ZAP report - salesforce1.kayako.com

Medium:

X-Frame-Options Header Not Set

This is false positive because in API endpoint X-Framing is not required. It is required for preventing clickjacking only in case of an UI application.

Reference:
http://stackoverflow.com/questions/34044966/is-it-meaningful-to-add-x-frame-options-in-an-restful-api

Low:

Private IP Disclosure

The API response returns the last seen IP of the user, therefore this error is flagged up. It provides no immediate threat.

X-Content-Type-Options Header Missing

This is not required as it is an API response and provides no immediate threat.

Web Browser XSS Protection Not Enabled

X-XSS-Protection header is provided in the response of parent page, all the further API requests are made through AJAX, and hence they don't require the header to be present since it is already present in the parent page. This is a false positive.

Cookie Without Secure Flag

It is referring to the wrong cookie. It interprets "cookie delete" as "cookie set". Our session cookies use **Secure Flag** and they cannot be sniffed in http requests.

Cross-Domain JavaScript Source File Inclusion

We use a cdn service for serving the static files, and hence all the static content like JS is served from a CDN. Since we control the content coming from this CDN, hence it provides no threat to our application.

Cookie No HttpOnly Flag

We cannot use HttpOnly because our JavaScript uses of these cookies. We have other measures to protect XSS attacks.