

1. Content Security Policy (CSP) Header Not Set

URL-<http://localhost:3000/>

DESCRIPTION- types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

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

The screenshot shows a software interface for managing security alerts. On the left, there's a sidebar with icons for search, refresh, and other functions. Below it is a tree view under the 'Alerts (6)' category, with one item selected: 'Content Security Policy (CSP) Header Not Set (Systemic)'. To the right of the tree view is a detailed panel for this specific alert:

Content Security Policy (CSP) Header Not Set	
URL:	http://localhost:3000/
Risk:	Medium
Confidence:	High
Parameter:	
Attack:	
Evidence:	
CWE ID:	693
WASC ID:	15
Source:	Passive (10038 - Content Security Policy (CSP) Header Not Set)
Alert Reference:	10038-1
Input Vector:	

2. Cross-Domain Misconfiguration

DESCRIPTION-Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

OTHER INFO-The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

SOLUTION-Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

The screenshot shows a software interface for monitoring web application security. The top navigation bar includes tabs for History, Search, Alerts, Output, Spider, AJAX Spider, Active Scan, and a plus sign icon. Below the navigation is a toolbar with icons for refresh, search, and various tools. A sidebar on the left lists 'Alerts (6)' with several items: Content Security Policy (CSP) Header Not Set (Systemic), Cross-Domain Misconfiguration (Systemic) (which is selected), Cross-Domain JavaScript Source File Inclusion (Systemic), Timestamp Disclosure - Unix (Systemic), Information Disclosure - Suspicious Comments (2), and Modern Web Application (Systemic). The main panel displays detailed information about the selected alert:

Cross-Domain Misconfiguration

URL: http://localhost:3000/runtime.js
Risk: Medium
Confidence: Medium
Parameter: |
Attack:
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)
Input Vector:
Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

3.Cross-Domain JavaScript Source File Inclusion

DESCRIPTION-The page includes one or more script files from a third-party domain.

SOLUTION-Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

The screenshot shows a software interface for monitoring web application security. The top navigation bar includes tabs for History, Search, Alerts, Output, Spider, AJAX Spider, Active Scan, and a plus sign icon. Below the navigation is a toolbar with icons for refresh, search, and various tools. A sidebar on the left lists 'Alerts (6)' with several items: Content Security Policy (CSP) Header Not Set (Systemic), Cross-Domain Misconfiguration (Systemic), Cross-Domain JavaScript Source File Inclusion (Systemic) (which is selected), Timestamp Disclosure - Unix (Systemic), Information Disclosure - Suspicious Comments (2), and Modern Web Application (Systemic). The main panel displays detailed information about the selected alert:

Cross-Domain JavaScript Source File Inclusion

URL: http://localhost:3000/
Risk: Low
Confidence: Medium
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Attack:
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829
WASC ID: 15
Source: Passive (10017 - Cross-Domain JavaScript Source File Inclusion)
Input Vector:
Description:

4.Timestamp Disclosure - Unix

DESCRIPTION-A timestamp was disclosed by the application/web server. - Unix

SOLUTION-Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

The screenshot shows a software interface for monitoring web application security. At the top, there are tabs for History, Search, Alerts, Output, Spider, AJAX Spider, Active Scan, and a plus sign icon. Below the tabs, there are icons for refresh, search, and other functions. A sidebar on the left lists 'Alerts (6)' with sub-items: Content Security Policy (CSP) Header Not Set (Systemic), Cross-Domain Misconfiguration (Systemic), Cross-Domain JavaScript Source File Inclusion (Systemic), Timestamp Disclosure - Unix (Systemic), Information Disclosure - Suspicious Comments (2), and Modern Web Application (Systemic). The 'Timestamp Disclosure - Unix (Systemic)' item is selected and highlighted with a blue background. To the right of the sidebar, detailed information about this alert is displayed:

Timestamp Disclosure - Unix

URL: http://localhost:3000/
Risk: Low
Confidence: Low
Parameter:
Attack:
Evidence: 1650485437
CWE ID: 497
WASC ID: 13
Source: Passive (10096 - Timestamp Disclosure)
Input Vector:
Description: A timestamp was disclosed by the application/web server. - Unix

5.Information Disclosure - Suspicious Comments

DESCRIPTION-The response appears to contain suspicious comments which may help an attacker.

SOLUTION-Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

The screenshot shows a software interface for monitoring web application security. At the top, there are tabs for History, Search, Alerts, Output, Spider, AJAX Spider, Active Scan, and a plus sign icon. Below the tabs, there are icons for refresh, search, and other functions. A sidebar on the left lists 'Alerts (6)' with sub-items: Content Security Policy (CSP) Header Not Set (Systemic), Cross-Domain Misconfiguration (Systemic), Cross-Domain JavaScript Source File Inclusion (Systemic), Timestamp Disclosure - Unix (Systemic), Information Disclosure - Suspicious Comments (2), and Modern Web Application (Systemic). The 'Information Disclosure - Suspicious Comments (2)' item is selected and highlighted with a blue background. To the right of the sidebar, detailed information about this alert is displayed:

Information Disclosure - Suspicious Comments

URL: http://localhost:3000/main.js
Risk: Informational
Confidence: Low
Parameter:
Attack:
Evidence: query
CWE ID: 615
WASC ID: 13
Source: Passive (10027 - Information Disclosure - Suspicious Comments)
Input Vector:
Description: The response appears to contain suspicious comments which may help an attacker.

6.Modern Web Application

DESCRIPTION-The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

OTHER INFO-No links have been found while there are scripts, which is an indication that this is a modern web application.

SOLUTION-This is an informational alert and so no changes are required.

The screenshot shows a software interface for web application security testing. At the top, there are several tabs: History, Search, Alerts (which is currently selected), Output, Spider, AJAX Spider, Active Scan, and a plus sign icon. Below the tabs is a toolbar with icons for refresh, search, and other functions. On the left, there is a sidebar with a tree view under the 'Alerts' node, which contains six items: Content Security Policy (CSP) Header Not Set (Systemic), Cross-Domain Misconfiguration (Systemic), Cross-Domain JavaScript Source File Inclusion (Systemic), Timestamp Disclosure - Unix (Systemic), Information Disclosure - Suspicious Comments (2), and Modern Web Application (Systemic). The 'Modern Web Application (Systemic)' item is highlighted with a blue selection bar. To the right of the sidebar, detailed information about this alert is displayed in a panel:

Modern Web Application

URL: http://localhost:3000/
Risk: Informational
Confidence: Medium
Parameter:
Attack:
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID:
WASC ID:
Source: Passive (10109 - Modern Web Application)
Input Vector:
Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.