**Missing x frame options header**

Severity: low

Summery: Used to indicate whether or not a browser should be allowed to render a page in a <frame> , <iframe> , <embed>**.**

Impact: When a user click on the top level page the attacker will hijack and routing them to another page.

Remediation: send the proper x-frame-options in http response header and employing defensive code

**Content-Security-Policy(benefit)**

Severity: best practice

Summary: an added layer of security that helps to detect and mitigate certain types of attacks, including Cross-Site Scripting (XSS) and data injection attacks.

Impact: there is no direct impact but it helps to prevent the cross site scripting

Remediation:separate multiple directives with a semicolon.

**x permitted cross domain policies**

Severity: low

Summary: a user-defined set of permitted data access rules encapsulated in a crossdomain. xml file.

Impact: Allow harmful requests from Adobe Flash or PDF documents.

Remediation: Unless the application requires Adobe products, set the X-Permitted-Cross-Domain-Policies to none in the server responses.