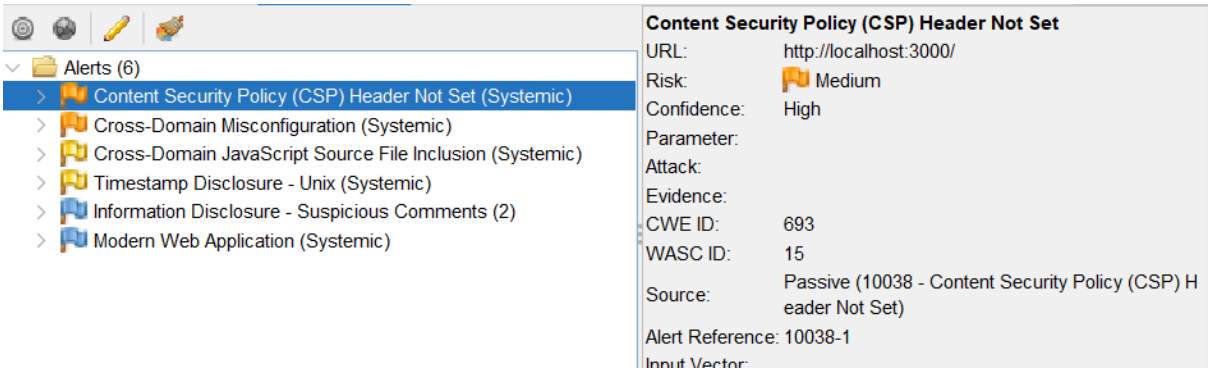
1. Content Security Policy (CSP) Header Not Set

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.

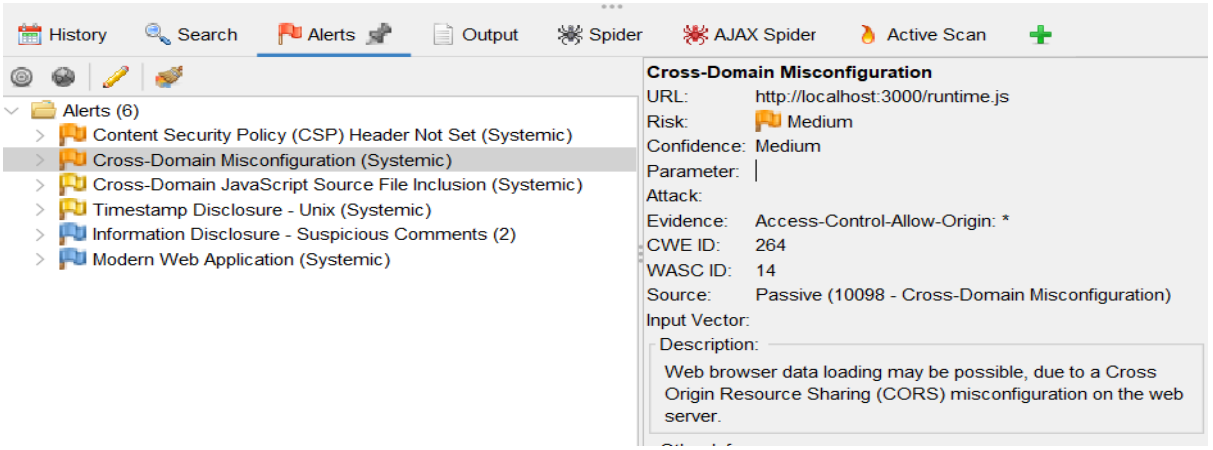


2. Cross-Domain Misconfiguration

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.

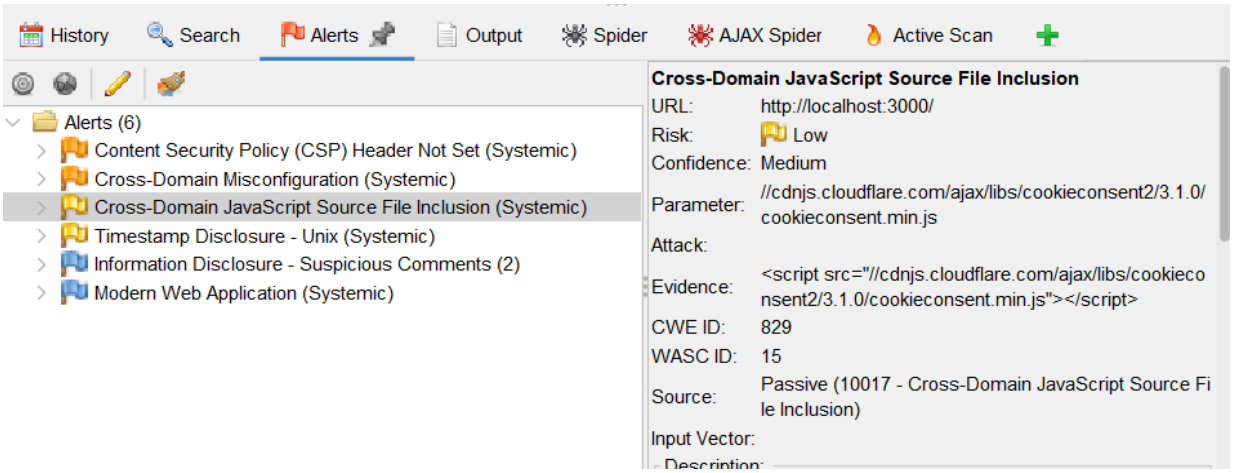
SOLUTION-Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).



3.Cross-Domain JavaScript Source File Inclusion

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

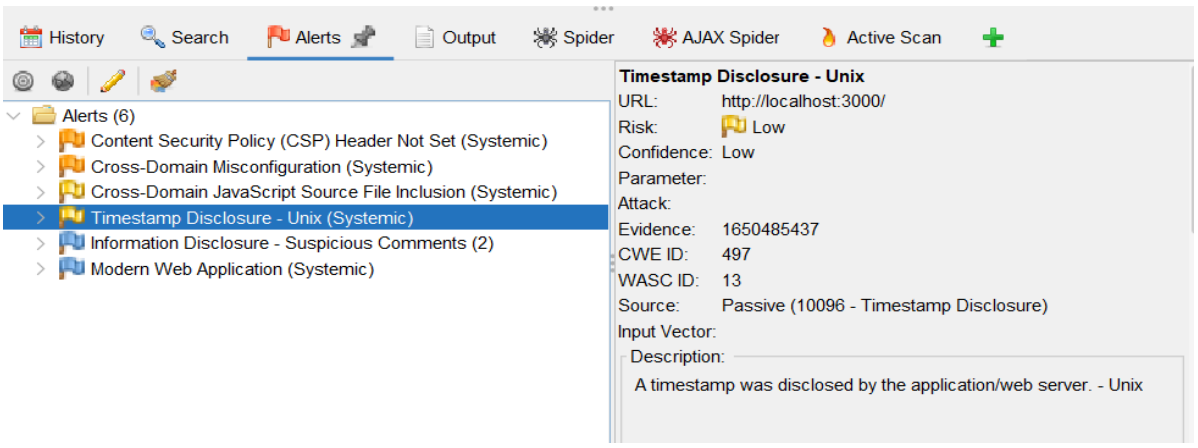
SOLUTION-Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.



4.Timestamp Disclosure - Unix

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

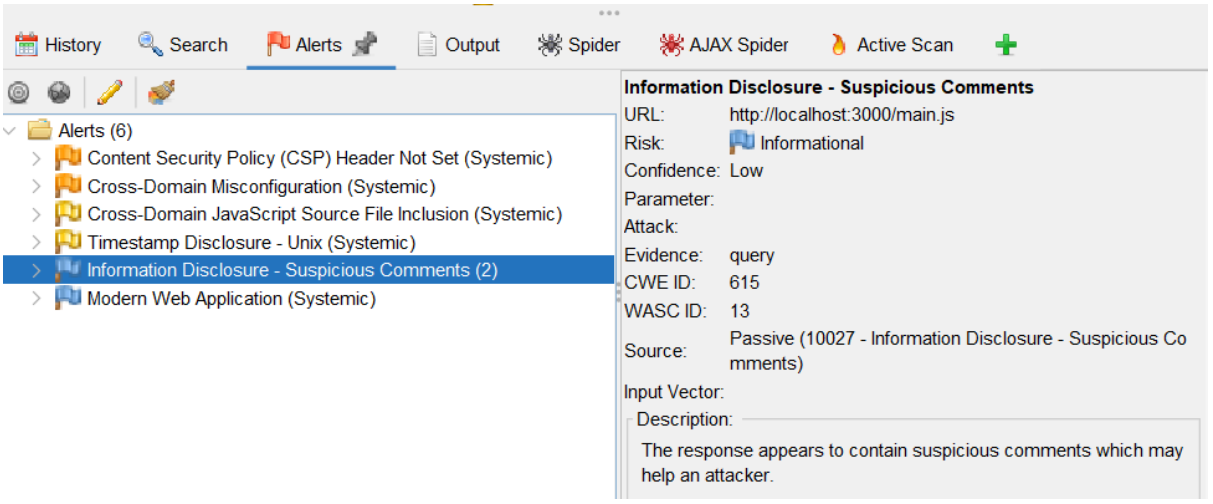
SOLUTION-Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.



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.



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.