DevSecOps Pipeline Security Report

SonarQube Hotspots

Hotspot #1

- File: src/middlewares/userValidation.ts
- Line: 15
- Risk: DOS (MEDIUM)
- Status: To Review
- Rule: typescript:S5852
- Author: spasicilija1@gmail.com
- Created: 2024-12-09T19:21:27+0000
- Updated: 2025-07-20T12:35:31+0000
- Description: Make sure the regex used here, which is vulnerable to super-linear runtime due to backtracking, cannot lead to denial of service.

ZAP Full Scan

Site: http://digital-library-app:3000

Alert 1: CSP: Failure to Define Directive with No Fallback

Risk: Medium (High) | Confidence: 3 | PluginID: 10055 | Ref: 10055-13

CWE ID: 693

WASC ID: 15

Description: The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding them is the same as allowing anything.

Solution: Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

References: https://www.w3.org/TR/CSP/
https://caniuse.com/#search=content+security+policy
https://content-security-policy.com/
https://github.com/HtmlUnit/htmlunit-csp
https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Instances:

- *http://digital-library-app:3000/ [GET] param: Content-Security-Policy | evidence: default-src 'none'*
  info: The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
- *http://digital-library-app:3000/robots.txt [GET] param: Content-Security-Policy | evidence: default-src 'none'*
  info: The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
- *http://digital-library-app:3000/sitemap.xml [GET] param: Content-Security-Policy | evidence: default-src 'none'*
  info: The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.

Alert 2: Permissions Policy Header Not Set

Risk: Low (Medium) | Confidence: 2 | PluginID: 10063 | Ref: 10063-1

CWE ID: 693

WASC ID: 15

Description: Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.

References: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy
https://developer.chrome.com/blog/feature-policy/
https://scotthelme.co.uk/a-new-security-header-feature-policy/
https://w3c.github.io/webappsec-feature-policy/
https://www.smashingmagazine.com/2018/12/feature-policy/

Instances:

- *http://digital-library-app:3000/ [GET]*
- *http://digital-library-app:3000/robots.txt [GET]*
- *http://digital-library-app:3000/sitemap.xml [GET]*

Alert 3: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Risk: Low (Medium) | Confidence: 2 | PluginID: 10037 | Ref: 10037

CWE ID: 497

WASC ID: 13

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

References:

https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework

https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Instances:

- http://digital-library-app:3000/ [GET] | evidence: X-Powered-By: Express

- http://digital-library-app:3000/robots.txt [GET] | evidence: X-Powered-By: Express

- http://digital-library-app:3000/sitemap.xml [GET] | evidence: X-Powered-By: Express

Alert 4: Storable and Cacheable Content

Risk: Informational (Medium) | Confidence: 2 | PluginID: 10049 | Ref: 10049

CWE ID: 524

WASC ID: 13

Description: The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution: Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:

Cache-Control: no-cache, no-store, must-revalidate, private

Pragma: no-cache

Expires: 0

This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.

References: https://datatracker.ietf.org/doc/html/rfc7234

https://datatracker.ietf.org/doc/html/rfc7231

https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html

Instances:

- http://digital-library-app:3000/ [GET]

info: In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.

- http://digital-library-app:3000/robots.txt [GET]

info: In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.

- http://digital-library-app:3000/sitemap.xml [GET]

info: In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.

ZAP API Scan

Site: http://digital-library-app:3000

Alert 1: Insufficient Site Isolation Against Spectre Vulnerability

Risk: Low (Medium) | Confidence: 2 | PluginID: 90004 | Ref: 90004-1

CWE ID: 693

WASC ID: 14

Description: Cross-Origin-Resource-Policy header is an opt-in header designed to counter side-channels attacks like Spectre. Resource should be specifically set as shareable amongst different origins.

Solution: Ensure that the application/web server sets the Cross-Origin-Resource-Policy header appropriately, and that it sets the Cross-Origin-Resource-Policy header to 'same-origin' for all web pages.

'same-site' is considered as less secured and should be avoided.

If resources must be shared, set the header to 'cross-origin'.

If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Resource-Policy header (https://caniuse.com/mdn-http_headers_cross-origin-resource-policy).

References: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy

Instances:

- http://digital-library-app:3000/openapi.json [GET] param: Cross-Origin-Resource-Policy

Alert 2: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Risk: Low (Medium) | Confidence: 2 | PluginID: 10037 | Ref: 10037

CWE ID: 497

WASC ID: 13

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Solution: Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

References:
https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework
https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Instances:

- http://digital-library-app:3000/openapi.json [GET] | evidence: X-Powered-By: Express

Alert 3: Unexpected Content-Type was returned

Risk: Low (High) | Confidence: 3 | PluginID: 100001 | Ref: 100001

Description: A Content-Type of text/html was returned by the server.
This is not one of the types expected to be returned by an API.
Raised by the 'Alert on Unexpected Content Types' script

Instances:

- http://digital-library-app:3000 [GET] | evidence: text/html

- http://digital-library-app:3000/ [GET] | evidence: text/html

- http://digital-library-app:3000/2011816408338318277 [GET] | evidence: text/html

...and 5 more instances

Alert 4: X-Content-Type-Options Header Missing

Risk: Low (Medium) | Confidence: 2 | PluginID: 10021 | Ref: 10021

CWE ID: 693

WASC ID: 15

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Solution: Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

References:

https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)

https://owasp.org/www-community/Security_Headers

Instances:

- http://digital-library-app:3000/openapi.json [GET] param: x-content-type-options

info: This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scan rule will not alert on client or server error responses.

Alert 5: Storable and Cacheable Content

Risk: Informational (Medium) | Confidence: 2 | PluginID: 10049 | Ref: 10049

CWE ID: 524

WASC ID: 13

Description: The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

Solution: Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:

Cache-Control: no-cache, no-store, must-revalidate, private

Pragma: no-cache

Expires: 0

This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.

References: https://datatracker.ietf.org/doc/html/rfc7234

https://datatracker.ietf.org/doc/html/rfc7231

https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html

Instances:

- http://digital-library-app:3000/openapi.json [GET]

info: In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.

Sun, 20 Jul 2025 12:33:57 ZAP - 2.16.1

Dependency Check

Dependency 1: brace-expansion:1.1.11

Path: /src/package-lock.json?minimatch:3.1.2/brace-expansion:^1.1.7

Vulnerability: CVE-2025-5889

Severity: Medium

Description: A vulnerability was found in juliangruber brace-expansion up to 1.1.11/2.0.1/3.0.0/4.0.0. It has been rated as problematic. Affected by this issue is the function expand of the file index.js. The manipulation leads to inefficient regular expression complexity. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. Upgrading to version 1.1.12, 2.0.2, 3.0.1 and 4.0.1 is able to address this issue. The name of the patch is a5b98a4f30d7813266b221435e1eaaf25a1b0ac5. It is recommended to upgrade the affected component.

Reference:
https://ossindex.sonatype.org/vulnerability/CVE-2025-5889?component-type=npm&component-name=brace-expansion&utm_source=dependency-check&utm_medium=integration&utm_content=12.1.3
Reference: https://github.com/advisories/GHSA-v6h2-p8h4-qcjw
Reference: https://github.com/juliangruber/brace-expansion/pull/65
Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-5889

Vulnerability: GHSA-v6h2-p8h4-qcjw

Severity: Low

Description: A vulnerability was found in juliangruber brace-expansion up to 1.1.11/2.0.1/3.0.0/4.0.0. It has been rated as problematic. Affected by this issue is the function expand of the file index.js. The manipulation leads to inefficient regular expression complexity. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. Upgrading to version 1.1.12, 2.0.2, 3.0.1 and 4.0.1 is able to address this issue. The name of the patch is `a5b98a4f30d7813266b221435e1eaaf25a1b0ac5`. It is recommended to upgrade the affected component.

Reference: https://github.com/advisories/GHSA-v6h2-p8h4-qcjw
Reference: https://gist.github.com/mmmssttt404/37a40ce7d6e5ca604858fe30814d9466
Reference: https://vuldb.com/?submit.585717
Reference: https://nvd.nist.gov/vuln/detail/CVE-2025-5889
Reference: https://github.com/juliangruber/brace-expansion/pull/65/commits/a5b98a4f30d7813266b221435e1eaaf25a1b0ac5
Reference: https://github.com/juliangruber/brace-expansion/commit/15f9b3c75ebf5988198241fecaebdc45eff28a9f
Reference: https://github.com/juliangruber/brace-expansion/commit/36603d5f3599a37af9e85eda30acd7d28599c36e
Reference: https://vuldb.com/?id.311660
Reference: https://github.com/juliangruber/brace-expansion/commit/0b6a9781e18e9d2769bb2931f4856d1360243ed2
Reference: https://vuldb.com/?ctiid.311660
Reference: https://github.com/juliangruber/brace-expansion/commit/c3c73c8b088defc70851843be88ccc3af08e7217

Dependency 2: express:4.21.1

Path: /src/package-lock.json?/express:4.21.1

Vulnerability: CVE-2024-10491

Severity: Medium

Description: A vulnerability has been identified in the Express response.links function, allowing for arbitrary

resource injection in the Link header when unsanitized data is used.
The issue arises from improper sanitization in `Link` header values, which can allow a combination of characters like `,`, `;`, and `<>` to preload malicious resources.
This vulnerability is especially relevant for dynamic parameters.
Sonatype's research suggests that this CVE's details differ from those defined at NVD. See https://ossindex.sonatype.org/vulnerability/CVE-2024-10491 for details
Reference: https://ossindex.sonatype.org/vulnerability/CVE-2024-10491?component-type=npm&component-name=express&utm_source=dependency-check&utm_medium=integration&utm_content=12.1.3
Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-10491
Reference: https://www.herodevs.com/vulnerability-directory/cve-2024-10491

Dependency 3: path-to-regexp:0.1.10

Path: /src/package-lock.json?/path-to-regexp:0.1.10

Vulnerability: CVE-2024-52798

Severity: High
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 in the 0.1.x release of path-to-regexp. Upgrade to 0.1.12. This vulnerability exists because of an incomplete fix for CVE-2024-45296.
Reference: https://github.com/pillarjs/path-to-regexp/security/advisories/GHSA-rhx6-c78j-4q9w
Reference: https://ossindex.sonatype.org/vulnerability/CVE-2024-52798?component-type=npm&component-name=path-to-regexp&utm_source=dependency-check&utm_medium=integration&utm_content=12.1.3
Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-52798

Vulnerability: GHSA-rhx6-c78j-4q9w

Severity: High
Description: ### Impact
The regular expression that is vulnerable to backtracking can be generated in versions before 0.1.12 of `path-to-regexp`, originally reported in CVE-2024-45296
Patches
Upgrade to 0.1.12.
Workarounds
Avoid using two parameters within a single path segment, when the separator is not `.` (e.g. no `/:a-:b`). Alternatively, you can define the regex used for both parameters and ensure they do not overlap to allow backtracking.
References
- https://github.com/advisories/GHSA-9wv6-86v2-598j
- https://blakeembrey.com/posts/2024-09-web-redos/
Reference: https://blakeembrey.com/posts/2024-09-web-redos
Reference: https://github.com/pillarjs/path-to-regexp/commit/f01c26a013b1889f0c217c643964513acf17f6a4
Reference: https://github.com/advisories/GHSA-rhx6-c78j-4q9w
Reference: https://security.netapp.com/advisory/ntap-20250124-0002
Reference: https://github.com/pillarjs/path-to-regexp/security/advisories/GHSA-rhx6-c78j-4q9w
Reference: https://nvd.nist.gov/vuln/detail/CVE-2024-52798

Generated by DevSecOps Pipeline 20-07-2025 12:46:38