**ZAP Security Scan Report**

**Generated by**: ZAP by Checkmarx  
**Scan Date**: Tue, 7 Jan 2025, at 10:14:57  
**ZAP Version**: 2.15.0  
**Report Generated for**: http://localhost:3000

**1. About This Report**

This report contains the results of a security scan performed using ZAP by Checkmarx. It highlights vulnerabilities found in the web application hosted at http://localhost:3000.

**Report Parameters:**

* **Contexts**: No contexts were selected, so all contexts were included by default.
* **Sites Scanned**: http://localhost:3000
* **Risk Levels Included**: High, Medium, Low, Informational
* **Confidence Levels Included**: User Confirmed, High, Medium, Low

**2. Summaries**

**2.1 Alert Counts by Risk and Confidence**

| **Confidence Level** | **High** | **Medium** | **Low** | **Informational** | **Total** |
| --- | --- | --- | --- | --- | --- |
| User Confirmed | 0 | 0 | 0 | 0 | 0 |
| High | 0 | 0 | 0 | 0 | 0 |
| Medium | 0 | 2 | 2 | 0 | 4 |
| Low | 0 | 0 | 3 | 1 | 4 |
| Informational | 0 | 0 | 1 | 1 | 2 |
| **Total** | 0 | 2 | 6 | 3 | 11 |

**2.2 Alert Counts by Site and Risk**

| **Site** | **High** | **Medium** | **Low** | **Informational** | **Total** |
| --- | --- | --- | --- | --- | --- |
| http://localhost:3000 | 1 | 4 | 4 | 2 | 11 |

**2.3 Alert Counts by Alert Type**

| **Alert Type** | **Risk** | **Count** |
| --- | --- | --- |
| Cloud Metadata Potentially Exposed | High | 1 |
| Content Security Policy (CSP) Header Not Set | Medium | 1 |
| Session ID in URL Rewrite | Medium | 1 |
| Cross-Domain Misconfiguration | Medium | 1 |
| Missing Anti-clickjacking Header | Medium | 1 |
| Cross-Domain JavaScript Source File Inclusion | Low | 1 |
| Private IP Disclosure | Low | 1 |
| Timestamp Disclosure - Unix | Low | 1 |
| X-Content-Type-Options Header Missing | Low | 1 |
| Information Disclosure - Suspicious Comments | Informational | 1 |
| Modern Web Application | Informational | 1 |

**3. Alerts**

**3.1 Risk=High, Confidence=Low**

* **Cloud Metadata Potentially Exposed**
  + **URL**: http://localhost:3000/latest/meta-data/
  + **Description**: Cloud metadata is exposed, which can potentially lead to security risks.

**3.2 Risk=Medium, Confidence=High**

* **Content Security Policy (CSP) Header Not Set**
  + **URL**: http://localhost:3000/
  + **Description**: The website lacks a Content Security Policy (CSP) header, leaving the site vulnerable to XSS attacks.
* **Session ID in URL Rewrite**
  + **URL**: http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=xBlMi6eLl\_AtmeeTAAAC
  + **Description**: The session ID is exposed in the URL, which could lead to session hijacking.

**3.3 Risk=Medium, Confidence=Medium**

* **Cross-Domain Misconfiguration**
  + **URL**: http://localhost:3000/
  + **Description**: The application is misconfigured for cross-origin resource sharing (CORS), allowing cross-domain requests that could be exploited.
* **Missing Anti-clickjacking Header**
  + **URL**: http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PGTY60q&sid=xBlMi6eLl\_AtmeeTAAAC
  + **Description**: The application does not include the X-Frame-Options header, making it vulnerable to clickjacking attacks.

**3.4 Risk=Low, Confidence=Medium**

* **Cross-Domain JavaScript Source File Inclusion**
  + **URL**: http://localhost:3000/
  + **Description**: The application is vulnerable to cross-domain JavaScript inclusion, which can lead to malicious scripts being executed.
* **Private IP Disclosure**
  + **URL**: http://localhost:3000/rest/admin/application-configuration
  + **Description**: The application leaks internal/private IP addresses.
* **X-Content-Type-Options Header Missing**
  + **URL**: http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PGTY5wA
  + **Description**: The X-Content-Type-Options header is missing, which could allow MIME type sniffing attacks.

**3.5 Risk=Low, Confidence=Low**

* **Timestamp Disclosure - Unix**
  + **URL**: http://localhost:3000/main.js
  + **Description**: Unix timestamps are exposed in a publicly accessible JavaScript file.

**3.6 Risk=Informational, Confidence=Medium**

* **Information Disclosure - Suspicious Comments**
  + **URL**: http://localhost:3000/main.js
  + **Description**: Suspicious comments were found within the JavaScript file that may leak sensitive information.

**3.7 Risk=Informational, Confidence=Low**

* **Modern Web Application**
  + **URL**: http://localhost:3000/
  + **Description**: The application is detected as a modern web application, which may provide a target for specific vulnerabilities.

**4. Recommendations**

**1. Cloud Metadata Exposure**

* **Action**: Secure cloud metadata to prevent unauthorized access. Ensure that metadata endpoints are not publicly accessible.

**2. Content Security Policy (CSP)**

* **Action**: Implement a Content Security Policy header to restrict which resources can be loaded by the browser, helping mitigate XSS attacks.

**3. Session ID in URL**

* **Action**: Never expose session IDs in URLs. Use secure, HttpOnly cookies for session management to prevent session hijacking.

**4. Cross-Domain Misconfiguration**

* **Action**: Review and configure CORS to only allow trusted origins to access the application’s resources.

**5. Anti-clickjacking Header**

* **Action**: Set the X-Frame-Options header to DENY or SAMEORIGIN to protect against clickjacking attacks.

**6. Cross-Domain JavaScript Source File Inclusion**

* **Action**: Ensure that JavaScript files are not sourced from untrusted domains and mitigate potential cross-domain script inclusions.

**7. Private IP Disclosure**

* **Action**: Avoid exposing internal/private IP addresses. Ensure proper security configurations for API endpoints.

**8. X-Content-Type-Options Header**

* **Action**: Set the X-Content-Type-Options: nosniff header to prevent MIME-sniffing attacks.

**9. Timestamp Disclosure**

* **Action**: Avoid exposing timestamps or any other sensitive information in publicly accessible files like JavaScript.

**10. Information Disclosure**

* **Action**: Review JavaScript files for any suspicious comments that may inadvertently disclose sensitive information.

**11. Modern Web Application Detection**

* **Action**: Regularly review and test the application to ensure it adheres to the latest security best practices for modern web applications.

**5. Conclusion**

This report highlights several high, medium, and low-risk vulnerabilities on the web application hosted at http://localhost:3000. By addressing the issues outlined, particularly the high-risk cloud metadata exposure and session management, you will significantly improve the application's security posture.

4o mini