Оглавление

Введение **12**

Часть I. Подготовка к взлому **19**

Подготовка к взлому 20
Запуск OWASP Juice Shop 20
Системные требования 20
Варианты запуска 21
Установка конкретной версии релиза 27
Функция самовосстановления 28
Ограничение для одного пользователя 28
Категории уязвимостей 28
Карта категорий 29
Отслеживание заданий 30
Панель результатов (Score Board) 30
Поиск по свободному тексту 34
Уведомления об успехе 34
Автоматическое сохранение и восстановление прогресса взлома 36
Ручное резервное копирование прогресса и настроек 36
Hacking Instructor 38
Задания по написанию кодов 42
Ссылки на меры противодействия 45
Потенциально опасные задания 45
Правила упражнений по взлому 47
Рекомендуемые инструменты для взлома 47
Получение подсказок 54
Вещи, считающиеся читерством 54
Прохождение «счастливого пути» 56

Часть II. Охота за задачами **77**

Охота за задачами 78
Решения задач 84
Поиск панели результатов 84
Задачи, рассматриваемые в этом разделе 84
Найдите тщательно скрытую страницу Score Board 84
Инъекция 85
Задачи, рассматриваемые в этом разделе 86
Рекомендации по разведке 86
Заказать рождественское специальное предложение 2014 года 87
Извлечь всю схему базы данных через SQL-инъекцию 87
Выполнить вход с несуществующей учетной записью бухгалтера, не регистрируя этого пользователя 88
Войти в систему, используя аккаунт администратора 89
Выполнить вход с учетной записью пользователя Бендера 89

Выполнить вход с учетной записью пользователя Джима ... 89
Заставить сервер на некоторое время заснуть ... 89
Все ваши заказы принадлежат нам ... 91
Обновить несколько отзывов о товарах одновременно ... 91
Заразить сервер сочным вредоносным ПО, злоупотребив выполнением произвольных команд ... 91
Извлечь список всех учетных данных пользователей через SQL-инъекцию ... 92
Нарушенная аутентификация ... 93
Задачи, рассматриваемые в этом разделе ... 93
Сбросить пароль аккаунта OWASP Бьёрна через механизм Forgot Password ... 94
Изменить пароль Бендера на slurmCl4ssic, не используя SQL-инъекцию или функцию Forgot Password ... 95
Выполнить вход с удаленного пользовательского аккаунта Криса ... 96
Выполнить вход с Gmail-аккаунта Бьёрна ... 96
Выполнить вход с учетными данными администратора без их предварительного изменения или применения SQL-инъекции ... 97
Сбросить пароль Бендера через механизм Forgot Password ... 97
Сбросить пароль внутреннего аккаунта Бьёрна через механизм Forgot Password ... 97
Сбросить пароль Джима через механизм Forgot Password ... 98
Решить задачу с 2FA для пользователя wurstbrot ... 98
Раскрытие конфиденциальных данных ... 99
Задачи, рассматриваемые в этом разделе ... 99
Получить доступ к любому файлу журнала доступа сервера ... 100
Получить доступ к конфиденциальному документу ... 101
Выполнить несанкционированное раскрытие информации, получив доступ к данным из другого домена ... 101
Разработчик по невнимательности жестко закодировал неиспользуемые, но все еще действительные учетные данные ... 101
Найти конечную точку, которая предоставляет данные об использовании для сбора популярной системой мониторинга ... 101
Получить доступ к забытому резервному файлу разработчика ... 102
Получить доступ к забытому резервному файлу менеджера по продажам ... 102
Похитить чужие персональные данные, не используя инъекции ... 103
Провести «дайвинг в мусорных баках» в интернете в поисках утекшего пароля и войти в исходную учетную запись пользователя, которой он принадлежит ... 103
Сообщить магазину об утекшем API-ключе ... 104
Идентифицировать опасный товар, который был изъят из магазина, и сообщить магазину, какие ингредиенты опасны ... 105
Войти, используя оригинальные учетные данные пользователя Эми ... 105
Войти, используя оригинальные учетные данные пользователя MC SafeSearch ... 106
Определить ответ на секретный вопрос Джона ... 106
Получить доступ к неуместному файлу сигнатур SIEM ... 106
Захватить кошелек, содержащий наш официальный непередаваемый токен ... 107
Сбросить пароль Увогина через механизм Forgot Password ... 107
Лишить магазин дохода, загрузив чертеж для одного из его товаров ... 107
Определить ответ на секретный вопрос Эммы ... 108
Внешние XML-сущности (XXE) ... 108
Задачи, рассматриваемые в этом разделе ... 109

Извлечь содержимое C:\Windows\system.ini или /etc/passwd с сервера.....109
Дать серверу что-то, что он будет «пережевывать» довольно долгое время 110
Некорректная проверка ввода.....110
Задачи, рассматриваемые в этом разделе.....110
Зарегистрироваться как пользователь с привилегиями администратора.....111
Получить премиум-подписку, не заплатив за нее.....111
Зарегистрировать пользователя с пустыми email и паролем 111
Успешно активировать код купона из просроченной кампании 111
Отчеканить NFT «Honey Pot», собрав BEE (жетоны-пчелы) из пчелиного убежища (bee-heaven) 112
Найти фотографию кота Бьёрна в «режиме ближнего боя» 112
Разместить заказ, который сделает вас богатым.....112
Обойти средство контроля безопасности с помощью Poison Null Byte 113
Следовать принципу DRY при регистрации пользователя 113
Загрузить файл размером более 100 Кб.....114
Загрузить файл, не имеющий расширения .pdf или .zip 114
Оставить для магазина сокрушительный отзыв (ноль звезд).....114
Нарушенный контроль доступа.....114
Задачи, рассматриваемые в этом разделе.....115
Получить доступ к разделу администрирования магазина 115
Изменить имя пользователя, выполнив межсайтовую подделку запроса из другого источника 116
⚠ Важная информация о совместимости с браузерами 116
Найти скрытое пасхальное яйцо.....117
Избавиться от всех отзывов клиентов с 5 звездами 117
Оставить отзыв от имени другого пользователя 117
Оставить рецензию на товар от имени другого пользователя или отредактировать существующую рецензию любого пользователя...118
Положить дополнительный товар в корзину покупок другого пользователя ..118
Изменить href ссылки в описании товара O-Saft.....118
Запросить скрытый ресурс на сервере через сервер 119
Просмотреть корзину покупок другого пользователя 119
Найти случайно развернутую кодовую песочницу.....120
Небезопасная конфигурация (Security Misconfiguration) 120
Задачи, рассматриваемые в этом разделе.....120
Прикрепить милых кросс-доменных котят на все наши коробки для доставки 120
Использовать устаревший B2B-интерфейс, который не был должным образом отключен.....121
Спровоцировать ошибку, которая обрабатывается не очень изящно и не единообразно 121
Войти, используя оригинальные учетные данные команды поддержки.....122
Межсайтовый скриптинг (XSS).....123
Задачи, рассматриваемые в этом разделе.....123
Выполнение сохраненной XSS-атаки без использования фронтенд-приложения 124
Использование бонусной полезной нагрузки в задании на DOM XSS 125
Обход политики безопасности контента и выполнение XSS-атаки на устаревшей странице 125
Выполнение сохраненной XSS-атаки с обходом клиентского механизма безопасности 126

Выполнение DOM XSS-атаки....126
Выполнение сохраненной XSS-атаки через HTTP-заголовок....127
Выполнение отраженной XSS-атаки....127
Выполнение сохраненной XSS-атаки с обходом серверного механизма безопасности....127
Встраивание XSS-полезной нагрузки в наше промовидео....128
Небезопасная десериализация....128
Задачи, рассматриваемые в этом разделе....129
Запустить удаленное выполнение кода, которое навсегда загрузило бы менее защищенное приложение....129
Поместить взрывоопасные данные (Memory bomb) в уязвимую конечную точку обработки файлов....130
Запустить удаленное выполнение кода, которое занимает сервер на некоторое время, не используя бесконечные циклы....130
Уязвимые компоненты....131
Задачи, рассматриваемые в этом разделе....131
Перезаписать файл с правовой информацией....131
Создать поддельный, почти правильно подписанный RSA JWT-токен....132
Сообщить магазину о подражателе, использующем тайпсквоттинг, который глубоко внедрился во фронтенд....133
Навсегда отключить чат-бот поддержки....134
Сообщить магазину о трюке с тайпсквоттингом, жертвой которого он стал....134
Получить доступ к чтению произвольного локального файла на веб-сервере....134
Сообщить команде разработчиков об опасности, угрожающей некоторым из их учетных данных....135
Создать поддельный, по сути, неподписанный JWT-токен....135
Сообщить магазину об уязвимой библиотеке, которую он использует....136
Безопасность через сокрытие контента....136
Задачи, рассматриваемые в этом разделе....137
Узнайте о продаже токенов до ее официального анонса....137
Докажите, что вы действительно прочитали нашу политику конфиденциальности....138
Сдайте известного злоумышленника, скрывающегося у всех на виду в магазине....138
Открытые перенаправления....140
Задачи, рассматриваемые в этом разделе....140
Осуществить принудительное перенаправление на страницу, на которую перенаправлять не разрешено....140
Позвольте нам перенаправить вас на один из наших адресов криптовалют....140
Нарушенная защита от ботов....141
Задачи, рассматриваемые в этом разделе....141
Отправить 10 или более отзывов клиентов в течение 20 с....141
Найти языковой файл, который так и не попал в производство....142
Поставить лайк любому отзыву как минимум три раза от одного и того же пользователя....143
Сбросить пароль Морти через механизм Forgot Password....144
Проблемы криптографии....144
Задачи, рассматриваемые в этом разделе....144
Создать поддельный код купона, который дает вам скидку не менее 80 %....145

Выполнить задание № 999 145
Применить продвинутый криптоанализ, чтобы найти настоящее пасхальное яйцо 146
Разблокировать премиум-задание для доступа к эксклюзивному контенту ...146
Сообщить магазину об алгоритме или библиотеке, которые ему определенно не следует использовать так, как он это делает 147
Сбои в наблюдаемости 148
Задания, рассмотренные в этой главе 148
Получение доступа к любому файлу журнала доступа сервера 148
Поиск конечной точки, которая предоставляет данные об использовании для сбора популярной системой мониторинга....149
Поиск в интернете утекшего пароля и вход в исходную учетную запись пользователя, которому он принадлежит 149
Получение доступа к неправильно расположенному файлу сигнатур SIEM 151
Разное 152
Задачи, рассматриваемые в этом разделе....152
Получить код купона от чат-бота поддержки 152
Закрыть несколько уведомлений «Задание решено» за один раз 152
Прочитать нашу политику конфиденциальности 152
Найти тщательно скрытую страницу Score Board....153
Juice Shop подвержен известной уязвимости в библиотеке, по которой уже выпущен совет....153
Вести себя как подобает любому «белому хакеру» до начала активных действий 153
Вывести из нового кошелька больше ETH, чем вы внесли....154

Часть III. Участие в проекте 155

Участие в проекте 156
Каналы в социальных сетях....156
Оставить отзыв....156
Каналы для обратной связи....156
Обратная связь по заданиям 157
Пожертвования 159
Поддержка Juice Shop....160
Целевые пожертвования....162
Указание авторства 162
Внести вклад в разработку....163
Советы для новичков 163
Контроль версий....163
Рекомендации по внесению вклада....165
Непрерывная интеграция и развертывание 169
Кодовая база 101 171
Клиентский уровень....171
Серверный уровень 182
Уровень хранения 189
Сквозные тесты (End-to-end tests)....193
Помощь в переводах....194
Crowdin....194
Перевод напрямую через GitHub PR 196

Часть IV. Расширенные руководства пользователя 197

Устранение неполадок 198
Проверки при запуске 198
Распространенные вопросы поддержки 202
Кастомизация 204
Как кастомизировать приложение 204
Конфигурационный файл YAML 205
Пример конфигурации 217
Цветовые темы Material 222
Предоставленные кастомизации 223
Проприетарная кастомизация 225
Ограничения 227
Дополнительные настройки браузера 227
Проведение мероприятия CTF 231
Запуск Juice Shop в режиме CTF 232
Инфраструктура мероприятия CTF 233
Настройка скоринг-серверов CTF для Juice Shop 235
Использование других фреймворков CTF 246
Отказ от ответственности за коммерческое использование 247
Платформа хостинга для нескольких пользователей 247
Руководство инструктора 250
Экземпляры 250
Кастомизация 250
Рекомендации для класса 251
Существующие тренинги 252
Задания для демонстраций 252
Обучение автоматизации с помощью инструментов безопасности 254
Руководство вендора 256
Задание по взлому против базовой уязвимости 256
Интеграция 257
API заданий 257
Файл объявления заданий 259
Веб-хук решения задания 260
API фрагментов уязвимого кода 262
Мониторинг 262
Метрики Prometheus 263
Панель мониторинга Grafana 264

Часть V. Расширенные руководства для разработчиков 265

Сценарии учебных пособий Hacking Instructor 266
Сценарии инструкций для заданий 266
Вспомогательные функции 268
Регистрация нового скрипта 269
Пример для справки 270
Обнаружение использования запрещенных приемов 273
Расчет показателя нарушения правил 274
Задания по написанию кодов 275
Общий показатель читерства 276
Ограничения 277

Задания по написанию кода 277
Фрагменты уязвимого кода 278
Комментарии-маркеры `vuln-code-snippet` 278
Файлы вариантов исправления 282
Информационный YAML-файл 286
Обучающие данные чат-бота 290
Определение разговорных намерений 291
Действия со специальными функциями 291
Пример обучающих данных 292

Приложение 299

Решения заданий 300
Задания сложности ⋆ 300
Задания сложности ⋆ ⋆ 309
Задания сложности ⋆ ⋆ ⋆ 315
Задания сложности ⋆ ⋆ ⋆ ⋆ 341
Задания сложности ⋆ ⋆ ⋆ ⋆ ⋆ 362
Задания сложности ⋆ ⋆ ⋆ ⋆ ⋆ ⋆ 391
Текст песенки (Jingle lyrics) 412
Табулатура для гитары 413

Об этой книге 414

Литература 415

Предметный указатель 418

Введение

Это официальное сопроводительное руководство к приложению OWASP Juice Shop. Будучи веб-приложением с огромным количеством намеренно внедренных уязвимостей безопасности, OWASP Juice Shop задуман как полная противоположность образцового приложения или шаблона для веб-разработчиков: это инструмент повышения осведомленности, обучения, демонстрации и отработки рисков безопасности современных веб-приложений. OWASP Juice Shop – это проект с открытым исходным кодом, поддерживаемый некоммерческой организацией Open Worldwide Application Security Project® (OWASP) и разрабатываемый и поддерживаемый добровольцами. Содержание данной книги написано для версии v19.0.0 OWASP Juice Shop.

Книга разделена на пять частей.

Часть I – Подготовка к взлому

Первая часть помогает запустить приложение и настроить опциональные инструменты для взлома.

Часть II – Охота за слабыми местами

Вторая часть дает обзор уязвимостей[1], присутствующих в OWASP Juice Shop, включая подсказки, как их найти и эксплуатировать в приложении.

Часть III – Участие в проекте

Третья часть описывает различные способы внести вклад в проект с открытым исходным кодом OWASP Juice Shop.

Часть IV – Руководства для продвинутых пользователей

Четвертая часть содержит раздел по устранению неисправностей, а также руководства по кастомизации тем оформления, проведению Capture-the-Flag[2], технической интеграции, мониторингу и рекомендации для наставников.

---

[1] Уязвимость в контексте информационной безопасности – это недостаток (ошибка, слабое место, дефект) в программном обеспечении, аппаратном обеспечении, настройках системы, архитектуре или процессах, который может быть использован злоумышленником для нарушения конфиденциальности, целостности или доступности данных/системы – получения несанкционированного доступа, выполнения произвольного кода, кражи информации, отказа в обслуживании и т. п. (по сути, это «дыра», через которую угроза может превратиться в реальную атаку; именно поэтому говорят: «угроза + уязвимость = инцидент»). – *Прим. ред.*

[2] Capture the Flag (CTF, «Захват флага») – это популярный формат соревнований по кибербезопасности и информационной безопасности, где участники (команды или индивидуально) решают разнообразные практические задачи по взлому систем, криптографии, реверс-инжинирингу, веб-эксплойтам, форензике и другим дисциплинам, чтобы найти и «захватить» скрытые флаги – специальные секретные строки (обычно в формате `flag{...}`), которые отправляются организаторам для начисления очков; цель – набрать максимум баллов за ограниченное время, имитируя реальные сценарии хакерских атак. – *Прим. ред.*

Часть V – Руководство для продвинутых разработчиков

Пятая часть дает подробные указания по специфическим «закулисным» темам, таким как обнаружение читов[3] или реализация заданий на программирование.

Пожалуйста, имейте в виду, что эта книга не предназначена для всестороннего введения в безопасность веб-приложений в целом. Для каждой категории уязвимостей, присутствующих в OWASP Juice Shop, вы найдете краткое объяснение – обычно путем цитирования и ссылки на существующий контент по данной теме.

Читайте сопроводительное руководство онлайн по адресу:

- *https://pwning.owasp-juice.shop*.

Скачайте файл .pdf или .epub здесь:

- *https://leanpub.com/juice-shop*.

Вносите контент, предложения и правки на GitHub:

- *https://github.com/juice-shop/pwning-juice-shop*.

Официальная домашняя страница проекта OWASP Juice Shop:

- *https://owasp-juice.shop*.



Open Worldwide Application Security Project и OWASP являются зарегистрированными товарными знаками OWASP Foundation, Inc. Данная работа защищена авторским правом © Bjoern Kimminich и лицензирована под Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Зачем нужен Juice Shop

Для неподготовленного пользователя Juice Shop выглядит просто как небольшой интернет-магазин, продающий (сюрприз!) фруктовые и овощные соки и связанные товары. За исключением полностью переоцененного аспекта опла-

[3] Обнаружение читов (cheat detection) – это набор технических методов, алгоритмов и систем, которые автоматически или полуавтоматически выявляют использование запрещенных программ, скриптов, модификаций или нечестных действий игроков в онлайн-играх, CTF-соревнованиях или других платформах. Оно анализирует поведение игрока, память процесса, сетевой трафик, ввод с клавиатуры/мыши, статистику действий, хеши файлов и другие признаки, чтобы отличить легитимную игру от читерства (aimbot, wallhack, speedhack, автоматизация, подмена данных и т. п.), после чего может выдать предупреждение, временный/постоянный бан или передать данные на ручную проверку. – *Прим. ред.*

ты и доставки в электронной коммерции, Juice Shop полностью функционален. Но это лишь вершина айсберга. Juice Shop содержит 110 заданий различной сложности, где вы должны воспользоваться базовыми уязвимостями безопасности. Уязвимости были намеренно внедрены в приложение именно для цели обучения, но способом, который действительно происходит в реальной веб-разработке!

Ваш прогресс взлома отслеживается приложением с помощью немедленных push-уведомлений об успешных эксплойтах[4], а также с помощью панели результатов (Score Board) для обзора прогресса. Найти эту панель результатов – на самом деле одно из (самых простых) заданий! Идея в том, чтобы использовать техники геймификации для мотивации вас к выполнению как можно большего количество заданий, – аналогично разблокировке достижений во многих современных видеоиграх.

Разработка Juice Shop началась в сентябре 2014 года как личная инициатива автора, когда его работодатель нуждался в более современной среде для упражнений по безопасности, предназначенной для внутреннего веб-приложения. Ранее используемая среда относилась к эпохе серверного рендеринга ASP/JSP/Servlet и не отражала реальности текущих веб-технологий. Juice Shop разрабатывался как ПО с открытым исходным кодом без какого-либо корпоративного брендинга с самого начала. К концу 2014 года большая часть текущей функциональности электронной коммерции была готова и запущена:

- вместе с первоначальным количеством внедренных уязвимостей. За годы было добавлено больше вариантов уязвимостей. Параллельно приложение поддерживалось в актуальном состоянии с последними веб-технологиями (например, WebSocket и OAuth 2.0) и фронтенд-фреймворками (т. е. путем миграции с AngularJS с Bootstrap на Angular с Material Design). Некоторые из этих дополнительных возможностей дали шанс добавить соответствующие уязвимости – и список заданий растет до сих пор.

Помимо задач обучения хакеров и повышения осведомленности, мы приглашаем разработчиков инструментов тестирования на проникновение и автоматизированные сканеры безопасности, чтобы они могли использовать Juice Shop как своего рода подопытное приложение для проверки, насколько хорошо их продукты справляются с фронтендами, сильно зависящими от JavaScript и REST API.

---

[4] Эксплойт (от англ. *exploit*) – это программа, фрагмент кода или последовательность действий, которые используют уязвимость в программном обеспечении, операционной системе или оборудовании. Цель эксплойта – получить несанкционированный доступ к системе, вызвать сбой в ее работе или повысить свои привилегии (например, стать администратором). Проще говоря, это «взломщик», который находит и использует «брешь» в защите, чтобы заставить программу делать то, что не предусмотрено ее разработчиками. – *Прим. ред.*

Что означает OWASP?

> Open Worldwide Application Security Project (OWASP) – это некоммерческий фонд, который работает над улучшением безопасности ПО. Наша деятельность включает: проекты ПО с открытым исходным кодом под руководством сообщества более 275 локальных отделений по всему миру, включающих десятки тысяч членов; ведущие в отрасли образовательные и обучающие конференции. Мы – открытое сообщество, посвященное тому, чтобы позволить организациям задумывать, разрабатывать, приобретать, эксплуатировать и поддерживать приложения, которым можно доверять. Все наши проекты, инструменты, документы, форумы и отделения бесплатны и открыты для всех, кто заинтересован в улучшении безопасности приложений. Фонд OWASP запущен 1 декабря 2001 года, став зарегистрированной некоммерческой благотворительной организацией США 21 апреля 2004 года. [1]

Через два года после создания, в сентябре 2016 года, Juice Shop был подан и принят как OWASP Tool Project проектом Open Worldwide Application Security Project. Этот шаг значительно увеличил известность и охват проекта, поскольку открыл его для большого сообщества практиков безопасности приложений.

После того как Juice Shop попал в портфель проектов OWASP, ему потребовалось всего восемь месяцев, чтобы получить повышение с начального уровня зрелости *Incubator* до уровня *Lab Projects*. К концу июля 2018 года Juice Shop был повышен до высшей стадии зрелости *Flagship* для проектов OWASP.



Откуда взялось название Juice Shop?

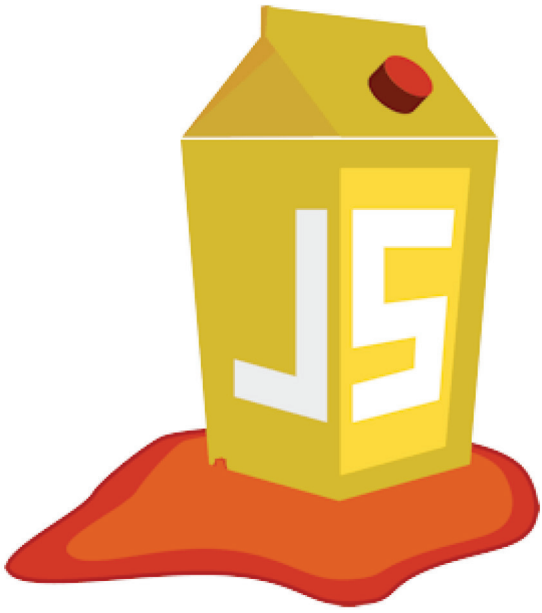
В немецком языке существует разговорное слово Saftladen (буквально «соковый магазин»), которое обозначает захудалый, сомнительный магазинчик, торгующий дешевым барахлом низкого качества, где клиенты и их удовлетворенность совершенно не в приоритете. Обратный перевод отдельно как Saft и Laden дает juice и shop на английском. Оттуда и взялось название проекта. Тот факт, что инициалы JS совпадают с теми, что обычно используются для JavaScript, был чистым совпадением и не связан с выбором технологии реализации.

Почему такой логотип?

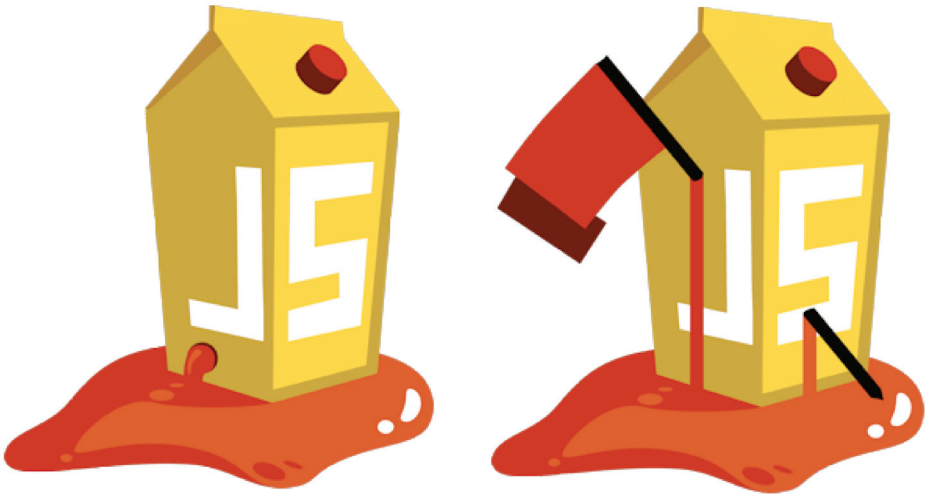
В отличие от названия логотип Juice Shop был разработан с явным учетом JavaScript:



Идея автора заключалась в преобразовании одного из неофициальных, но популярных щитов-логотипов JavaScript в протекающую коробку сока, потому что форма оказалась довольно подходящей для этой проделки.



В 2017 году логотип получил подтяжку лица и спин-офф, когда Juice Shop ввел свое расширение Capture-the-Flag.



Зачем еще одно уязвимое веб-приложение?

Существенное количество уязвимых веб-приложений уже существовало до создания Juice Shop. OWASP Vulnerable Web Applications Directory (VWAD) ведет список этих приложений. Когда родился Juice Shop, в VWAD были только приложения с серверным рендерингом, однако приложения в стиле Rich Internet Application (RIA) или Single Page Application (SPA) в то время уже были товаром. Juice Shop предназначался для заполнения этого пробела.

Многие из существующих уязвимых веб-приложений были весьма рудиментарными по функциональному охвату. Таким образом, целью Juice Shop было также продемонстрировать функционально полное приложение электронной коммерции, которое могло бы существовать в «диком» виде.

Обзор архитектуры

OWASP Juice Shop – это чистое веб-приложение, реализованное на JavaScript и TypeScript (который компилируется в обычный JavaScript). В фронтенде популярный фреймворк Angular используется для создания так называемого Single Page Application[5]. Макет пользовательского интерфейса реализует Material Design Google с использованием компонентов Angular Material. Все иконки, найденные в интерфейсе, происходят из библиотеки Font Awesome.

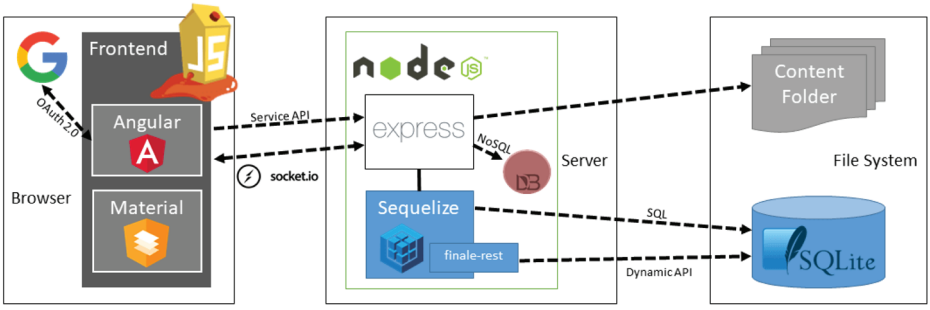
[5] Single Page Application (SPA) – это веб-приложение, работающее в рамках одной единственной HTML-страницы, которая подгружается с сервера один раз, а все дальнейшее взаимодействие с пользователем происходит через динамическую перезапись текущей страницы с помощью JavaScript. Вместо того чтобы каждый раз загружать целиком новые HTML-страницы с сервера (как это делают классические сайты), SPA просто обменивается с сервером данными (обычно в формате JSON) и плавно обновляет только нужные части интерфейса, что делает приложение более похожим на настольную программу и обеспечивает очень быструю работу. – *Прим. ред.*

JavaScript также используется в бэкенде как единственный язык программирования: приложение Express, размещенное в сервере Node.js, доставляет клиентский код в браузер. Оно также предоставляет необходимую функциональность бэкенда клиенту через RESTful API. В качестве подлежащей базы данных выбрана легкая SQLite из-за ее файловой природы. Это делает базу данных легкой для создания с нуля программно, без нужды в выделенном сервере. Sequelize и finale-rest используются как уровень абстрагирования от базы данных. Это позволяет использовать динамически созданные конечные точки API для простых взаимодействий (т. е. CRUD-операций) с ресурсами базы данных, при этом обеспечивая выполнение пользовательских SQL для более сложных запросов.

В качестве дополнительного хранилища данных в OWASP Juice Shop входит MarsDB. Это JavaScript-производная от широко используемой NoSQL-базы данных MongoDB, она совместима с большинством ее операций запроса/модификации.

Push-уведомления, которые показываются при успешном взломе задания, реализованы через протокол WebSocket. Приложение также предлагает удобную регистрацию пользователей через OAuth 2.0, так что пользователи могут войти с помощью своих учетных записей Google.

Следующая диаграмма показывает высокоуровневые пути связи между клиентом, сервером и слоями данных:



Часть I

Подготовка к взлому

Подготовка к взлому

OWASP Juice Shop предлагает несколько способов быть развернутым и использованным. Автор сам видел его работающим на следующих устройствах или ресурсах:

- ограниченных корпоративных компьютерах Windows;
- сильно кастомизированных дистрибутивах Linux;
- всех видах оборудования Apple;
- разогнанных игровых ноутбуках Windows;
- различных Chromebook с нативной поддержкой Linux;
- различных облачных платформах.

Шанс, что вы сможете запустить OWASP Juice Shop на своем компьютере, довольно высок. Эта часть книги поможет вам установить и запустить Juice Shop, а также проведет вас через приложение и некоторые фундаментальные правила и подсказки для его взлома.

Если вы столкнетесь с проблемами во время установки или запуска приложения, пожалуйста, не стесняйтесь просить помощи в чате сообщества или открывая GitHub issue! Просто убедитесь, что вы сначала пролистали приложение по устранению неисправностей.

Запуск OWASP Juice Shop

Системные требования

Запуск отдельного экземпляра Juice Shop предъявляет следующие требования к памяти и CPU. Эти ресурсы нужны для самого процесса приложения Juice Shop, и они основаны на следующем:

- среднем за 30 дней использовании CPU и RAM процесса официальной публичной демонстрационной инстанции, работающей на v14.0.1 Juice Shop;
- тренинге с ~30 участниками на кластере MultiJuicer, размещенном на OpenShift с Juice Shop v14.0.1.

Пожалуйста, обратите внимание, что любые дополнительные ресурсы, необходимые вашей среде (например, Docker или Vagrant), идут сверху.

- Минимальная системная спецификация
    - 256 Мб RAM.

Конец ознакомительного фрагмента.
Приобрести книгу можно
в интернет-магазине
«Электронный универс»
e-Univers.ru