

PortSwigger Academy как инструмент для обучения веб-безопасности и анализа уязвимостей

Болтовский Гавриил Александрович

Приамурский государственный университет им. Шолом-Алейхема

Студент

Аннотация

Цель исследования анализ возможностей платформы PortSwigger Academy для изучения веб-безопасности и практического освоения методов тестирования на проникновение. Рассмотрены ключевые функциональные особенности платформы, включая тематическое наполнение и практические задания по анализу уязвимостей веб-приложений. В результате работы определены преимущества использования платформы в образовательной и профессиональной деятельности, связанные с углублением понимания механизмов кибератак и способов их предотвращения.

Ключевые слова: информационная безопасность, веб-безопасность, этичный хакинг

PortSwigger Academy as a tool for web security training and vulnerability analysis

Boltovsky Gavriil Alexandrovich

Sholom-Aleichem Priamursky State University

Student

Abstract

The purpose of the article is to analyze the capabilities of the PortSwigger Academy platform for learning web security and practical penetration testing methods. The key functional features of the platform are considered, including thematic content and practical tasks for analyzing web application vulnerabilities. As a result of the work, the advantages of using the platform in educational and professional activities related to deepening the understanding of cyberattack mechanisms and ways to prevent them were identified.

Keywords: information security, web security, ethical hacking

1 Введение

1.1 Актуальность исследования

Современные угрозы информационной безопасности требуют эффективных методов обучения специалистов по кибербезопасности. Платформа PortSwigger Academy [1] предоставляет уникальные возможности для практического освоения анализа уязвимостей веб-приложений, что делает

её актуальным инструментом для повышения квалификации специалистов и подготовки новых кадров в области информационной безопасности.

1.2 Обзор исследований

Вопросы информационной безопасности всё чаще рассматриваются как неотъемлемая часть экономической стабильности организаций. В исследовании З.М. Ибрагимовой, З.Б. Батчаевой и А.Л. Ткаченко подчёркивается необходимость разработки и эксплуатации информационных систем, отвечающих современным требованиям безопасности. [2] Рассматриваемая информационная система, связанная с деятельностью предприятия в различных секторах, демонстрирует важность её роли в обеспечении условий экономической безопасности.

Понятие информационной безопасности носит комплексный характер, охватывая множество аспектов, которые подробно анализируются А.Д.Чесноковым [3]. Им выделяются ключевые направления, определяющие эффективность реализации мер безопасности, и раскрывает основные структурные компоненты этой сферы.

Современные подходы к автоматизации тестирования веб-приложений включают использование механизмов машинного обучения. Применение таких методов для обнаружения XSS-атак представляет собой актуальное направление исследований, о чём свидетельствует работа J. Kaur, U. Garg и G. Bathla [4], в которой проведён обзор современных методов обнаружения XSS-уязвимостей с использованием машинного обучения.

Вопрос защиты веб-приложений от CSRF-атак остаётся важной задачей, несмотря на достигнутые успехи в этой области. Считается, что современные JavaScript-фреймворки обладают встроенными механизмами защиты, однако детальный анализ их эффективности представлен в работе X. Likaj, S. Khodayari и G. Pellegrino [5]. Ими исследуются уязвимости существующих решений и дают оценку текущего состояния защиты от CSRF-атак в рамках популярных фреймворков.

1.3 Цель исследования

Цель статьи является анализ возможностей платформы PortSwigger Academy для изучения веб-безопасности и практического освоения методов тестирования на проникновение.

1.4 Постановка задачи

Для достижения поставленной цели следует проанализировать возможности платформы PortSwigger Academy для обучения основам веб-безопасности и практического освоения методов анализа и предотвращения уязвимостей веб-приложений.

2 Методы исследования

Для анализа функциональных возможностей платформы PortSwigger Academy проводилось детальное исследование её интерфейса и структуры

тематических модулей. Особое внимание уделялось практическому выполнению лабораторных заданий, ориентированных на поиск и эксплуатацию уязвимостей. Дополнительно проводилось сравнение возможностей платформы с аналогичными решениями, что позволило выявить её сильные стороны.

В процессе работы использовались инструменты, доступные на платформе, включая Burp Suite Community Edition [6]. Этот инструмент, разработанный компанией PortSwigger, представляет собой мощный инструмент для анализа и тестирования безопасности веб-приложений. Интеграция с платформой PortSwigger Academy позволяет применять Burp Suite в реальных лабораторных условиях, что усиливает практическую направленность обучения. Инструмент применялся для анализа сетевого трафика и моделирования атак, что обеспечивало реальный опыт работы с веб-приложениями. Для выполнения лабораторных заданий платформа предоставляла эмуляторы, позволяющие воссоздавать реальные сценарии атак и изучать их особенности.

3 Результаты и обсуждения

PortSwigger Academy предоставляет пользователям доступ к структурированным учебным материалам, организованным по тематическим модулям, каждый из которых ориентирован на отдельный аспект веб-безопасности. Ключевые темы включают такие направления, как инъекции SQL, межсайтовый скриптинг (XSS), атаки на управление сессиями и уязвимости, связанные с обходом авторизации. Каждый модуль сопровождается теоретической базой и практическими заданиями, которые моделируют реальные атаки на веб-приложения. Например, в разделе, посвященном SQL-инъекциям, пользователи учатся выявлять уязвимости в запросах к базам данных и использовать их для извлечения конфиденциальной информации. В свою очередь, модуль по XSS подробно объясняет механизмы внедрения вредоносного кода в веб-страницы, демонстрируя, как злоумышленники могут использовать эти атаки для компрометации данных пользователей.

На изображении ниже (рис. 1) представлена страница отслеживания прогресса обучения на платформе PortSwigger Academy. Интерфейс содержит несколько разделов, информирующих пользователя о текущем уровне знаний, выполненных лабораторных работах и подготовке к сертификации.

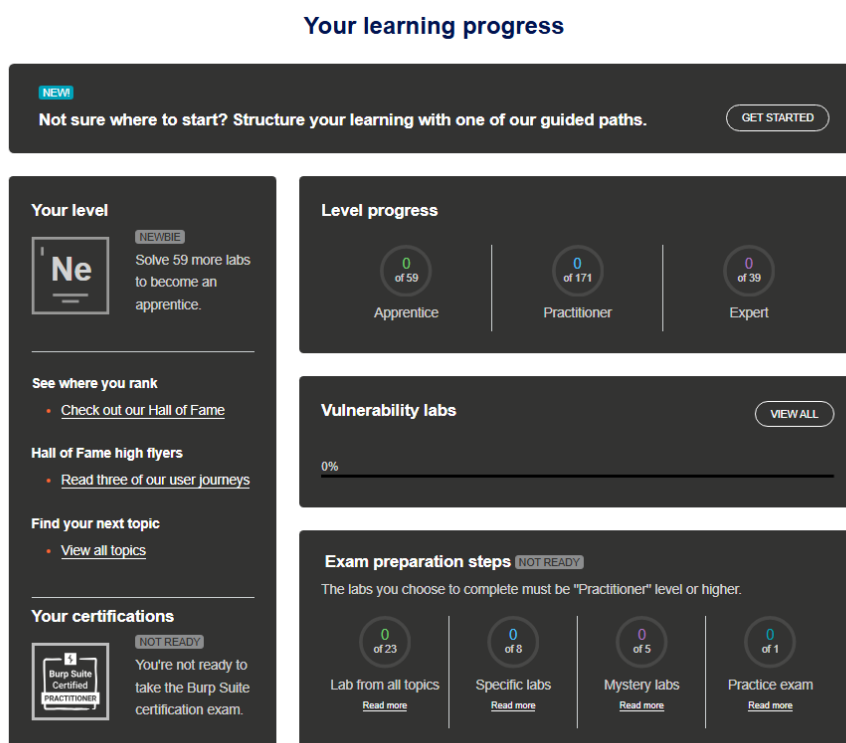


Рисунок 1 – Страница прогресса

В верхней части экрана размещен баннер с рекомендацией воспользоваться структурированными учебными путями, которые помогают организовать процесс обучения. Далее представлена информация об уровне пользователя: для перехода на следующий уровень необходимо решить еще 59 задач. Также доступен рейтинг пользователей, где можно ознакомиться с таблицей лидеров (Hall of Fame), а также выбрать следующую тему для изучения.

В нижней части экрана представлен раздел Exam preparation steps, который включает несколько этапов подготовки к сертификации. Для успешного прохождения экзамена необходимо завершить лабораторные задания из всех категорий, пройти специализированные тесты и выполнить Practice exam.

После выбора направления подготовки перед пользователем открывается теоретическая часть, содержащая подробное объяснение ключевых концепций и механизмов атак (рис. 2). Материалы изложены в структурированном формате, включая текстовые описания, схемы и примеры реальных уязвимостей. Каждая тема сопровождается практическими примерами, демонстрирующими, как злоумышленники могут эксплуатировать найденные слабости веб-приложений. В процессе изучения пользователь знакомится с методами защиты и рекомендациями по устранению уязвимостей, что позволяет не только понять принципы атак, но и освоить стратегии их предотвращения.

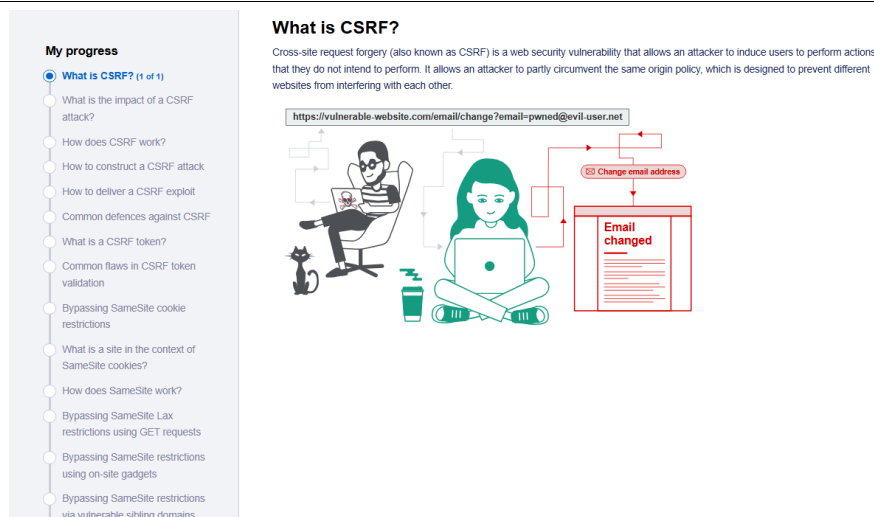


Рисунок 2 – Теория из направления подготовки CSRF

Например, при изучении межсайтовой подделки запроса (CSRF) студентам предлагается лабораторная работа, демонстрирующая уязвимость функции изменения электронной почты в тестовом веб-приложении. Цель задания – создать эксплойт, который автоматически отправляет вредоносный запрос от имени аутентифицированного пользователя, изменяя его email без его ведома.

Лаборатория предоставляет персональный экземпляр уязвимого веб-приложения. После входа в систему под учетной записью wiener:peter студент обнаруживает, что форма изменения email не защищена CSRF-токенами (рис. 3).

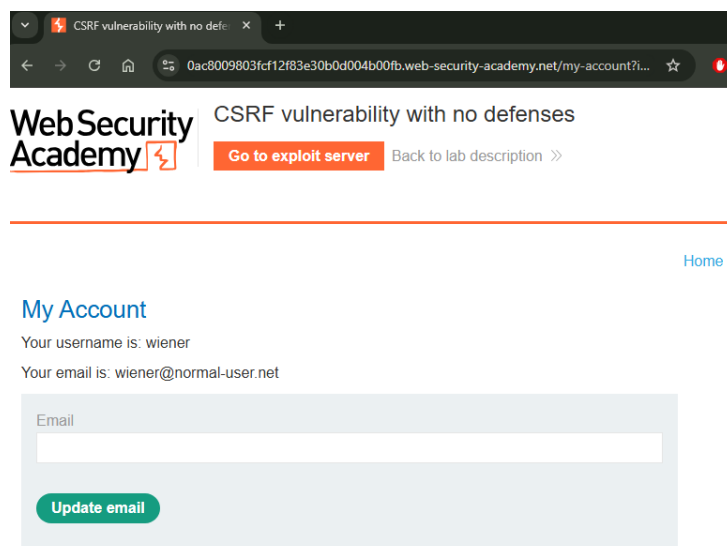


Рисунок 3 – Уязвимая для CSRF атаки форма

Для успешной эксплуатации CSRF-уязвимости студенту требуется выполнить ряд действий. Первым шагом становится перехват запроса на изменение email с помощью инструментов анализа сетевого трафика, таких как Burp Suite, с последующим изучением его структуры – это позволяет определить параметры, которые необходимо воспроизвести в эксплойте.

Далее создается HTML-страница, содержащая скрытую форму, полностью имитирующую легитимный запрос к уязвимому эндпоинту; критически важно, чтобы форма автоматически отправлялась при загрузке страницы, что достигается за счет интеграции JavaScript-скрипта. При этом необходимо использовать уникальный email-адрес, не занятый другими пользователями, чтобы избежать конфликтов данных и гарантировать корректное выполнение задания. Такой подход обеспечивает не только эксплуатацию уязвимости, но и понимание механизмов, лежащих в основе CSRF-атак.

Пример эксплойта выглядит следующим образом:

```
<html>
<body>
  <form action="https://vulnerable-lab.net/email/change" method="POST">
    <input type="hidden" name="email" value="hacked@example.com">
  </form>
  <script>
    document.forms[0].submit();
  </script>
</body>
</html>
```

Студент загружает разработанный эксплойт на предоставленный платформой сервер эксплойтов. Когда жертва (эмулируемая платформой) открывает страницу с вредоносным кодом, скрытая форма автоматически отправляет POST-запрос на изменение email, подставляя значение, указанное в параметре value. В случае успешного выполнения атаки система автоматически фиксирует изменение данных в профиле пользователя и подтверждает завершение лабораторной работы, демонстрируя реальные последствия CSRF-уязвимости.

Использование PortSwigger Academy демонстрирует высокую эффективность за счет сочетания интерактивных лабораторий и разнообразия реальных сценариев.

PortSwigger Academy занимает уникальную нишу среди образовательных платформ по кибербезопасности, выделяясь на фоне таких конкурентов, как Hack The Box [7] и TryHackMe [8]. В отличие от Hack The Box, ориентированного на продвинутое пентестирование с упором на практику и минимальным вниманием к теоретическим основам, PortSwigger Academy предлагает глубоко структурированное обучение с детальным разбором веб-уязвимостей, подкрепленным интерактивными лабораториями.

PortSwigger Academy представляет собой эффективный инструмент для обучения веб-безопасности. Практическая направленность заданий и интеграция с профессиональными инструментами способствуют углубленному пониманию методов тестирования на проникновение. Платформа рекомендована для применения как в образовательных учреждениях, так и в самостоятельной подготовке специалистов.

3. Выводы

Платформа PortSwigger Academy предоставляет обширные возможности для освоения веб-безопасности и практического изучения уязвимостей, что способствует формированию компетенций специалистов в условиях роста кибератак.

Библиографический список

1. PortSwigger Academy [Электронный ресурс]. URL: <https://portswigger.net/web-security> (дата обращения: 29.01.2025).
2. Ибрагимова З. М., Батчаева З. Б., Ткаченко А. Л. Информационная безопасность как элемент экономической безопасности // Инженерный вестник Дона. – 2022. – №. 11 (95). – С. 26-33.
3. Чесноков А. Д. Информационная безопасность // StudNet. – 2022. – Т. 5. №. 1. С. 478-489.
4. Kaur J., Garg U., Bathla G. Detection of cross-site scripting (XSS) attacks using machine learning techniques: a review // Artificial Intelligence Review. 2023. Т. 56. №. 11. С. 12725-12769.
5. Likaj X., Khodayari S., Pellegrino G. Where we stand (or fall): An analysis of CSRF defenses in web frameworks // Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses. 2021. С. 370-385.
6. Burp Suite Community Edition. URL: <https://portswigger.net/burp/communitydownload> (дата обращения: 29.01.2025).
7. Hack The Box. URL: <https://www.hackthebox.com> (дата обращения: 29.01.2025).
8. TryHackMe. URL: <https://tryhackme.com> (дата обращения: 29.01.2025).