ОБУЧЕНИЕ ТЕСТИРОВАНИЮ БЕЗОПАСНОСТИ WEB-РЕСУРСОВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Медведев О. С., Довгун М. А., Петлицкий Н. О.

Меженная М. М. – канд. техн. наук,
доцент каф.. ИПиЭ

Цель разработки – создание и внедрение программного комплекса для обучения студентов тестированию безопасности web-ресурсов. Программный комплекс реализуется в виде web-приложения с искусственно созданными уязвимостями, представляющими собой наиболее распростаненные для web-приложений дефекты безопасности.

Программный комплекс представляет собой страницу авторизации (с логином, паролем), для успешного прохождения которой необходимо обнаружить и воспользоваться имеющейся уязвимостью. Предусмотрены разичные по уровню сложности уязвимости, включая тривиальные логин и пароль, искомую информацию в комментариях исходного кода, SQL-инъекции, запускаемые скрипты и другие. Для оценки успешности обучения тестированию безопасности предусмотрена модульная система. Имеется возможность запроса подсказки в случае, если студент затрудняется обнаружить уязвимость самостоятельно, однако, запрос подсказки приводит к снижению оценки за текущее задание.

Программный комплекс имеет трехуровневую архитектуру и включает клиентскую часть, серверную часть, базу данных. Для создания и поддержки данных в веб-приложении необходимо иметь возможность за короткий промежуток времени произвести изменения на сайте или добавить новый материал. Для достижения указанной цели в серверной части используется язык программирования Java, технология Servlet, фреймворк Spring [1-3]. Для одновременной работы с сайтом большого количества пользователей реализован connection pooling. В качестве системы управления базой данных используется MySQL. Клиентская часть представляет собой код на языке разметки гипертекста HTML с использованием каскадной таблицы стилей CSS, а также модулей JavaScript (рисунок 1). Для каждой страницы создан свой шаблон, к которому подключены необходимые функции. Меню и страницы легко настраиваются, что позволяет гораздо быстрее адаптировать сайт под конкретные нужды. Пример отображения страницы авторизации с искусственно созй уязвимостью в безопасности и предоставления подсказки для ее обнаружения отображено на рис.1.

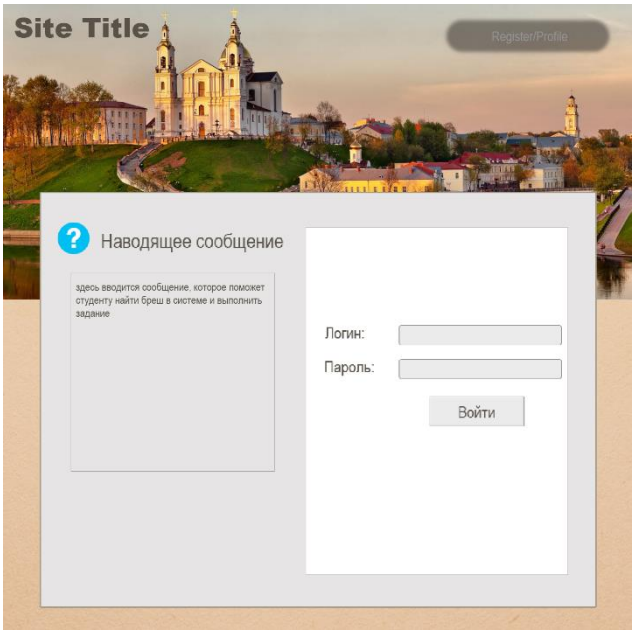

Рисунок1 – Пример отображения страницы авторизации

По итогам обучения тестированию безопасности в программном комплексе отображается результирующая информация с перечнем уязвимостей, которые обнаружены студентом, количеством запрошенных подсказок, а также результирующей оценкой.

Список использованных источников:

1. И.Н. Блинов, В.С. Романчик "Java. Методы программирования" 2013, Минск. – 768 с.
2. Философия Java / Б. Эккель : Питер, 2016. – 1168 с.
3. Spring framework в действии / Р.Брейдбах : Питер, 2014. 531 с.