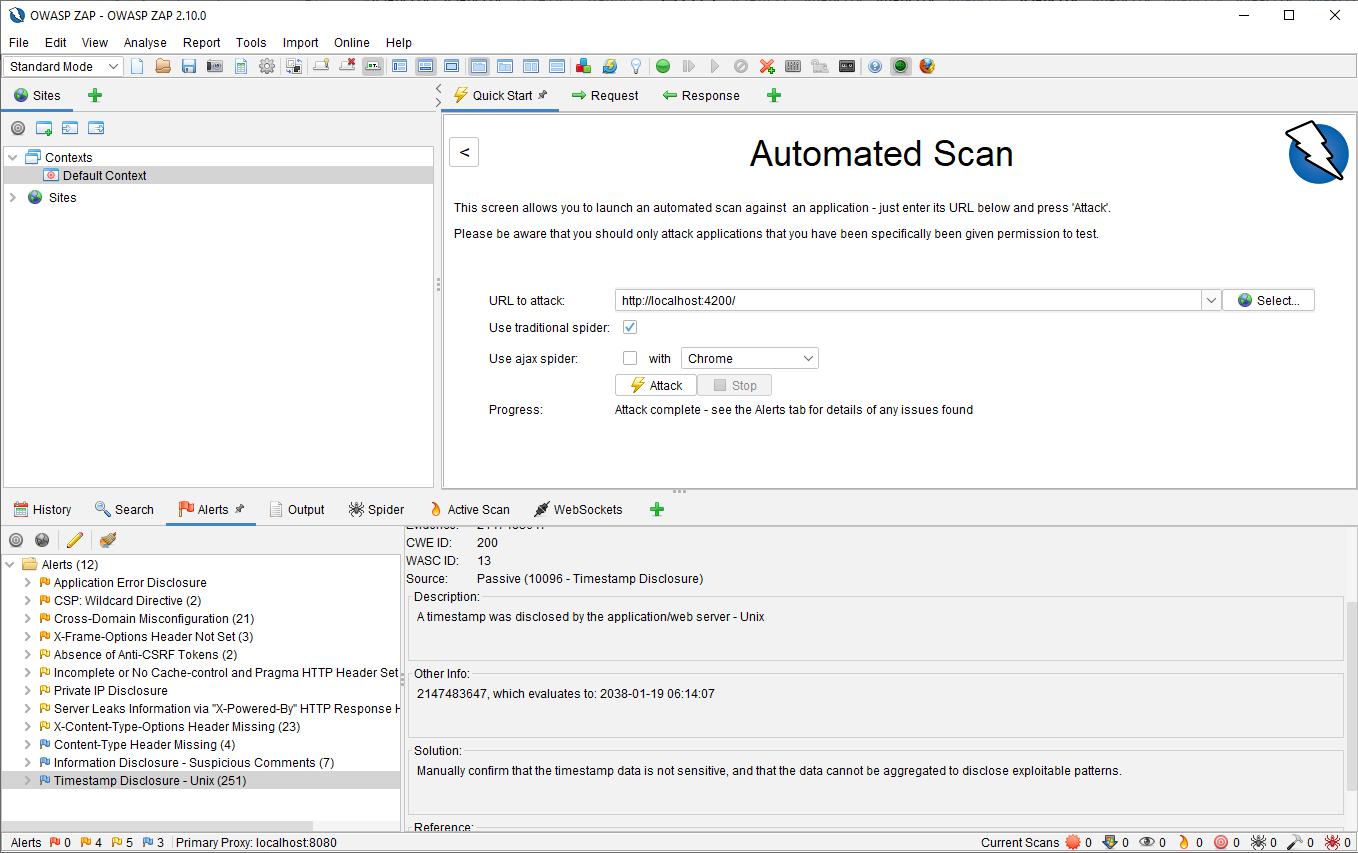
**Отчет по лабораторной работе анализ сайта утилитой OWASP ZAP**

В рамках лабораторной работы было установлено программное обеспечение OWASP ZAP и проведено тестирование сайта, который представляет собой канбан доску для управления проектами.

В ходе проверки не было выявлено предупреждений критического уровня но было выявлено 4 типа средних, 3 низких и 3 информационных.  


Application Error Disclosure – говорит о том что необработанные ошибки исключений отправляются клиенту и потенциально могут нести важную информацию о серверной части приложения.

Было исправлено путем добавления в конвейер обработки дополнительного обработчика ошибок, который в случае неописанной ошибки возвращает костюмную страницу об ошибке.

CSP: Wildcard Directive – говорит об отсутствие настроенной cors политики.

Cross-Domain Misconfiguration – так же связанно с отсутствием настроенной CORS политики.

X-Frame-Options Header Not Set – так же связанна с отсутствием нормальной настройки CORS политики.

Были исправлены путем обновления CORS политики.

Absence of Anti-CSRF Tokens – говорит об отсутствие anti-csrf токенов в формах отправки. Что может повлечь подделку межсайтового запроса.

Была исправлена путем добавления библиотеки anti-CRSF

Incomplete or No Cache-control and Pragma HTTP Header Set – говорит о том что http заголовки не установлены правильно что позволяет браузером кэшировать запросы.

Была исправлена путем настройки заголовков.

Private IP – говорит о том что в респонзе содержится локальный IP.

Исправлен путем удаления приватного IP адреса из респонза.

По итогу виду простоты проекта и использования стандартных инструментов виде web api и angular библиотек почти все ошибки связанны лишь с неправильной настройкой заголовком респонза.

Результат проверки после исправлений

