create: false}, function(fileEntry) {
    fileEntry.createWriter(function(fileWriter) {
      fileWriter.seek(fileWriter.length);
      var bb = new BlobBuilder();
      bb.append('Appending to a file');
      if (fileWriter.length + bb.size <= MAX_FILE_LEN) {
        fileWriter.write(bb.getBlob('text/plain'));
      }
    }, errorHandler);
  }, errorHandler);
}

window.requestFileSystem(window.TEMPORARY, 1024*1024, oninit, errorHandler);
```

Issue Summary
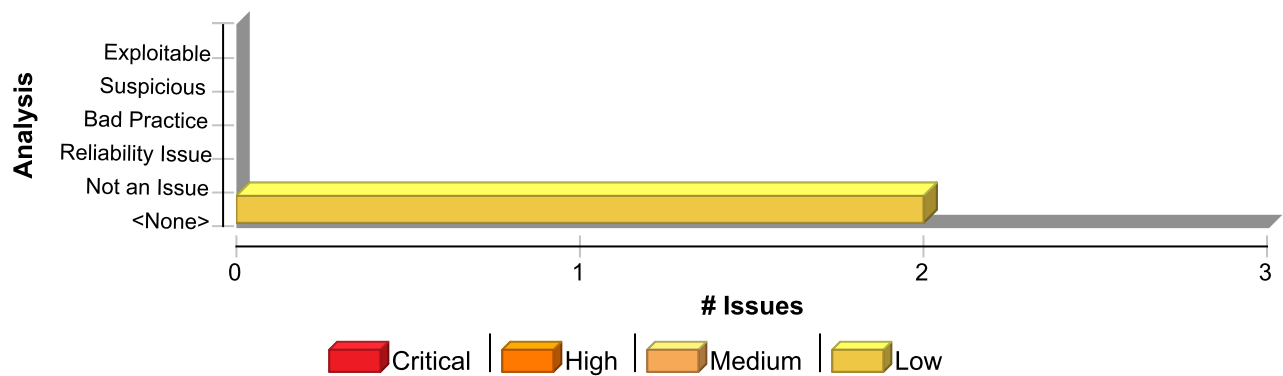
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Denial of Service	2	0	0	2
Total	**2**	**0**	**0**	**2**

Denial of Service	Low

Package: .src.plugins

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ formidable/src/plugins/octetstream.js, line 57 (Denial of Service)	Low

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: write
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/formidable/src/plugins/octetstream.js:57
Taint Flags:

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ formidable/src/Formidable.js, line 370 (Denial of Service)	Low

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: write
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/formidable/src/Formidable.js:370
Taint Flags:

`No snippet available`

Header Manipulation (3 issues)

Abstract

Including unvalidated data in an HTTP response header can enable cache-poisoning, cross-site scripting, cross-user defacement, page hijacking, cookie manipulation or open redirect.

Explanation

2023   9   12   4:23

Header Manipulation vulnerabilities occur when: 1. Data enters a web application through an untrusted source, most frequently an HTTP request. 2. The data is included in an HTTP response header sent to a web user without being validated. As with many software security vulnerabilities, Header Manipulation is a means to an end, not an end in itself. At its root, the vulnerability is straightforward: an attacker passes malicious data to a vulnerable application, and the application includes the data in an HTTP response header. One of the most common Header Manipulation attacks is HTTP Response Splitting. To mount a successful HTTP Response Splitting exploit, the application must allow input that contains CR (carriage return, also given by %0d or \r) and LF (line feed, also given by %0a or \n)characters into the header. These characters not only give attackers control of the remaining headers and body of the response the application intends to send, but also allows them to create additional responses entirely under their control. Many of today's modern application servers will prevent the injection of malicious characters into HTTP headers. If your application server prevents setting headers with new line characters, then your application is not vulnerable to HTTP Response Splitting. However, solely filtering for new line characters can leave an application vulnerable to Cookie Manipulation or Open Redirects, so care must still be taken when setting HTTP headers with user input. **Example:** The following code segment reads the name of the author of a weblog entry, `author`, from an HTTP request and sets it in a cookie header of an HTTP response.

```
author = form.author.value;
...
document.cookie = "author=" + author + ";expires="+cookieExpiration;
...
```

Assuming a string consisting of standard alphanumeric characters, such as "Jane Smith", is submitted in the request the HTTP response including this cookie might take the following form:

```
HTTP/1.1 200 OK
...
Set-Cookie: author=Jane Smith
...
```

However, because the value of the cookie is formed of unvalidated user input the response will only maintain this form if the value submitted for `AUTHOR_PARAM` does not contain any CR and LF characters. If an attacker submits a malicious string, such as "Wiley Hacker\r\nHTTP/1.1 200 OK\r\n...", then the HTTP response would be split into two responses of the following form:

```
HTTP/1.1 200 OK
...
Set-Cookie: author=Wiley Hacker

HTTP/1.1 200 OK
...
```

Clearly, the second response is completely controlled by the attacker and can be constructed with any header and body content desired. The ability of attacker to construct arbitrary HTTP responses permits a variety of resulting attacks, including: web and browser cache poisoning, cross-site scripting, and page hijacking. **Cache Poisoning:** The impact of a maliciously constructed response can be magnified if it is cached either by a web cache used by multiple users or even the browser cache of a single user. If a response is cached in a shared web cache, such as those commonly found in proxy servers, then all users of that cache will continue receive the malicious content until the cache entry is purged. Similarly, if the response is cached in the browser of an individual user, then that user will continue to receive the malicious content until the cache entry is purged, although only the user of the local browser instance will be affected. **Cross-Site Scripting:** Once attackers have control of the responses sent by an application, they have a choice of a variety of malicious content to provide users. Cross-site scripting is common form of attack where malicious JavaScript or other code included in a response is executed in the user's browser. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data such as cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site. The most common and dangerous attack vector against users of a vulnerable application uses JavaScript to transmit session and authentication information back to the attacker who can then take complete control of the victim's account. **Page Hijacking:** In addition to using a vulnerable application to send malicious content to a user, the same root vulnerability can also be leveraged to redirect sensitive content generated by the server and intended for the user to the attacker instead. By submitting a request

that results in two responses, the intended response from the server and the response generated by the attacker, an attacker may cause an intermediate node, such as a shared proxy server, to misdirect a response generated by the server for the user to the attacker. Because the request made by the attacker generates two responses, the first is interpreted as a response to the attacker's request, while the second remains in limbo. When the user makes a legitimate request through the same TCP connection, the attacker's request is already waiting and is interpreted as a response to the victim's request. The attacker then sends a second request to the server, to which the proxy server responds with the server generated request intended for the victim, thereby compromising any sensitive information in the headers or body of the response intended for the victim. **Cookie Manipulation:** When combined with attacks like cross-site request forgery, attackers may change, add to, or even overwrite a legitimate user's cookies. **Open Redirect:** Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.

Recommendation

The solution to prevent Header Manipulation is to ensure that input validation occurs in the required places and checks for the correct properties. Since Header Manipulation vulnerabilities occur when an application includes malicious data in its output, one logical approach is to validate data immediately before it leaves the application. However, because web applications often have complex and intricate code for generating responses dynamically, this method is prone to errors of omission (missing validation). An effective way to mitigate this risk is to also perform input validation for Header Manipulation. Web applications must validate all input to prevent other vulnerabilities, such as SQL injection, so augmenting an application's existing input validation mechanism to include checks for Header Manipulation is generally relatively easy. Despite its value, input validation for Header Manipulation does not take the place of rigorous output validation. An application might accept input through a shared data store or other trusted source, and that data store might accept input from a source that does not perform adequate input validation. Therefore, the application cannot implicitly rely on the safety of this or any other data. This means that the best way to prevent Header Manipulation vulnerabilities is to validate everything that enters the application or leaves the application destined for the user. The most secure approach to validation for Header Manipulation is to create an allow list of safe characters that can appear in HTTP response headers and accept input composed exclusively of characters in the approved set. For example, a valid name might only include alphanumeric characters or an account number might only include digits 0-9. A more flexible, but less secure approach is to implement a deny list, which selectively rejects or escapes potentially dangerous characters before using the input. To form such a list, you first need to understand the set of characters that hold special meaning in HTTP response headers. Although the CR and LF characters are at the heart of an HTTP response splitting attack, other characters, such as ':' (colon) and '=' (equal), have special meaning in response headers as well. After you identify the correct points in an application to perform validation for Header Manipulation attacks and what special characters the validation should consider, the next challenge is to identify how your validation handles special characters. The application should reject any input destined to be included in HTTP response headers that contains special characters, particularly CR and LF, as invalid. Many application servers attempt to limit an application's exposure to HTTP response splitting vulnerabilities by providing implementations for the functions responsible for setting HTTP headers and cookies that perform validation for the characters essential to an HTTP response splitting attack. Do not rely on the server running your application to make it secure. For any developed application, there are no guarantees about which application servers it will run on during its lifetime. As standards and known exploits evolve, there are no guarantees that application servers will continue to stay in sync.

Issue Summary
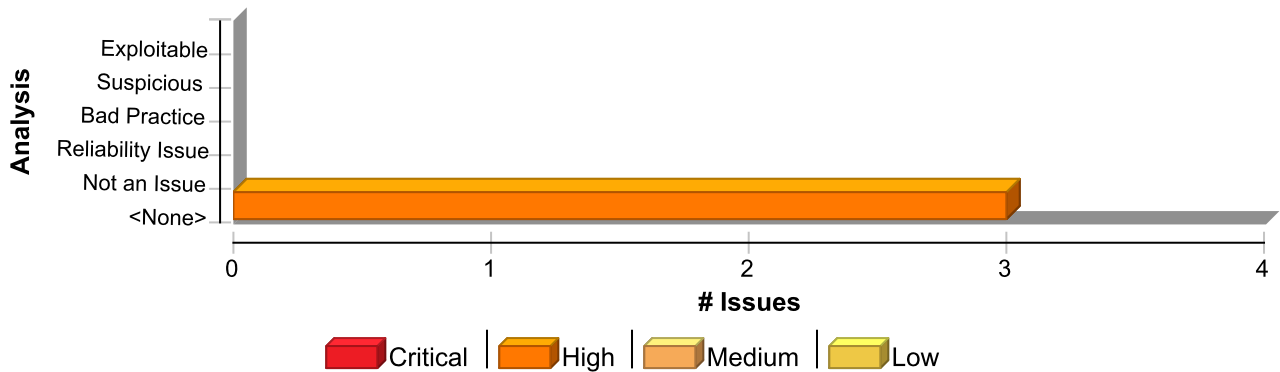
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Header Manipulation	3	0	0	3
Total	**3**	**0**	**0**	**3**

Header Manipulation	High

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/request.js, line 1180 (Header Manipulation)	High

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: Read self.response
From: pipeDest
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/requ est.js:1174

```
1171
1172 Request.prototype.pipeDest = function (dest) {
1173  var self = this
1174  var response = self.response
1175  // Called after the response is received
1176  if (dest.headers && !dest.headersSent) {
1177  if (response.caseless.has('content-type')) {
```

Sink Details

Sink: ~JS_Generic.setHeader()
Enclosing Method: pipeDest()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:1180
Taint Flags: WEB, XSS

```
No snippet available
```

Header Manipulation	High

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/request.js, line 1200 (Header Manipulation)	High

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: Read self.response
From: pipeDest
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:1174

```
1171
1172  Request.prototype.pipeDest = function (dest) {
1173    var self = this
1174    var response = self.response
1175    // Called after the response is received
1176    if (dest.headers && !dest.headersSent) {
1177      if (response.caseless.has('content-type')) {
```

Sink Details

Sink: ~JS_Generic.setHeader()
Enclosing Method: pipeDest()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:1200
Taint Flags: WEB, XSS

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/request.js, line 1189 (Header Manipulation)	High

Issue Details

Kingdom: Input Validation and Representation
Scan Engine: SCA (Data Flow)

Source Details

Source: Read self.response
From: pipeDest
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:1174

Header Manipulation	High
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.request	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/request.js, line 1189 (Header Manipulation)	**High**

```
1171
1172 Request.prototype.pipeDest = function (dest) {
1173  var self = this
1174  var response = self.response
1175  // Called after the response is received
1176  if (dest.headers && !dest.headersSent) {
1177   if (response.caseless.has('content-type')) {
```

Sink Details

Sink: ~JS_Generic.setHeader()
Enclosing Method: pipeDest()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:1189
Taint Flags: WEB, XSS

```
No snippet available
```

Insecure Randomness (5 issues)

Abstract

Standard pseudorandom number generators cannot withstand cryptographic attacks.

Explanation

Insecure randomness errors occur when a function that can produce predictable values is used as a source of randomness in a security-sensitive context. Computers are deterministic machines, and as such are unable to produce true randomness. Pseudorandom Number Generators (PRNGs) approximate randomness algorithmically, starting with a seed from which subsequent values are calculated. There are two types of PRNGs: statistical and cryptographic. Statistical PRNGs provide useful statistical properties, but their output is highly predictable and form an easy to reproduce numeric stream that is unsuitable for use in cases where security depends on generated values being unpredictable. Cryptographic PRNGs address this problem by generating output that is more difficult to predict. For a value to be cryptographically secure, it must be impossible or highly improbable for an attacker to distinguish between the generated random value and a truly random value. In general, if a PRNG algorithm is not advertised as being cryptographically secure, then it is probably a statistical PRNG and should not be used in security-sensitive contexts, where its use can lead to serious vulnerabilities such as easy-to-guess temporary passwords, predictable cryptographic keys, session hijacking, and DNS spoofing. **Example:** The following code uses a statistical PRNG to create a URL for a receipt that remains active for some period of time after a purchase.

```
function genReceiptURL (baseURL){
  var randNum = Math.random();
  var receiptURL = baseURL + randNum + ".html";
  return receiptURL;
}
```

This code uses the `Math.random()` function to generate "unique" identifiers for the receipt pages it generates. Since `Math.random()` is a statistical PRNG, it is easy for an attacker to guess the strings it generates. Although the underlying design of the receipt system is also faulty, it would be more secure if it used a random number generator that did not produce predictable receipt identifiers, such as a cryptographic PRNG.

Recommendation

When unpredictability is critical, as is the case with most security-sensitive uses of randomness, use a cryptographic PRNG. Regardless of the PRNG you choose, always use a value with sufficient entropy to seed the algorithm. (Do not use values such as the current time because it offers only negligible entropy.) In JavaScript, the typical recommendation is to use the `window.crypto.random()` function in the Mozilla API. However, this method does not work in many browsers, including more recent versions of Mozilla Firefox. There is currently no cross-browser solution for a robust cryptographic PRNG. In the meantime, consider handling any PRNG functionality outside of JavaScript.

Issue Summary
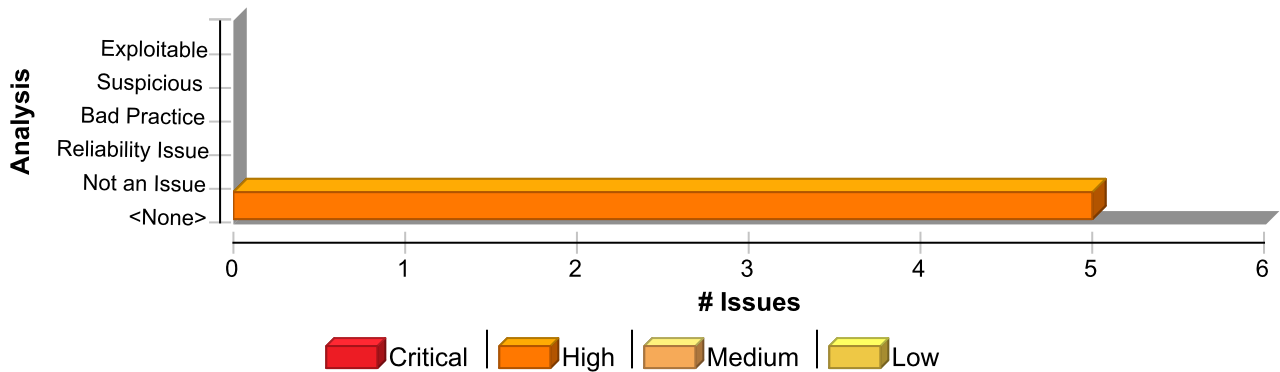
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Insecure Randomness	5	0	0	5
Total	**5**	**0**	**0**	**5**

Insecure Randomness	High

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ form-data/lib/form_data.js, line 321 (Insecure Randomness)	High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: random
Enclosing Method: _generateBoundary()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/form-data/lib/ form_data.js:321
Taint Flags:

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ jsbn/index.js, line 1145 (Insecure Randomness)	High

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: random
Enclosing Method: bnpMillerRabin()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsbn/index.js:1145
Taint Flags:

`No snippet available`

Insecure Randomness	High

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.jsbn	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ jsbn/index.js, line 1269 (Insecure Randomness)	**High**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: random
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsbn/index.js:1269
Taint Flags:

`No snippet available`

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.jsprim.lib	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ jsprim/lib/jsprim.js, line 570 (Insecure Randomness)	**High**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: random
Enclosing Method: randElt()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsprim/lib/jsprim.js:570
Taint Flags:

`No snippet available`

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.rndm	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ rndm/index.js, line 22 (Insecure Randomness)	**High**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: random
Enclosing Method: rndm()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/rndm/index.js:22
Taint Flags:

`No snippet available`

Insecure Transport (5 issues)

Abstract

The call uses an unencrypted protocol instead of an encrypted protocol to communicate with the server.

Explanation

All communication over HTTP, FTP, or gopher is unauthenticated and unencrypted. It is therefore subject to compromise, especially in the mobile environment where devices frequently connect to unsecured, public, wireless networks using WiFi connections. **Example 1:** The following example reads data using the HTTP protocol (instead of using HTTPS).
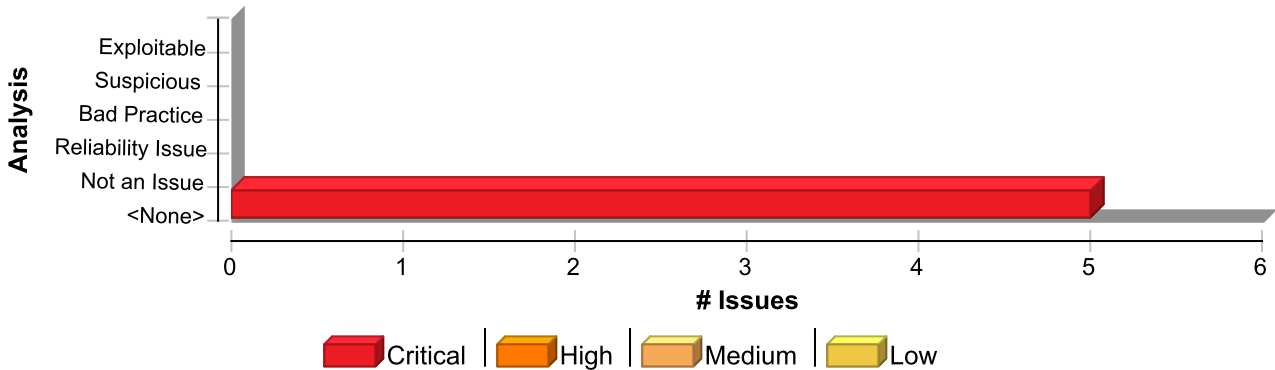
```
var http = require('http');
...
http.request(options, function(res){
  ...
});
...
```

The incoming `http.IncomingMessage` object,`res`, may have been compromised as it is delivered over an unencrypted and unauthenticated channel.

Recommendation

Use secure protocols such as HTTPS to exchange data with the server whenever possible.

Issue Summary

Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Insecure Transport	5	0	0	5
Total	**5**	**0**	**0**	**5**

Insecure Transport	Critical
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js, line 119 (Insecure Transport)	Critical
Issue Details	

    Kingdom: Security Features
    Scan Engine: SCA (Structural)

Insecure Transport	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js, line 119 (Insecure Transport)	Critical

Sink Details

Sink: FunctionPointerCall: listen
Enclosing Method: ~file_function()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js:119
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js, line 356 (Insecure Transport)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: listen
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:356
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js, line 356 (Insecure Transport)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: listen
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:356
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/db_server.js, line 145 (Insecure Transport)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: listen
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/db_server.js:145
Taint Flags:

Insecure Transport	Critical

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/db_server.js, line 145 (Insecure Transport)	Critical

```
No snippet available
```

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.form-data.lib	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ form-data/lib/form_data.js, line 424 (Insecure Transport)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: request
Enclosing Method: submit()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/form-data/lib/ form_data.js:424
Taint Flags:

```
No snippet available
```

Password Management: Empty Password (1 issue)

Abstract

Empty passwords may compromise system security in a way that cannot be easily remedied.

Explanation

It is never a good idea to have an empty password. It also makes fixing the problem extremely difficult once the code is in production. The password cannot be changed without patching the software. If the account protected by the empty password is compromised, the owners of the system must choose between security and availability. **Example:** The following code has an empty password to connect to an application and retrieve address book entries:

```
...
obj = new XMLHttpRequest();
obj.open('GET','/fetchusers.jsp?id='+form.id.value,'true','scott','');
...
```
This code will run successfully, but anyone can access when they know the username.

Recommendation

Passwords should never be empty and should generally be obfuscated and managed in an external source. Storing passwords in plain text anywhere on the web site allows anyone with sufficient permissions to read and potentially misuse the password. For JavaScript calls that require passwords, it is better to prompt the user for the password at connection time.

Issue Summary
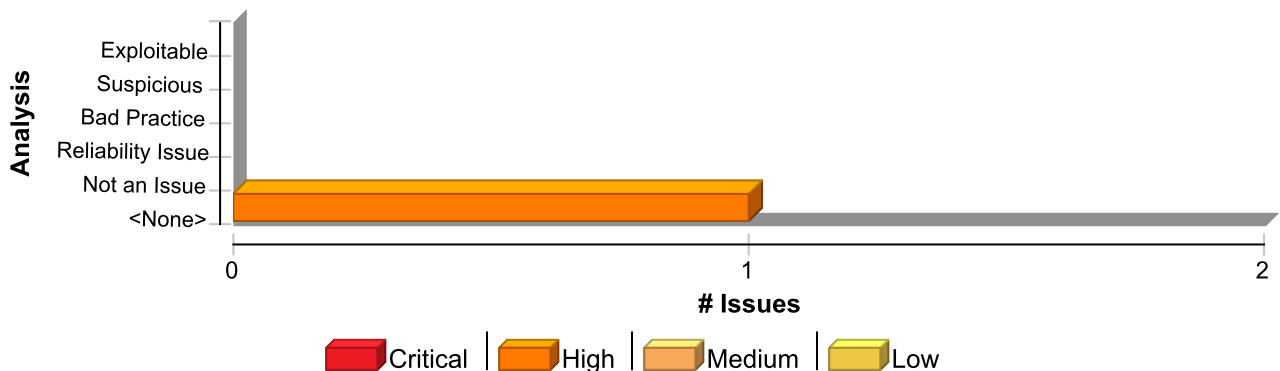
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Password Management: Empty Password	1	0	0	1
Total	**1**	**0**	**0**	**1**

Password Management: Empty Password	High
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.node-windows.lib	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/binaries.js, line 73 (Password Management: Empty Password)	High
Issue Details	

Password Management: Empty Password	High

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/binaries.js, line 73 (Password Management: Empty Password)	High

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: VariableAccess: password
Enclosing Method: sudo()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/binaries.js:73
Taint Flags:

```
No snippet available
```

Password Management: Hardcoded Password (14 issues)

Abstract

Hardcoded passwords can compromise system security in a way that is difficult to remedy.

Explanation

Never hardcode passwords. Not only does it expose the password to all of the project's developers, it also makes fixing the problem extremely difficult. After the code is in production, a program patch is probably the only way to change the password. If the account protected by the password is compromised, the organization must choose between security and system availability. **Example:** The following URL uses a hardcoded password:

```
...
https://user:secretpassword@example.com
...
```

Recommendation

Never hardcode passwords. Always obfuscate and manage passwords in an external source. Storing passwords in plain text anywhere on the system enables anyone with sufficient permissions to read and potentially misuse the password.

Issue Summary
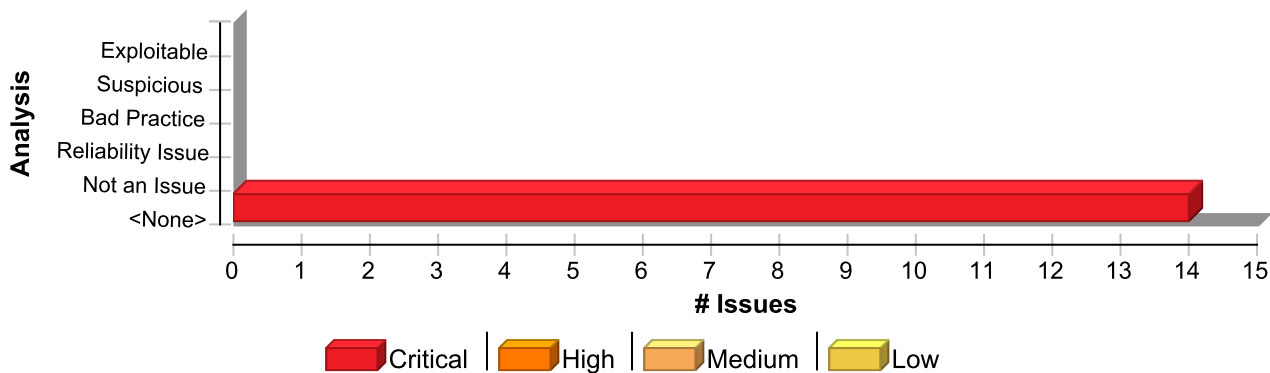
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Password Management: Hardcoded Password	14	0	0	14
Total	**14**	**0**	**0**	**14**

Password Management: Hardcoded Password	Critical
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.hosted-git-info	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ hosted-git-info/index.js, line 119 (Password Management: Hardcoded Password)	**Critical**
Issue Details	

Password Management: Hardcoded Password	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ hosted-git-info/index.js, line 119 (Password Management: Hardcoded Password)	Critical

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/hosted-git-info/ index.js:119
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ hosted-git-info/index.js, line 118 (Password Management: Hardcoded Password)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/hosted-git-info/ index.js:118
Taint Flags:

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/pg-pool/test/connection-strings.js, line 8 (Password Management: Hardcoded Password)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/pg-pool/test/connection-strings.js:8
Taint Flags:

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/ test.js, line 658 (Password Management: Hardcoded Password)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Password Management: Hardcoded Password	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js, line 658 (Password Management: Hardcoded Password)	Critical

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:658
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js, line 1049 (Password Management: Hardcoded Password)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:1049
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js, line 436 (Password Management: Hardcoded Password)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:436
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js, line 1214 (Password Management: Hardcoded Password)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:1214
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js, line 857 (Password Management: Hardcoded Password)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Password Management: Hardcoded Password	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js, line 857 (Password Management: Hardcoded Password)	Critical

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:857
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js, line 651 (Password Management: Hardcoded Password)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:651
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js, line 1202 (Password Management: Hardcoded Password)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:1202
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js, line 1050 (Password Management: Hardcoded Password)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:1050
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js, line 1203 (Password Management: Hardcoded Password)	Critical

Issue Details

Password Management: Hardcoded Password	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js, line 1203 (Password Management: Hardcoded Password)	Critical

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:1203
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js, line 437 (Password Management: Hardcoded Password)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:437
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js, line 1215 (Password Management: Hardcoded Password)	Critical

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Configuration)

Sink Details

File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/url/test.js:1215
Taint Flags:

`No snippet available`

Password Management: Null Password (3 issues)

Abstract

Null passwords can lead to confusion in the code.

Explanation

It is not a good idea to have a `null` password. **Example:** The following code sets the password initially to `null`:

```
...
var password=null;
...
{
    password=getPassword(user_data);
    ...
}
...
if(password==null){
    // Assumption that the get didn't work
    ...
    }
...
```

Recommendation

To avoid confusion, password variables should immediately be assigned to the correct variable.

Issue Summary
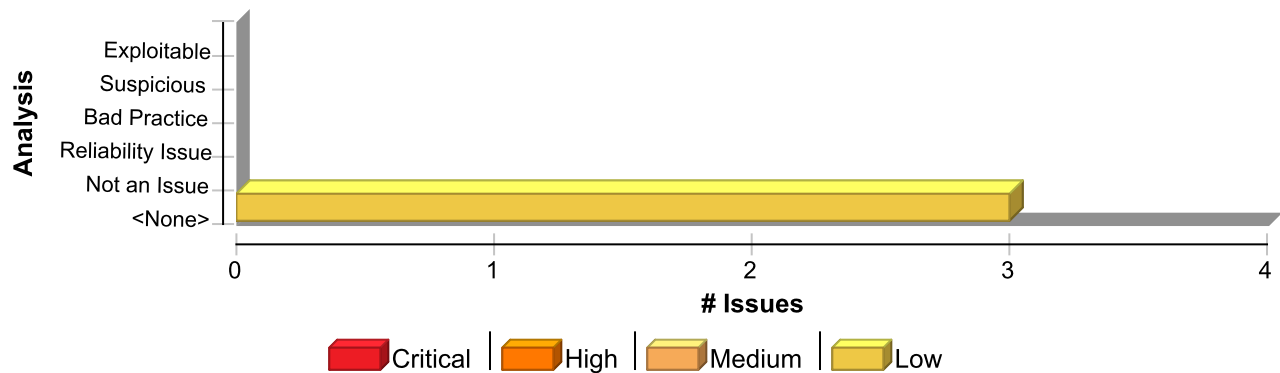
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Password Management: Null Password	3	0	0	3
Total	**3**	**0**	**0**	**3**

Password Management: Null Password	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/daemon.js, line 374 (Password Management: Null Password)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: password
Enclosing Method: daemon()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:374
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/daemon.js, line 414 (Password Management: Null Password)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: password
Enclosing Method: daemon()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:414
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/daemon.js, line 439 (Password Management: Null Password)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FieldAccess: password
Enclosing Method: daemon()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:439
Taint Flags:

```
No snippet available
```

Password Management: Password in Comment (15 issues)

Abstract

Storing passwords or password details in plain text anywhere in the system or system code might compromise system security in a way that cannot be easily remedied.

Explanation

It is never a good idea to hardcode a password. Storing password details within comments is equivalent to hardcoding passwords. Not only is the password visible to the project's developers, it also makes fixing the problem extremely difficult. After the code is in production, the password is now leaked to the outside world and cannot be protected or changed without patching the software. If the account protected by the password is compromised, the owners of the system must choose between security and availability. **Example:** The following comment specifies the default password to connect to a database:

```
...
// Default username for database connection is "scott"
// Default password for database connection is "tiger"
...
```

This code will run successfully, but anyone who has access to it will have access to the password. An employee with access to this information can use it to break into the system.

Recommendation

Passwords should never be hardcoded and should generally be obfuscated and managed in an external source. Storing passwords in plain text anywhere on the system allows anyone with sufficient permissions to read and potentially misuse the password.

Issue Summary
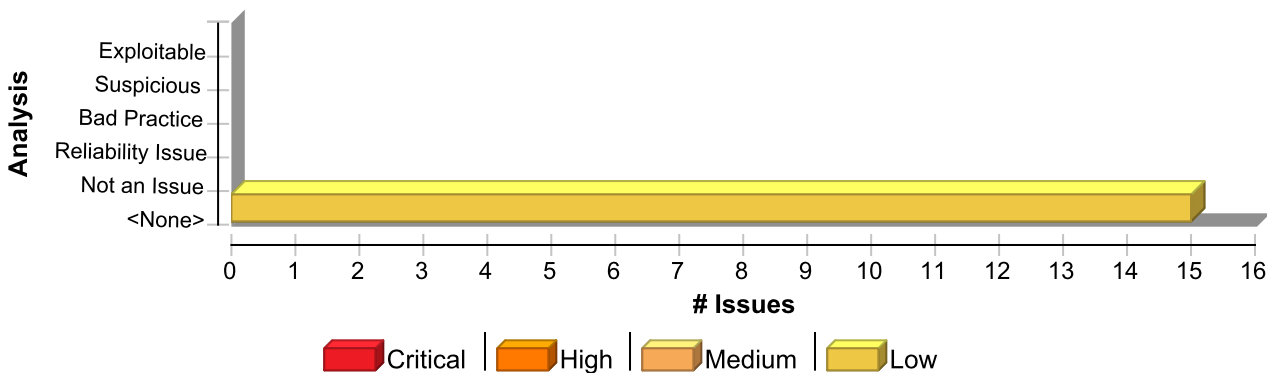
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Password Management: Password in Comment	15	0	0	15
Total	**15**	**0**	**0**	**15**

Password Management: Password in Comment	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.include.jquery@3.3.1	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/include/ jquery@3.3.1/jquery.min.js, line 9312 (Password Management: Password in Comment)	**Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/include/jquery@3.3.1/jquery.min.js:9312
Taint Flags:

`No snippet available`

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.include.jqueryui@1.13.0.external.jquer	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/include/ jqueryui@1.13.0/external/jquery/jquery.js, line 9368 (Password Management: Password in Comment)	**Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/include/jqueryui@1.13.0/external/jquery/jquery.js:9368
Taint Flags:

`No snippet available`

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.debug.src	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ debug/src/node.js, line 203 (Password Management: Password in Comment)	**Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/debug/src/node.js:203
Taint Flags:

`No snippet available`

Password Management: Password in Comment	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ hosted-git-info/index.js, line 117 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/hosted-git-info/ index.js:117
Taint Flags:

```
No snippet available
```

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ jws/lib/data-stream.js, line 25 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jws/lib/data-stream.js:25
Taint Flags:

```
No snippet available
```

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/daemon.js, line 339 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/ daemon.js:339
Taint Flags:

```
No snippet available
```

Password Management: Password in Comment	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/daemon.js, line 378 (Password Management: Password in Comment)	**Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:378
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/daemon.js, line 433 (Password Management: Password in Comment)	**Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:433
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/daemon.js, line 776 (Password Management: Password in Comment)	**Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/daemon.js:776
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/binaries.js, line 19 (Password Management: Password in Comment)	**Low**

Issue Details

Password Management: Password in Comment	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/binaries.js, line 19 (Password Management: Password in Comment)	Low

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/binaries.js:19
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/binaries.js, line 47 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/binaries.js:47
Taint Flags:

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/winsw.js, line 3 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/winsw.js:3
Taint Flags:

```
No snippet available
```

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/pg/lib/defaults.js, line 13 (Password Management: Password in Comment)	Low

Issue Details

Password Management: Password in Comment	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/pg/lib/defaults.js, line 13 (Password Management: Password in Comment)	Low

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/pg/lib/defaults.js:13
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/pg/lib/connection-parameters.js, line 69 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/pg/lib/connection-parameters.js:69
Taint Flags:

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js, line 73 (Password Management: Password in Comment)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: Comment
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js:73
Taint Flags:

`No snippet available`

Poor Logging Practice: Use of a System Output Stream (2 issues)

Abstract

Using `process.stdout` or `process.stderr` rather than a dedicated logging facility makes it difficult to monitor the behavior of the program.

Explanation

Example 1: A simple program an early Node.js developer may write to read from stdin and write it back to stdout again may look like the following:

```
process.stdin.on('readable', function(){
    var s = process.stdin.read();
    if (s != null){
      process.stdout.write(s);
    }
});
```

While most programmers go on to learn many nuances and subtleties about JavaScript and Node.js in particular, many will hang on to this first lesson and never give up on writing messages to standard output using `process.stdout.write()`. The problem is that writing directly to standard output or standard error is often used as an unstructured form of logging. Structured logging facilities provide features like logging levels, uniform formatting, a logger identifier, timestamps, and, perhaps most critically, the ability to direct the log messages to the right place. When the use of system output streams is jumbled together with the code that uses loggers properly, the result is often a well-kept log that is missing critical information. Developers widely accept the need for structured logging, but many continue to use system output streams in their "pre-production" development. If the code you are reviewing is past the initial phases of development, use of `process.stdout` or `process.stderr` may indicate an oversight in the move to a structured logging system.

Recommendation

Use a Node.js logging facility rather than `process.stdout` or `process.stderr`. **Example 2:** For example, the application can be rewritten as the following:

```
process.stdin.on('readable', function(){
  var s = process.stdin.read();
  if (s !== null && s !== undefined){
    console.log(s);
  }
});
```

This is not ideal, as it is still basic information, not including a timestamp, process ID or any other information, and inserts user-controlled data into the log. A third party library for logging such as "Winston" or "Bunyan" is best, but if only a timestamp is required for your particular situation, the following may be suitable:

```
log = function(msg){
  if (msg !== null && msg !== undefined){
    console.log('[' + new Date() + '] ' + msg);
  }
}

process.stdin.on('readable', function(){
  var s = process.stdin.read();
  if (s !== null && s !== undefined){
    log("User input read");
  } else {
    log("Waiting for user input");
  }
});
```

Issue Summary
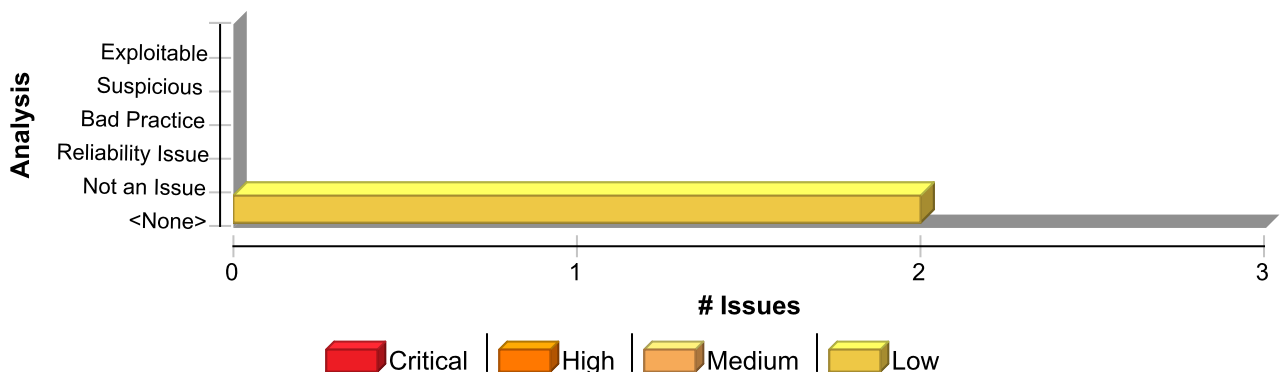
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Poor Logging Practice: Use of a System Output Stream	2	0	0	2
Total	**2**	**0**	**0**	**2**

Poor Logging Practice: Use of a System Output Stream	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ csurf/node_modules/depd/index.js, line 244 (Poor Logging Practice: Use of a System Output Stream)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: write
Enclosing Method: log()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/csurf/node_modules/ depd/index.js:244
Taint Flags:

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ depd/index.js, line 260 (Poor Logging Practice: Use of a System Output Stream)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: write
Enclosing Method: log()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/depd/index.js:260
Taint Flags:

`No snippet available`

Race Condition (4 issues)

Abstract

The set callback could lead to a race condition.

Explanation

Node.js allows developers to assign callbacks to IO-blocked events. This allows better performance as the callbacks run asynchronously such that the main application isn't blocked by IO. However, this in turn may lead to race conditions when something outside the callback relies upon code within the callback to be run first. **Example 1:** The following code checks a user against a database for authentication.

```
...
var authenticated = true;
...
database_connect.query('SELECT * FROM users WHERE name == ? AND password = ?
LIMIT 1', userNameFromUser, passwordFromUser, function(err, results){
  if (!err && results.length > 0){
    authenticated = true;
  }else{
    authenticated = false;
  }
});

if (authenticated){
  //do something privileged stuff
  authenticatedActions();
}else{
  sendUnathenticatedMessage();
}
```

In this example we're supposed to be calling to a backend database to confirm a user's credentials for login, and if confirmed we set a variable to `true`, otherwise `false`. Unfortunately, since the callback is blocked by IO, it will run asynchronously and may be run after the check to `if (authenticated)`, and since the default was true, it will go into the if-statement whether the user is actually authenticated or not.

Recommendation

When creating Node.js applications you must be careful of IO-blocked events and what functionality the related callbacks perform. There may be a series of callbacks that need to be called in a certain order, or code that can only be reached once a certain callback is run. **Example 2:** The following code fixes the race condition in `Example 1`.

```
...
database_connect.query('SELECT * FROM users WHERE name == ? AND password = ?
LIMIT 1', userNameFromUser, passwordFromUser, function(err, results){
  if (!err && results.length > 0){
    // do privileged stuff
    authenticatedActions();
  }else{
    sendUnauthenticatedMessage();
  }
});
...
```

This is a simple example and real life scenarios may be far more complex and fixing them may require a larger refactoring of the codebase. A simple way to try and avoid these problems is by using APIs that utilize `promises`, as they represent the eventual outcome of asynchronous operations, and allow you to specify a callback for success and a callback for failure. If this piece of code is to be used often, it's best to create an API that returns a `promise` for the authentication, so the code the developer needs to write could be simplified to:

```
promiseAuthentication()
.then(authenticatedActions, sendUnauthenticatedMessage);
```

This in turn makes it easier to follow the code and prevent race conditions, as the code will always run in a clearly defined order.

Issue Summary
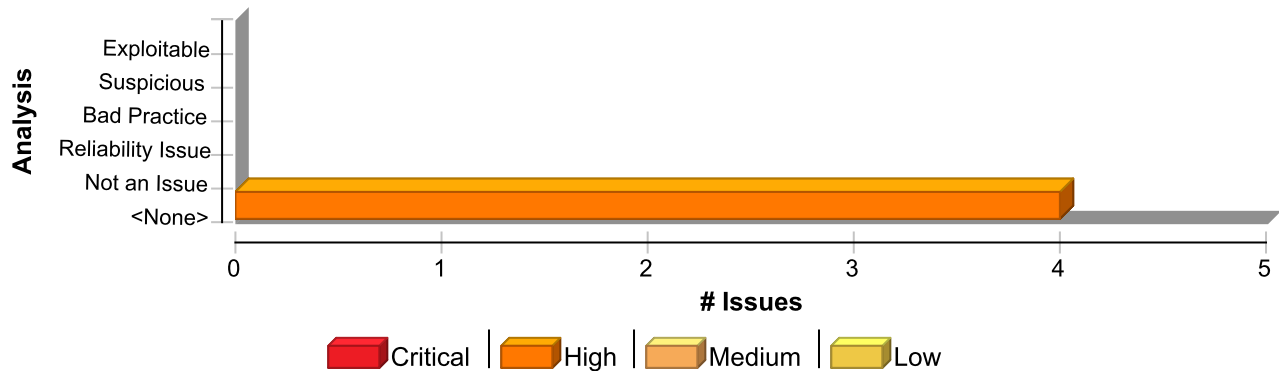
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Race Condition	4	0	0	4
Total	**4**	**0**	**0**	**4**

Race Condition	High

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/request.js, line 888 (Race Condition)	High

 Issue Details

Race Condition	High

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/request.js, line 888 (Race Condition)	High

Kingdom: Time and State
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: on
Enclosing Method: onRequestResponse()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:888
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/request.js, line 1086 (Race Condition)	High

Issue Details

Kingdom: Time and State
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: on
Enclosing Method: onRequestResponse()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:1086
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/request.js, line 888 (Race Condition)	High

Issue Details

Kingdom: Time and State
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: on
Enclosing Method: onRequestResponse()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:888
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/request.js, line 888 (Race Condition)	High

Issue Details

Kingdom: Time and State
Scan Engine: SCA (Structural)

Sink Details

Race Condition	High
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.request	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/request.js, line 888 (Race Condition)	**High**

Sink: FunctionPointerCall: on
Enclosing Method: onRequestResponse()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/request.js:888
Taint Flags:

`No snippet available`

System Information Leak: External (42 issues)

Abstract

Revealing system data or debugging information could enable an adversary to use system information to plan an attack.

Explanation

An external information leak occurs when system data or debug information leaves the program to a remote machine via a socket or network connection. External leaks can help an attacker by revealing specific data about operating systems, full pathnames, the existence of usernames, or locations of configuration files, and are more serious than internal information leaks, which are more difficult for an attacker to access. **Example 1:** The following code leaks Exception information into a text area within a web page:

```
...
dirReader.readEntries(function(results){
  ...
}, function(error){
  $("#myTextArea").val('There was a problem: ' + error);
});
...
```

This information can be exposed to a remote user. In some cases, the error message provides the attacker with the precise type of attack to which the system is vulnerable. For example, a database error message can reveal that the application is vulnerable to a SQL injection attack. Other error messages can reveal more oblique clues about the system. In Example 1, the leaked information could imply information about the type of operating system, the applications installed on the system, and the amount of care that the administrators have put into configuring the program.

Recommendation

Write error messages with security in mind. In production environments, turn off detailed error information in favor of brief messages. Restrict the generation and storage of detailed output that can help administrators and programmers diagnose problems. Debug traces can sometimes appear in non-obvious places (embedded in comments in the HTML for an error page, for example). Even brief error messages that do not reveal stack traces or database dumps can potentially aid an attacker. For example, an "Access Denied" message can reveal that a file or user exists on the system. Because of this, never send information to a resource directly outside the program.

Issue Summary
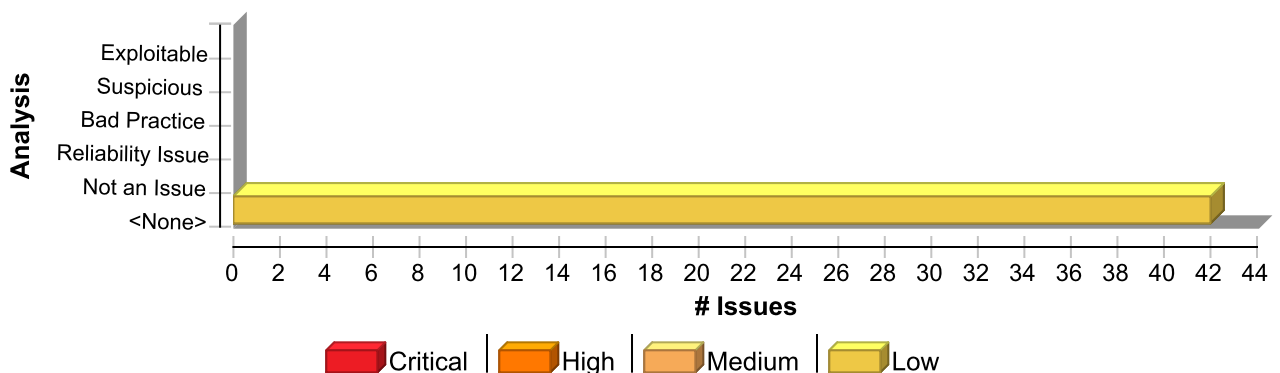
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
System Information Leak: External	42	0	0	42
Total	**42**	**0**	**0**	**42**

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js, line 243 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:241

```
238   axios_post({}).then((result) => {
239   console.log(result);
240   res.send({ "Server Start Time": server_start_time, "Database connected":
      result["Database connected"], "DBServer Start Time": result["DBServer Start
      Time"] })
241   }).catch((err) => {
242   console.log(err);
243   res.send({ "Server Start Time": server_start_time, "Database connected":
      false,err })
244   })
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:243
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js, line 243 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:241

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js, line 243 (System Information Leak: External)	Low

```
238   axios_post({}).then((result) => {
239   console.log(result);
240   res.send({ "Server Start Time": server_start_time, "Database connected":
result["Database connected"], "DBServer Start Time": result["DBServer Start
Time"] })
241   }).catch((err) => {
242   console.log(err);
243   res.send({ "Server Start Time": server_start_time, "Database connected":
false,err })
244   })
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:243
Taint Flags: SYSTEMINFO

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1384 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1382

```
1379   ).then(function (result) {
1380   delete result.data.content.data
1381   res.send(result.data);
1382   }).catch(function (reason) {
1383   console.log(reason);
1384   res.send(reason);
1385   });
```

Sink Details

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1384 (System Information Leak: External)	Low

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1384
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1404 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1402

```
1399   ).then(function (result) {
1400   delete result.data.content.data
1401   res.send(result.data);
1402   }).catch(function (reason) {
1403   console.log(reason);
1404   res.send(reason);
1405   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1404
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1425 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1423

System Information Leak: External	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1425 (System Information Leak: External)	Low

```
1420  ).then(function (result) {
1421  delete result.data.content.data
1422  res.send(result.data);
1423  }).catch(function (reason) {
1424  console.log(reason);
1425  res.send(reason);
1426  });
```

Sink Details

> **Sink:** ~JS_Generic.send()
> **Enclosing Method:** lambda()
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1425
> **Taint Flags:** SYSTEMINFO

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1445 (System Information Leak: External)	Low

Issue Details

> **Kingdom:** Encapsulation
> **Scan Engine:** SCA (Data Flow)

Source Details

> **Source:** lambda(0)
> **From:** lambda
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1443

```
1440  ).then(function (result) {
1441  delete result.data.content.data
1442  res.send(result.data);
1443  }).catch(function (reason) {
1444  console.log(reason);
1445  res.send(reason);
1446  });
```

Sink Details

> **Sink:** ~JS_Generic.send()
> **Enclosing Method:** lambda()
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1445
> **Taint Flags:** SYSTEMINFO

No snippet available

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1468 (System Information Leak: External)	**Low**

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1466

```
1463   // delete result.data.content.data
1464   result.data.content.data
1465   res.send(result.data);
1466   }).catch(function (reason) {
1467   console.log(reason);
1468   res.send(reason);
1469   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1468
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1361 (System Information Leak: External)	**Low**

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js :1359

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1361 (System Information Leak: External)	Low

```
1356  ).then(function (result) {
1357  delete result.data.content.data
1358  res.send(result.data);
1359  }).catch(function (reason) {
1360  console.log(reason);
1361  res.send(reason);
1362  });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1361
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1381 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1379

```
1376  ).then(function (result) {
1377  delete result.data.content.data
1378  res.send(result.data);
1379  }).catch(function (reason) {
1380  console.log(reason);
1381  res.send(reason);
1382  });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1381
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: External	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1400 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1398

```
1395    }).then(function (result) {
1396    delete result.data.content.data
1397    res.send(result.data);
1398    }).catch(function (reason) {
1399    console.log(reason);
1400    res.send(reason);
1401    });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1400
Taint Flags: SYSTEMINFO

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1420 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1418

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1420 (System Information Leak: External)	Low

```
1415   ).then(function (result) {
1416   delete result.data.content.data
1417   res.send(result.data);
1418   }).catch(function (reason) {
1419   console.log(reason);
1420   res.send(reason);
1421   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1420
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1443 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1441

```
1438   // delete result.data.content.data
1439   result.data.content.data
1440   res.send(result.data);
1441   }).catch(function (reason) {
1442   console.log(reason);
1443   res.send(reason);
1444   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1443
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1327 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1325

```
1322   }
1323   });
1324   })
1325   server_stream.on("error", (err) => {
1326   console.log(err.stack);
1327   res.send(err)
1328   })
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1327
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1304 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js :1302

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1304 (System Information Leak: External)	Low

```
1299    }
1300    });
1301    })
1302    server_stream.on("error", (err) => {
1303    console.log(err.stack);
1304    res.send(err)
1305    })
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1304
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 844 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:842

```
839    ).then(function (result) {
840    console.log(result.data);
841    res.send({ success: true, content: result.data.content });
842    }).catch(function (reason) {
843    console.log('Check File Version Error');
844    res.send({ success: false, content: reason });
845    });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:844
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: External	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 879 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:877

```
874   ).then(function (result) {
875   var connect = result.data.content
876   res.send({ success: true, connect });
877   }).catch(function (reason) {
878   console.log('Select table Error');
879   res.send({ success: false, content: reason });
880   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:879
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 893 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:891

```
888   headers: { 'Content-Type': 'application/json' }
889   }).then(function (result) {
890   res.send({ success: true, content: result.data.content });
891   }).catch(function (reason) {
892   console.log('List table Error');
893   res.send({ success: false, content: reason });
894   });
```

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 893 (System Information Leak: External)	Low

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:893
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1019 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1017

```
1014  ).then((result) => {
1015  console.log(result.data);
1016  res.send({ success: true, file_obj: upload_result.file_obj, uid:
upload_result.data.uuid })
1017  }).catch((reason) => {
1018  if (reason) console.log(reason);
1019  res.send({ success: false, content: reason });
1020  })
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1019
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1111 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1111 (System Information Leak: External)	Low

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1109

```
1106  }).then(function (result) {
1107  var connect = result.data.content
1108  res.send({ success: true, connect });
1109  }).catch(function (reason) {
1110  console.log('trainrecord_download_plus Error');
1111  res.send({ success: false, content: reason });
1112  });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1111
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1126 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1124

```
1121  }).then(function (result) {
1122  var connect = result.data.content
1123  res.send({ success: true, connect });
1124  }).catch(function (reason) {
1125  console.log('List table Error');
1126  res.send({ success: false, content: reason });
1127  });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1126
Taint Flags: SYSTEMINFO

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1126 (System Information Leak: External)	Low

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1143 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1141

```
1138  ).then(function (result) {
1139  var connect = result.data.content
1140  res.send({ success: true, connect });
1141  }).catch(function (reason) {
1142  console.log('List table Error');
1143  res.send({ success: false, content: reason });
1144  });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1143
Taint Flags: SYSTEMINFO

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1157 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1155

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1157 (System Information Leak: External)	Low

```
1152   headers: { 'Content-Type': 'application/json' }
1153   }).then(function (result) {
1154   res.send({ success: true, content: result.data.content });
1155   }).catch(function (reason) {
1156   console.log('List table Error');
1157   res.send({ success: false, content: reason });
1158   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1157
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1184 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1182

```
1179   ).then(function (result) {
1180   console.log('NPC             ');
1181   res.send({ success: true, file_uuid: upload_result.data.file_uuid,
file_fullname: upload_result.data.fullname });
1182   }).catch(function (reason) {
1183   console.log('Insert Into table Error');
1184   res.send({ success: false, content: reason });
1185   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1184
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1207 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1205

```
1202  ).then(function (result) {
1203  var connect = result.data.content
1204  res.send({ success: true, connect });
1205  }).catch(function (reason) {
1206  console.log('Select table Error');
1207  res.send({ success: false, content: reason });
1208  });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1207
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1224 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1222

```
1219  ).then(function (result) {
1220  var connect = result.data.content
1221  res.send({ success: true, connect });
1222  }).catch(function (reason) {
1223  console.log('Select table Error');
1224  res.send({ success: false, content: reason });
1225  });
```

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js, line 1224 (System Information Leak: External)	Low

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1224
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js, line 1241 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1239

```
1236  ).then(function (result) {
1237  console.log(result.data);
1238  res.send({ success: true, content: result.data.content });
1239  }).catch(function (reason) {
1240  console.log('List table Error');
1241  res.send({ success: false, content: reason });
1242  });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1241
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js, line 1281 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1279

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1281 (System Information Leak: External)	Low

```
1276   if (!result.state) {
1277   res.send({ success: true, connect: result.data.result });
1278   }
1279   }).catch(function (reason) {
1280   console.log(reason);
1281   res.send({ success: false, Error_msg: reason });
1282   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1281
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1364 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1362

```
1359   }
1360   ).then(function (result) {
1361   res.send(result.data);
1362   }).catch(function (reason) {
1363   console.log('Delete Error');
1364   res.send({ success: false, content: reason });
1365   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1364
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 823 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:821

```
818  ).then(function (result) {
819  console.log(result.data);
820  res.send({ success: true, content: result.data.content });
821  }).catch(function (reason) {
822  console.log('Check File Version Error');
823  res.send({ success: false, content: reason });
824  });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:823
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 858 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:856

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 858 (System Information Leak: External)	Low

```
853    ).then(function (result) {
854    var connect = result.data.content
855    res.send({ success: true, connect });
856    }).catch(function (reason) {
857    console.log('Select table Error');
858    res.send({ success: false, content: reason });
859    });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:858
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 872 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:870

```
867    headers: { 'Content-Type': 'application/json' }
868    }).then(function (result) {
869    res.send({ success: true, content: result.data.content });
870    }).catch(function (reason) {
871    console.log('List table Error');
872    res.send({ success: false, content: reason });
873    });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:872
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 998 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:996

```
993   ).then((result) => {
994   console.log(result.data);
995   res.send({ success: true, file_obj: upload_result.file_obj, uid:
upload_result.data.uuid })
996   }).catch((reason) => {
997   if (reason) console.log(reason);
998   res.send({ success: false, content: reason });
999   })
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:998
Taint Flags: SYSTEMINFO

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1090 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1088

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1090 (System Information Leak: External)	Low

```
1085   }).then(function (result) {
1086   var connect = result.data.content
1087   res.send({ success: true, connect });
1088   }).catch(function (reason) {
1089   console.log('trainrecord_download_plus Error');
1090   res.send({ success: false, content: reason });
1091   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1090
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1105 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js :1103

```
1100   }).then(function (result) {
1101   var connect = result.data.content
1102   res.send({ success: true, connect });
1103   }).catch(function (reason) {
1104   console.log('List table Error');
1105   res.send({ success: false, content: reason });
1106   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1105
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1122 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1120

```
1117  ).then(function (result) {
1118  var connect = result.data.content
1119  res.send({ success: true, connect });
1120  }).catch(function (reason) {
1121  console.log('List table Error');
1122  res.send({ success: false, content: reason });
1123  });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1122
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1136 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1134

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1136 (System Information Leak: External)	Low

```
1131   headers: { 'Content-Type': 'application/json' }
1132   }).then(function (result) {
1133   res.send({ success: true, content: result.data.content });
1134   }).catch(function (reason) {
1135   console.log('List table Error');
1136   res.send({ success: false, content: reason });
1137   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1136
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1163 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1161

```
1158   ).then(function (result) {
1159   console.log('NPC              ');
1160   res.send({ success: true, file_uuid: upload_result.data.file_uuid,
file_fullname: upload_result.data.fullname });
1161   }).catch(function (reason) {
1162   console.log('Insert Into table Error');
1163   res.send({ success: false, content: reason });
1164   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1163
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: External	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1184 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1182

```
1179   }).then(function (result) {
1180   var connect = result.data.content
1181   res.send({ success: true, connect });
1182   }).catch(function (reason) {
1183   console.log('Select table Error');
1184   res.send({ success: false, content: reason });
1185   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1184
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1201 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1199

System Information Leak: External	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1201 (System Information Leak: External)	Low

```
1196  ).then(function (result) {
1197  var connect = result.data.content
1198  res.send({ success: true, connect });
1199  }).catch(function (reason) {
1200  console.log('Select table Error');
1201  res.send({ success: false, content: reason });
1202  });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1201
Taint Flags: SYSTEMINFO

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1218 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js :1216

```
1213  ).then(function (result) {
1214  console.log(result.data);
1215  res.send({ success: true, content: result.data.content });
1216  }).catch(function (reason) {
1217  console.log('List table Error');
1218  res.send({ success: false, content: reason });
1219  });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1218
Taint Flags: SYSTEMINFO

```
No snippet available
```

System Information Leak: External	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1258 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1256

```
1253   if (!result.state) {
1254   res.send({ success: true, connect: result.data.result });
1255   }
1256   }).catch(function (reason) {
1257   console.log(reason);
1258   res.send({ success: false, Error_msg: reason });
1259   });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1258
Taint Flags: SYSTEMINFO

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1341 (System Information Leak: External)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1339

System Information Leak: External	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1341 (System Information Leak: External)	Low

```
1336    }
1337    ).then(function (result) {
1338    res.send(result.data);
1339    }).catch(function (reason) {
1340    console.log('Delete Error');
1341    res.send({ success: false, content: reason });
1342    });
```

Sink Details

Sink: ~JS_Generic.send()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1341
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: Internal (50 issues)

Abstract

Revealing system data or debugging information could enable an adversary to use system information to plan an attack.

Explanation

An internal information leak occurs when system data or debug information is sent to a local file, console, or screen via printing or logging. **Example 1:** The following code writes an exception to the standard error stream:

```
var http = require('http');
...

http.request(options, function(res){
  ...
}).on('error', function(e){
  console.log('There was a problem with the request: ' + e);
});
...
```

Depending upon the system configuration, this information can be dumped to a console, written to a log file, or exposed to a user. In some cases, the error message provides the attacker with the precise type of attack to which the system is vulnerable. For example, a database error message can reveal that the application is vulnerable to a SQL injection attack. Other error messages can reveal more oblique clues about the system. In `Example 1`, the leaked information could imply information about the type of operating system, the applications installed on the system, and the amount of care that the administrators have put into configuring the program.

Recommendation

Write error messages with security in mind. In production environments, turn off detailed error information in favor of brief messages. Restrict the generation and storage of detailed output that can help administrators and programmers diagnose problems. Debug traces can sometimes appear in non-obvious places (embedded in comments in the HTML for an error page, for example). Even brief error messages that do not reveal stack traces or database dumps can potentially aid an attacker. For example, an "Access Denied" message can reveal that a file or user exists on the system.

Issue Summary
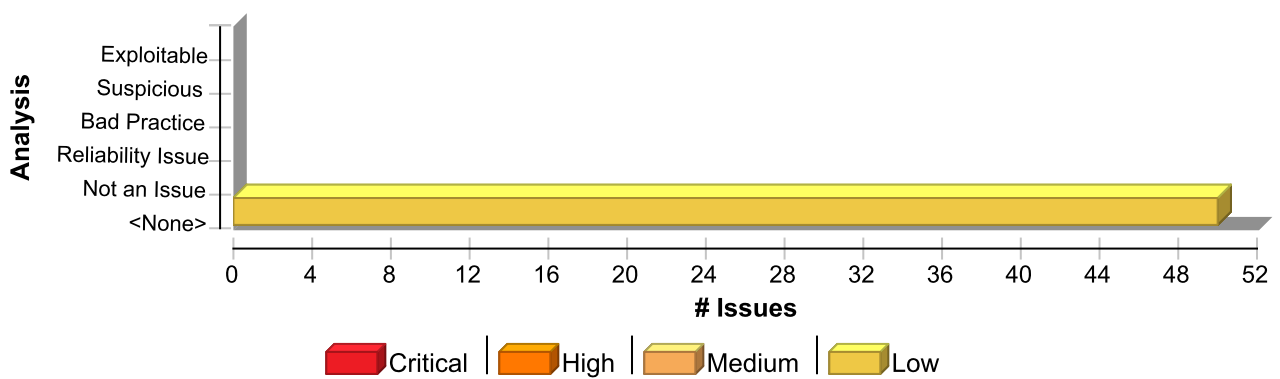
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
System Information Leak: Internal	50	0	0	50
Total	**50**	**0**	**0**	**50**

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js, line 204 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:203

```
200   start: 0,
201   end: 2
202   });
203   readStream.on('error', function (err) {
204   console.log("readStream" + err);
205   console.log(err);
206   next();
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:204
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js, line 204 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:203

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js, line 204 (System Information Leak: Internal)	Low

```
200    start: 0,
201    end: 2
202    });
203    readStream.on('error', function (err) {
204    console.log("readStream" + err);
205    console.log(err);
206    next();
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:204
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js, line 20 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js:19

```
16    // nodeOptions: ["--port=11506"],
17    });
18
19    svc.on('error', (err) => {
20    console.error(`Service ${serviceName} registration failed:`, err);
21    resolve(-1);
22    });
```

Sink Details

Sink: ~JS_Generic.error()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js:20
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

System Information Leak: Internal	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD	

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js, line 55 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js:54

```
51   });
52
53
54   svc.on('error', (err) => {
55   console.error(`Service ${serviceName} registration failed:`, err);
56   resolve(-1);
57   });
```

Sink Details

Sink: ~JS_Generic.error()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js:55
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js, line 92 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js:91

```
88   });
89
90
91   svc.on('error', (err) => {
92   console.error(`Service ${serviceName} registration failed:`, err);
93   resolve(-1);
94   });
```

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js, line 92 (System Information Leak: Internal)	Low

Sink Details

Sink: ~JS_Generic.error()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service.js:92
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js, line 20 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js:19

```
16   // nodeOptions: ["--port=11506"],
17   });
18
19   svc.on('error', (err) => {
20   console.error(`Service ${serviceName} registration failed:`, err);
21   resolve(-1);
22   });
```

Sink Details

Sink: ~JS_Generic.error()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js:20
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js, line 72 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js:71

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js, line 72 (System Information Leak: Internal)	Low

```
68  });
69
70
71  svc.on('error', (err) => {
72  console.error(`Service ${serviceName} registration failed:`, err);
73  resolve(-1);
74  });
```

Sink Details

Sink: ~JS_Generic.error()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js:72
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js, line 125 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js:124

```
121  });
122
123
124  svc.on('error', (err) => {
125  console.error(`Service ${serviceName} registration failed:`, err);
126  resolve(-1);
127  });
```

Sink Details

Sink: ~JS_Generic.error()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/service_un.js:125
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js, line 205 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:203

```
200   start: 0,
201   end: 2
202   });
203   readStream.on('error', function (err) {
204   console.log("readStream" + err);
205   console.log(err);
206   next();
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:205
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js, line 205 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:203

```
200   start: 0,
201   end: 2
202   });
203   readStream.on('error', function (err) {
204   console.log("readStream" + err);
205   console.log(err);
206   next();
```

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js, line 205 (System Information Leak: Internal)	Low

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:205
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js, line 174 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js:164

```
161  }
162 });
163
164 server.on('error', function (e) {
165  if (e.code === 'EADDRINUSE') {
166  console.log('Error: Port %d is already in use, select a different
port.', port);
167  console.log('Example: node server.js --port %d', port + 1);
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/log.js:174
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js, line 426 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js, line 426 (System Information Leak: Internal)	Low

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:416

```
413  }
414  });
415
416  server.on('error', function (e) {
417  if (e.code === 'EADDRINUSE') {
418  console.log('Error: Port %d is already in use, select a different
port.', argv.port);
419  console.log('Example: node server.js --port %d', argv.port + 1);
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:426
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js, line 426 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:416

```
413  }
414  });
415
416  server.on('error', function (e) {
417  if (e.code === 'EADDRINUSE') {
418  console.log('Error: Port %d is already in use, select a different
port.', argv.port);
419  console.log('Example: node server.js --port %d', argv.port + 1);
```

Sink Details

System Information Leak: Internal	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD	

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js, line 426 (System Information Leak: Internal)	Low

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:426
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js, line 242 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:241

```
238   axios_post({}).then((result) => {
239   console.log(result);
240   res.send({ "Server Start Time": server_start_time, "Database connected":
result["Database connected"], "DBServer Start Time": result["DBServer Start
Time"] })
241   }).catch((err) => {
242   console.log(err);
243   res.send({ "Server Start Time": server_start_time, "Database connected":
false,err })
244   })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/server.js:242
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js, line 242 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

System Information Leak: Internal	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js, line 242 (System Information Leak: Internal)	Low

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:241

```
238   axios_post({}).then((result) => {
239   console.log(result);
240   res.send({ "Server Start Time": server_start_time, "Database connected":
result["Database connected"], "DBServer Start Time": result["DBServer Start
Time"] })
241   }).catch((err) => {
242   console.log(err);
243   res.send({ "Server Start Time": server_start_time, "Database connected":
false,err })
244   })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/temp_server.js:242
Taint Flags: SYSTEMINFO

```
No snippet available
```

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.node-windows.lib	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/winsw.js, line 77 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: Read process.execPath
From: generateXml
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/winsw.js:72

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ node-windows/lib/winsw.js, line 77 (System Information Leak: Internal)	Low

```
69    {id: config.id},
70    {name: config.name},
71    {description: config.description||''},
72    {executable: config.execPath || process.execPath}
73    ];
74
75    multi('argument',config.nodeOptions, ' ');
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: generateXml()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/node-windows/lib/winsw.js:77
Taint Flags: SYSTEMINFO

```
No snippet available
```

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1326 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1325

```
1322    }
1323    });
1324    })
1325    server_stream.on("error", (err) => {
1326    console.log(err.stack);
1327    res.send(err)
1328    })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1326
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1326 (System Information Leak: Internal)	Low

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1303 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js :1302

```
1299    }
1300    });
1301    })
1302    server_stream.on("error", (err) => {
1303    console.log(err.stack);
1304    res.send(err)
1305    })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1303
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 162 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:161

System Information Leak: Internal	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 162 (System Information Leak: Internal)	Low

```
158   } else {
159   return resolve(result.data)
160   }
161   }).catch((reason) => {
162   if (reason) console.log(reason);
163   return resolve({ success: false, content: reason });
164   })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:162
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 321 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:320

```
317   } else {
318   return resolve(result.data)
319   }
320   }).catch((reason) => {
321   if (reason) console.log(reason);
322   return resolve({ success: false, content: reason });
323   })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:321
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 462 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:461

```
458   } else {
459   return resolve(result.data)
460   }
461   }).catch((reason) => {
462   if (reason) console.log(reason);
463   return resolve({ success: false, content: reason });
464   })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:462
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 612 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:611

```
608   } else {
609   return resolve(result.data)
610   }
611   }).catch((reason) => {
612   if (reason) console.log(reason);
613   return resolve({ success: false, content: reason });
614   })
```

System Information Leak: Internal	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 612 (System Information Leak: Internal)	Low

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:612
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1018 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1017

```
1014   ).then((result) => {
1015   console.log(result.data);
1016   res.send({ success: true, file_obj: upload_result.file_obj, uid:
upload_result.data.uuid })
1017   }).catch((reason) => {
1018   if (reason) console.log(reason);
1019   res.send({ success: false, content: reason });
1020   })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1018
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1260 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1260 (System Information Leak: Internal)	Low

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1259

```
1256  ).then(function (result) {
1257  console.log(result);
1258  res.send(result.data);
1259  }).catch(function (reason) {
1260  console.log(reason);
1261  res.send({ success: false });
1262  });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1260
Taint Flags: SYSTEMINFO

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1280 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1279

```
1276  if (!result.state) {
1277  res.send({ success: true, connect: result.data.result });
1278  }
1279  }).catch(function (reason) {
1280  console.log(reason);
1281  res.send({ success: false, Error_msg: reason });
1282  });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1280
Taint Flags: SYSTEMINFO

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1280 (System Information Leak: Internal)	Low

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1346 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1345

```
1342   else {
1343   res.send({ success: false, Error_msg: 'file_uuid cannot found' })
1344   }
1345   }).catch(function (reason) {
1346   console.log(reason);
1347   res.send({ success: false, Error_msg: 'Post Error' });
1348   });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1346
Taint Flags: SYSTEMINFO

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1383 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1382

System Information Leak: Internal	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js, line 1383 (System Information Leak: Internal)	Low

```
1379   ).then(function (result) {
1380   delete result.data.content.data
1381   res.send(result.data);
1382   }).catch(function (reason) {
1383   console.log(reason);
1384   res.send(reason);
1385   });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1383
Taint Flags: SYSTEMINFO

No snippet available

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js, line 1403 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1402

```
1399   ).then(function (result) {
1400   delete result.data.content.data
1401   res.send(result.data);
1402   }).catch(function (reason) {
1403   console.log(reason);
1404   res.send(reason);
1405   });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1403
Taint Flags: SYSTEMINFO

No snippet available

System Information Leak: Internal	Low

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1424 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1423

```
1420   ).then(function (result) {
1421   delete result.data.content.data
1422   res.send(result.data);
1423   }).catch(function (reason) {
1424   console.log(reason);
1425   res.send(reason);
1426   });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1424
Taint Flags: SYSTEMINFO

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1444 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1443

```
1440   ).then(function (result) {
1441   delete result.data.content.data
1442   res.send(result.data);
1443   }).catch(function (reason) {
1444   console.log(reason);
1445   res.send(reason);
1446   });
```

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1444 (System Information Leak: Internal)	Low

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1444
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ api.router.js, line 1467 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1466

```
1463   // delete result.data.content.data
1464   result.data.content.data
1465   res.send(result.data);
1466   }).catch(function (reason) {
1467   console.log(reason);
1468   res.send(reason);
1469   });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/api.router.js:1467
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 152 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js :151

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 152 (System Information Leak: Internal)	Low

```
148    } else {
149    return resolve(result.data)
150    }
151    }).catch((reason) => {
152    if (reason) console.log(reason);
153    return resolve({ success: false, content: reason });
154    })
```

Sink Details

> **Sink:** ~JS_Generic.log()
> **Enclosing Method:** lambda()
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:152
> **Taint Flags:** SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 179 (System Information Leak: Internal)	Low

Issue Details

> **Kingdom:** Encapsulation
> **Scan Engine:** SCA (Data Flow)

Source Details

> **Source:** lambda(0)
> **From:** lambda
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
> :178

```
175    } else {
176    return resolve(result.data)
177    }
178    }).catch((reason) => {
179    if (reason) console.log(reason);
180    return resolve({ success: false, content: reason });
181    })
```

Sink Details

> **Sink:** ~JS_Generic.log()
> **Enclosing Method:** lambda()
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:179
> **Taint Flags:** SYSTEMINFO

`No snippet available`

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 310 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js :309

```
306   } else {
307   return resolve(result.data)
308   }
309   }).catch((reason) => {
310   if (reason) console.log(reason);
311   return resolve({ success: false, content: reason });
312   })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:310
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 444 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js :443

System Information Leak: Internal	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 444 (System Information Leak: Internal)	Low

```
440   } else {
441   return resolve(result.data)
442   }
443   }).catch((reason) => {
444   if (reason) console.log(reason);
445   return resolve({ success: false, content: reason });
446   })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:444
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 471 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:470

```
467   } else {
468   return resolve(result.data)
469   }
470   }).catch((reason) => {
471   if (reason) console.log(reason);
472   return resolve({ success: false, content: reason });
473   })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:471
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: Internal	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 591 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:590

```
587   } else {
588   return resolve(result.data)
589   }
590   }).catch((reason) => {
591   if (reason) console.log(reason);
592   return resolve({ success: false, content: reason });
593   })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:591
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 997 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:996

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 997 (System Information Leak: Internal)	Low

```
993  ).then((result) => {
994  console.log(result.data);
995  res.send({ success: true, file_obj: upload_result.file_obj, uid:
     upload_result.data.uuid })
996  }).catch((reason) => {
997  if (reason) console.log(reason);
998  res.send({ success: false, content: reason });
999  })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:997
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1237 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1236

```
1233  ).then(function (result) {
1234  console.log(result);
1235  res.send(result.data);
1236  }).catch(function (reason) {
1237  console.log(reason);
1238  res.send({ success: false });
1239  });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1237
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: Internal	Low

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

| **D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1257 (System Information Leak: Internal)** | **Low** |

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1256

```
1253   if (!result.state) {
1254   res.send({ success: true, connect: result.data.result });
1255   }
1256   }).catch(function (reason) {
1257   console.log(reason);
1258   res.send({ success: false, Error_msg: reason });
1259   });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1257
Taint Flags: SYSTEMINFO

`No snippet available`

| **D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1323 (System Information Leak: Internal)** | **Low** |

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1322

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1323 (System Information Leak: Internal)	Low

```
1319   else {
1320   res.send({ success: false, Error_msg: 'file_uuid cannot found' })
1321   }
1322   }).catch(function (reason) {
1323   console.log(reason);
1324   res.send({ success: false, Error_msg: 'Post Error' });
1325   });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1323
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1360 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1359

```
1356   ).then(function (result) {
1357   delete result.data.content.data
1358   res.send(result.data);
1359   }).catch(function (reason) {
1360   console.log(reason);
1361   res.send(reason);
1362   });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1360
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1380 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1379

```
1376  ).then(function (result) {
1377  delete result.data.content.data
1378  res.send(result.data);
1379  }).catch(function (reason) {
1380  console.log(reason);
1381  res.send(reason);
1382  });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1380
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1399 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1398

System Information Leak: Internal	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.router	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1399 (System Information Leak: Internal)	Low

```
1395   }).then(function (result) {
1396   delete result.data.content.data
1397   res.send(result.data);
1398   }).catch(function (reason) {
1399   console.log(reason);
1400   res.send(reason);
1401   });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1399
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1419 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js :1418

```
1415   ).then(function (result) {
1416   delete result.data.content.data
1417   res.send(result.data);
1418   }).catch(function (reason) {
1419   console.log(reason);
1420   res.send(reason);
1421   });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1419
Taint Flags: SYSTEMINFO

`No snippet available`

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/ temp.api.router.js, line 1442 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js
:1441

```
1438   // delete result.data.content.data
1439   result.data.content.data
1440   res.send(result.data);
1441   }).catch(function (reason) {
1442   console.log(reason);
1443   res.send(reason);
1444   });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/router/temp.api.router.js:1442
Taint Flags: SYSTEMINFO

No snippet available

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/runtime.js, line 23 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/runtime.js:21

System Information Leak: Internal	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/runtime.js, line 23 (System Information Leak: Internal)	Low

```
18  }
19  ).then(function (result) {
20  console.log(result.data);
21  }).catch(function (reason) {
22  console.log('Check File Version Error');
23  console.log(reason);
24  });
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/runtime.js:23
Taint Flags: SYSTEMINFO

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js, line 72 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js:71

```
68  var c = new Client();
69  c.connect(settle);
70
71  c.on('error', function (e) {
72  console.log(e);
73  resolve({ success: false })
74  })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js:72
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

`No snippet available`

System Information Leak: Internal	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.util	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js, line 97 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js:96

```
93   var c = new Client();
94   c.connect(settle);
95
96   c.on('error', function (e) {
97   console.log(e);
98   resolve({ success: false })
99   })
```

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js:97
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

```
No snippet available
```

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js, line 122 (System Information Leak: Internal)	Low

Issue Details

Kingdom: Encapsulation
Scan Engine: SCA (Data Flow)

Source Details

Source: lambda(0)
From: lambda
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js:121

```
118   var c = new Client();
119   c.connect(settle);
120
121   c.on('error', function (e) {
122   console.log(e);
123   resolve({ success: false })
124   })
```

System Information Leak: Internal | Low

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js, line 122 (System Information Leak: Internal) | Low

Sink Details

Sink: ~JS_Generic.log()
Enclosing Method: lambda()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/util/ftp_client.js:122
Taint Flags: EXCEPTIONINFO, SYSTEMINFO

```
No snippet available
```

Weak Cryptographic Hash (27 issues)

Abstract

Weak cryptographic hashes cannot guarantee data integrity and should not be used in security-critical contexts.

Explanation

MD2, MD4, MD5, RIPEMD-160, and SHA-1 are popular cryptographic hash algorithms often used to verify the integrity of messages and other data. However, as recent cryptanalysis research has revealed fundamental weaknesses in these algorithms, they should no longer be used within security-critical contexts. Effective techniques for breaking MD and RIPEMD hashes are widely available, so those algorithms should not be relied upon for security. In the case of SHA-1, current techniques still require a significant amount of computational power and are more difficult to implement. However, attackers have found the Achilles' heel for the algorithm, and techniques for breaking it will likely lead to the discovery of even faster attacks.

Recommendation

Discontinue the use of MD2, MD4, MD5, RIPEMD-160, and SHA-1 for data-verification in security-critical contexts. Currently, SHA-224, SHA-256, SHA-384, SHA-512, and SHA-3 are good alternatives. However, these variants of the Secure Hash Algorithm have not been scrutinized as closely as SHA-1, so be mindful of future research that might impact the security of these algorithms.

Issue Summary
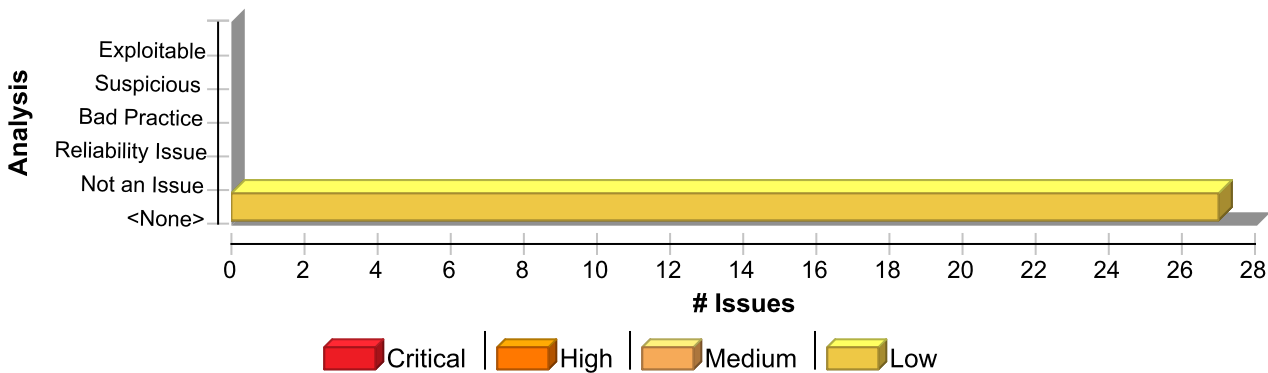
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Weak Cryptographic Hash	27	0	0	27
Total	**27**	**0**	**0**	**27**

Weak Cryptographic Hash	Low
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.aws-sign2	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ aws-sign2/index.js, line 71 (Weak Cryptographic Hash)	Low
Issue Details	

Weak Cryptographic Hash	Low

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ aws-sign2/index.js, line 71 (Weak Cryptographic Hash)	Low

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: hmacSha1
Enclosing Method: init^()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/aws-sign2/index.js:71
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ aws-sign2/index.js, line 87 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: hmacSha1
Enclosing Method: sign()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/aws-sign2/index.js:87
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ aws-sign2/index.js, line 103 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: hmacSha1
Enclosing Method: signQuery()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/aws-sign2/index.js:103
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ cookie-signature/index.js, line 42 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Weak Cryptographic Hash	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ cookie-signature/index.js, line 42 (Weak Cryptographic Hash)	Low

Sink Details

Sink: FunctionPointerCall: sha1
Enclosing Method: unsign()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/cookie-signature/index.js:42
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ cookie-signature/index.js, line 42 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: sha1
Enclosing Method: unsign()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/cookie-signature/index.js:42
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ cookie-signature/index.js, line 49 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: sha1
Enclosing Method: init^()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/cookie-signature/index.js:49
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ cookie-signature/index.js, line 50 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Weak Cryptographic Hash	Low

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.cookie-signature	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ cookie-signature/index.js, line 50 (Weak Cryptographic Hash)	Low

Sink: FunctionPointerCall: createHash
Enclosing Method: sha1()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/cookie-signature/ index.js:50
Taint Flags:

`No snippet available`

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.csrf	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ csrf/index.js, line 152 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: createHash
Enclosing Method: hash()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/csrf/index.js:152
Taint Flags:

`No snippet available`

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.express-session	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ express-session/index.js, line 608 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: createHash
Enclosing Method: hash()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/express-session/ index.js:608
Taint Flags:

`No snippet available`

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.oauth-sign	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ oauth-sign/index.js, line 86 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Weak Cryptographic Hash	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ oauth-sign/index.js, line 86 (Weak Cryptographic Hash)	Low

Sink Details

Sink: FunctionPointerCall: sha
Enclosing Method: hmacsign()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/oauth-sign/index.js:86
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ oauth-sign/index.js, line 3 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: sha
Enclosing Method: init^()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/oauth-sign/index.js:3
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ oauth-sign/index.js, line 96 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: sha
Enclosing Method: hmacsign256()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/oauth-sign/index.js:96
Taint Flags:

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/lib/oauth.js, line 70 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Weak Cryptographic Hash	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/oauth.js, line 70 (Weak Cryptographic Hash)	Low

Sink: FunctionPointerCall: createHash
Enclosing Method: buildBodyHash()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/oauth.js:70
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/helpers.js, line 31 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: createHash
Enclosing Method: md5()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/helpers.js:31
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js, line 96 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: md5
Enclosing Method: digest()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js:96
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/helpers.js, line 30 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: md5
Enclosing Method: init^()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/helpers.js:30
Taint Flags:

`No snippet available`

Weak Cryptographic Hash	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/lib/auth.js, line 97 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: md5
Enclosing Method: digest()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js:97
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/lib/auth.js, line 94 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: md5
Enclosing Method: digest()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js:94
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/lib/auth.js, line 84 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: md5
Enclosing Method: ha1Compute()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js:84
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ request/lib/auth.js, line 82 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Weak Cryptographic Hash	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js, line 82 (Weak Cryptographic Hash)	Low

> **Sink:** FunctionPointerCall: md5
> **Enclosing Method:** ha1Compute()
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/request/lib/auth.js:82
> **Taint Flags:**

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/sshpk/lib/utils.js, line 117 (Weak Cryptographic Hash)	Low

Issue Details

> **Kingdom:** Security Features
> **Scan Engine:** SCA (Structural)

Sink Details

> **Sink:** FunctionPointerCall: createHash
> **Enclosing Method:** opensslKeyDeriv()
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/sshpk/lib/utils.js:117
> **Taint Flags:**

`No snippet available`

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/sshpk/lib/formats/putty.js, line 143 (Weak Cryptographic Hash)	Low

Issue Details

> **Kingdom:** Security Features
> **Scan Engine:** SCA (Structural)

Sink Details

> **Sink:** FunctionPointerCall: createHash
> **Enclosing Method:** derivePPK2EncryptionKey()
> **File:** D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/sshpk/lib/formats/putty.js:143
> **Taint Flags:**

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/sshpk/lib/formats/putty.js, line 147 (Weak Cryptographic Hash)	Low

Issue Details

> **Kingdom:** Security Features
> **Scan Engine:** SCA (Structural)

Sink Details

Weak Cryptographic Hash	Low

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.sshpk.lib.formats	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ sshpk/lib/formats/putty.js, line 147 (Weak Cryptographic Hash)	**Low**

Sink: FunctionPointerCall: createHash
Enclosing Method: derivePPK2EncryptionKey()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/sshpk/lib/formats/putty.js:147
Taint Flags:

`No snippet available`

Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.uuid.dist	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ uuid/dist/md5.js, line 12 (Weak Cryptographic Hash)	**Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: md5
Enclosing Method: init^()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/uuid/dist/md5.js:12
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ uuid/dist/sha1.js, line 12 (Weak Cryptographic Hash)	**Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: sha1
Enclosing Method: init^()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/uuid/dist/sha1.js:12
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ uuid/dist/sha1.js, line 19 (Weak Cryptographic Hash)	**Low**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Weak Cryptographic Hash	Low

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ uuid/dist/sha1.js, line 19 (Weak Cryptographic Hash)	Low

Sink: FunctionPointerCall: createHash
Enclosing Method: sha1()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/uuid/dist/sha1.js:19
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ uuid/dist/md5.js, line 19 (Weak Cryptographic Hash)	Low

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: createHash
Enclosing Method: md5()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/uuid/dist/md5.js:19
Taint Flags:

`No snippet available`

Weak Encryption (4 issues)

Abstract

The identified call uses a weak encryption algorithm that cannot guarantee the confidentiality of sensitive data.

Explanation

Antiquated encryption algorithms such as DES no longer provide sufficient protection for use with sensitive data. Encryption algorithms rely on key size as one of the primary mechanisms to ensure cryptographic strength. Cryptographic strength is often measured by the time and computational power needed to generate a valid key. Advances in computing power have made it possible to obtain small encryption keys in a reasonable amount of time. For example, the 56-bit key used in DES posed a significant computational hurdle in the 1970s when the algorithm was first developed, but today DES can be cracked in less than a day using commonly available equipment.

Recommendation

Use strong encryption algorithms with large key sizes to protect sensitive data. A strong alternative to DES is AES (Advanced Encryption Standard, formerly Rijndael). Before selecting an algorithm, first determine if your organization has standardized on a specific algorithm and implementation.

Issue Summary
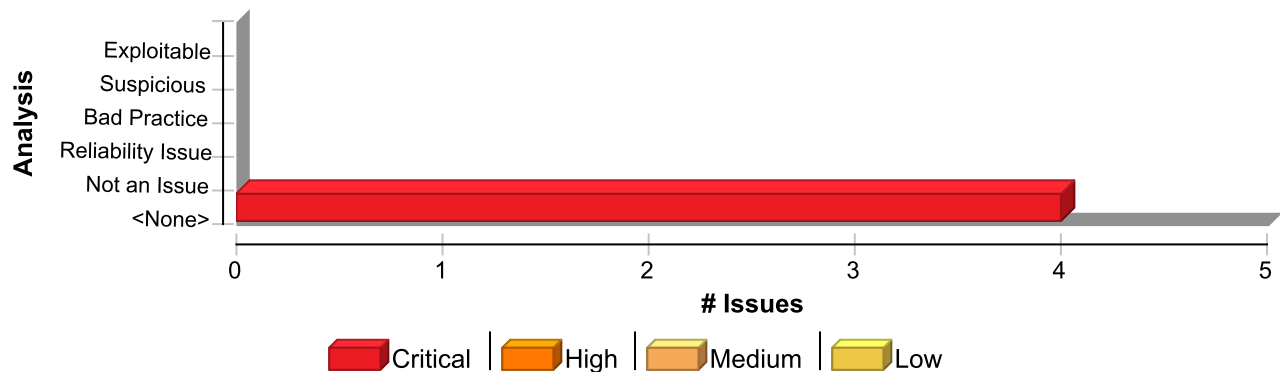
Engine Breakdown

	SCA	WebInspect	SecurityScope	Total
Weak Encryption	4	0	0	4
Total	**4**	**0**	**0**	**4**

Weak Encryption	Critical
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.jsbn	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ jsbn/index.js, line 1304 (Weak Encryption)	Critical
Issue Details	

Kingdom: Security Features
Scan Engine: SCA (Structural)

Weak Encryption	Critical

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

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ jsbn/index.js, line 1304 (Weak Encryption)	**Critical**

Sink Details

Sink: FunctionCall: Arcfour
Enclosing Method: init^()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsbn/index.js:1304
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ jsbn/index.js, line 1341 (Weak Encryption)	**Critical**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionPointerCall: init^
Enclosing Method: prng_newstate()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsbn/index.js:1341
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ jsbn/index.js, line 1311 (Weak Encryption)	**Critical**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: ARC4init
Enclosing Method: init^()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsbn/index.js:1311
Taint Flags:

`No snippet available`

D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ jsbn/index.js, line 1326 (Weak Encryption)	**Critical**

Issue Details

Kingdom: Security Features
Scan Engine: SCA (Structural)

Sink Details

Sink: FunctionCall: ARC4next
Enclosing Method: init^()
File: D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/jsbn/index.js:1326
Taint Flags:

Weak Encryption	Critical
Package: D:.SCA.SCACODE.G9_IN.898109.NF17027-2.CODE.HbYTDWfD.node_modules.jsbn	
D:/SCA/SCACODE/G9_IN/898109/NF17027-2/CODE/HbYTDWfD/node_modules/ jsbn/index.js, line 1326 (Weak Encryption)	**Critical**

```
No snippet available
```

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.

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.