

Геймификация в образовательном процессе на примере веб-приложения OWASP Juice Shop

Болтовский Гавриил Александрович

Приамурский государственный университет им. Шолом-Алейхема

Студент

Аннотация

Цель статьи – анализ применения геймификации для обучения кибербезопасности на примере OWASP Juice Shop. В работе рассматриваются механизмы мотивации, реализованные в приложении, включая рейтинговую систему и систему начисления баллов за успешное выполнение атак. В результате демонстрируются возможности геймификации для повышения вовлечённости обучающихся и формирования практических навыков.

Ключевые слова: информационная безопасность, геймификация, OWASP Juice Shop

Gamification in the educational process on the example of web application OWASP Juice Shop

Boltovsky Gavriil Alexandrovich

Sholom-Aleichem Priamursky State University

Student

Abstract

The purpose of the paper is to analyze the application of gamification for cybersecurity training using the OWASP Juice Shop as an example. The paper discusses the motivation mechanisms implemented in the application, including a rating system and a system of awarding points for successful execution of attacks. As a result, the possibilities of gamification for increasing learner engagement and building practical skills are demonstrated.

Keywords: information security, gamification, OWASP Juice Shop

1 Введение

1.1 Актуальность исследования

Актуальность исследования обусловлена возрастающей потребностью в эффективных методах обучения кибербезопасности, учитывающих как теоретические аспекты, так и развитие практических навыков. В условиях увеличения количества киберугроз и сложности современных атак традиционные образовательные подходы зачастую оказываются недостаточными для формирования устойчивых компетенций у обучающихся. Геймификация, являясь инновационным инструментом, способствует повышению мотивации и вовлечённости, обеспечивая интерактивный и

результативный процесс обучения. Исследование применения элементов геймификации на примере OWASP Juice Shop позволяет выявить их потенциал для подготовки специалистов в области кибербезопасности и формирования у них устойчивых практических навыков.

1.2 Обзор исследований

Проблема геймификации в образовательном процессе подробно рассматривается в работе Л. П. Варениной [1], где уделяется внимание сущности данного понятия, причинам его активного развития, а также основным функциям игр в обучении. В исследовании О. В. Орловой и В. Н. Титовой [2] проводится сравнительный анализ традиционных игровых практик и геймификации в образовательной среде. Отмечается, что геймификация представляет собой лишь способ организации учебного процесса, при котором образовательные цели сохраняют приоритетное значение, тогда как игровые элементы используются для поддержания внутренней мотивации обучающихся.

Аспекты применения геймификации в области обучения информационной безопасности изучены в работе А. В. Хардина [3]. В данном исследовании рассматриваются уникальные методики, внедренные не в образовательных учреждениях, а непосредственно на рабочих местах сотрудников различных организаций с целью повышения их осведомленности в сфере информационной безопасности.

Применение игровых технологий в школьном курсе информатики представлено в исследовании К. А. Таракановой и О. А. Завьяловой [4], где освещается опыт внедрения геймификации при изучении темы «Основы информационной безопасности и защиты информации», демонстрируются возможности данного подхода для повышения вовлеченности обучающихся и формирования практических навыков.

1.3 Цель исследования

Цель статьи – анализ применения геймификации для обучения кибербезопасности на примере OWASP Juice Shop.

1.4 Постановка задачи

В рамках работы проведён анализ возможностей геймификации, реализованных в веб-приложении OWASP Juice Shop [5]. Рассмотрены механизмы начисления баллов и рейтинговая система, способствующие повышению мотивации обучающихся.

2 Методы исследования

OWASP Juice Shop – это веб-приложение, разработанное для обучения основам веб-безопасности на практике. Оно представляет собой уязвимый интернет-магазин, содержащий широкий спектр преднамеренных уязвимостей. Приложение предоставляет пользователям безопасную среду для отработки навыков проведения атак и выявления уязвимостей.

Одной из ключевых особенностей OWASP Juice Shop является внедрение элементов геймификации, которые повышают вовлеченность пользователей и способствуют более эффективному усвоению материала. Геймификация представляет собой применение игровых механизмов и подходов в неигровых контекстах, таких как образование и профессиональная подготовка. Основной целью геймификации является усиление мотивации обучающихся за счет использования таких элементов, как рейтинговые таблицы, система начисления баллов, достижений и наград за выполнение определенных задач.

3 Результаты и обсуждения

Для изучения геймификационных механизмов, реализованных в OWASP Juice Shop, необходимо развернуть приложение на локальной машине. Одним из наиболее удобных способов установки является использование пакетного менеджера `npm`, который позволяет быстро запустить приложение без необходимости задействования дополнительных средств контейнеризации. Перед установкой требуется предварительно настроить рабочее окружение, установив `Node.js`, `git` и `npm`. Развертывание приложения осуществляется с помощью следующих команд:

```
git clone https://github.com/juice-shop/juice-shop.git
cd juice-shop
npm install
npm start
```

После успешного запуска OWASP Juice Shop становится доступным в браузере по адресу `http://localhost:3000` (рис. 1). Помимо установки через `npm`, приложение также может быть развернуто с использованием контейнеризации на базе `Docker`, что обеспечивает дополнительную гибкость в образовательном процессе.

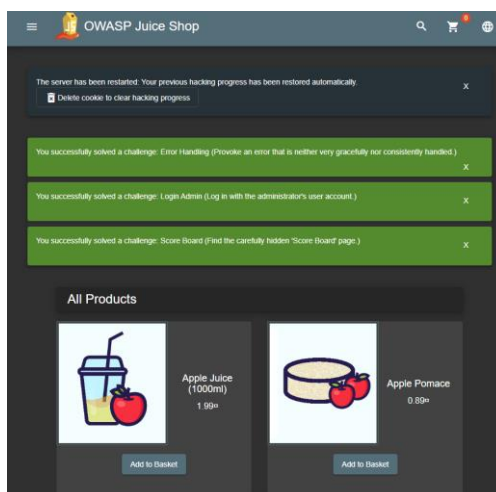


Рисунок 1 – Запуск веб-приложения OWASP Juice Shop

На рисунке выше демонстрируется, что OWASP Juice Shop сохраняет достигнутые результаты и прогресс пользователя даже после повторного запуска приложения. В частности, после перезагрузки локального сервера приложение распознает ранее выполненные достижения: поздравляет пользователя с успешным входом в учетную запись администратора и открытием таблицы достижений. Эти базовые достижения играют важную роль в обучении работе с приложением и служат отправной точкой для дальнейшего изучения его функционала.

Получение доступа к учетной записи администратора, что достигается путем эксплуатации уязвимости, связанной с SQL-инъекцией. Для успешного выполнения данной атаки пользователь вводит в поле email следующую строку:

```
' OR 1=1--
```

В качестве пароля можно указать любую произвольную комбинацию символов. После отправки формы сервер обрабатывает введенные данные, и благодаря уязвимости в механизме аутентификации пользователь получает несанкционированный доступ к учетной записи администратора, обладающей расширенными правами (рис. 2).

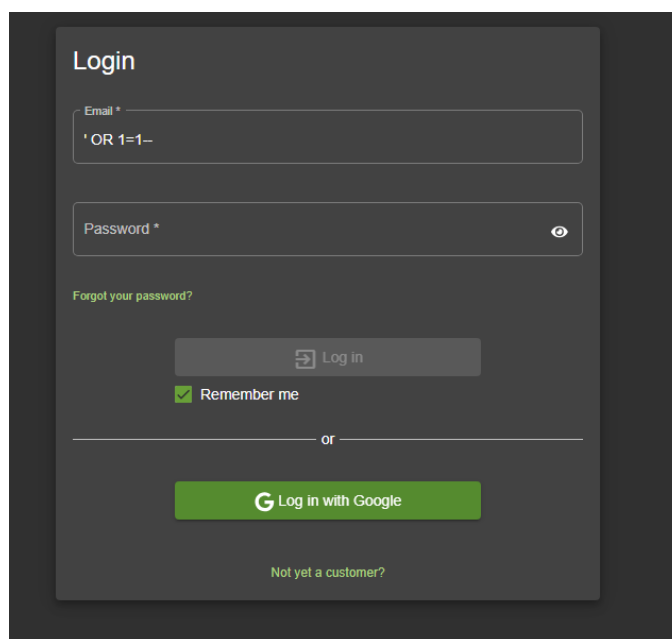


Рисунок 2 – SQL-инъекция на странице входа

Данный сценарий демонстрирует один из наиболее распространенных векторов атак на веб-приложения и позволяет обучающимся на практике понять принципы работы SQL-инъекций, а также важность внедрения надежных механизмов защиты пользовательских данных.

Для открытия таблицы достижений пользователю предлагается исследовать структуру веб-приложения с помощью инструментов разработчика, таких как инспектор элементов браузера, или интуитивно

определить возможное расположение данной страницы. Этот процесс способствует развитию навыков анализа веб-приложений и понимания их внутренней структуры.

Используя инструменты разработчика, обучающийся может изучить HTML-код и выявить скрытые или недокументированные ссылки, ведущие к странице достижений. Также возможен путь интуитивного поиска, при котором пользователь анализирует навигацию приложения, URL-адреса и возможные шаблоны построения интерфейса.

На рисунке (рис. 3) показан внешний вид страницы достижений, где отображаются различные выполненные задания и полученные награды. Эта таблица предоставляет обучающимся обратную связь о прогрессе, стимулируя их к дальнейшему изучению функционала приложения и решению новых задач, что способствует повышению мотивации и вовлеченности.

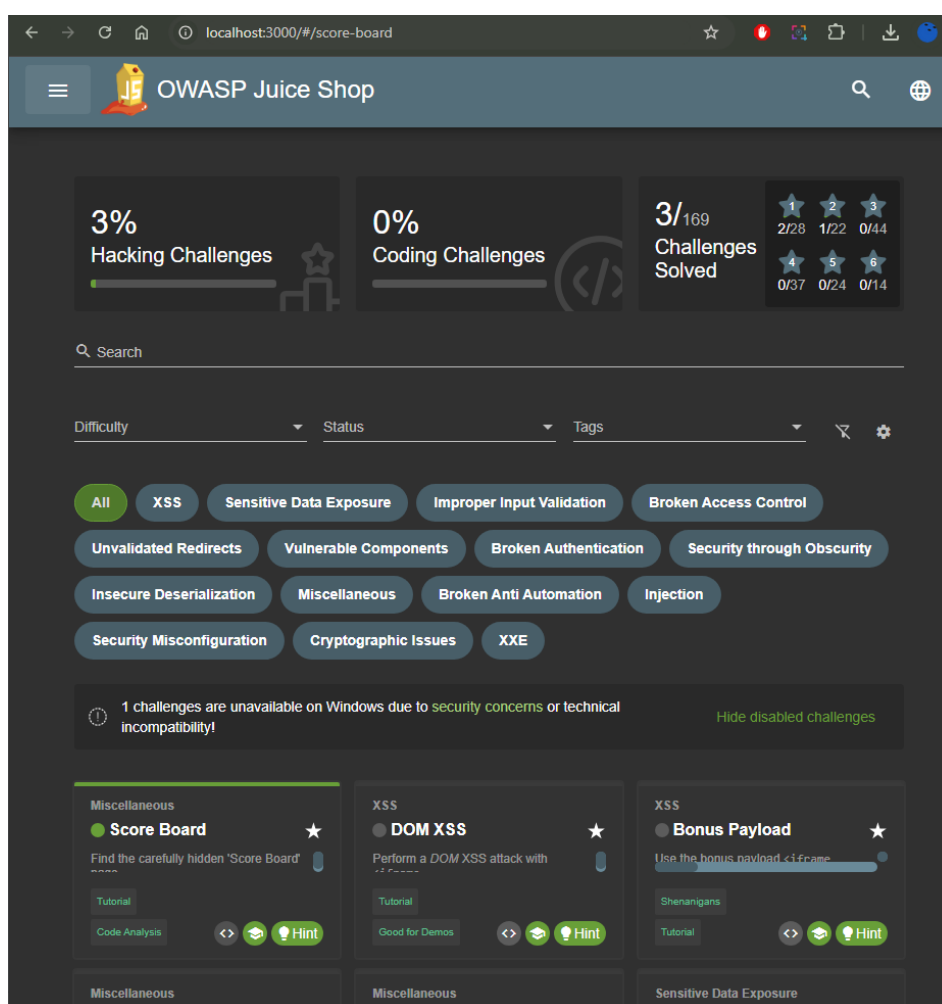


Рисунок 3 – Табло достижений

Каждая задача имеет своё описание, предлагает фрагмент кода, где можно увидеть уязвимость, а также можно получить подсказку, часто эта кнопка ведёт на обширную документацию. Все задачи распределены по темам: XSS, контроль доступа, SQL-инъекции, проблемы криптографии и так далее.

Геймификация в OWASP Juice Shop проявляется через различные механизмы, способствующие вовлечению обучающихся в процесс изучения кибербезопасности. Одним из ключевых элементов является система достижений, которая визуализирует прогресс пользователя, фиксируя выполненные задания и полученные награды. Это создает дополнительную мотивацию, побуждая обучающихся стремиться к завершению все большего количества задач. Важную роль играет и система челленджей, представляющая собой набор практических заданий, таких как взлом учетной записи администратора с использованием SQL-инъекции или поиск скрытых страниц. Эти задания формируют у пользователей практические навыки, применяемые в реальных условиях, и способствуют глубокому пониманию тематики.

Процесс обучения включает в себя исследовательские элементы, требующие изучения структуры сайта с помощью инструментов разработчика или самостоятельного нахождения страниц. При использовании OWASP Juice Shop в учебных группах таблица достижений способствует созданию соревновательной среды, в которой обучающиеся могут сравнивать свои результаты и стремиться к улучшению показателей.

3. Выводы

Применение геймификации в образовательном процессе на примере OWASP Juice Shop демонстрирует её эффективность в повышении мотивации обучающихся и развитии практических навыков в области кибербезопасности.

Библиографический список

1. Варенина Л. П. Геймификация в образовании //Историческая и социально-образовательная мысль. 2014. №. 6-2. С. 314-317.
2. Орлова О. В., Титова В. Н. Геймификация как способ организации обучения //Вестник Томского государственного педагогического университета. 2015. №. 9 (162). С. 60-64.
3. Хардин А. В. Мировой опыт использования геймификации в области обучения информационной безопасности //Экономика знаний: теория и практика. 2017. №. 2. С. 79-86.
4. Тараканова К. А., Завьялова О. А. Использование элементов геймификации в преподавании темы «Основы информационной безопасности и защиты информации» // Современные проблемы и перспективы обучения математике, физике, информатике в школе и вузе. 2021. С. 181-187.
5. OWASP Juice Shop. URL: <https://owasp.org/www-project-juice-shop/> (дата обращения: 25.01.2025).