Scan Report

# vdharmava/vulnerable-node

Grouped By: Vulnerability Type

Scanned Branch Name: main

Project Created: 12 Jun, 2025 | 9:24 PM UTC+0

Last Scanned: 16 Jun, 2025 | 10:39 AM UTC+0

Scanners: SAST, IaC, SCA, SCS

C 7

H 18

M 27

52

## Table of Contents

Filtered By ... 3
Scan Information ... 3
Project & Scan Tags ... 3
Scan Results Overview ... 4
- By Scanner ... 4
- By Status ... 4
- By Severity ... 4
- By State ... 4
- By Language ... 4
- By Package ... 4
- By SAST Vulnerability ... 6
- Top 10 SAST Vulnerabilities ... 6
- Top 10 SAST Vulnerable Files ... 6
- 5 Oldest SAST Vulnerabilities ... 6

SAST Vulnerabilities ... 8
- By Severity ... 8

SAST Scan Results ... 8
- Reflected_XSS ... 8
- Use_Of_Hardcoded_Password ... 11
- Open_Redirect ... 12
- Missing_HSTS_Header ... 14

SCA Vulnerabilities ... 15
- By Severity ... 15

SCA Scan Results ... 15
- Npm-semver-4.3.6 ... 15
- Npm-ejs-0.8.8 ... 15
- Npm-qs-4.0.0 ... 17
- Npm-path-to-regexp-0.1.7 ... 18
- Npm-negotiator-0.5.3 ... 18
- Npm-ejs-2.7.4 ... 19
- Npm-mime-1.3.4 ... 20
- Npm-semver-4.3.2 ... 20
- Npm-fresh-0.3.0 ... 20
- Npm-body-parser-1.13.3 ... 21
- Npm-express-4.13.4 ... 21
- Npm-log4js-0.6.38 ... 22
- Npm-bootstrap-3.3.6 ... 22
- Npm-cookie-0.1.3 ... 24
- Npm-cookie-0.1.5 ... 24
- Npm-debug-2.2.0 ... 25
- Npm-ms-0.7.1 ... 25
- Npm-ms-0.7.2 ... 25
- Npm-send-0.13.1 ... 26

Npm-send-0.13.2 . . . . . 26
Npm-serve-static-1.10.3 . . . . . 27
Npm-pg-5.1.0 . . . . . 27
Npm-morgan-1.6.1 . . . . . 27
SAST Resolved Vulnerabilities . . . . . 29
Categories . . . . . 30
ASA Mobile Premium . . . . . 30
ASA Premium . . . . . 30
ASD STIG 6.1 . . . . . 30
Base Preset . . . . . 30
CWE top 25 . . . . . 30
FISMA 2014 . . . . . 30
MOIS(KISA) Secure Coding 2021 . . . . . 31
NIST SP 800-53 . . . . . 31
OWASP ASVS . . . . . 31
OWASP Top 10 2013 . . . . . 31
OWASP Top 10 2017 . . . . . 31
OWASP Top 10 2021 . . . . . 32
OWASP Top 10 API . . . . . 32
OWASP Top 10 API 2023 . . . . . 32
PCI DSS v3.2.1 . . . . . 32
PCI DSS v4.0 . . . . . 32
SANS top 25 . . . . . 33
Top Tier . . . . . 33
Vulnerability Details . . . . . 34
Reflected_XSS . . . . . 34
Use_Of_Hardcoded_Password . . . . . 34
Open_Redirect . . . . . 35
Missing_HSTS_Header . . . . . 35

## Filtered By

Severity: C H M

Excluded: Low, Information

Result State: To Verify, Confirmed, Urgent

Excluded: Not Exploitable, Proposed Not Exploitable

Status: New, Recurrent

Excluded: None

Scanners: SAST, SCA

Excluded: IaC, SCS

Queries: Link

Results limited to: 10000

## Scan Information

- Scan Id: 843b61c9-e03b-46c7-9622-98561509e43b
- Scan Duration: 0h 2m 10s
- Preset: ASA High
- LOC Scanned: 3375
  - SAST: 3320
  - IaC: 55
- Files Scanned: 22
  - SAST: 18
  - IaC: 4
- Density: 8.3
  - SAST: 3.92
  - IaC: 272.73
- Initiator: venu_dharmavaram
- Online Results: Link

- Source Origin: zip
- Main Branch: N/A
- Scan Type: Incremental
- Scanned Branch Name: main
- Groups: None
- Scanner Status:
  - SCS: Completed
  - SAST: Completed
  - SCA: Completed
  - IaC: Completed

## Project & Scan Tags

Project Tags:

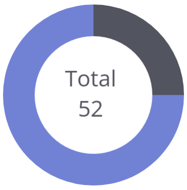
None

Scan Tags:

None

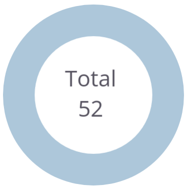
## Scan Results Overview

### By Scanner



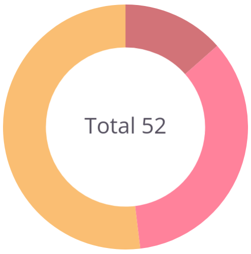
■ SAST (13, 25%)
■ SCA (39, 75%)

### By Status (SAST & IaC & SCA & SCS)



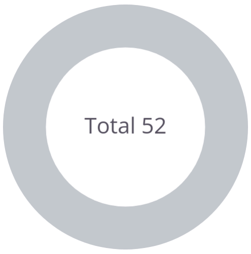
■ New (0, 0%)
■ Recurrent (52, 100%)

### By Severity



| Legend | Density (SAST & IaC) |
|---|---|
| ■ Critical (7, 13.46%) | 0.00 |
| ■ High (18, 34.62%) | 1.51 |
| ■ Medium (27, 51.92%) | 2.41 |

### By State

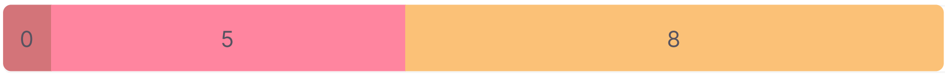


| Legend | Density (SAST & IaC) |
|---|---|
| ■ To Verify (52, 100.00%) | 3.92 |
| ■ Confirmed (0, 0.00%) | 0.00 |
| ■ Urgent (0, 0.00%) | 0.00 |

### By Language (SAST)

Density (SAST)

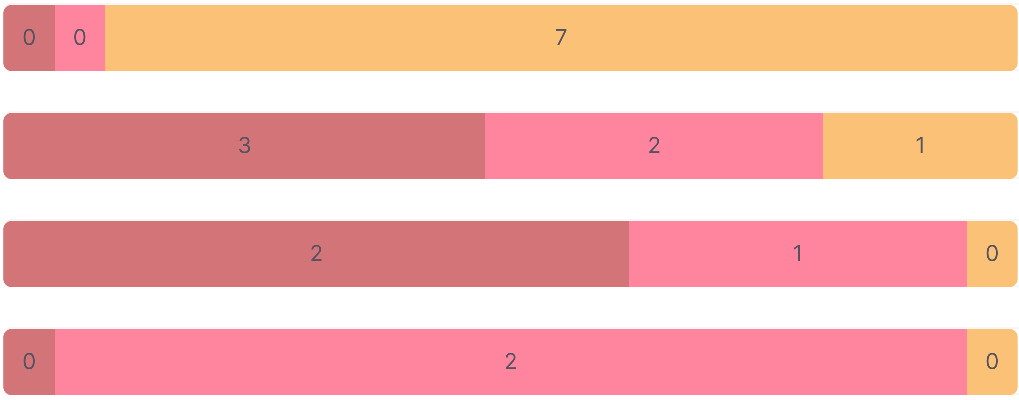
javascript (13)



3.92

### By Package (SCA)

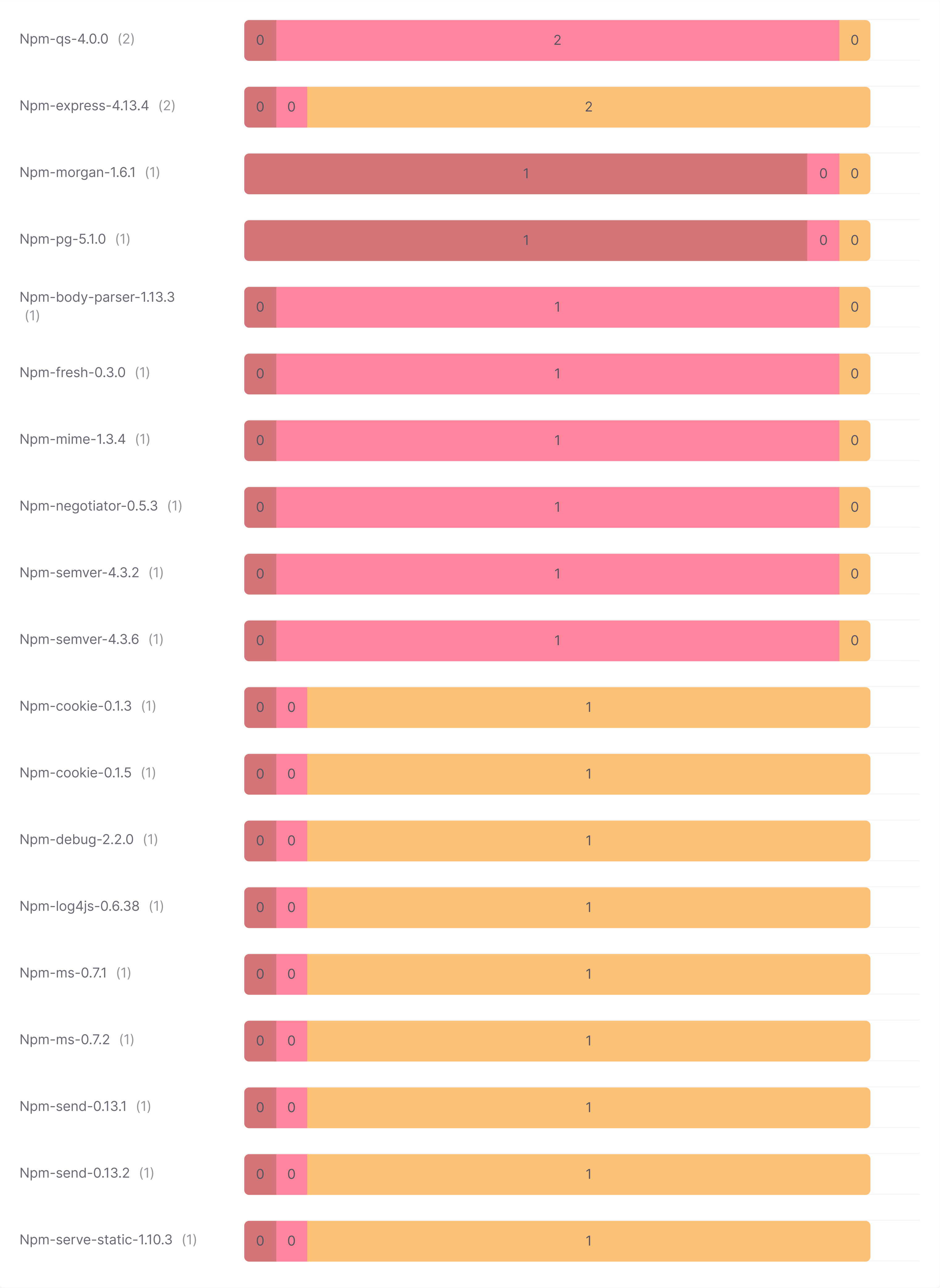
Npm-bootstrap-3.3.6 (7)



Npm-ejs-0.8.8 (6)

Npm-ejs-2.7.4 (3)

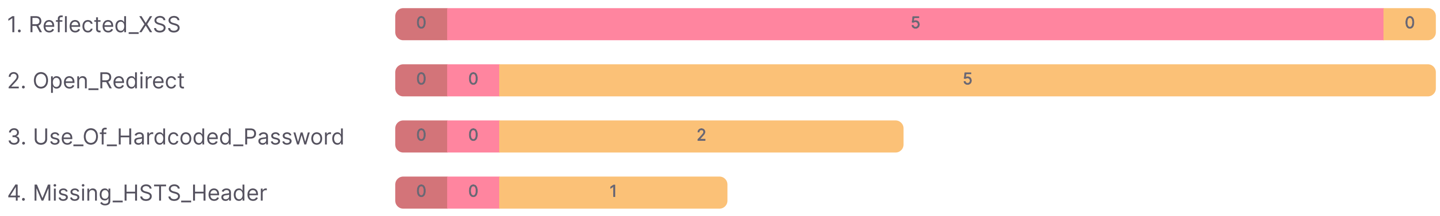
Npm-path-to-regexp-0.1.7 (2)


Npm-qs-4.0.0 (2)
0
2
0
Npm-express-4.13.4 (2)
0
0
2
Npm-morgan-1.6.1 (1)
1
0
0
Npm-pg-5.1.0 (1)
1
0
0
Npm-body-parser-1.13.3 (1)
0
1
0
Npm-fresh-0.3.0 (1)
0
1
0
Npm-mime-1.3.4 (1)
0
1
0
Npm-negotiator-0.5.3 (1)
0
1
0
Npm-semver-4.3.2 (1)
0
1
0
Npm-semver-4.3.6 (1)
0
1
0
Npm-cookie-0.1.3 (1)
0
0
1
Npm-cookie-0.1.5 (1)
0
0
1
Npm-debug-2.2.0 (1)
0
0
1
Npm-log4js-0.6.38 (1)
0
0
1
Npm-ms-0.7.1 (1)
0
0
1
Npm-ms-0.7.2 (1)
0
0
1
Npm-send-0.13.1 (1)
0
0
1
Npm-send-0.13.2 (1)
0
0
1
Npm-serve-static-1.10.3 (1)
0
0
1

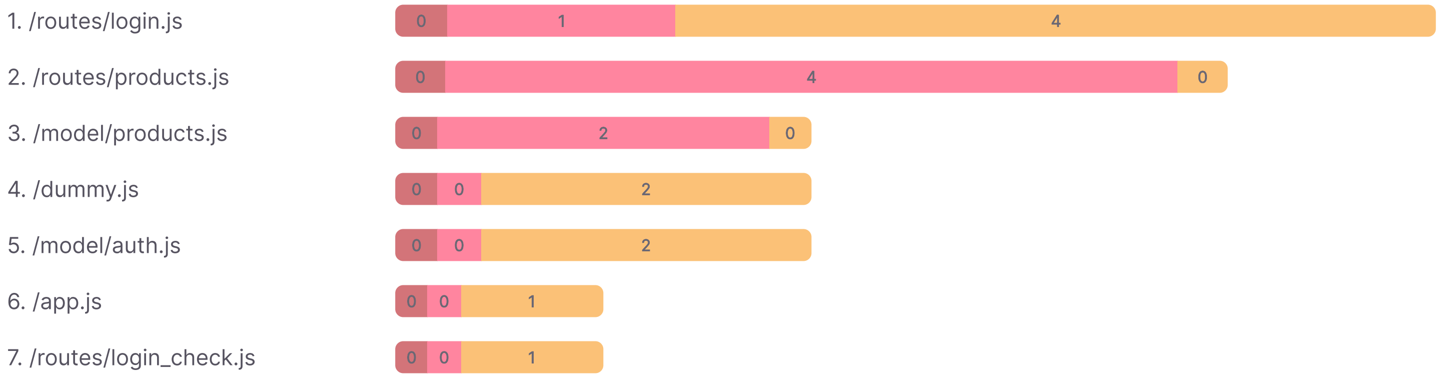
## By SAST Vulnerability

|  | Vulnerability Type | C | H | M |
|---|---|---|---|---|
| H | Reflected_XSS<br>In 3 Files | 0 | 5 | 0 |
| M | Open_Redirect<br>In 3 Files | 0 | 0 | 5 |
| M | Use_Of_Hardcoded_Password<br>In 1 Files | 0 | 0 | 2 |
| M | Missing_HSTS_Header<br>In 1 Files | 0 | 0 | 1 |
|  | Total<br>In 7 Files | 0 | 5 | 8 |

## Top 10 SAST Vulnerabilities (13/7 Vulnerable files)



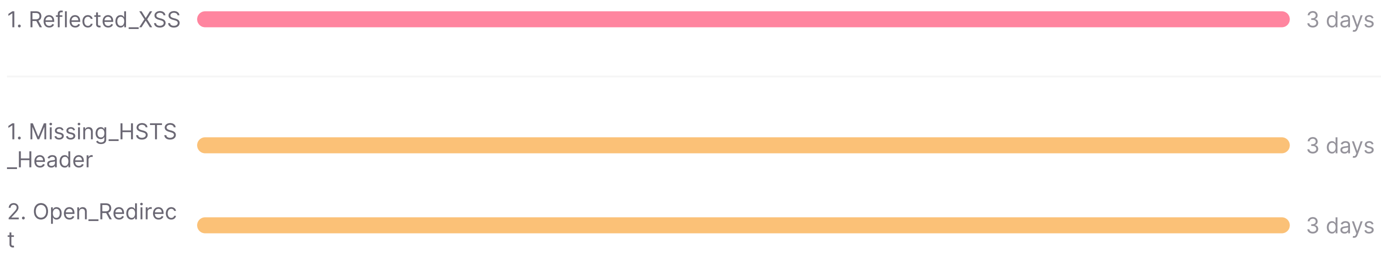
## Top 10 SAST Vulnerable Files (7/18 Files)



## 5 Oldest SAST Vulnerabilities by severity

C H M

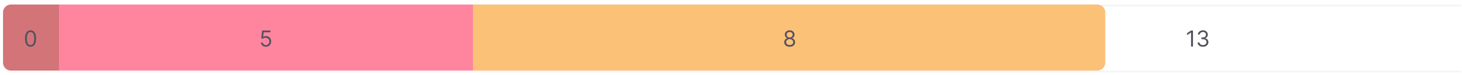
*No data to show for Critical severity*



3. Use_Of_Hardcoded_Password
3 days

## SAST Vulnerabilities

### By Severity



## SAST Scan Results (13)

### Reflected_XSS (Type)

Query Path: JavaScript/JavaScript_Server_Side_Vulnerabilities/Reflected_XSS

CWE Id: 79

Total results: 5

Description: The method @DestinationMethod embeds untrusted data in generated output with @DestinationElement, at line @DestinationLine of @DestinationFile. This untrusted data is embedded into the output without proper sanitization or encoding, enabling an attacker to inject malicious code into the generated web-page. The attacker would be able to alter the returned web page by simply providing modified data in the user input @SourceElement, which is read by the @SourceMethod method at line @SourceLine of @SourceFile. This input then flows through the code straight to the output web page, without sanitization.  This can enable a Reflected Cross-Site Scripting (XSS) attack.

Category:

- ASA Premium: ASA Premium
- ASD STIG 6.1: APSC-DV-002490 - CAT I The application must protect from Cross-Site Scripting (XSS) vulnerabilities.
- CWE top 25: CWE top 25
- FISMA 2014: System And Information Integrity
- MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
- NIST SP 800-53: SI-15 Information Output Filtering (P0)
- OWASP ASVS: V05 Validation, Sanitization and Encoding
- OWASP Top 10 2013: A3-Cross-Site Scripting (XSS)
- OWASP Top 10 2017: A7-Cross-Site Scripting (XSS)
- OWASP Top 10 2021: A3-Injection
- PCI DSS v3.2.1: PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS)
- PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development
- SANS top 25: SANS top 25
- Top Tier: Top Tier

Result 1 of 5
High • Link • Recurrent • To Verify • Similarity Id: 30247190 • Found First: 12 Jun, 2025 • Found Last: 16 Jun, 2025
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

### Source

File Name: /routes/products.js

Method: Lambda

Element: url

### Destination

File Name: /routes/products.js

Method: Lambda

Element: render

### Code Snippets

```
66 | var url_params = url.parse(req.url, true).query;
```

```
77 | res.render('search', { in_query: query, products: data });
```

Result 2 of 5

High • Link • Recurrent • To Verify • Similarity Id: -1768556801 • Found First: 12 Jun, 2025 • Found Last: 16 Jun, 2025
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

| Source | Destination |
|---|---|
| File Name: /routes/products.js | File Name: /routes/products.js |
| Method: Lambda | Method: Lambda |
| Element: user_name | Element: render |

Code Snippets

```
28 | db_products.getPurchased(req.session.user_name)
```

```
32 | res.render('bought_products', { products: data });
```

Result 3 of 5

High • Link • Recurrent • To Verify • Similarity Id: -33785946 • Found First: 12 Jun, 2025 • Found Last: 16 Jun, 2025
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

| Source | Destination |
|---|---|
| File Name: /routes/login.js | File Name: /routes/login.js |
| Method: Lambda | Method: Lambda |
| Element: url | Element: render |

Code Snippets

```
12 | var url_params = url.parse(req.url, true).query;
```

```
14 | res.render('login', {returnurl: url_params.returnurl, auth_error: url_params.error});
```

Result 4 of 5

High • Link • Recurrent • To Verify • Similarity Id: -627346917 • Found First: 12 Jun, 2025 • Found Last: 16 Jun, 2025
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

| Source | Destination |
|---|---|
| File Name: /routes/products.js | File Name: /routes/products.js |
| Method: Lambda | Method: Lambda |
| Element: url | Element: render |

Code Snippets

```
45 | var url_params = url.parse(req.url, true).query;
```

```
51 | res.render('product_detail', { product: data });
```

Result 5 of 5

High • Link • Recurrent • To Verify • Similarity Id: 75362801 • Found First: 12 Jun, 2025 • Found Last: 16 Jun, 2025
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

| Source | Destination |
|---|---|
| File Name: /routes/products.js | File Name: /routes/products.js |
| Method: Lambda | Method: Lambda |
| Element: url | Element: render |

### Code Snippets

```
66 | var url_params = url.parse(req.url, true).query;
```

```
83 | res.render('search', { in_query: query, products: [] });
```

### Use_Of_Hardcoded_Password (Type)

Query Path: JavaScript/JavaScript_Server_Side_Vulnerabilities/Use_Of_Hardcoded_Password

CWE Id: 259

Total results: 2

Description: The application uses the hard-coded password @SourceElement for authentication purposes, either using it to verify users' identities, or to access another remote system. This password at line @SourceLine of @SourceFile appears in the code, implying it is accessible to anyone with source code access, and cannot be changed without rebuilding the application.

Category:

- ASA Mobile Premium: ASA Mobile Premium
- ASA Premium: ASA Premium
- CWE top 25: CWE top 25
- FISMA 2014: Identification And Authentication
- MOIS(KISA) Secure Coding 2021: MOIS(KISA) Security Functions
- NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
- OWASP ASVS: V02 Authentication
- OWASP Top 10 2017: A3-Sensitive Data Exposure
- OWASP Top 10 2021: A7-Identification and Authentication Failures
- OWASP Top 10 API: API2-Broken Authentication
- PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development
- SANS top 25: SANS top 25

#### Result 1 of 2

Medium • Link • Recurrent • To Verify • Similarity Id: -71926403 • Found First: 12 Jun, 2025 • Found Last: 16 Jun, 2025
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

| Source | Destination |
|---|---|
| File Name: /dummy.js | File Name: /dummy.js |
| Method: | Method: |
| Element: "asdfpiuw981" | Element: password |

**Code Snippets**

```
12 | "password": "asdfpiuw981"
```

#### Result 2 of 2

Medium • Link • Recurrent • To Verify • Similarity Id: 462095005 • Found First: 12 Jun, 2025 • Found Last: 16 Jun, 2025
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

| Source | Destination |
|---|---|
| File Name: /dummy.js | File Name: /dummy.js |
| Method: | Method: |
| Element: "admin" | Element: password |

**Code Snippets**

```
8 | "password": "admin"
```

**Open_Redirect** (Type)

Query Path: JavaScript/JavaScript_Server_Side_Vulnerabilities/Open_Redirect

CWE Id: 601

Total results: 5

Description: The potentially tainted value provided by @SourceElement in @SourceFile at line @SourceLine is used as a destination URL by @DestinationElement in @DestinationFile at line @DestinationLine, potentially allowing attackers to perform an open redirection.

Category:

- ASA Premium: ASA Premium
- FISMA 2014: System And Information Integrity
- MOIS(KISA) Secure Coding 2021: MOIS(KISA) Verification and representation of input data
- NIST SP 800-53: SI-10 Information Input Validation (P1)
- OWASP ASVS: V05 Validation, Sanitization and Encoding
- OWASP Top 10 2021: A1-Broken Access Control
- OWASP Top 10 API 2023: API10-Unsafe Consumption of APIs
- PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

### Result 1 of 5

Medium • Link • Recurrent • To Verify • Similarity Id: 1457361836 • Found First: 12 Jun, 2025 • Found Last: 16 Jun, 2025
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

| Source | Destination |
|---|---|
| File Name: /routes/login.js | File Name: /routes/login.js |
| Method: Lambda | Method: Lambda |
| Element: password | Element: redirect |

**Code Snippets**

```
22 | var password = req.body.password;
```

```
39 | res.redirect("/login?returnurl=" + returnurl + "&error=" + err.message);
```

### Result 2 of 5

Medium • Link • Recurrent • To Verify • Similarity Id: -887704556 • Found First: 12 Jun, 2025 • Found Last: 16 Jun, 2025
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

| Source | Destination |
|---|---|
| File Name: /routes/login.js | File Name: /routes/login.js |
| Method: Lambda | Method: Lambda |
| Element: returnurl | Element: redirect |

**Code Snippets**

```
23 | var returnurl = req.body.returnurl;
```

```
39 | res.redirect("/login?returnurl=" + returnurl + "&error=" + err.message);
```

Result 3 of 5

Medium • Link • Recurrent • To Verify • Similarity Id: -484454744 • Found First: 12 Jun, 2025 • Found Last: 16 Jun, 2025
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

| Source | Destination |
|---|---|
| File Name: /routes/login_check.js | File Name: /routes/login_check.js |
| Method: check_logged | Method: check_logged |
| Element: url | Element: redirect |

Code Snippets

```
res.redirect("/login?returnurl=" + req.url);
```

Result 4 of 5

Medium • Link • Recurrent • To Verify • Similarity Id: -1379743135 • Found First: 12 Jun, 2025 • Found Last: 16 Jun, 2025
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

| Source | Destination |
|---|---|
| File Name: /routes/login.js | File Name: /routes/login.js |
| Method: Lambda | Method: Lambda |
| Element: username | Element: redirect |

Code Snippets

```
var user = req.body.username;
```

```
res.redirect("/login?returnurl=" + returnurl + "&error=" + err.message);
```

Result 5 of 5

Medium • Link • Recurrent • To Verify • Similarity Id: 317234720 • Found First: 12 Jun, 2025 • Found Last: 16 Jun, 2025
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

| Source | Destination |
|---|---|
| File Name: /routes/login.js | File Name: /routes/login.js |
| Method: Lambda | Method: Lambda |
| Element: returnurl | Element: redirect |

Code Snippets

```
var returnurl = req.body.returnurl;
```

```
res.redirect(returnurl);
```

**Missing_HSTS_Header** (Type)

Query Path: JavaScript/JavaScript_Medium_Threat/Missing_HSTS_Header

CWE Id: 346

Total results: 1

Description: The web-application does not define an HSTS header, leaving it vulnerable to attack.

Category:

- ASA Premium: ASA Premium
- Base Preset: Base Preset
- OWASP ASVS: V14 Configuration
- OWASP Top 10 2021: A7-Identification and Authentication Failures
- PCI DSS v4.0: PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development

Result 1 of 1

Medium • Link • Recurrent • To Verify • Similarity Id: 537279645 • Found First: 12 Jun, 2025 • Found Last: 16 Jun, 2025
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

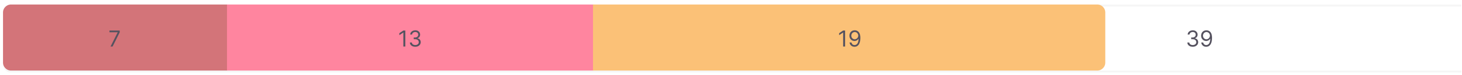
| Source | Destination |
|---|---|
| File Name: /app.js | File Name: /app.js |
| Method: Lambda | Method: Lambda |
| Element: render | Element: render |

**Code Snippets**

```
res.render('error', {
```

## SCA Vulnerabilities

### By Severity



## SCA Scan Results (39 Results)

### Npm-semver-4.3.6 (1 Result)

Package Name: semver

Version: 4.3.6

Total Results: 1

Category: CWE-1333
Total Results: 1

**Result 1 of 1 - Vulnerability**
High • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: wqWygNEFB0xrfhtcLpGoZ5+8U0er69GyHu//erDtJb4= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2022-25883
> Description: The package semver versions prior to 5.7.2, 6.x through 6.3.0 and 7.x through 7.5.1 are vulnerable to Regular Expression Denial of Service (ReDoS) via the function "new Range", when untrusted user data is provided as a range.
> References: Advisory • Commit • Pull request • Commit • Commit

### Npm-ejs-0.8.8 (6 Results)

Package Name: ejs

Version: 0.8.8

Total Results: 2

Category: CWE-20
Total Results: 2

**Result 1 of 2 - Vulnerability**
High • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: 8Sq7j/5d5t410cTITUTPqMj0JdbC9bmcn9WUv/Z7MHY= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2017-1000189
> Description: nodejs ejs version older than 2.5.4 is vulnerable to a denial-of-service due to weak input validation in the ejs.renderFile()
> References: Commit • Advisory

**Result 2 of 2 - Vulnerability**

Critical • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •

Result ID: 6jyi6c+hHVw7bEWhMfyKsGPQrj+KH1575WUkO8IY7Pw= •

First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2017-1000228
>
> Description: nodejs ejs versions older than 2.5.3 is vulnerable to remote code execution due to weak input validation in ejs.renderFile() function
>
> References: Commit • Advisory

Package Name: ejs

Version: 0.8.8

Total Results: 1

Category: CWE-1321

Total Results: 1

**Result 1 of 1 - Vulnerability**

High • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •

Result ID: 2h5mYepGRgE0u0yUQ9ah1qRQq2dMz1Veh0fapQBXLaE= •

First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2024-33883
>
> Description: The ejs (aka Embedded JavaScript templates) package versions prior to 3.1.10 for Node.js lacks certain pollution protection.
>
> References: Advisory • Commit

Package Name: ejs

Version: 0.8.8

Total Results: 1

Category: CWE-79

Total Results: 1

**Result 1 of 1 - Vulnerability**

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •

Result ID: OKhZNwRBr85fjkPlmlG85WlvL+6R274uakWuo8QhYkM= •

First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2017-1000188
>
> Description: nodejs ejs version older than 2.5.4 is vulnerable to a Cross-site-scripting in the ejs.renderFile() resulting in code injection
>
> References: Commit • Advisory

Package Name: ejs

Version: 0.8.8

Total Results: 1

Category: CWE-74

Total Results: 1

**Result 1 of 1 - Vulnerability**

Critical • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: rr1j45prhcASJNSsDa269LPxc0j4eBU3iNbg/fQHybQ= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2022-29078
> Description: The ejs (aka Embedded JavaScript templates) package up to 3.1.6 for Node.js allows server-side template injection in settings[view options][outputFunctionName]. This is parsed as an internal option, and overwrites the outputFunctionName option with an arbitrary OS command (which is executed upon template compilation).
> References: Advisory • Blog Post • Commit • Issue • Pull request

Package Name: ejs

Version: 0.8.8

Total Results: 1

Category: CWE-94
Total Results: 1

**Result 1 of 1 - Vulnerability**

Critical • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: e/fVJ26Vd85zzHVcVl93ylvupDEWBtDds6zECIPiyal= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: Cx35ef42d7-054c
> Description: ejs package before 3.1.6 is vulnerable to arbitrary code injection. The vulnerability exists due to improper input validation passed via the options parameter - the filename, compileDebug, and client option.
> References: Issue • Commit

**Npm-qs-4.0.0** (2 Results)

Package Name: qs

Version: 4.0.0

Total Results: 1

Category: CWE-20
Total Results: 1

**Result 1 of 1 - Vulnerability**

High • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: g/9Pk3skSmEH66OlvVVmjlYJU/3jqxM6uznfxdSQyos= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2017-1000048
> Description: the web framework using ljharb's qs module older than v6.3.2, v6.2.3, v6.1.2, and v6.0.4 is vulnerable to a DoS. A malicious user can send a evil request to cause the web framework crash.
> References: Commit • Commit • Advisory • Advisory • Issue • Pull request •
> Pull request

Package Name: qs

Version: 4.0.0

Total Results: 1

Category: CWE-1321

Total Results: 1

**Result 1 of 1 - Vulnerability**

High • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: TPooHWA4P/EiKJ+GZ4V3IsTsJDdXhghNvlrC/9HEZhw= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2022-24999
> Description: The qs package as used in Express through 4.17.3 and other products, allows attackers to cause a Node process hang for an Express application because an "__ proto__ key" can be used. In many typical Express use cases, an unauthenticated remote attacker can place the attack payload in the query string of the URL that is used to visit the application, such as "a[__proto__]=b&a[__proto__]&a[length]=100000000". This vulnerability affects qs versions through 6.2.3, 6.3.0 through 6.3.2, 6.4.0, 6.5.0 through 6.5.2, 6.6.0, 6.7.0 through 6.7.2, 6.8.0 through 6.8.2, 6.9.0 through 6.9.6 and 6.10.0 through 6.10.2 (and therefore Express 4.17.3, which has "deps: qs@6.9.7" in its release description, is not vulnerable).
> References: Advisory • Disclosure • Release Note • Pull request • Commit

**Npm-path-to-regexp-0.1.7** (2 Results)

Package Name: path-to-regexp

Version: 0.1.7

Total Results: 2

Category: CWE-1333
Total Results: 2

**Result 1 of 2 - Vulnerability**

High • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: YRS+sREg7KzAx8C16Q6gMxbGQw4znTiFE+lwJ/ugUjQ= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2024-52798
> Description: path-to-regexp turns path strings into a regular expressions. In certain cases, path-to-regexp will output a regular expression that can be exploited to cause poor performance. The regular expression that is vulnerable to backtracking can be generated. This issue affects path-to-regexp package versions through 0.1.11. Users are advised to upgrade to 0.1.12. This vulnerability exists because of an incomplete fix for CVE-2024-45296.
> References: Advisory • Release Note • Commit • Blog Post

**Result 2 of 2 - Vulnerability**

High • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: nq38iAgxD2OIWlmqF4hkKmBVD/5uyllGW27J5yob1ME= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2024-45296
> Description: The path-to-regexp turns path strings into regular expressions. In certain cases, path-to-regexp will output a regular expression that can be exploited to cause poor performance. Because JavaScript is single threaded and regex matching runs on the main thread, poor performance will block the event loop and lead to a DoS. The bad regular expression is generated any time you have two parameters within a single segment, separated by something that is not a period (.). This issue affects path-to-regexp versions through 0.1.9, 0.2.0 through 1.8.0, 2.0.0 through 3.2.0, 4.0.0 through 6.2.2, and 7.0.0 through 7.2.0.
> References: Advisory • Commit • Commit • Release Note

**Npm-negotiator-0.5.3** (1 Result)

Package Name: negotiator

Version: 0.5.3

Total Results: 1

Category: CWE-20
Total Results: 1

**Result 1 of 1 - Vulnerability**

High • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: bME45I/U2cislJAHr3NV2I4OQkH+rEkysJQKwLPPuCU= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2016-10539
> Description: negotiator is an HTTP content negotiator for Node.js and is used by many modules and frameworks including Express and Koa. The header for "Accept-Language", when parsed by negotiator 0.6.0 and earlier is vulnerable to Regular Expression Denial of Service via a specially crafted string.
> References: Commit • Advisory • Advisory

**Npm-ejs-2.7.4** (3 Results)

Package Name: ejs

Version: 2.7.4

Total Results: 1

Category: CWE-1321
Total Results: 1

**Result 1 of 1 - Vulnerability**

High • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: DmTXQV14ytiH/qTKNoPB+3huHHJrrJOldDssDTzk1s0= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2024-33883
> Description: The ejs (aka Embedded JavaScript templates) package versions prior to 3.1.10 for Node.js lacks certain pollution protection.
> References: Advisory • Commit

Package Name: ejs

Version: 2.7.4

Total Results: 1

Category: CWE-74
Total Results: 1

**Result 1 of 1 - Vulnerability**

Critical • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: Vj3pr1PVO2khqZ5UgMiRSWJ6gwnspL8GrBWPiMZcCIU= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2022-29078
> Description: The ejs (aka Embedded JavaScript templates) package up to 3.1.6 for Node.js allows server-side template injection in settings[view options][outputFunctionName]. This is parsed as an internal option, and overwrites the outputFunctionName option with an arbitrary OS command (which is executed upon template compilation).
> References: Advisory • Blog Post • Commit • Issue • Pull request

Package Name: ejs

Version: 2.7.4

Total Results: 1

Category: CWE-94

Total Results: 1

**Result 1 of 1 - Vulnerability**

Critical • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •

Result ID: aLvQmvHX/9B8btf87OftmUHzS43kpXzWsQI547qhDgA= •

First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: Cx35ef42d7-054c
>
> Description: ejs package before 3.1.6 is vulnerable to arbitrary code injection. The vulnerability exists due to improper input validation passed via the options parameter - the filename, compileDebug, and client option.
>
> References: Issue • Commit

### **Npm-mime-1.3.4** (1 Result)

Package Name: mime

Version: 1.3.4

Total Results: 1

Category: CWE-400

Total Results: 1

**Result 1 of 1 - Vulnerability**

High • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •

Result ID: nduXQIKdrCatWjl+hA4UA1ulnYG8HtY4EzaISgGAnbs= •

First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2017-16138
>
> Description: The mime module < 1.4.1 and 2.0.0 through 2.0.2 is vulnerable to regular expression denial of service when a mime lookup is performed on untrusted user input.
>
> References: Commit • Commit • Advisory • Advisory • Issue

### **Npm-semver-4.3.2** (1 Result)

Package Name: semver

Version: 4.3.2

Total Results: 1

Category: CWE-1333

Total Results: 1

**Result 1 of 1 - Vulnerability**

High • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •

Result ID: kS6xwaz/URFCpDNR612HrMR9weWYfptfrHpDmgugw54= •

First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2022-25883
>
> Description: The package semver versions prior to 5.7.2, 6.x through 6.3.0 and 7.x through 7.5.1 are vulnerable to Regular Expression Denial of Service (ReDoS) via the function "new Range", when untrusted user data is provided as a range.
>
> References: Advisory • Commit • Pull request • Commit • Commit

### **Npm-fresh-0.3.0** (1 Result)

Package Name: fresh

Version: 0.3.0

Total Results: 1

Category: CWE-400
Total Results: 1

**Result 1 of 1 - Vulnerability**
High • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: 6T8YeD1CmwNch7APdj68t6QRdORvPG7prAuCqwwvfsk= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

CVE: CVE-2017-16119
Description: Fresh is a module used by the Express.js framework for HTTP response freshness testing. Prior to v0.5.2 it is vulnerable to a regular expression denial of service when it is passed specially crafted input to parse. This causes the event loop to be blocked causing a denial of service condition.
References: Advisory • Commit

### Npm-body-parser-1.13.3 (1 Result)

Package Name: body-parser

Version: 1.13.3

Total Results: 1

Category: CWE-405
Total Results: 1

**Result 1 of 1 - Vulnerability**
High • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: zejtYTxvtu+ubSgRr8ax7C+aCOt+bLrRPwQtr/H2TeY= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

CVE: CVE-2024-45590
Description: The body-parser is Node.js body parsing middleware. The body-parser package versions prior to 1.20.3 and 2.0.x prior to 2.0.0 are vulnerable to Denial of Service when URL encoding is enabled. A malicious actor using a specially crafted payload could flood the server with a large number of requests, resulting in Denial of Service.
References: Advisory • Commit • Release Note

### Npm-express-4.13.4 (2 Results)

Package Name: express

Version: 4.13.4

Total Results: 1

Category: CWE-79
Total Results: 1

**Result 1 of 1 - Vulnerability**

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: iWiyp4EPUCDB78/888a62LsME80wYEPar9Lwoe9fTXI= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2024-43796
> Description: Express.js minimalist web framework for node. In express versions prior to 4.20.0 and 5.0.x prior to 5.0.0, passing untrusted user input even after sanitizing it to "response.redirect()" may execute untrusted code.
> References: Advisory • Commit • Release Note • Pull request

Package Name: express

Version: 4.13.4

Total Results: 1

Category: CWE-1286
Total Results: 1

**Result 1 of 1 - Vulnerability**

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: PzRzHmTyB9rsi9wVnMZDN6VYGPVNUKq4GFLtg8SJ4KU= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2024-29041
> Description: Express.js minimalist web framework for node. Express.js versions prior to 4.19.2, and 5.0.x prior to 5.0.0-beta.3 are affected by an open redirect vulnerability using malformed URLs. When a user of Express performs a redirect using a user-provided URL Express performs an encode using "encodeurl" on the contents before passing it to the "location" header. This can cause malformed URLs to be evaluated in unexpected ways by common redirect allow list implementations in Express applications, leading to an Open Redirect via bypass of a properly implemented allow list. The main method impacted is "res.location()" but this is also called from within "res.redirect()".
> References: Advisory • Release Note • Pull request • Commit • Pull request •
> Commit

**Npm-log4js-0.6.38** (1 Result)

Package Name: log4js

Version: 0.6.38

Total Results: 1

Category: CWE-276
Total Results: 1

**Result 1 of 1 - Vulnerability**

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: 99t5kD4w3JxsLdM7cCiFzDi6wa0rem2rOksxwnBZ62Q= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2022-21704
> Description: log4js-node is a port of log4js to node.js. In affected versions default file permissions for log files created by the file, fileSync and dateFile appenders are world-readable (in unix). This could cause problems if log files contain sensitive information. This would affect any users that have not supplied their own permissions for the files via the mode parameter in the config. Users are advised to update.
> References: Advisory • Release Note • Commit • Pull request

**Npm-bootstrap-3.3.6** (7 Results)

Package Name: bootstrap

Version: 3.3.6

Total Results: 7

Category: CWE-79
Total Results: 7

### Result 1 of 7 - Vulnerability

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: s+ljiuxFbPajhGUZbo5BSC61R0BTc9XMU7wsua8Kk5A= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2016-10735
> Description: In Bootstrap before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.
> References: Advisory • Issue • Pull request • Commit • Pull request • Commit • Pull request • Commit • Advisory

### Result 2 of 7 - Vulnerability

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: +f4SvxMrs9Dy0FbysRG2gVHjlATtzsns3TAwgn8bo+8= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2018-14040
> Description: In Bootstrap before 3.4.0 and 4.0.0 through 4.1.1, XSS is possible in the collapse data-parent attribute.
> References: Advisory • Advisory • Release Note • Mail Thread • Issue • Issue • Pull request • Commit • Commit

### Result 3 of 7 - Vulnerability

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: Jji3u78UmuS0LegsnH13shwa86uQBxlXTYRdkZ+GYDk= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2018-14042
> Description: In Bootstrap before 3.4.0 and 4.0.0 through 4.1.1, XSS is possible in the data-container property of tooltip.
> References: Advisory • Advisory • Release Note • Issue • Issue • Pull request • Commit • Commit

### Result 4 of 7 - Vulnerability

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: pZj4yA4UmqPWXqbH9krSkwg/jyM7qHb4u/CcQ0VKM/U= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2018-20676
> Description: In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.
> References: Advisory • Pull request • Issue • Commit

### Result 5 of 7 - Vulnerability

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: UYmjm0S78RGeZUFlaBYcaVCNi7aT57KeJhiuXSznJp8= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2018-20677
> Description: In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.
> References: Advisory • Pull request • Issue • Commit

### Result 6 of 7 - Vulnerability

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: IkPeoBFRCweZCSxxdrby96KvjGgu0xN2bvflDvDdVA8= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2019-8331
> Description: In Bootstrap before 3.4.1 and 4.x.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.
> References: Advisory • Advisory • Advisory • Release Note • Release Note • Pull request • Commit

### Result 7 of 7 - Vulnerability

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: bfHs1JTh3dB9qLBG6wQqa2hXTBRui7hR5VpTWDmq1/8= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2024-6485
> Description: A security vulnerability has been discovered in the package bootstrap that could enable Cross-Site Scripting (XSS) attacks. The vulnerability is associated with the data-loading-text attribute within the button plugin. This vulnerability can be exploited by injecting malicious JavaScript code into the attribute, which would then be executed when the button's loading state is triggered. this vulnerability affect 2.0.0 through 3.4.1.
> References: Advisory • Disclosure

## Npm-cookie-0.1.3 (1 Result)

Package Name: cookie

Version: 0.1.3

Total Results: 1

Category: CWE-74
Total Results: 1

### Result 1 of 1 - Vulnerability

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: BvIb0bxzRaD/UCI346L11VBbdU1rzz3kbZKPxjQB3as= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2024-47764
> Description: The NPM package cookie is a basic HTTP cookie parser and serializer for HTTP servers. The cookie name could be used to set other fields of the cookie, resulting in an unexpected cookie value. A similar escape can be used for "path" and "domain", which could be abused to alter other fields of the cookie. This vulnerability affects cookie package versions prior to 0.7.0. Users are advised to upgrade to a fixed version, which updates the validation for "name", "path", and "domain".
> References: Advisory • Commit • Pull request • Release Note • Issue

## Npm-cookie-0.1.5 (1 Result)

Package Name: cookie

Version: 0.1.5

Total Results: 1

Category: CWE-74
Total Results: 1

**Result 1 of 1 - Vulnerability**

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: IwrRv62j/VEdNKo+V7rtblVN0hYmK/uaXk/58seYxYY= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2024-47764
> Description: The NPM package cookie is a basic HTTP cookie parser and serializer for HTTP servers. The cookie name could be used to set other fields of the cookie, resulting in an unexpected cookie value. A similar escape can be used for "path" and "domain", which could be abused to alter other fields of the cookie. This vulnerability affects cookie package versions prior to 0.7.0. Users are advised to upgrade to a fixed version, which updates the validation for "name", "path", and "domain".
> References: Advisory • Commit • Pull request • Release Note • Issue

**Npm-debug-2.2.0** (1 Result)

Package Name: debug

Version: 2.2.0

Total Results: 1

Category: CWE-400
Total Results: 1

**Result 1 of 1 - Vulnerability**

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: nYIZesuo8Ei+tGR3DW/FvzKTfkd0beFP0No+ANZy1GE= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2017-16137
> Description: The debug module is vulnerable to regular expression denial of service when untrusted user input is passed into the o formatter. It takes around 50k characters to block for 2 seconds making this a low severity issue.
> References: Issue • Pull request • Advisory • Commit • Advisory

**Npm-ms-0.7.1** (1 Result)

Package Name: ms

Version: 0.7.1

Total Results: 1

Category: CWE-1333
Total Results: 1

**Result 1 of 1 - Vulnerability**

Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: 2/4AGDJ0EBIP3PfW4WJDLET+Ois+9itl08YVQ0A99aE= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2017-20162
> Description: A vulnerability was found in vercel ms prior to 2.0.0, which was classified as problematic. This issue affects the function "parse" of the file "index.js". The manipulation of the argument "str" leads to inefficient regular expression complexity. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217451.
> References: Advisory • Pull request • Release Note • Commit • Issue

**Npm-ms-0.7.2** (1 Result)

Package Name: ms

Version: 0.7.2

Total Results: 1

Category: CWE-1333
Total Results: 1

**Result 1 of 1 - Vulnerability**
Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: FwMXeB58l8l3oleVuwXQbjgG3du5daXAYTTIE8Ubr+0= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2017-20162
> Description: A vulnerability was found in vercel ms prior to 2.0.0, which was classified as problematic. This issue affects the function "parse" of the file "index.js". The manipulation of the argument "str" leads to inefficient regular expression complexity. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217451.
> References: Advisory • Pull request • Release Note • Commit • Issue

**Npm-send-0.13.1** (1 Result)

Package Name: send

Version: 0.13.1

Total Results: 1

Category: CWE-79
Total Results: 1

**Result 1 of 1 - Vulnerability**
Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: GT8ws7LrFlaaZk6lBk4ee33j0NM0nPUUD7XB35PT3SI= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2024-43799
> Description: Send is a library for streaming files from the file system as an HTTP response. Send passes untrusted user input to "SendStream.redirect()" which executes untrusted code. This vulnerability affects send versions through 0.18.0, and 1.0.0-beta.1 through 1.0.0.
> References: Advisory • Commit • Release Note

**Npm-send-0.13.2** (1 Result)

Package Name: send

Version: 0.13.2

Total Results: 1

Category: CWE-79
Total Results: 1

**Result 1 of 1 - Vulnerability**
Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: HvFcpTSi6Lfji5lSwl7pFprMcv6hGKHWQaCimJIJAhw= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2024-43799
> Description: Send is a library for streaming files from the file system as an HTTP response. Send passes untrusted user input to "SendStream.redirect()" which executes untrusted code. This vulnerability affects send versions through 0.18.0, and 1.0.0-beta.1 through 1.0.0.
> References: Advisory • Commit • Release Note

**Npm-serve-static-1.10.3** (1 Result)

Package Name: serve-static

Version: 1.10.3

Total Results: 1

Category: CWE-79
Total Results: 1

**Result 1 of 1 - Vulnerability**
Medium • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: Jft2UGmyemV9UdgP2l79hqIAIvKINpHc/4WcY70A9OE= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2024-43800
> Description: serve-static serves static files. serve-static passes untrusted user input even after sanitizing it to "redirect()" and may execute untrusted code. This issue affects serve-static versions prior to 1.16.0 and 2.0.x prior to 2.1.0.
> References: Advisory • Commit • Pull request • Release Note

**Npm-pg-5.1.0** (1 Result)

Package Name: pg

Version: 5.1.0

Total Results: 1

Category: CWE-94
Total Results: 1

**Result 1 of 1 - Vulnerability**
Critical • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: +YBX8Fjj5AxgMJn1AFqqlDq91V8by8hZA7syPSN0UMk= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2017-16082
> Description: A remote code execution vulnerability was found within the pg module when the remote database or query specifies a specially crafted column name. There are 2 likely scenarios in which one would likely be vulnerable. 1) Executing unsafe, user-supplied sql which contains a malicious column name. 2) Connecting to an untrusted database and executing a query which returns results where any of the column names are malicious.
> References: Commit • Advisory • Advisory

**Npm-morgan-1.6.1** (1 Result)

Package Name: morgan

Version: 1.6.1

Total Results: 1

Category: CWE-77
Total Results: 1

**Result 1 of 1 - Vulnerability**

Critical • Recurrent • To Verify • Outdated: yes • Found First: 12 Jun, 2025 • Found Last: 12 Jun, 2025 •
Result ID: yVyGc7b7×9xvKnJgms+KMEbEkAjtTySoQ8tI04wxVFs= •
First Scan ID: 332730ba-a9ae-41f4-a8e5-acd9c18e9030

> CVE: CVE-2019-5413
> Description: An attacker could use the format parameter to inject arbitrary commands in the NPM package "morgan" before 1.9.1.
> References: Advisory • Commit • Disclosure

## SAST Resolved Vulnerabilities

*No data to show*

Categories

### ASA Mobile Premium

| Category | C | H | M |
|---|---|---|---|
| ASA Mobile Premium | 0 | 0 | 2 |

### ASA Premium

| Category | C | H | M |
|---|---|---|---|
| ASA Premium | 0 | 5 | 8 |

### ASD STIG 6.1

| Category | C | H | M |
|---|---|---|---|
| APSC-DV-002490 - CAT I The application must protect from Cross-Site Scripting (XSS) vulnerabilities. | 0 | 5 | 0 |

### Base Preset

| Category | C | H | M |
|---|---|---|---|
| Base Preset | 0 | 0 | 1 |

### CWE top 25

| Category | C | H | M |
|---|---|---|---|
| CWE top 25 | 0 | 5 | 2 |

### FISMA 2014

| Category | C | H | M |
|---|---|---|---|
| System And Information Integrity | 0 | 5 | 5 |

|  |  |  |  |
|---|---|---|---|
| Identification And Authentication | 0 | 0 | 2 |

### MOIS(KISA) Secure Coding 2021

| Category | C | H | M |
|---|---|---|---|
| MOIS(KISA) Verification and representation of input data | 0 | 5 | 5 |
| MOIS(KISA) Security Functions | 0 | 0 | 2 |

### NIST SP 800-53

| Category | C | H | M |
|---|---|---|---|
| SI-15 Information Output Filtering (P0) | 0 | 5 | 0 |
| SC-28 Protection of Information at Rest (P1) | 0 | 0 | 2 |
| SI-10 Information Input Validation (P1) | 0 | 0 | 5 |

### OWASP ASVS

| Category | C | H | M |
|---|---|---|---|
| V05 Validation, Sanitization and Encoding | 0 | 5 | 5 |
| V02 Authentication | 0 | 0 | 2 |
| V14 Configuration | 0 | 0 | 1 |

### OWASP Top 10 2013

| Category | C | H | M |
|---|---|---|---|
| A3-Cross-Site Scripting (XSS) | 0 | 5 | 0 |

### OWASP Top 10 2017

| Category | C | H | M |
|---|---|---|---|
| A3-Sensitive Data Exposure | 0 | 0 | 2 |
| A7-Cross-Site Scripting (XSS) | 0 | 5 | 0 |

### OWASP Top 10 2021

| Category | C | H | M |
|---|---|---|---|
| A7-Identification and Authentication Failures | 0 | 0 | 3 |
| A1-Broken Access Control | 0 | 0 | 5 |
| A3-Injection | 0 | 5 | 0 |

### OWASP Top 10 API

| Category | C | H | M |
|---|---|---|---|
| API2-Broken Authentication | 0 | 0 | 2 |

### OWASP Top 10 API 2023

| Category | C | H | M |
|---|---|---|---|
| API10-Unsafe Consumption of APIs | 0 | 0 | 5 |

### PCI DSS v3.2.1

| Category | C | H | M |
|---|---|---|---|
| PCI DSS (3.2.1) - 6.5.7 - Cross-site scripting (XSS) | 0 | 5 | 0 |

### PCI DSS v4.0

| Category | C | H | M |
|---|---|---|---|

| | | | |
|---|---|---|---|
| PCI DSS (4.0) - 6.2.4 Vulnerabilities in software development | 0 | 5 | 8 |

### SANS top 25

| Category | C | H | M |
|---|---|---|---|
| SANS top 25 | 0 | 5 | 2 |

### Top Tier

| Category | C | H | M |
|---|---|---|---|
| Top Tier | 0 | 5 | 0 |

## Vulnerability Details

### Reflected_XSS (CWE 79)

#### What Is The Risk

A successful XSS exploit would allow an attacker to rewrite web pages and insert malicious scripts which would alter the intended output. This could include HTML fragments, CSS styling rules, arbitrary JavaScript, or references to third party code. An attacker could use this to steal users' passwords, collect personal data such as credit card details, provide false information, or run malware. From the victim's point of view, this is performed by the genuine website, and the victim would blame the site for incurred damage. The attacker could use social engineering to cause the user to send the website modified input, which will be returned in the requested web page.

#### What Can Cause It

The application creates web pages that include untrusted data, whether from user input, the application's database, or from other external sources. The untrusted data is embedded directly in the page's HTML, causing the browser to display it as part of the web page. If the input includes HTML fragments or JavaScript, these are displayed too, and the user cannot tell that this is not the intended page. The vulnerability is the result of directly embedding arbitrary data without first encoding it in a format that would prevent the browser from treating it like HTML or code instead of plain text. Note that an attacker can exploit this vulnerability either by modifying the URL, or by submitting malicious data in the user input or other request fields.

#### General Recommendations

* Fully encode all dynamic data, regardless of source, before embedding it in output.
    * Encoding should be context-sensitive. For example:
        * HTML encoding for HTML content
        * HTML Attribute encoding for data output to attribute values
        * JavaScript encoding for server-generated JavaScript
    * It is recommended to use the platform-provided encoding functionality, or known security libraries for encoding output.
    * Implement a Content Security Policy (CSP) with explicit whitelists for the application's resources only.
    * As an extra layer of protection, validate all untrusted data, regardless of source (note this is not a replacement for encoding).
Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
        * Data type
        * Size
        * Range
        * Format
        * Expected values
    * In the `Content-Type` HTTP response header, explicitly define character encoding (charset) for the entire page.
    * Set the `HTTPOnly` flag on the session cookie for "Defense in Depth", to prevent any successful XSS exploits from stealing the
cookie.

### Use_Of_Hardcoded_Password (CWE 259)

#### What Is The Risk

Hardcoded passwords expose the application to password leakage. If an attacker gains access to the source code, she will be able to steal the embedded passwords, and use them to impersonate a valid user. This could include impersonating end users to the application, or impersonating the application to a remote system, such as a database or a remote web service.  Once the attacker succeeds in impersonating the user or application, she will have full access to the system, and be able to do anything the impersonated identity could do.

#### What Can Cause It

The application codebase has string literal passwords embedded in the source code. This hardcoded value is used either to compare to user-provided credentials, or to authenticate downstream to a remote system (such as a database or a remote web service).   An attacker only needs to gain access to the source code to reveal the hardcoded password. Likewise, the attacker can reverse engineer the compiled application binaries, and easily retrieve the embedded password. Once found, the attacker can easily use the password in impersonation attacks, either directly on the application or to the remote system.  Furthermore, once stolen, this password cannot be easily changed to prevent further misuse, unless a new version of the application is compiled. Moreover, if this application is distributed to numerous systems, stealing the password from one system automatically allows a class break in to all the deployed systems.

#### General Recommendations

* Do not hardcode any secret data in source code, especially not passwords.
    * In particular, user passwords should be stored in a database or directory service, and protected with a strong password hash
(e.g. bcrypt, scrypt, PBKDF2, or Argon2). Do not compare user passwords with a hardcoded value.
    * Sytem passwords should be stored in a configuration file or the database, and protected with strong encryption (e.g. AES-256).
Encryption keys should be securely managed, and not hardcoded.

## Open_Redirect (CWE 601)

### What Is The Risk

An attacker could use social engineering to get a victim to click a link to the application, so that the user will be immediately redirected to another site of the attacker's choice. An attacker can then craft a destination website to fool the victim; for example - they may craft a phishing website with an identical looking UI as the previous website's login page, and with a similar looking URL, convincing the user to submit their access credentials in the attacker's website. Another example would be a phishing website with an identical UI as that of a popular payment service, convincing the user to submit their payment information.

### What Can Cause It

The application redirects the user’s browser to a URL provided by a tainted input, without first ensuring that URL leads to a trusted destination, and without warning users that they are being redirected outside of the current site. An attacker could use social engineering to get a victim to click a link to the application with a parameter defining another site to which the application will redirect the user’s browser. Since the user may not be aware of the redirection, they may be under the misconception that the website they are currently browsing can be trusted.

### General Recommendations

1. Ideally, do not allow arbitrary URLs for redirection. Instead, create a mapping from user-provided parameter values to legitimate URLs.
2. If it is necessary to allow arbitrary URLs:
    * For URLs inside the application site, first filter and encode the user-provided parameter, and then either:
        * Create a white-list of allowed URLs inside the application
        * Use variables as a relative URL as an absolute one, by prefixing it with the application site domain - this will ensure all redirection will occur inside the domain
    * For URLs outside the application (if necessary), either:
        * White-list redirection to allowed external domains by first filtering URLs with trusted prefixes. Prefixes must be tested up to the third slash \[/\] - `scheme://my.trusted.domain.com/,` to prevent evasion. For example, if the third slash \[/\] is not validated and scheme://my.trusted.domain.com is trusted, the URL scheme://my.trusted.domain.com.evildomain.com would be valid under this filter, but the domain actually being browsed is evildomain.com, not domain.com.
        * For fully dynamic open redirection, use an intermediate disclaimer page to provide users with a clear warning that they are leaving the site.

## Missing_HSTS_Header (CWE 346)

### What Is The Risk

Failure to set an HSTS header and provide it with a reasonable "max-age" value of at least one year may leave users vulnerable to Man-in-the-Middle attacks.

### What Can Cause It

Many users browse to websites by simply typing the domain name into the address bar, without the protocol prefix. The browser will automatically assume that the user's intended protocol is HTTP, instead of the encrypted HTTPS protocol. When this initial request is made, an attacker can perform a Man-in-the-Middle attack and manipulate it to redirect users to a malicious web-site of the attacker's choosing. To protect the user from such an occurence, the HTTP Strict Transport Security (HSTS) header instructs the user's browser to disallow use of an unsecure HTTP connection to the the domain associated with the HSTS header. Once a browser that supports the HSTS feature has visited a web-site and the header was set, it will no longer allow communicating with the domain over an HTTP connection. Once an HSTS header was issued for a specific website, the browser is also instructed to prevent users from manually overriding and accepting an untrusted SSL certificate for as long as the "max-age" value still applies. The recommended "max-age" value is for at least one year in seconds, or 31536000.

### General Recommendations

* Before setting the HSTS header - consider the implications it may have:
    * Forcing HTTPS will prevent any future use of HTTP, which could hinder some testing
    * Disabling HSTS is not trivial, as once it is disabled on the site, it must also be disabled on the browser
* Set the HSTS header either explicitly within application code, or using web-server configurations.
* Ensure the "max-age" value for HSTS headers is set to 31536000 to ensure HSTS is strictly enforced for at least one year.
* Include the "includeSubDomains" to maximize HSTS coverage, and ensure HSTS is enforced on all sub-domains under the current domain
    * Note that this may prevent secure browser access to any sub-domains that utilize HTTP; however, use of HTTP is very severe and highly discouraged, even for websites that do not contain any sensitive information, as their contents can still be tampered via Man-in-the-Middle attacks to phish users under the HTTP domain.
* Once HSTS has been enforced, submit the web-application's address to an HSTS preload list - this will ensure that, even if a client is accessing the web-application for the first time (implying HSTS has not yet been set by the web-application), a browser that respects the HSTS preload list would still treat the web-application as if it had already issued an HSTS header. Note that this requires the server to have a trusted SSL certificate, and issue an HSTS header with a maxAge of 1 year (31536000)
* Note that this query is designed to return one result per application. This means that if more than one vulnerable response without an HSTS header is identified, only the first identified instance of this issue will be highlighted as a result. If a misconfigured instance of HSTS is identified (has a short lifespan, or is missing the "includeSubDomains" flag), that result will be flagged. Since HSTS is required to be enforced across the entire application to be considered a secure deployment of HSTS functionality, fixing this issue only where the query highlights this result is likely to produce subsequent results in other sections of the application; therefore, when adding this header via code, ensure it is uniformly deployed across the entire application. If this header is added via configuration, ensure that this configuration applies to the entire application.
* Note that misconfigured HSTS headers that do not contain the recommended max-age value of at least one year or the "includeSubDomains" flag will still return a result for a missing HSTS header.