

ZAP Scanning Report

Site: <http://localhost:3333>

Generated on Mon, 19 Aug 2024 10:43:10

ZAP Version: 2.15.0

ZAP is supported by the [Crash Override Open Source Fellowship](#)

Summary of Alerts

| Risk Level | Number of Alerts |
|---------------|------------------|
| High | 0 |
| Medium | 1 |
| Low | 1 |
| Informational | 0 |

Alerts

| Name | Risk Level | Number of Instances |
|---|------------|---------------------|
| CSP: Wildcard Directive | Medium | 2 |
| X-Content-Type-Options Header Missing | Low | 4 |

Alert Detail

| Medium | CSP: Wildcard Directive |
|-------------|--|
| Description | Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files. |
| URL | http://localhost:3333/robots.txt |
| Method | GET |
| Attack | |
| Evidence | default-src 'none' |
| Other Info | The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything. |
| URL | http://localhost:3333/sitemap.xml |
| Method | GET |
| Attack | |
| Evidence | default-src 'none' |
| | |

| | |
|------------|---|
| Other Info | The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything. |
| Instances | 2 |
| Solution | Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header. |
| Reference | 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 |
| CWE Id | 693 |
| WASC Id | 15 |
| Plugin Id | 10055 |

| | |
|-------------|--|
| Low | X-Content-Type-Options Header Missing |
| 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. |
| URL | http://localhost:3333/api/v1/categories |
| Method | GET |
| Attack | |
| Evidence | |
| Other 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. |
| URL | http://localhost:3333/api/v1/customers |
| Method | GET |
| Attack | |
| Evidence | |
| Other 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. |
| URL | http://localhost:3333/api/v1/orders |
| Method | GET |
| Attack | |
| Evidence | |
| Other 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. |
| URL | http://localhost:3333/api/v1/products |
| Method | GET |
| Attack | |
| | |

| | |
|------------|--|
| Evidence | |
| Other 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. |
| Instances | 4 |
| Solution | <p>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.</p> <p>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.</p> |
| Reference | 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 |
| CWE Id | 693 |
| WASC Id | 15 |
| Plugin Id | 10021 |