Лабораторная работа 5

Студента 4 курса 12 группы

Жумигиной Евгении

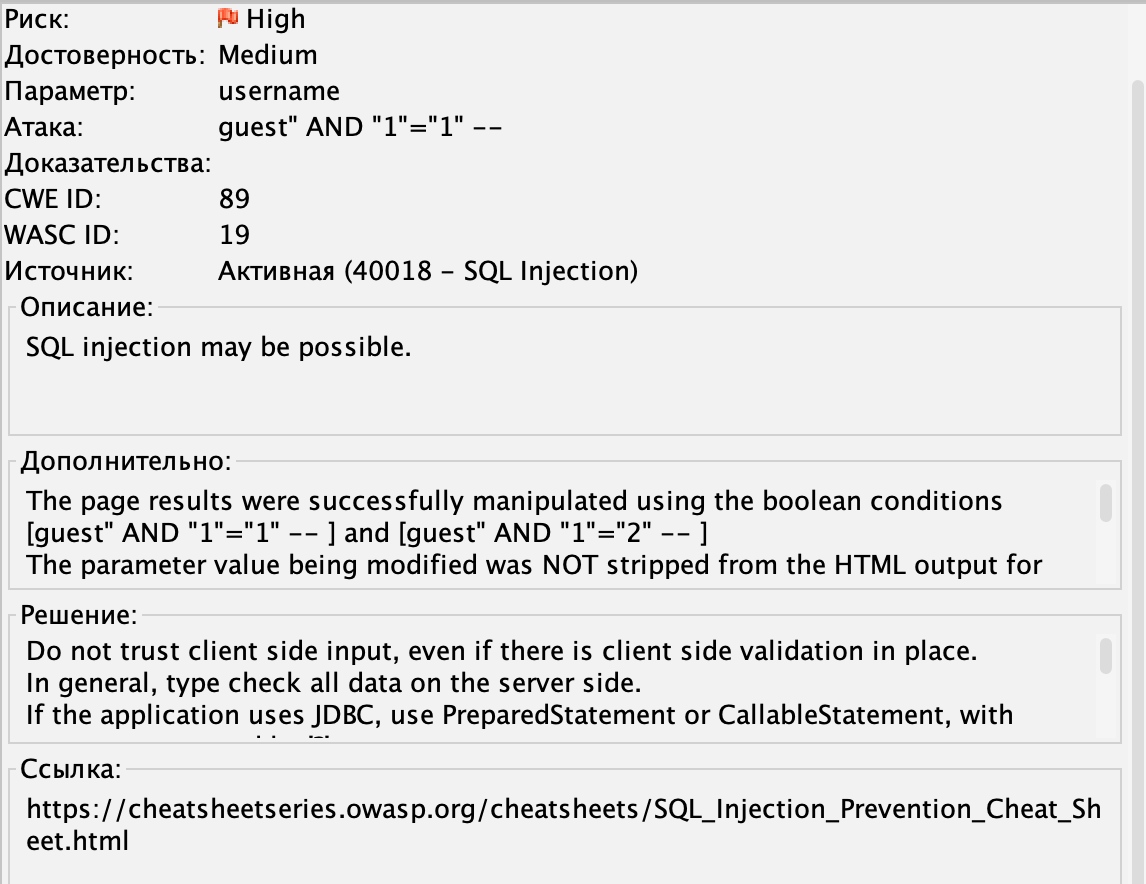
В результате данной лабораторной работы была рассмотрена система edu.fpmi, используемая как система для дистанционного обучения студентов БГУ.

Для должного исследования необходимо создать виртуальное окружение для системе и запустить ее локально.

Для тестирования системы на уязвимости воспользуемся программой OWASP ZAP. Во время тестирования можно заметить большое количество запросов на сайт, что обеспечивает проверку всех возможных уязвимых мест на сайте и возможное обнаружение злоумышленника.

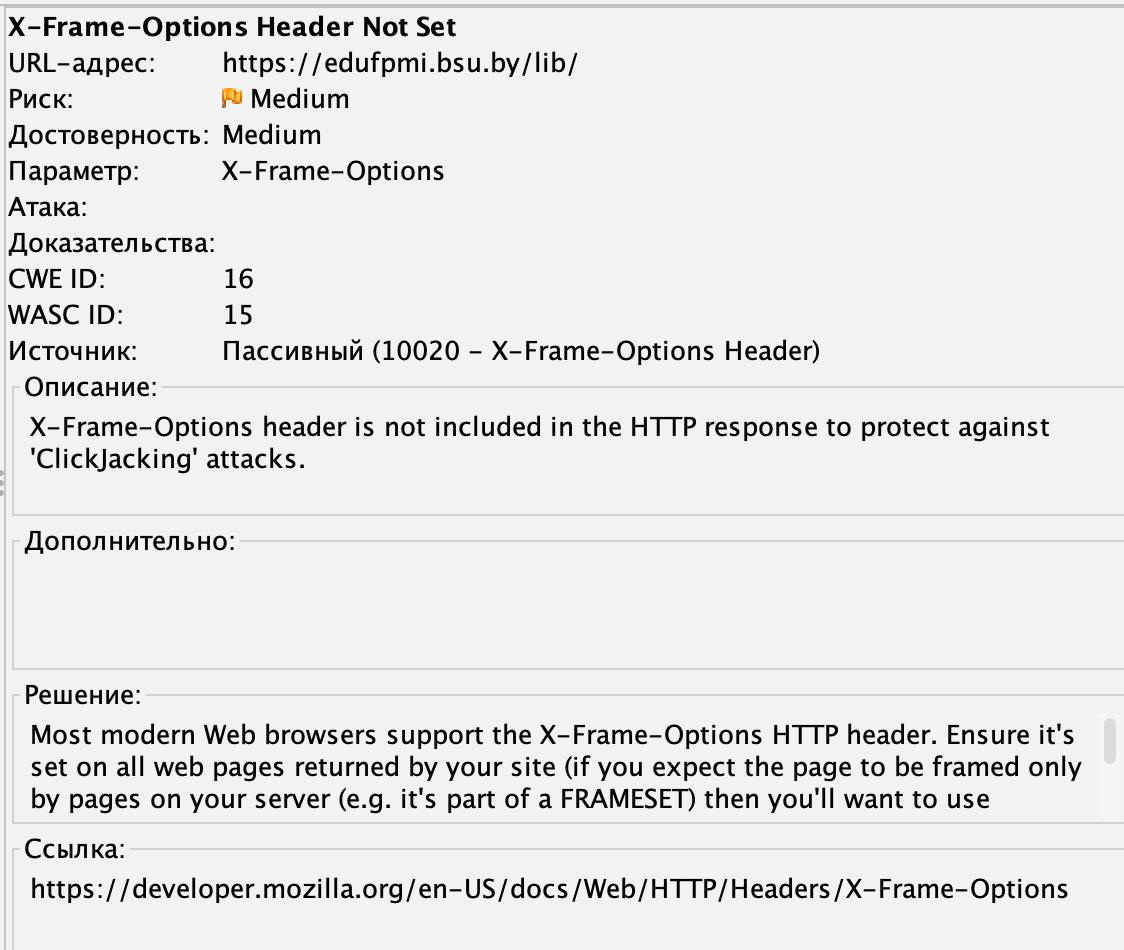


Рассмотрим некоторые уязвимости :

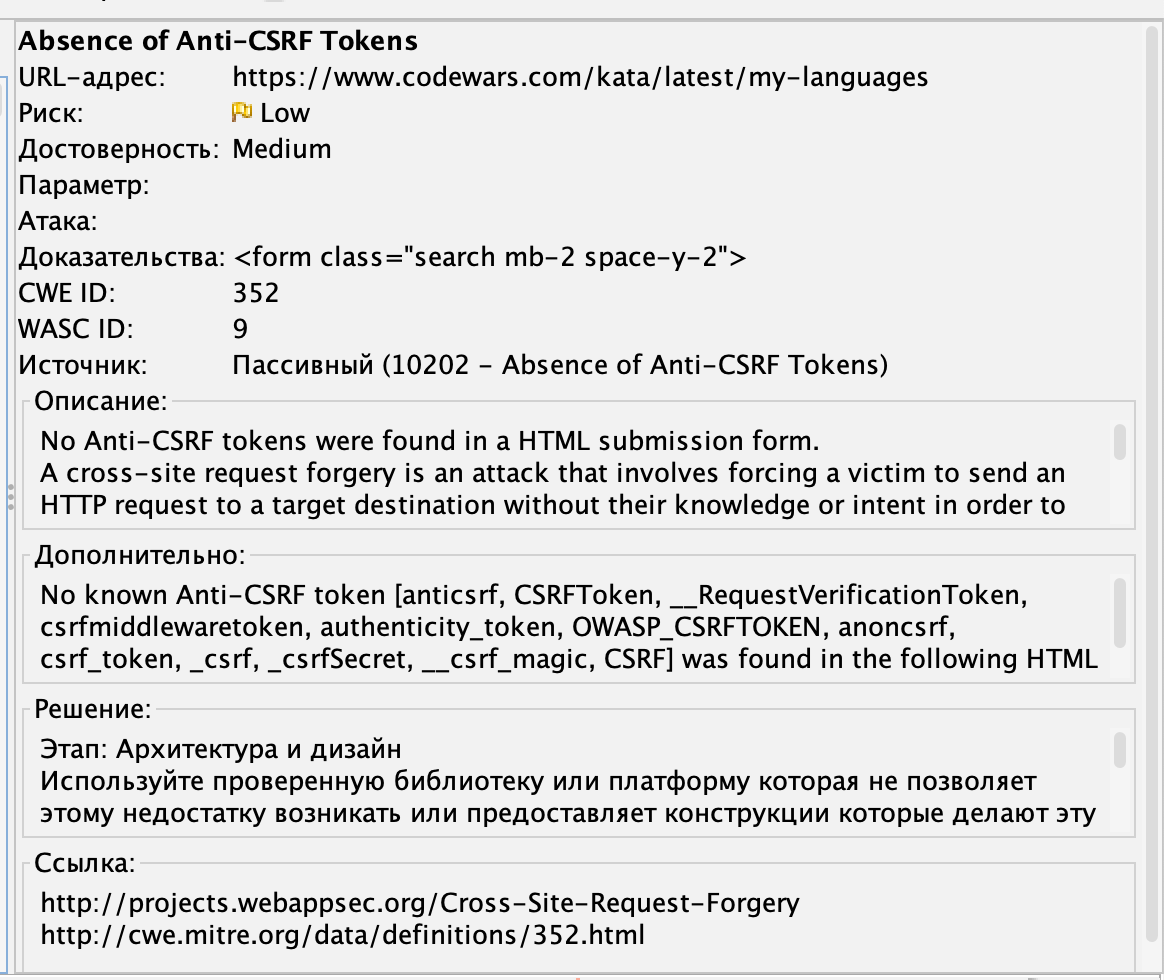


Одна из уязвимостей заключается в не совсем корректном использовании SQL запроса и его обработки. Для устранения этой уязвимости можно использовать PreparedStatement или CallableStatement.

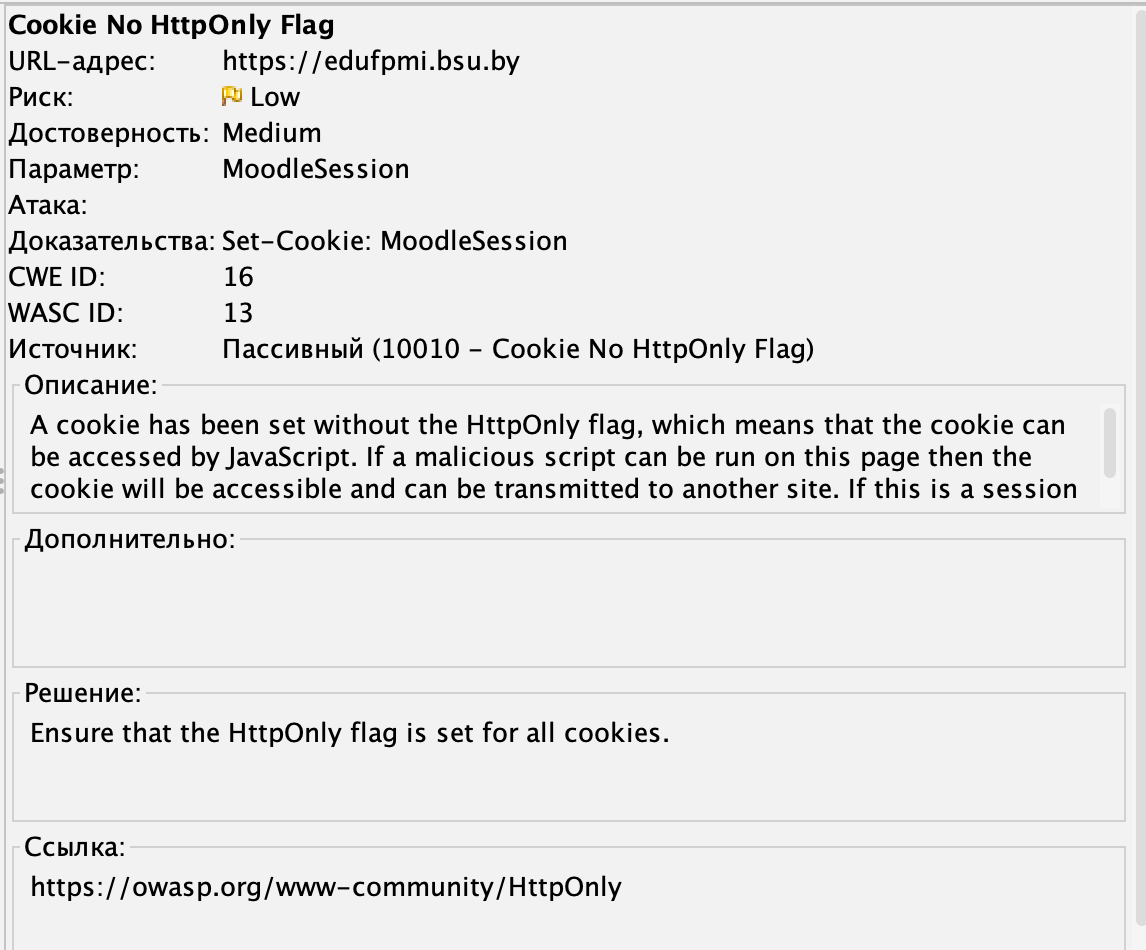
Рассмотрим некоторые другие уязвимости:



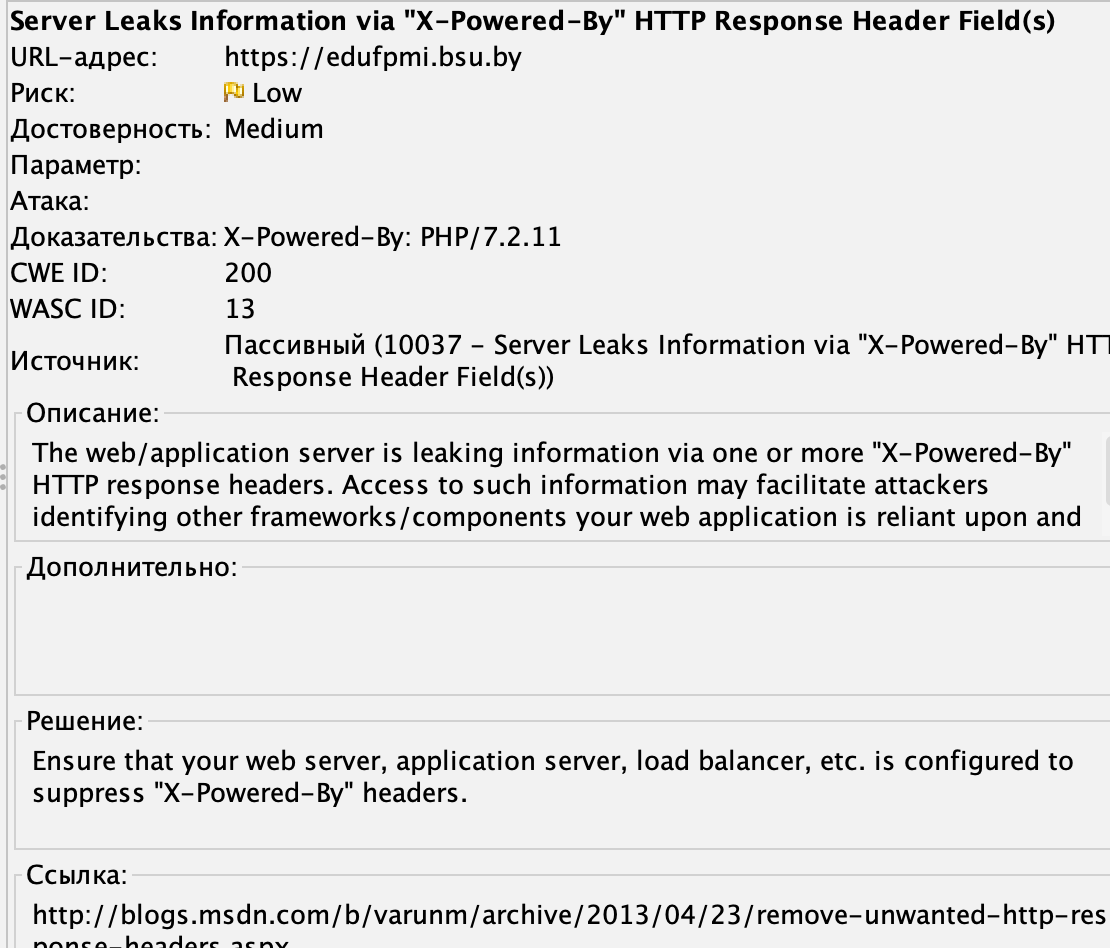
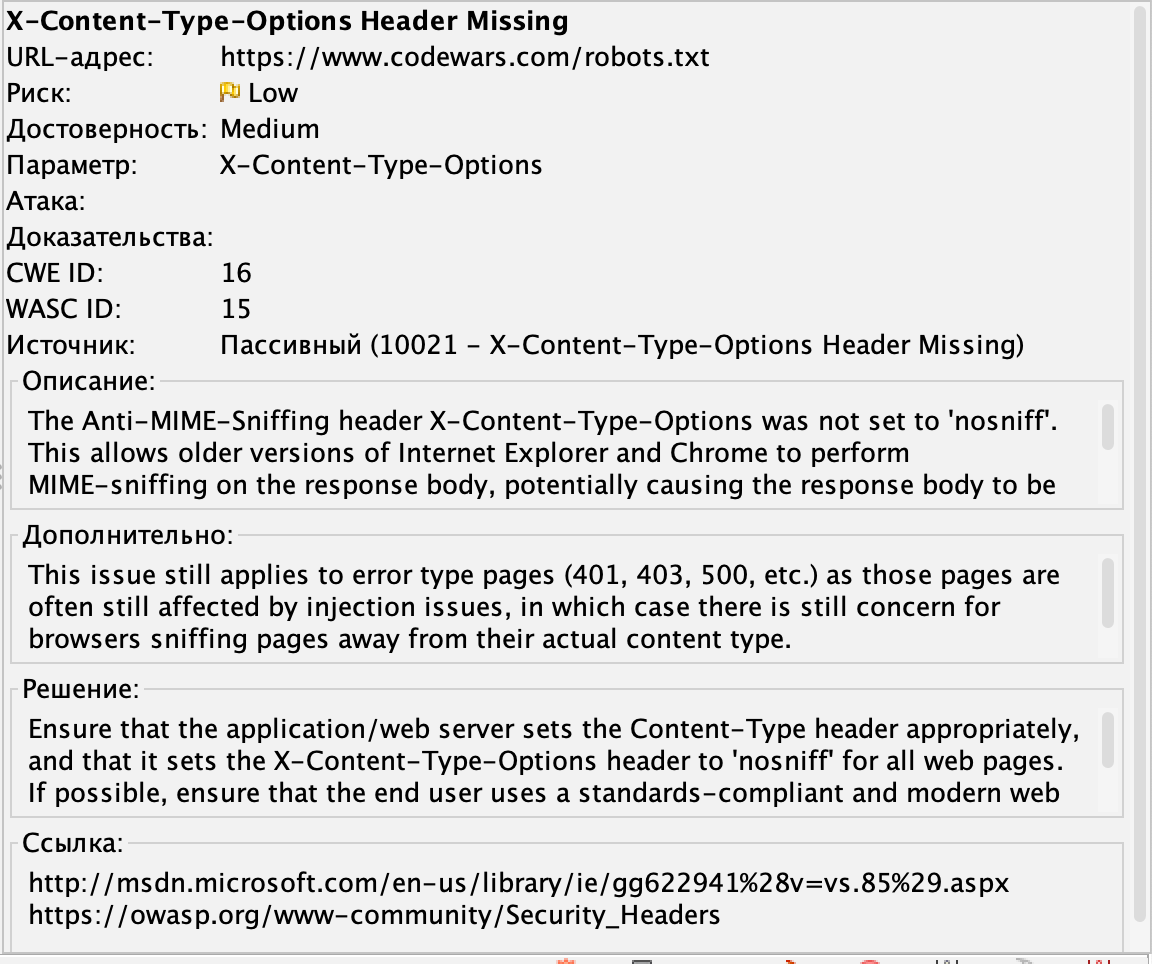
Подобная уязвимость может быть использована при атаке Кликджекингом(пользователь получает ссылку на вредоносный контент, что дает возможность получения доступа к аккаунту пользователя. Данный тип атаки используется для получения доступа к функции автозаполнения менеджера паролей. Для устранения уязвимости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



Следующая уязвимость 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.**



Следующая уязвимость(как и некоторые последующие) заключается в отсутствии необходимых HTTP-флагов и хэдеров, что решается простым их добавлением.



После исправления уязвимостей получим обновленный отчет.