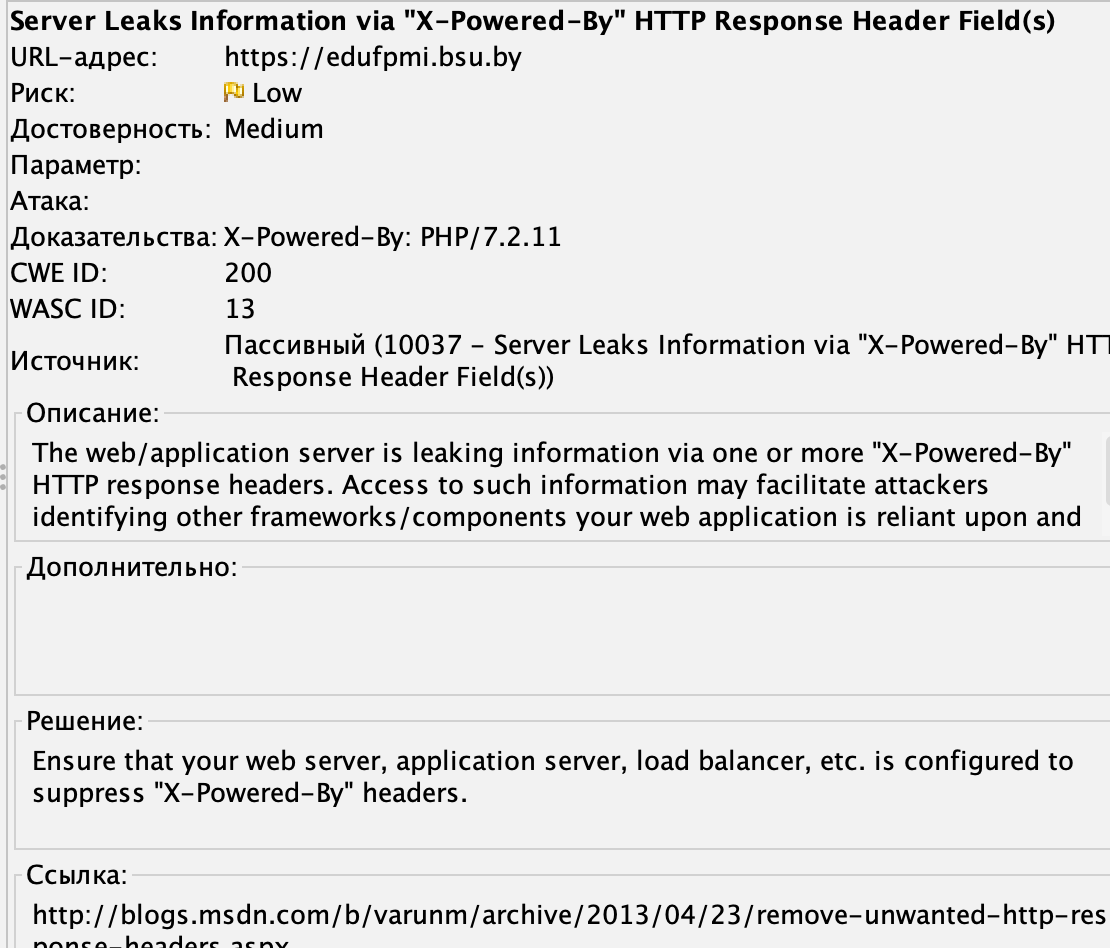
**Отчет по лабораторной работе №5**

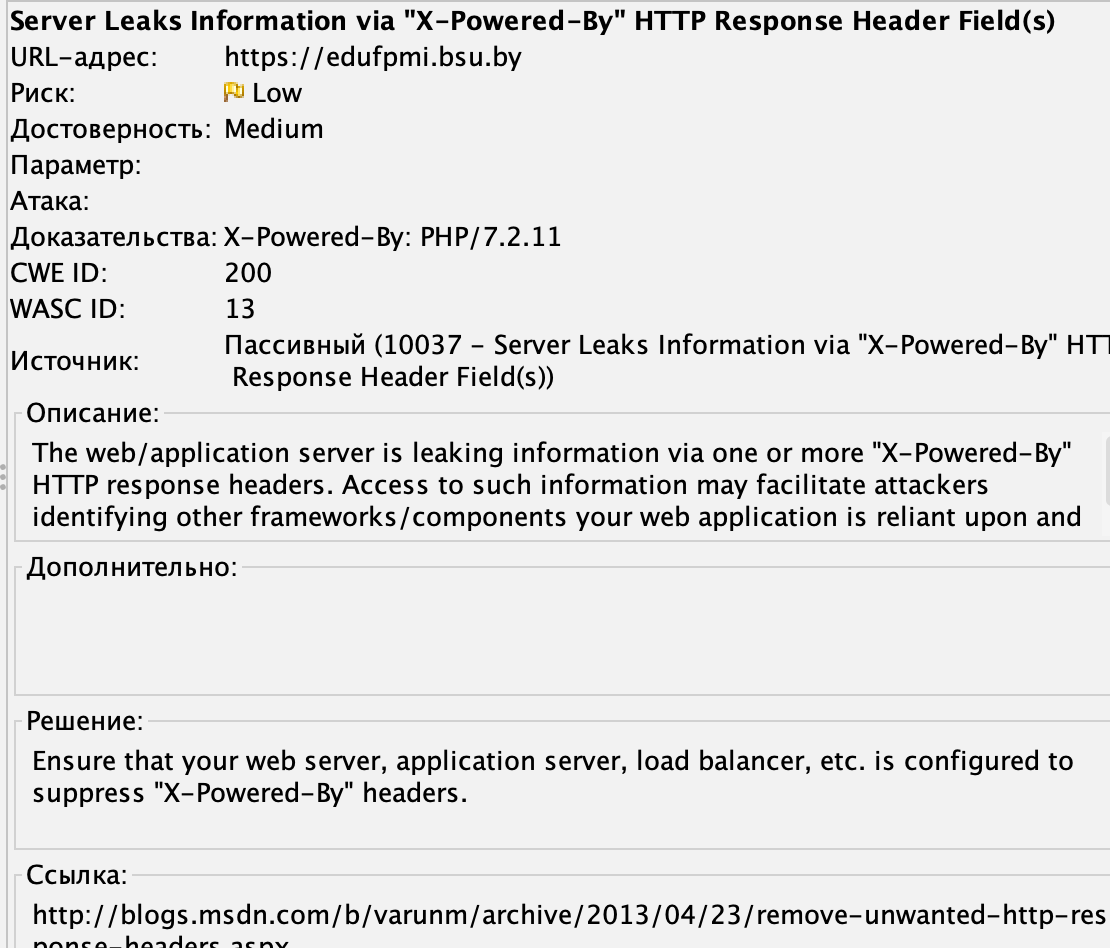
**Анализ уязвимостей с помощью OWASP ZAP**

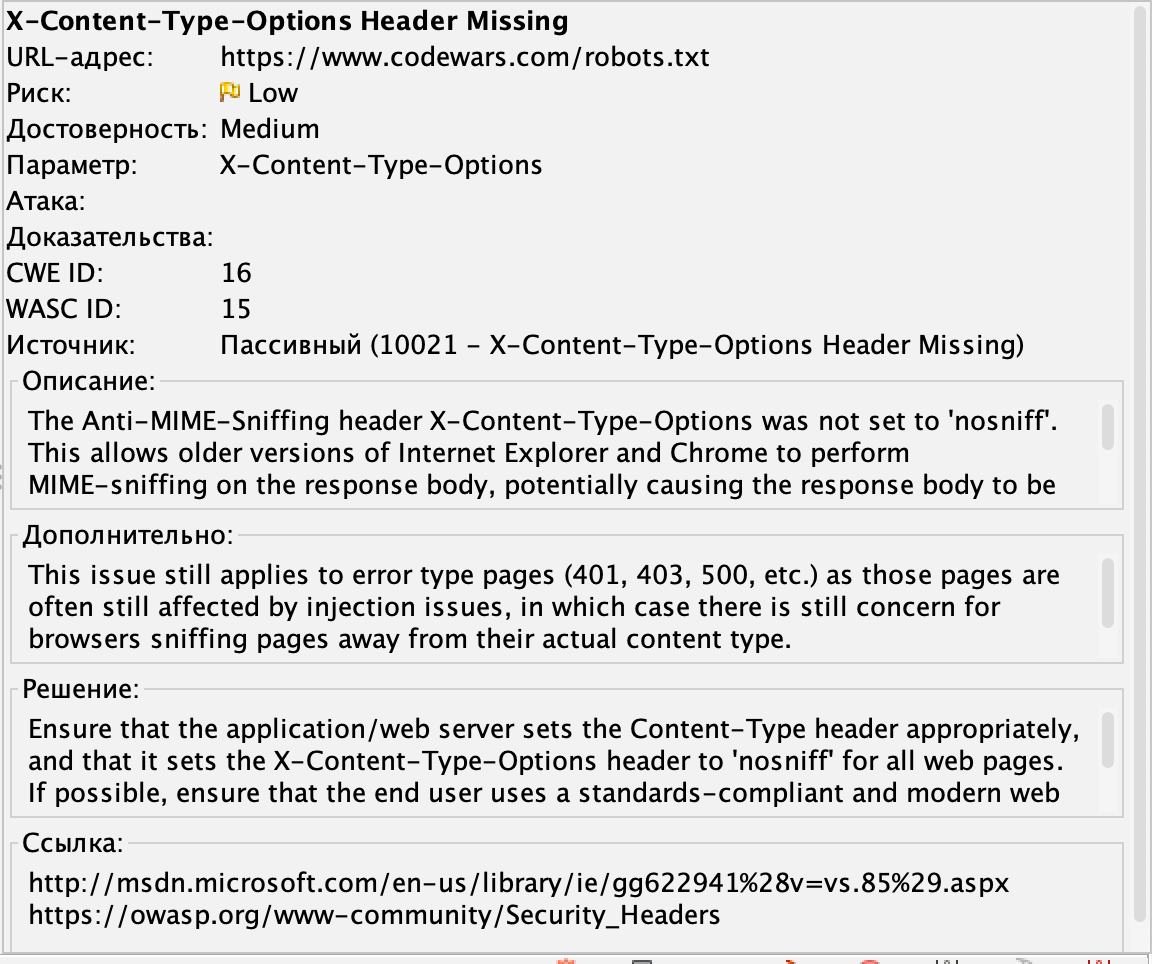
Для анализа на уязвимости использовалась система дистанционного обучения БГУ - edufpmi.bsu.by. Для должного исследования должно быть создано виртуальное окружение для системы, которая должна запускаться локально. Я не успела разобраться, как установить у себя систему подобного рода, потому просто провела анализ по url адресу образовательного портала и рассмотрела уязвисомти и способы их решения.

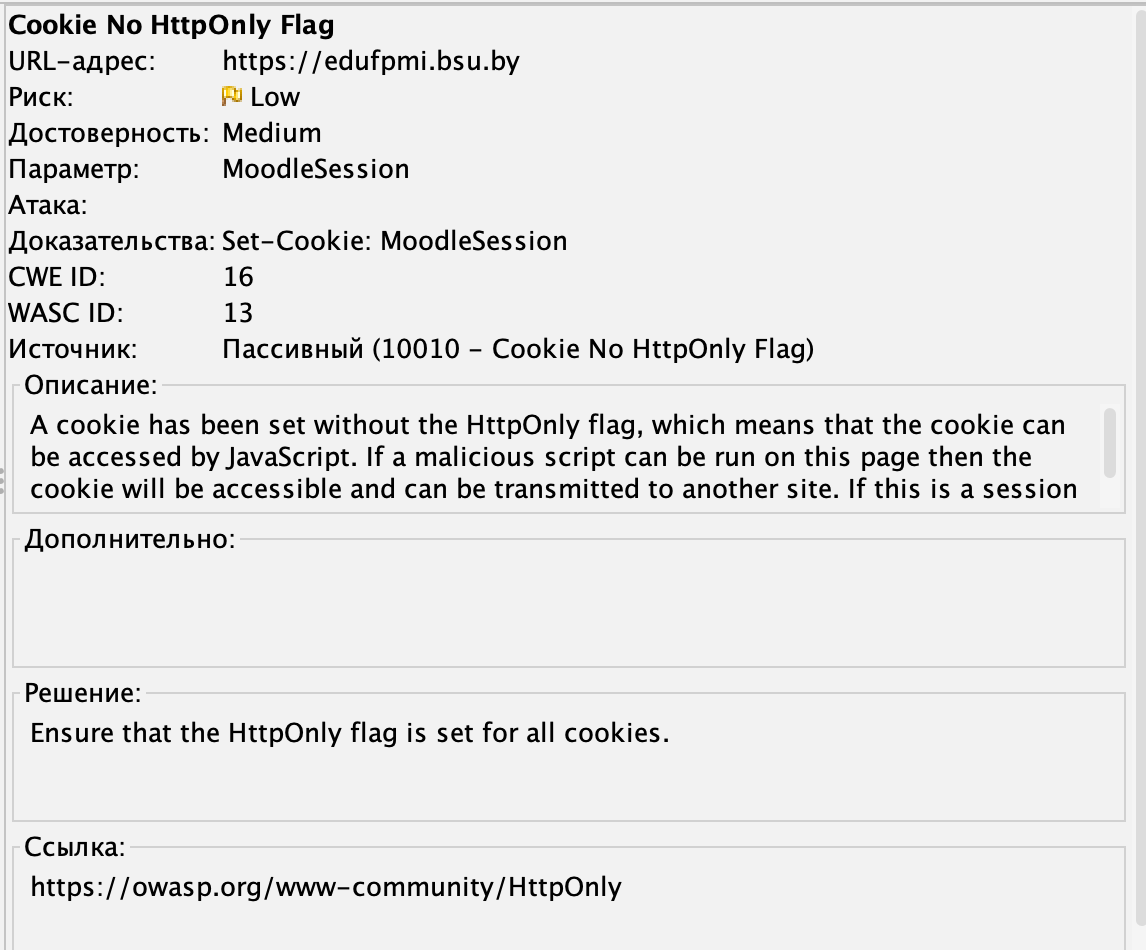
Для анализа уязвимостей портала был установлен программный инструментарий под названием OWASP ZAP.

Были обнаружены следующие уязвимости:

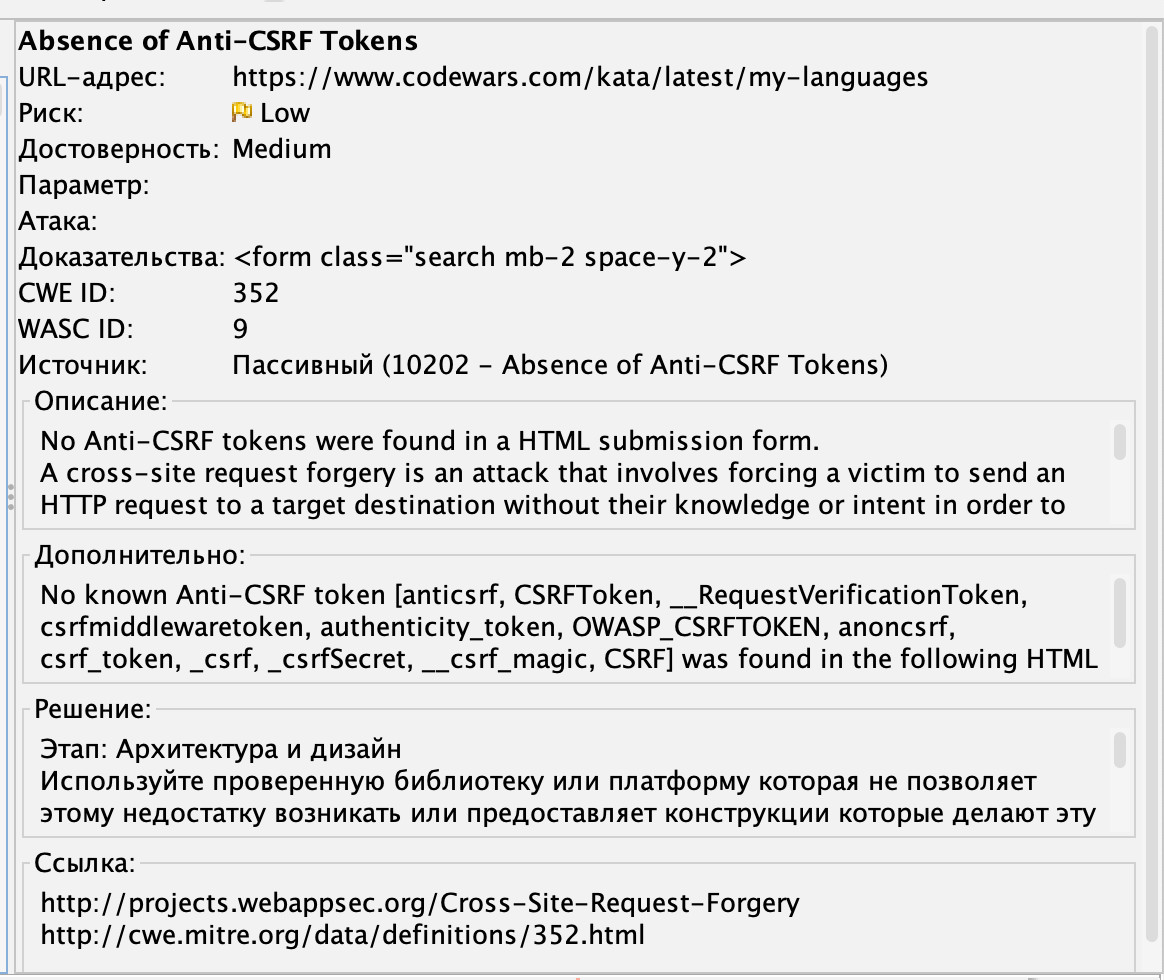




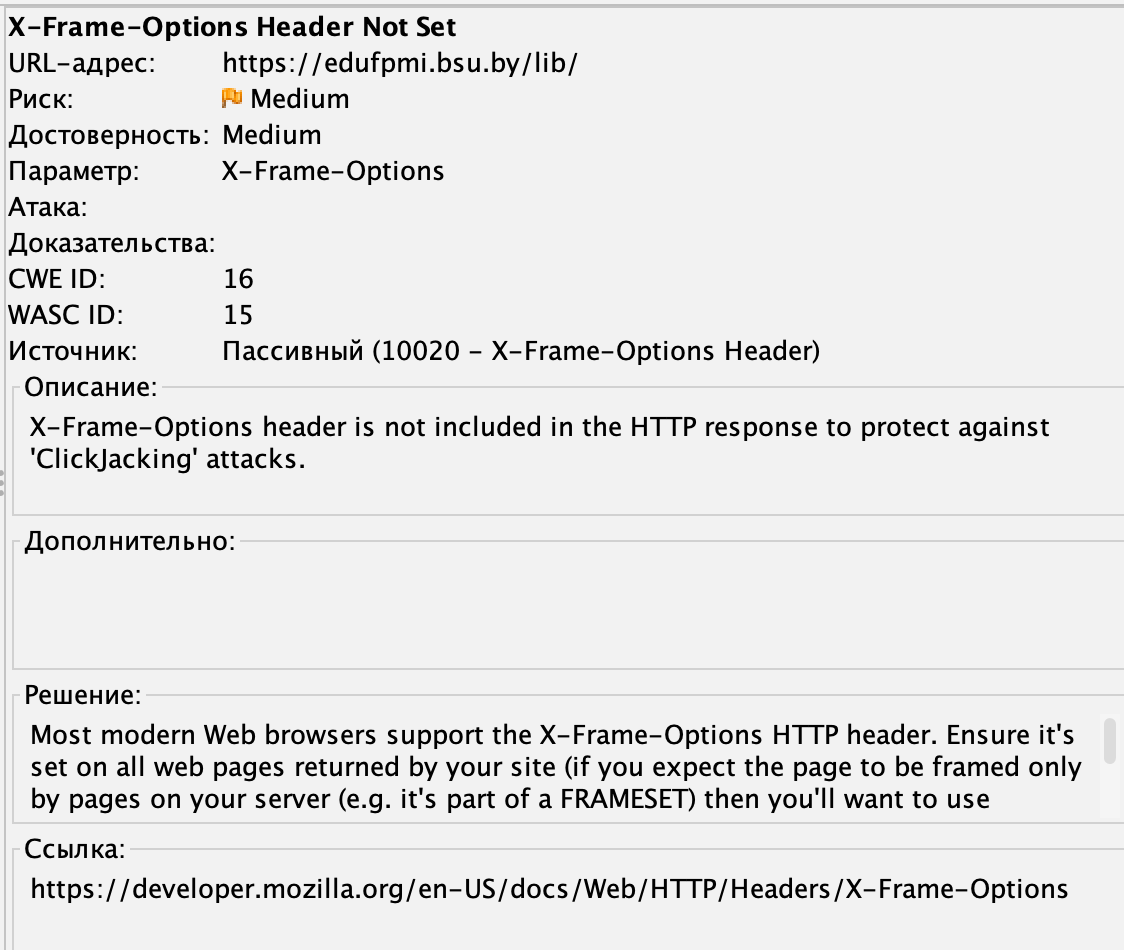




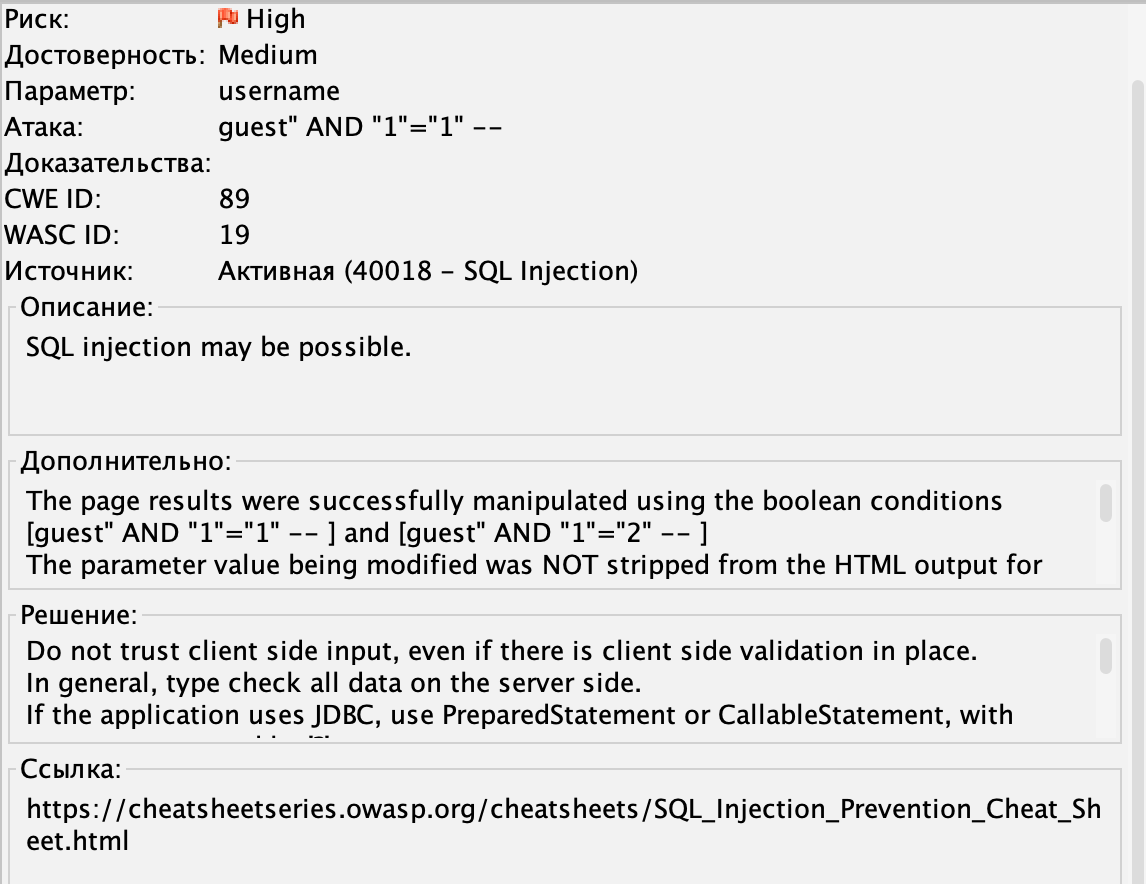
Приведенные выше уязвимости означают отсутствие некоторых необходимых HTTP-флагов и header-ов. Как указано в блоках решения данных уязвимостей, достаточно просто добавить недостающие элементы, чтобы избавиться от проблемы.



Данная уязвимость (выше) заключается в «подделке» межсайтовых запросов. Браузер отправляет токены аутентификации с каждым новым запросом, от лица жетвы на сайте злоумышленника отправляется запрос на другой сервер, который осуществляет вредоносные операции. Данная уязвимость исправляется путем добавления AntiforgeryFieldName.



А эта уязвимость может быть использована при атаке Кликджекингом (пользователь получает ссылку на вредоносный контент, что дает возможность получения доступа к аккаунту пользователя. Данный тип атаки используется для получения доступа к функции автозаполнения менеджера паролей. Для устранения уязвимости необходимо использовать HTTP-заголовок X-Frame-Options.



Уязвимость с наибольшим уровнем риска заключается в возможности проведения SQL injection. Для устранения этой уязвимости можно использовать PreparedStatement или CallableStatement на стороне сервера.