Cross-Domain Misconfiguration

Description:

The website https://beta4.digitallocker.gov.in/signin# was scanned using OWASP ZAP. Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

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.

Risk: Medium

Solution:

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

References:

http://www.hpenterprisesecurity.com/vulncat/en/vulncat/vb/html5_overly_permissive_cors_policy.html

Evidence: Access-Control-Allow-Origin: *