Сравнительный анализ CTF-платформ для обучения кибербезопасности

О.Р. Лапонина, В.А. Матошенко

***Аннотация* – В статье рассмотрена процедура внедрения игровых механизмов в образовательный процесс. Описаны основные элементы геймификации, понятие игрового элемента «Захват флага» («CaptureTheFlag» - CTF), рассмотрены основные принципы архитектуры CTF-платформ и общая схема организации CTF-соревнований. Рассмотрены следующие виды CTF-соревнований - «Опрос» («Quiz»), «Атака-Оборона» («Attack-Defense»), «Анализ рисков» или «Решение задач» («Jeopardy» или «Task-Based»), «Царь Горы» («King of the Hill»), «Смешанный» («Mixed»). В статье определены основные требования к CTF-платформам и критерии из сравнения. В качестве требования к CTF-платформам выделены следующие: простота установки, кроссплатформенность, лёгкость конфигурирования, мониторинг состояния, расширяемость, интерактивность.**

В настоящей статье рассмотрены пять CTF-платформ: WebGoat и Security Shepherd от OWASP, CTFd, FBCTF, RootTheBox от сторонних производителей. Последние три CTF-платформы в качестве демонстративно уязвимого приложения используют JuiceShop от OWASP, который рассмотрен отдельно. Во всех платформах реализованы основные уязвимости из Top 10 OWASP. Все платформы имеют открытый исходный код и доступны на GitHub.

***Ключевые слова* – геймификация, кибербезопасность, CTF, CaptureTheFlag, веб-безопасность, Top 10 OWASP, WebGoat, Security Shepherd, CTFd, FBCTF, RootTheBox, JuiceShop, SQL-инъекции, взлом аутентификации, XSS, XXE.**

I. Введение

Рост преступлений в киберпространстве заставляют компании и государства развивать и поддерживать такую отрасль, как информационная и кибербезопасность. В связи с этим возникает острая потребность в технических специалистах, обладающих необходимым набором знаний и навыков для обеспечения штатного функционирования информационных инфраструктур различных организаций.

Статья получена 07 февраля 2022.

В.А. Матошенко – МГУ им. М.В. Ломоносова (e - mail: matoshenkova@mail.ru).

О.Р. Лапонина – МГУ имени М.В. Ломоносова (email: laponina@oit.cmc.msu.ru).

.

Компьютерные игры, появившиеся еще на заре развития компьютерной техники, во многом повлияли на технологии обучения специалистов в области информационной безопасности.

A. Процесс геймификации

Геймификация – это технология использования игровых методов для обучения практическим навыкам [1, 2].

Современное поколение молодых людей с самого раннего возраста увлекалось компьютерными играми, и для них соревновательный процесс в обучении выглядит вполне естественным и интересным. Выполнение заданий различных уровней, от более простых к более сложным, решение задач и головоломок, различные виды цифровых поощрений — всё это делает процесс обучения интересным и познавательным.

B. Элементы геймификации

Для процесса геймификации характерны следующие особенности.

1. Использование различных способов взаимодействия между учащимися.
2. Возможность изменения сценариев в режиме реального времени.
3. Различные системы мотивации не только в виде оценок.

C. «Захват флага» («CaptureTheFlag»)

Игровой элемент, связанный с захватом и защитой флага или «CaptureTheFlag» (CTF) возник в первых сетевых компьютерных онлайн-играх. CTF – это соревновательный режим игры, в котором участники пытаются захватить «флаги» противников и защитить свой. Специалистам и экспертам в области информационной безопасности пришла идея спроецировать CTF-формат на образовательный процесс по ИБ-специальностям.

Под флагом в CTF-соревнованиях, как правило, понимают цифровую последовательность произвольных символов, полученную в ходе решения задачи. CTF по информационной безопасности со временем видоизменился, и на сегодняшний день не все этапы соревнований представляют из себя захват и удержание флага. Основные преимущества геймификации – это быстрый переход от теоретического курса к практическим занятиям, игровой атмосфере и командной работе. Таким образом, у участников происходит более качественное усвоение материала благодаря получению практических навыков.

II. Архитектура CTF-платформ

Для организации соревнований по принципу CTF необходима программная платформа, позволяющая запускать одновременно несколько экземпляров взаимодействующих между собой приложений. На самом абстрактном уровне архитектура представлена на рис. 1.

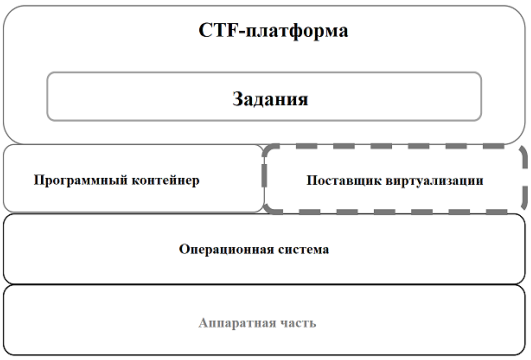

Рис. 1. Абстрактные архитектурные слои CTF-платформы

Персональным местом участника CTF-соревнования является рабочая станция с развёрнутой операционной системой. Над ОС, как правило, надстраивается средство виртуализации с программным контейнером. Программный контейнер в свою очередь уже содержит графическую оболочку с формой для регистрации, набором заданий, а также специальной формой для вставки ответов в виде цифровой последовательности, называемой флагом. Как правило, программные платформы для организации соревнований сами по себе не являются полигоном для решения задач. Платформы служат интерфейсом управления процессом соревнований, неким связующим звеном между организаторами и участниками.

Основные функции CTF-платформ:

- регистрация отдельных участников или команд;

- размещение текста заданий и дополнительной информации;

- размещение объявлений и подсказок;

- проверка флагов;

- подсчёт командных очков;

- составление таблицы рейтинга в реальном времени.

Неотъемлемой частью архитектуры CTF-соревнований наряду с самой платформой является веб-сервер и веб-приложение с набором уязвимостей, которые следует найти. Для таких приложений существует устоявшийся термин vulnerable box или сокращённо «vulnbox». «Vulnbox» чаще всего представляет из себя образ виртуальной машины с предустановленной *nix системой, на которой запущены различные веб-сервисы.

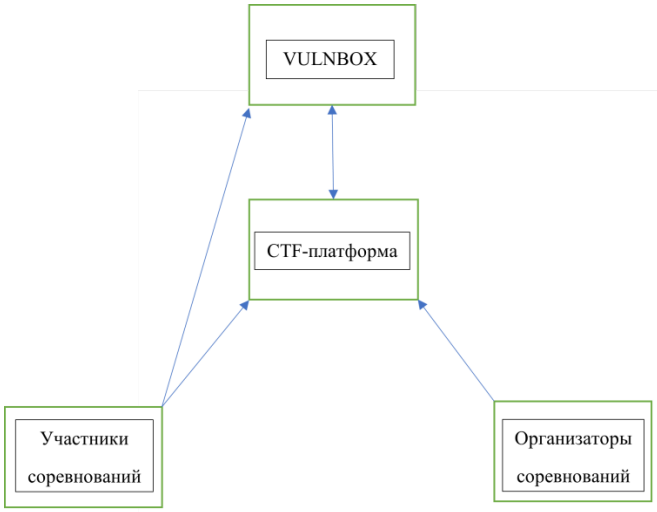

Рис. 2. Общая схема организации CTF-соревнований

На рис. 2 представлен общий принцип построения соревнований. Участники соревнований могут быть как отдельными игроками, так и командами. Они взаимодействуют как с CTF-платформой, так и с vulnbox. На CTF-платформе участники проходят регистрацию, получают задания и подсказки, а также вставляют флаги для получения очков. Основные действия, связанные с демонстрацией практических навыков, выполняются учащимися на vulnbox. Перечень заданий определяет модели цифровых навыков кибербезопасности [3]. Организаторы в свою очередь осуществляют управление мероприятием через единую систему доступа CTF-платформы. Также с использованием CTF-платформы вносятся изменения и объявления, и осуществляется управление vulnbox.

III. Виды CTF-соревнований

На сегодняшний день можно выделить пять основных видов CTF-соревнований:

- «Опрос» («Quiz»),
- «Атака-Оборона» («Attack-Defense»),
- «Анализ рисков» или «Решение задач» («Jeopardy» или «Task-Based»),
- «Царь Горы» («King of the Hill»)
- «Смешанный» («Mixed»). Формат «Mixed» является производным от всех остальных видов, так как по сути представляет из себя различные их комбинации.

Все виды различаются внутренними правилами соревновательного процесса, установленными организаторами соревнований в соответствии с тем или иным форматом. Остановимся более подробно на каждом из видов.

A. «Опрос» («Quiz»)

«Опрос» («Quiz») – это своего рода викторина, состоящая из заданий типа «вопрос-ответ» из области кибербезопасности или из связанных тем [4, 5]. В качестве ответов представлено несколько вариантов, из которых один или несколько могут быть верные. За каждый правильный ответ предполагается начисление баллов. Формат проведения CTF-соревнований в виде «Quiz» больше напоминает тестирование и рассчитан

преимущественно на закрепление полученных теоретических знаний и не предполагает решение практических задач.

B. «Атака-Оборона» («Attack-Defense»)

Классический вид CTF-соревнований называется «Attack-Defense» или «Classic» [6]. Данный вид соревнований полностью включает в себя все элементы геймификации «CaptureTheFlag». После того как организаторы раздают участникам «vulnbox», начинается основной этап соревнования. Задача участников соревнования заключается в поиске устранения критических уязвимостей на своем веб-сервере, а также в попытке использовать уязвимости серверов других участников. Общий принцип построения этого вида соревнования представлен на рис. 3.

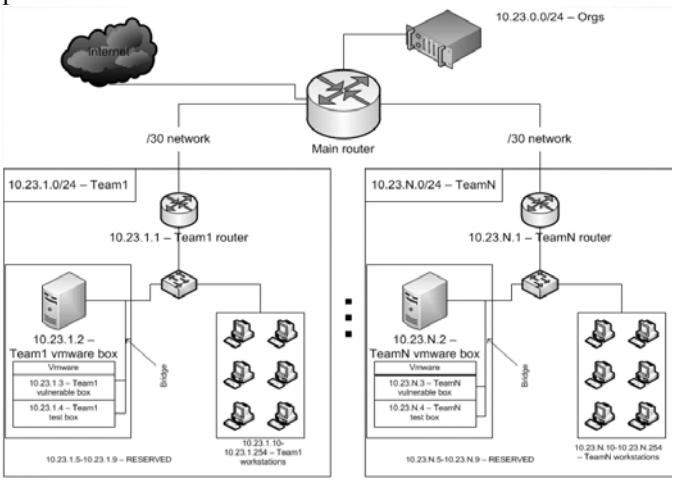

Рис. 3. Общая топология сети в соревновании «Attack-Defense»

Классический вид CTF – это командное соревнование, в котором большое число команд, объединенных сетью, сражаются друг с другом в общей информационной среде. Участникам разрешается использовать любые конфигурации, изменять настройки на своё усмотрение, выстраивать оборону сетевого периметра, осуществлять мониторинг, настраивать автоматическую фильтрацию трафика и многое другое.

C. «Анализ рисков» («Jeopardy»)

Ещё одним видом CTF-соревнований является «Jeopardy» или, как его еще называют, «Task-Based» [7, 8]. Он основан на выполнении практических заданий, за успешное решение которых дают флаг. Каждое задание оценивается очками, чем сложнее задание, тем больше очков за него дают. В настоящее время повсеместно наблюдается тенденция роста популярности именно этого вида CTF-соревнований. «Jeopardy» проводится в следующих категориях тем:

1. Reverse – классический реверс-инжиниринг;
2. Exploit – использование уязвимостей;
3. Web – задания на веб-безопасность;
4. Crypto – уязвимости криптографических алгоритмов;
5. Stegano – извлечение скрытой информации;
6. Forensic – расследование инцидентов и анализ образов и файлов;
7. PPC – спортивное программирование в прикладной форме.
8. OSINT – Opensource Intelligence или разведка по открытым источникам информации в сети «Интернет».

D. «Царь горы» («King Of The Hill»)

«Царь горы» — это самый молодой вид CTF-соревнований [9. Целью участников в соревновании вида «King Of The Hill» или «KotH» является поиск уязвимостей архитектуры системы и несанкционированное проникновение в неё. На следующем этапе в системе необходимо закрепиться и не позволить другим участникам перехватить управление. Основное отличие от других видов CTF-соревнований заключается в том, что через установленные администрацией промежутки времени веб-серверы возвращаются в исходное состояние и соревнование начинается заново. Такой подход к организации соревнований полностью соответствует духу известной модели жизненного цикла киберугроз под названием Cyber-Kill Chain [10].

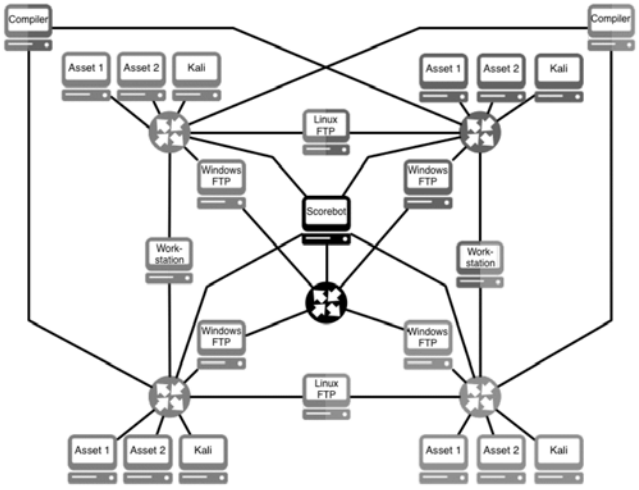

Рис. 4. Общая топология сети в соревновании «KotH»

E. «Смешанный» («Mixed»)

С ростом популярности CTF-соревнований происходит трансформация составов заданий и смешивание форматов проведения мероприятий. Так появляются новые виды CTF под общим названием «Mixed», включающие в себя комбинирование заданий из видов «Attack-Defense» и «Jeopardy»**.** В данном виде соревнований командам приходится помимо решения заданий организовывать защиту своего веб-сервера и искать уязвимости серверов других участников. Комбинирование нескольких видов CTF в одном соревновании повышает интерес участников и степень вовлеченности в игровой процесс, а также поднимает престиж турнира.

IV. Сравнительный анализ open-source CTF-платформ

A. *Требования к CTF-платформе и критерии сравнения*

Считается, что тестирование инструментальных средств анализа уязвимостей должно выполняться в специально созданных для этих целей программных средах.

На сегодняшний день существует более трёх десятков CTF-платформ с открытым исходным кодом от разных разработчиков. Одним из лидеров в разработке CTF-платформ является консорциум Open Web Application Security Project (OWASP). Это открытое сообщество, состоящее из различных компаний, образовательных организаций и специалистов со всего мира [11]. Целью консорциума OWASP являются разработка рекомендаций, документации, учебных материалов, статей, инструментов и технологий, направленных на поддержку грамотного использования технологий обеспечения безопасности. Проект OWASP Vulnerable Web Applications Directory (VWAD) ведет всеобъемлющий и обновляемый реестр демонстративно уязвимых веб-приложений [12]. Эти приложения могут использоваться в учебных целях веб-разработчиками, аудиторами безопасности и тестировщиками на проникновение для проверки своих навыков, а также для тестирования различных инструментов взлома и методов проведения атак. Уязвимые веб-приложения разделены на три категории: онлайн, офлайн и виртуальные машины/ISO.

Определим ряд требований, которым должна удовлетворять CTF-платформа.

1. **Простота установки**: CTF-платформа должна легко устанавливаться, не вызывая затруднений.
2. **Кроссплатформенность**: возможность установки на разные ОС.
3. **Лёгкость конфигурирования**: CTF-платформа должна быть легко настраиваемой, обладать дружественным интерфейсом, достаточным набором функционала для проведения различного типа соревнований и тренингов.
4. **Мониторинг состояния**: CTF-платформа должна иметь возможности отслеживать действий пользователей и выводить результаты на специальное табло в режиме реального времени.
5. **Расширяемость**: CTF-платформа должна обеспечивать возможность легкого изменения заданий, их модификации, добавлении новых и удаление старых.
6. **Интерактивность**: возможность взаимодействие между атакующей и защищающейся сторонами во время соревнования. Далеко не все платформы поддерживают данный функционал.

В [4] приведен сравнительный анализ различных CTF-платформ с открытым исходным кодом. Автор классифицирует платформы по способу установки программного обеспечения и методам доступа к ним. Выделены следующие **способы установки CTF-платформы и доступа к соревнованию**:

1. Размещение платформ с помощью **услуг хостинга**.
2. **Локальная установка**. Участие в соревновании в месте его проведения.
3. Возможность проведения **онлайн-соревнований** в режиме реального времени.
4. Возможность проведения **онлайн-обучения**.

Сравнение различных open-source CTF-платформ возможно также по следующим параметрам.

1. **Программные среды**, на которые ставится CTF-платформа.
2. **Конструктивные особенности** и функциональность CTF-платформы.
3. **Типы задач**, поддерживаемые CTF-платформой.
4. **ПО**, используемое для настройки и управления CTF-соревнованиями.

В [13] приведена статистика по числу соревнований, проводимых с 2012 по 2020 год в дистанционном и очном форматах в трех категориях «Jeopardy», «Attack-Defense» и «HackQuest». Разновидность соревнований под названием «HackQuest» по утверждению авторов мало чем отличается от «Jeopardy».

В настоящей статье будут рассмотрены пять CTF-платформ: WebGoat и Security Shepherd от OWASP, CTFd, FBCTF, RootTheBox от сторонних производителей. Последние три CTF-платформы в качестве демонстративно уязвимого приложения используют JuiceShop от OWASP, который будет рассмотрен отдельно.

Все платформы имеют открытый исходный код и доступны на GitHub.

Таблица 1. Общие сведения о разработке платформ

Название платформы	Разработчик платформы	Год выпуска
WebGoat	Bruce Mayhew, OWASP	2002
Security Shepherd	Mark Denihan, Sean Duggan, OWASP	2014
CTFd	KevinChung	2017
FBCTF	FaceBook Inc.	2017
RootTheBox	Joe D. (Alias: Moloch)	2016

Таблица 2. Сравнение CTF-платформ по критериям управляемости

CTF-платформа	Лёгкость конфигурирования	Мониторинг состояния	Расширяемость	Интерактивность
WebGoat	-	-	+	-
Security Shepherd	-	-	+	-
CTFd	+	+	+	-
FBCTF	+	+	+	-
RootTheBox	+	+	+	-

Таблица 3. Общие характеристики рассматриваемых CTF-платформ

CTF-платформа	Тип ОС	Установка	Язык программирования	Поддержка	Вид лицензии
WebGoat	Любая	Локальная, Docker	Java	Да	GNU General Public License v2.0
Security Shepherd	Любая	Локальная, Docker	Java	Да	GNU General Public License v3.0
CTFd	Любая	Локальная, Vagrant, Docker	PHP	Да	Apache License 2.0
FBCTF	Любая, рекомендуется Ubuntu 16.04 LTS	Локальная, Vagrant, Docker	Python	Нет	Attribution-NonCommercial 4.0 International
RootTheBox	Linux, BSD, OSX	Локальная, Docker	Python	Да	Apache License 2.0

Таблица 4. Характеристики платформ по видам соревнований

Название платформы	Quiz	Attack-Defense	Jeopardy	KingOfTheHill
WebGoat	+	-	+	-
Security Shepherd	+	-	+	-
CTFd	+	-	+	-
FBCTF	+	-	+	+
RootTheBox	+	-	+	+

B. WebGoat

Основная цель проекта WebGoat – создание юридически безупречной интерактивной обучающей среды для тестирования безопасности веб-приложений. WebGoat – это полноценное веб-приложение, позволяющее разработчикам проанализировать типичные уязвимости, обычно обнаруживаемые в Java приложениях, а также протестировать инструментальные средства поиска уязвимостей [14, 15].

В WebGoat можно выполнить около 30 видов атак. Дополнительно к WebGoat разработано приложение WebWolf, которое может помочь при решении некоторых заданий. WebWolf является отдельным веб-приложением, имитирующим сервер атакующей стороны. Наличие такого сервера позволяет корректно имитировать последовательность взаимодействий между уязвимым веб-сервером, браузером и сервером злоумышленника. В WebWolf реализованы следующие возможности: загрузка файлов, доступ к электронной почте, целевая страница на сервере атакующего для имитации атак типа XSS, CSRF и аналогичных. В некоторых случаях возможно использование других инструментов тестирования, например, «netcat».

Конфигурация WebGoat по умолчанию привязывается к localhost для минимизации рисков. В WebGoat реализована наиболее простая и удобная архитектура, позволяющая любому настроить среду обучения и начать выполнять задания. Сборка и управление проектом осуществляется с помощью Maven. WebGoat 8 написан на Spring Boot.

На корневом уровне есть файл pom.xml, который определяет параметры всех компонент WebGoat и WebWolf. На корневом уровне используются следующие плагины:

- Flatten maven, позволяет создавать версию POM-файла со следующими характеристиками:
  - Удаляются элементы, специфичные для сборки и разработки;
  - Все переменные разрешаются (resolved), все родительские связи разрешаются (resolved), сглаживаются и удаляются.
- Checkstyle maven, создает отчет в соответствии со стилем кода, используемым разработчиками.
- Pmd maven, выполняет статический анализ кода.

Проект WebGoat состоит из следующих модулей:

- webgoat-контейнер использует следующие плагины:
  - Surefire maven, который позволяет использовать различные провайдеры тестирования.
  - Jar maven, который позволяет выполнять сборку jar-файлов.
- webgoat-уроки состоит из плагинов для каждой реализованной уязвимости.
- webgoat-сервер состоит из следующих плагинов:
  - Spring boot maven обеспечивает поддержку Spring Boot для WebGoat;
  - Jar maven, который позволяет выполнять сборку jar-файлов.
- webwolf состоит из следующих плагинов:
  - Spring boot maven обеспечивает поддержку Spring Boot для WebGoat;
  - Jar maven, который позволяет выполнять сборку jar-файлов.
- webgoat-интеграционные тесты

Обучение основным типам уязвимостей веб-приложений проводится в следующей последовательности:

- теоретическое описание конкретной уязвимости, например, раскрывается назначение и использование данной уязвимости;
- практическое применение уязвимости на простом примере с демонстрацией возможностей ущерба;
- закрепление полученного навыка в виде дополнительного теоретического подкрепления. На этом этапе слушатель получает обзор возможных решений и исправлений, которые могут быть применены в будущем.

WebGoat 8 содержит примеры для основных категорий уязвимостей 2017г. по версии OWASP:

1. Инъекционные атаки (A01-2017 – Injections);
2. Взлом аутентификации (A02-2017 – Broken Authentication);
3. Незащищённость критичных данных (A03-2017 – Sensitive Data Exposure);

4. Внешние объекты XML (A04-2017 – XML External Entities – XXE);
5. Взлом управления доступом (A05-2017 – Broken Access control);
6. Межсайтовый скриптинг (A07-2017 – Cross Site Scripting – XSS);
7. Небезопасная десериализация (A08-2017 – Insecure Deserialization);
8. Использование компонентов с известными уязвимостями (A09-2017 – Using Components with known vulnerabilities);
9. Подделки запросов (A08-2013 – Request Forgeries).

В целом приложение Webgoat является достаточно старым, но очень популярным среди специалистов по информационной безопасности и по праву заслужило высокий рейтинг за счёт простоты архитекутры и насыщенности разнообразных заданий по большому спектру уязвимостей веб-приложений. И хоть формат проведения обучения больше похож на «Quiz» с элементами «Jeopardy», приложение по праву можно считать эталоном в области обучения специалистов по веб-безопасности.

C. Security Shepherd

Security Shepherd – проект OWASP, предназначенный для обучения специалистов веб-безопасности приложений [16, 17].

Проект Security Shepherd позволяет приобрести или улучшить навыки ручного тестирования веб-приложений. Как и во многих других аналогичных приложениях, пользователю вначале объясняются угрозы безопасности, а затем предлагается решить практические задачи. Под угрозой понимаются недостаточно хорошо проработанные меры защиты, благодаря которым существует возможность эксплуатации уязвимостей. В приложении реализованы уязвимости не только из списка OWASP Top 10.

В отличие от платформы WebGoat, Security Shepherd использует один из основных элементов CTF-соревнований – флаг, который представляет из себя цифровую последовательность символов, которая становится доступной в результате верно решённого задания.

Пользователи изучают также распространение уязвимостей и их влияние на прикладную систему. Также участники CTF-соревнования приобретают навык создания укрепленной среды выполнения, защищающей от основных угроз.

Преподаватель может настроить среду выполнения, чтобы учащиеся могли пройти только определенные темы или модули. Настройки системы позволяют использовать платформу как одним пользователем, взаимодействующим с системой локально, так и сообществом пользователей, участвующим в CTF-соревновании, в том числе и онлайн.

Проект Security Shepherd охватывает следующие категории уязвимостей:

1. SQL-инъекции;
2. Взлом аутентификации и управления сессией;
3. Межсайтовый скриптинг.
4. Небезопасная прямая ссылка на объект.
5. Неверная конфигурация безопасности.
6. Раскрытие конфиденциальных данных.
7. Отсутствие управления доступом на уровне функций.
8. Подделка межсайтовых запросов.
9. Некорректные перенаправления и переадресации.
10. Недостаточная проверка данных.
11. Небезопасное хранение данных.
12. Непреднамеренная утечка данных.
13. Плохая аутентификация и авторизация.
14. Криптографическая уязвимость.
15. Внедрение на стороне клиента.
16. Отсутствие двухфакторной защиты.

Security Shepherd включает в себя:

1. Обучающий инструмент по обеспечению безопасности веб-приложений;
2. Обучающий инструмент по тестированию на проникновение веб-приложений;
3. Обучающий инструмент по тестированию на проникновение мобильных приложений;
4. Безопасную игровую площадку для отработки методов Application Security;
5. Демонстрацию примеров реальных угроз безопасности.

Режимы работы платформы

Настройки платформы достаточно вариативны и позволяют настроить разные режимы работы.

Режим CTF

В режиме CTF пользователь может в каждый момент времени получить доступ только к одному незавершенному модулю. Первый модуль, к которому предоставлен доступ пользователю, является самым простым и помечается преподавателем как открытый. Сложность уровней постепенно увеличивается, и происходит переход от одной темы к другой. Такой режим рекомендуется для тренировок.

Режим открытого доступа

Когда платформа развернута в режиме открытого доступа, пользователь может получить доступ к любому уровню, который помечен преподавателем как доступный для прохождения. Модули отсортированы по категориям уязвимостей и прохождение теоретических занятий является приоритетным перед началом игрового процесса обучения. Этот режим подходит для желающих изучить подробно все основные уязвимости из списка OWASP Top 10.

Режим турнира

В режиме турнира пользователь может получить доступ к любому уровню, открытому преподавателем. Модули отсортированы по уровням сложности, от наименее к наиболее сложному. Такой режим подходит для проведения CTF-соревнований по безопасности веб-приложений.

Таблица 5. Свойства платформы Security Shepherd

Свойство	Описание
Широкий охват тем	Платформа включает более семидесяти уровней по всему спектру безопасности веб- и мобильных приложений
Постепенное усложнение изучаемого материала	Идеальная отправная точка для студентов, только начинающих изучение вопросов, связанных с безопасностью веб-приложений, так как сложность заданий увеличивается постепенно
Начальный уровень учащихся может быть достаточно низким	Каждая концепция безопасности описана простым языком, поэтому в ней легко разобраться начинающим специалистам
Реальные примеры атак	Уязвимости безопасности платформы – это настоящие уязвимости, воздействие которых на приложение и пользователя просто несколько ослаблено, чтобы не наносить вред приложению и пользователям. Это не моделирование реальных угроз, при котором для прохождения уровня следует выполнить определенную последовательность действий. Векторы атаки в заданиях – это то, как выполняется атака в реальной ситуации
Масштабируемость	Платформа может использоваться локально одним пользователем или в качестве сервера в многопользовательском режиме
Полностью настраиваемая платформа	Преподаватель может настраивать какие уровни доступны в настоящий момент и в каком режиме (открытом, CTF и режиме турнира)
Подходит для обучения в группе	Индивидуальные ключи, используемые для решения заданий, позволяют гарантировать самостоятельность выполнения задания участниками
Табло с результатами	В платформу встроено настраиваемое табло, что позволяет визуализировать конкурентность среды обучения. Пользователи, завершившие первый, второй и третий уровни, получают «медали» и «бонусные баллы», которые выводятся на табло.
Большие возможности администрирования аккаунтами пользователей	Администраторы могут создавать аккаунты пользователей и администраторов, приостанавливать, отменять приостановку, добавлять бонусные баллы или снимать штрафные баллы с учетных записей пользователей. Администраторы также могут разбивать участников на группы по классам и отслеживать прогресс, достигнутый каждым классом для выявления участников, испытывающих трудности. Администратор может закрыть публичную регистрацию и вручную создать пользователей, если они хотят пройти испытание самостоятельно
Поддержка локализации	Материалы платформы доступны на нескольких языках. Учащиеся с альтернативными языковыми предпочтениями могут без проблем соревноваться с другими участниками в одном и том же соревновании
Надежный сервис	Платформа использовалась для запуска онлайн-CTF, таких как OWASP «Global CTF» и OWASP «LATAM Tour CTF 2015», число участников которых превышало 200 активных пользователей, при этом сервисы работали без сбоев, за исключением плановых периодов обслуживания
Настраиваемая обратная связь	Администратор может использовать обратную связь. В этом случае участники должны явно завершать каждый уровень. Такой режим применяется для улучшения проекта на основе представленных отзывов, а также для сбора информации об уровне понимания заданий участниками
Детализированное ведение журнала	В платформе настроено журналирование и сбор логов по всем участникам и процессам

В целом приложение Security Shepherd обладает большим функционалом, чем аналогичное приложение WebGoat. Платформа позволяет настраивать режимы обучения и организовывать настоящие CTF-соревнования в режиме онлайн. Также реализованы флаги, с помощью которых предодаватель может задавать последовательность прохождения заданий. Платформа оставляет положительное впечатление от её использования и привлекает к себе простотой графического интерфейса и разнообразием заданий.

D. JuiceShop

JuiceShop – веб-приложение с огромным количеством уязвимостей, которое активно поддерживается ИБ-сообществом по всему миру [18]. Проект также принадлежит консорциуму OWASP и распространяется под свободными лицензиями. Его можно использовать в тренингах по безопасности, ознакомительных демонстрациях, CTF-соревнованиях и в качестве испытательного полигона для тестирования безопасности. JuiceShop включает в себя уязвимости из списка OWASP TOP 10, а также множество других уязвимостей, обнаруженных в реальных приложениях. На основе этого приложения разработаны не менее трёх CTF-платформ с открытым исходным кодом: CTFd, FaceBookCTF и RootTheBox. В этих платформах веб-приложение JuiceShop используется в качестве полигона для тренировок. Общая архитектура приложения представлена на рис.5.

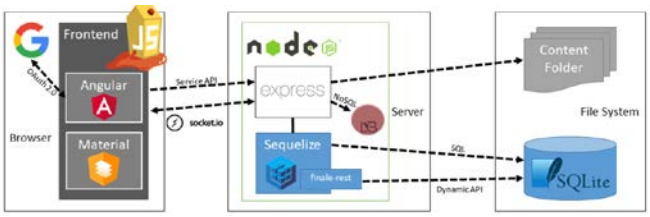

Рис. 5. Архитектура веб-приложения JuiceShop

Клиентская часть JuiceShop реализована на фреймворках с открытым исходным кодом Angular и Material-UI. В клиентской части реализована возможность аутентификации по протоколу OAuth 2.0 с google-аккаунтом. Серверная часть реализована на Node.js. В качестве базы данных используется NoSQL MongoDB. Также на серверной стороне используется Express - минималистичный и гибкий веб-фреймворк для приложений Node.js, предоставляющий обширный набор функций для мобильных и веб-приложений. Веб-фреймворк взаимодействует с Angular клиентской части и с основным контентом в файловой системе. Для взаимодействия с файловой системой используется объектно-реляционное отображение Sequelize, которое с помощью SQL запросов обращается к SQLite.

Уязвимости, реализованные в JuiceShop, подразделяются на несколько различных категорий. Большинство из них охватывают различные типы

рисков, описанных в таких документах, как OWASP Top 10, OWASP ASVS, OWASP Automated Threat Handbook, OWASP API Security Top 10 и Common Weakness Enumeration MITRE. Все задачи, которые требуется решить для нахождения уязвимостей, имеют название, задачи помечены определенным тегом, и указана их сложность. В таблице 6 представлены основные категории уязвимостей и перечислены названия задач, которые требуется решить для использования каждой уязвимости. Дополнительно в приложение встроены специальные теги. Теги не представляют категории уязвимостей, но служат дополнительной метаинформацией о принадлежности к тому или иному классу. Они позволяют определить сходства или особенности уязвимостей.

Таблица 6. Основные примеры атак в приложении JuiceShop

#	Категория	Сложность	Тег	Описание
1.	**I. Взлом управления доступом**	**	Подходит для демонстрации	Доступ к административному хранилищу.
2.		***		Изменение имени пользователя для выполнения межсайтовой подделки запросов (Cross-Site Request Forgery) из другого источника.
3.		****	Идеи, подходит для демонстрации, подделки	Поиск скрытых данных.
4.		**		Удаление нежелательных отзывов клиентов.
5.		***	Руководство	Опубликование отзыва от имени другого пользователя.
6.		***		Опубликование отзыва о продукте от имени другого пользователя или редактирование существующего отзыва любого пользователя.
7.		***		Добавление товара в корзину некоторого пользователя.
8.		***		Изменение адреса (href) ссылки в OWASP SSL Advanced Forensic Tool (O-Saft) описании продукта на https://owasp.slack.com.
9.		******	Анализ кода	Запрос скрытого ресурса на сервере, используя сервер.
10.		**	Подходит для демонстрации, руководство	Просмотр корзины покупок другого пользователя.
1.	**II. Взлом защиты от ботов**	***	Грубая сила	Отправка 10 и более отзывов клиентов в течение 10 секунд.
2.		*****	Грубая сила	Получение языкового файла, который не находится в production-версии.
3.		******		Отметка «Нравится» любого отзыва не менее трех раз от имени одного и того же пользователя.
4.		*****	Грубая сила, OSINT	Сброс пароля с помощью механизма «Забыт пароль» при запутанном ответе на контрольный вопрос.
1.	**III. Взлом аутентификации**	***	OSINT	Сброс пароля учетной записи OWASP с помощью механизма «Забыт пароль», указав исходный ответ на контрольный вопрос.
2.		*****		Изменение пароля **без** использования SQL-инъекции или «Забыт пароль».
3.		***		Вход со стертого пользовательского аккаунта.
4.		****	Анализ кода	Вход с Gmail-аккаунта, **без** предварительного изменения его пароля с использованием SQL-инъекции или взломав Google-аккаунт.
5.		**	Грубая сила, руководство	Вход с правами администратора **без** предварительного изменения его пароля или применения SQL-инъекции.
6.		****	OSINT	Переустановка пароля посредством механизма «Забыт пароль», отвечая на контрольный вопрос пользователя.
7.		*****	OSINT	Переустановка пароля внутреннего аккаунта посредством механизма «Забыт пароль», отвечая на контрольный вопрос пользователя.
8.		***	OSINT	Переустановка пароля посредством механизма «Забыт пароль» с исходным ответом на контрольный вопрос.
9.		*****		Решение задач двухфакторного обмена (запрет, обход или перезапись двухфакторных установок не считается решением).
1.	**IV. Криптографические проблемы**	******	Анализ кода, подходит для демонстрации	Подделка кода купона, который дает скидку не менее 80%.
2.		******	Анализ кода, подделки	Решение несуществующей задачи.
3.		****	Подходит для демонстрации, подделки	Применение продвинутого криптоанализа для нахождения слабых мест.
4.		******	Подделки	Разблокировка «Премиального вызова» для получения доступа к эксклюзивному контенту.

5.		**		Информирование магазина об алгоритме или библиотеке, которые он не должен использовать так, как он это делает.
1.	**V. Некорректная проверка ввода**	***		Регистрация в качестве пользователя с администраторскими правами.
2.		***		Получение премиального членства без оплаты.
3.		****		Успешное использование купона с истекшим сроком действия.
4.		*	Подделки	Получение скрытой фотографии.
5.		***		Размещение выгодного заказа.
6.		****	Предпосылка	Обход управления безопасностью с использованием «нулевого байта» для получения доступа к скрытому.
7.		*		Следование принципу «Не повторяться» при регистрации пользователя.
8.		***		Загрузка файла размером более 100 kB.
9.		***		Загрузка файла, который не имеет расширение .pdf или .zip.
10.		*		Дать магазину отрицательный и разрушительный отзыв.
1.	**VI. Инъекции**	****		Заказ специального предложения прошлых лет.
2.		***		Получение всей схемы базы данных посредством SQL-инъекции.
3.		****		Вход в систему с несуществующего аккаунта без регистрации.
4.		**	Подходит для демонстрации, руководство	Вход с администраторского аккаунта.
5.		***	Руководство	Вход с пользовательского аккаунта.
6.		***	Руководство	Вход с пользовательского аккаунта.
7.		****	Опасная зона	Перевод сервера в спящий режим.
8.		*****	Опасная зона	Получение чужих заказов.
9.		****		Обновление нескольких отзывов о товаре одновременно.
10.		******	Анализ кода, приспособление, опасная зона	Инфицирование сервера вредоносным ПО, выполнив произвольную команду.
11.		****		Получение списка всех учетных данных пользователей с помощью SQL-инъекции.
1.	**VII. Небезопасная десериализация**	*****	Опасная зона	Удаленное выполнение кода, который навсегда перегрузит недостаточно защищенное приложение.
2.		******	Опасная зона	Удаленное выполнение кода, который загрузит сервер, при этом не будет использоваться бесконечный цикл.
1.	**VIII. Разное**	*	Грубая сила, махинации	Получение кода купона от чат-бота службы поддержки.
2.		*	Лучшие практики, подходит для демонстрации, руководство	Чтение политики конфиденциальности.
3.		*	Анализ кода, руководство	Обнаружение станиц, не доступных по ссылкам.
4.		**	Лучшие практики	Принципы «этичного хакера».
1.	**IX. Ошибки конфигурации**	*****	Идеи	Возможность пометить все междоменные ссылки.
2.		**	Идеи, предпосылка атаки	Использование устаревшего B2B интерфейса, который не обеспечивает корректный останов (shut down).
3.		*	Предпосылка атаки	Провоцирование ошибки, которая некорректно обрабатывается.
4.		******	Идеи	Вход в систему с правами пользователя группы сопровождения без использования SQL-инъекции или другой технологии обхода.
1.	**X. Безопасность через неизвестность**	*****	Анализ кода, идеи	Возможность узнать о продажах до их официального объявления.
2.		***	Подходит для демонстрации, махинации	Возможность доказать, что вы действительно прочитали политику конфиденциальности.
3.		****	Махинации	Возможность определять скрытые символы.
1.	**XI. Раскрытие чувствительных данных**	****		Получение произвольного доступа к файлу логов на сервере.
2.		*	Подходит для демонстрации	Получение доступа к конфиденциальному документу.
3.		*****		Раскрытие информации с помощью междоменного доступа к данным.
4.		*	Лучшие практики	Нахождение конечной точки, которая используется для сбора данных популярной системой мониторинга.
5.		****	Идеи, подходит для демонстрации, предпосылка атаки	Получение доступа к файлу резервной копии, который забыл удалить разработчик.
6.		****	Идеи	Доступ к файлу резервной копии, который забыл удалить продавец.
7.		****		Возможность украсть персональные данные без использования инъекций.
8.		*****	OSINT	Обнаружение логинов и паролей с интернете и вход по ним в аккаунт пользователя. (Создание нового аккаунта с тем же самым паролем не считается решением.)

9.		****	OSINT, махинации	Определение небезопасного продукта, который был удален из магазина, и информирование магазина об опасных элементах.
10.		***	OSINT	Вход с правами законного пользователя. (Быстрее, чем с использованием метода «Грубой силы»)
11.		**	OSINT, махинации	Вход в MC SafeSearch с правами законного пользователя без применения SQL-инъекции или другого способа обхода.
12.		**	OSINT	Определение ответа на контрольный вопрос посредством просмотра загрузок и используя этот ответ для сброса пароля с помощью механизма «Забыт пароль».
13.		****	Идеи, лучшие практики	Доступ к некорректно расположенному файлу подписи SIEM.
14.		****	OSINT	Переустановка пароля посредством механизма «Забыт пароль» с корректным ответом на контрольный вопрос.
15.		*****		Лишение магазина заработка с помощью скачивания чертежа одного из его товаров.
16.		**	OSINT	Определение ответа на контрольный вопрос с помощью просмотра загруженной информации, и использование его для сброса пароля с помощью механизма «Забыт пароль».
1.	**XII. Некорректные перенаправления**	****	Предпосылка атаки	Перенаправление на страницу, на которую не должно быть перенаправления.
2.		*	Анализ кода	Перенаправление на страницу, которая больше не рекламируется.
1.	**XIII. Уязвимые компоненты**	******	Опасная зона, предпосылка атаки	Перезаписывание юридически значимого файла.
2.		*****		Информирование магазина об опечатке в коде на стороне клиента, указав точное название компонента.
3.		*****	Анализ кода	Отключение навсегда чат-бота службы поддержки, чтобы он больше не мог отвечать на запросы клиентов.
4.		****		Информирование магазина об уловке с опечаткой, жертвой которой он стал.
5.		*****	Опасная зона, OSINT	Получение доступа по чтению к произвольному локальному файлу на веб-сервере.
6.		*****	OSINT	Информирование команды разработчиков об опасности некоторых их креденциалов. (Послать URL отчета, или соответствующий CVE, или другой идентификатор данной уязвимости)
7.		*****		Подделка фактически не подписанного JWT-токена, в котором указан несуществующий пользователь.
8.		****	OSINT	Информирование магазина об использовании уязвимой библиотеки, указав название библиотеки и версию компонента.
1.	**XIV. XSS-атаки**	***	Опасная зона	Выполнение хранимой XSS-атаки, используя `<iframe src = "javascript:alert(`xss`)">` без использования приложения на стороне клиента.
2.		*	Махинации, руководство	Выполнение DOM XSS-атаки, используя `<iframe …> </iframe>`
3.		****	Опасная зона	Обход CSP и выполнение XSS-атаки, используя `<script> alert(`xss`) </script>` на странице приложения.
4.		***	Опасная зона	Выполнение хранимой XSS-атаки, используя `<iframe src = "javascript:alert (`xss`)">` и обходя механизм защиты на стороне клиента.
5.		*	Подходит для демонстрации, руководство	Выполнение DOM XSS-атаки, используя `<iframe src = "javascript:alert ( `xss` )">`.
6.		****	Опасная зона	Выполнение хранимой XSS-атак, используя `<iframe src = "javascript:alert(`xss`)">` в HTTP-заголовке.
7.		**	Опасная зона, подходит для демонстрации	Выполнение отраженной XSS-атаки, используя `<iframe src = "javascript:alert (`xss`)">`.
8.		****	Опасная зона	Выполнение хранимой XSS-атаки, используя `<iframe src = "javascript:alert (`xss`) ">`, обходя механизм безопасности на стороне сервера.
9.		******	Опасная зона	Встроенное в видео содержимое XSS-атаки `</script> <script> alert (`xss`) </script>`.
1.	**XV. XXE-атаки**	***	Опасная зона	Получение с сервера содержимое C:\Windows\system.ini или /etc/passwd.
2.		*****	Опасная зона	Замедление работы сервера.

Основные преимущества подхода, реализованного в приложении Juice Shop:

1. Открытый исходный код, решение open source;
2. Простота инсталляции под операционные системы Windows/Mac/ Linux с помощью node.js, Docker и Vagrant;
3. Возможность установки для облачных решений;
4. Автономность, включающая в себя все необходимые для работы зависимости;
5. Подходит для обучения с «нуля» благодаря скриптам «Hacking Instructor» с дополнительным учебным режимом;
6. Внедрены процессы геймификации;
7. Автоматически сохраняется текущий уровень прогресса в браузере или с помощью локального резервного копирования;
8. При каждом новом запуске приложения все поля очищаются;

9. Полностью настраиваемый интерфейс в соответствии с корпоративными требованиями;
10. Поддержка CTF-режима;
11. Интероперабильность: поддержка интеграции с собственными системами обучения через WebHook, отслеживание глобальных показателей или получение информации о задачах напрямую через API или импорт файлов.

В результате анализа функционала уязвимого веб-приложения JuiceShop можно сделать вывод о том, что это мощный инструмент, предназначенный для тестирования уязвимостей веб-сайтов и приложений, позволяющий в игровом режиме решать задачи обучению специалистов в области безопасности веб-приложений.

E. FacebookCTF

Компания Facebook занимается внедрением CTF-платформ с 2013 года, целевой аудиторией для них являются школьники и студенты. Благодаря платформам с открытым исходным кодом школы, студенческие группы и организации всех уровней квалификации могут проводить собственные соревнования, практические занятия и конференции для обучения навыкам информатики и безопасности. FacebookCTF (FBCTF) – это платформа для проведения соревнований в формате «Mixed», объединяющая такие стили как «King of the Hill» и «Jeopardy» [19, 20]. Платформа достаточно гибкая, позволяет использовать различные типы установок в зависимости от потребностей конечного пользователя. Платформа FBCTF может быть установлена либо в режиме разработки, либо в производственном режиме, а также поддерживает многопользовательский режим. Текущий набор задач включает проблемы в области обратного проектирования, криминалистики, безопасности веб-приложений, криптографии и использования двоичных файлов. Существует возможность создавать свои собственные задачи для использования в платформе FBCTF.

Функционал платформы весьма разнообразен и позволяет конфигурировать настройки через панель управления под учётной записью администратора.

CTF предоставляют безопасный и легальный способ попробовать свои силы в решении задач обхода блокировок и различных видов нарушения целостности веб-сайтов. Платформа также использует преимущества других проектов Facebook с открытым исходным кодом, включая HHVM и Flow.

В панели управления администратора платформы существует возможность выбора ручной регистрации участников соревнований. Также доступна опция самостоятельной регистрации на мероприятие. Доступны два типа регистрации. В открытом режиме регистрация является публичной. В токенизированном режиме входа в систему администраторы должны генерировать и раздавать токены регистрирующимся игрокам. Эти токены используются в качестве входных данных при регистрации команды.

В платформе реализованы три типа задач:

1. *Вопросы* – викторина, на каждый вопрос есть только один ответ, причем ответы могут быть любыми, от одного слова до целого предложения.
2. *Флаги* – задачи, решение которых состоит в последовательности шагов.Вв результате выполнения этих шагов участник получает «флаг», который необходимо отправить для начисления баллов. Все флаги должны быть в формате *flag{some_text_here}*, что является устоявшейся практикой при организации соревнований. Если в задаче не используется флаг, это должно быть явно указано в описании. В типичной задаче с флагом может быть указан URL веб-сайта, который необходимо взломать, или служба, к которой нужно подключиться, используя netcat. Цели задач могут варьироваться, например, запись флага из базы данных в систему, получение доступа к командной строке в системе или простой обман приложения для отображения флага.
3. *Базовые задачи* – это задачи, которые *являются* частью игры вида «Царь горы». Они представляют собой систему, которая должна быть взломана, и кто ее первый взламывает, тот получает определенное количество баллов. После этого данный участник получает баллы пропорционально времени удержания системы. Все эти числа можно полностью настроить в разделе «Конфигурация» на странице администратора. Ссылка на взламываемую систему указывается в формате <IP address:port>.

Для настройки базовой задачи требуется агент, работающий во взламываемой системе, который будет подсчитывать очки участников. Участники должны записать название своей команды в определенный файл с помощью любой команды, например, `echo "ThisIsATeamName">tmp/SCORE_POINTS`. Очки будут начислены данной команде.

Платформа FBCTF поддерживает возможность указать подсказки, которые созданы организатором соревнований. В некоторых случаях подсказки будут в описании задачи. В других случаях кнопка подсказки расположена под задачей. Если отсутствует штраф за подсказку, следует нажать на кнопку для получения подсказки. Если есть штраф, то он будет отображаться на кнопке, и его можно «оплатить» баллами, чтобы получить доступ к подсказке.

F. RootTheBox

RootTheBox – это CTF-платформа со встроенным механизмом подсчета очков в режиме реального времени [21, 22]. Приложение можно легко настроить и изменить для любого стиля CTF-игры. Платформа позволяет участвовать как новичкам, так и опытным игрокам, сочетая увлекательную игровую среду с реалистичными задачами, в результате решения которых участники знания, необходимые для реальной защиты веб-приложений, такие как тестирование на проникновение, реагирование на инциденты, цифровая криминалистика и поиск угроз.

Как и в других CTF-играх, каждая команда или игрок решают задачи различной сложности с целью собрать флаги. RootTheBox добавляет в игру дополнительные возможности. В платформу встроена поддержка

«ботнетов», которые можно загружать на целевые машины. Команды периодически вознаграждаются внутриигровыми деньгами за каждого бота в этой сети. Есть своя банковская система, в которой можно использовать внутриигровые деньги вместо очков для открытия новых уровней, покупки подсказок для флагов, загрузки исходного кода цели или даже «спецназа» для других игроков. Хэши паролей для банковских счетов игроков также могут быть публично отображены, что позволяет конкурентам взламывать их и красть деньги друг друга.

Основные возможности «RootTheBox»

1. Командная игра или индивидуальная игра.
2. Анимированные табло, графики и обновления статуса в реальном времени, используя веб-сокеты.
3. Определены различные типы флагов: статические, с регулярными выражениями, с датой и временем, флаги при множественном выборе, флаги для файла с параметрами.
4. Определены различные варианты штрафов, подсказок, попыток, бонусов за решения задач, динамический подсчет очков, различные категории задач и т.д.
5. Встроенные возможности обмена файлами и текстом в команде и распределения материалов об игре администратором.
6. Поддержка чата с интеграцией Rocket Chat.
7. Табло CTF поддерживает JSON.
8. Поддержка экспорта из OWASP JuiceShop.
9. Возможность заморозить табло на определенное время.
10. Дополнительные расширенные функции, такие как внутриигровые ботнеты, игроки «SWAT», внутриигровые деньги и табло, на котором отображаются взломанные пароли.
11. Возможности разблокировки компонент и обновления табло по мере того, как участники захватывают флаги.
12. Экспорт и публикация призовых элементов игры.
13. Поддержка нескольких языков.
14. Возможность настройки цветовой гаммы и другие интересные возможности.

G. CTFd

CTFd – это образовательная платформа Capture The Flag, ориентированная на простоту использования и настройки, благодаря различным плагинам и темам визуального оформления [19, 23, 24]. Платформа построена на разновидности соревнований «Jeopardy». В ней есть все необходимые функции для запуска соревновательного и образовательного процесса. Платформа основана на свободно распространяемом исходном коде и использует проект JuiceShop от OWASP.

Функции CTFd

1. Создание своих собственных задач, категорий, подсказок и флагов.
2. Возможность динамического подсчета очков.
3. Поддержка возможности блокировать и разблокировать задачи.
4. Архитектура plugin «Challenge» позволяет создавать собственные задачи.
5. Определены статические флаги и на основе регулярных выражений.
6. Возможность создания plugin для определения пользовательских флагов.
7. Всплывающие подсказки.
8. Возможность загрузки файлов на сервер или серверную часть, совместимую с Amazon S3.
9. Ограничение количества попыток решения задач и сокрытия задач.
10. Автоматическая защита от перебора.
11. Возможность как индивидуального решения задач, так и проведение командных соревнований.
12. Участники могут играть сами по себе или объединяться в команды.
13. Наличие табло с автоматическим подсчётом очков.
14. Возможность скрыть результаты от других участников.
15. Возможность зафиксировать результаты в определенное время.
16. Графики результатов, сравнивающие 10 лучших команд, и графики прогресса команд.
17. Система управления контентом Markdown;
18. Поддержка SMTP и Mailgun по электронной почте.
20. Восстановление забытого пароля.
21. Автоматическое начало и завершения соревнования.
22. Управление командой, удаление и ограничение доступа.
23. Расширенные возможности настройки, используя интерфейсы плагинов и тем.
24. Импорт и экспорт данных CTF для архивирования.

V. Выводы

В результате сравнительного анализа рассматриваемых платформ можно выделить целый ряд преимуществ платформы CTFd. Она обладает более дружелюбным интерфейсом, легко настраивается, позволяет быстро адаптироваться к новым условиям проведения обучения или соревнований, а также не требует от организатора специальных знаний в области программирования для управления, редактирования и настройки. Кроме того, возможность интеграции платформы с проектом OWASP JuiceShop позволяет разнообразить игровой процесс обучения на реальных примерах уязвимого веб-приложения. В полной мере присутствуют игровые механики, а также используется наиболее популярный вид CTF-соревнований «Jeopardy».

Платформы RootTheBox и FaceBookCTF также позволяют взаимодействовать с проектом JuiceShop. Обе платформы обладают прекрасными элементами геймификации, будь то статус, поощрения и открытия, вознаграждения и др. Более того они обладают своим собственным сюжетом, позволяющим вовлечь участников в игровой процесс. Среди недостатков платформы FaceBookCTF можно отметить, что на данный момент разработчики поместили исходный код проекта на GitHub в архив, тем самым прекратилась его поддержка со стороны сообщества. Среди недостатков

платформы RootTheBox можно отметить трудные настройки интерфейса и управления. Отсутствует готовая к работе база данных пользователей из-за чего становиться доступен только режим администрирования. Однако, в этом режиме нет возможности проходить задания.

Платформы WebGoat и Security Shepherd легко устанавливаются и запускаются, обладают достаточно дружелюбным интерфейсом, однако трудны в настройке, так как требуют практических навыков веб-программирования на Java. Платформа WebGoat ближе всего к виду соревнований Quiz, что с точки зрения целей работы делает её менее привлекательной. Следует отметить прекрасные игровые механики, заложенные в платформу Security Shepherd.

По совокупности признаков среди рассмотренных платформ можно выделить платформу CTFd, позволяющую легко и быстро развернуть обучение или соревнование по кибербезопасности в формате Jeopardy, редактировать, добавлять и изменять задания по своему усмотрению, организовывать командные турниры и проверять навыки участников.

Библиография

[1] Daniel Berube, Motivate player for better engagement and retention [Электронный ресурс]. // URL: https://thinkgamedesign.com/player-retention-engagement, (2022).

[2] Вербах, Кевин, Д. Хантер. "Вовлекай и властвуй." Игровое мышление на службе бизнеса. М.: Манн, Иванов и Фербер (2015): 16-25, 10-50 с.

[3] Сухомлин В.А., Белякова О. С., Климина А.С., Полянская М. С., Русанов А. А. «Модель цифровых навыков кибербезопасности.» (2021).

[4] S. Kucek, M. Leitner «An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments», Journal of Network and Computer Applications, Volume 151, 2020, 102470, ISSN 1084-8045.

[5] Pew Research Center, Cybersecurity Knowledge Quiz, March 22, 2017, [Электронный ресурс]. // URL: https://www.pewresearch.org/internet/quiz/cybersecurity-knowledge/, (2022).

[6] S. Choi, J. Cha, S.K. "Git-based {CTF}: «A simple and effective approach to organizing in-course attack-and-defense security competition". In: 2018 {USENIX} Workshop on Advances in Security Education {ASE} 18.

[7] M. Swann, J. Rose, G. Bendiab, S. Shiaeles and F. Li, "Open Source and Commercial Capture The Flag Cyber Security Learning Platforms - A Case Study," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, pp. 198-205, doi: 10.1109/CSR51186.2021.9527941.

[8] Nakaya, Makoto, S. Akagi, and Hiroyuki Tominaga. "Implementation and trial practices for hacking competition CTF as introductory educational experience for information literacy and security learning." In Proceedings of ICIA 2016, vol. 5, pp. 57-62. (2016).

[9] Bock, Kevin, George Hughey, and Dave Levin. "King of the hill: A novel cybersecurity competition for teaching penetration testing." In 2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18).

[10] Smussenko, Diana Alexandrovna. "Cyber kill chain." Язык в сфере профессиональной коммуникации. — Екатеринбург, (2021): 569-575.

[11] M. Bach-Nutman "Understanding the Top 10 OWASP Vulnerabilities." arXiv preprint arXiv:2012.09960 (2020).

[12] Registry of all known vulnerable web applications OWASP-VWAD, [Электронный ресурс]. // URL: https://owasp.org/www-project-vulnerable-web-applications-directory, (2022).

[13] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková. "Cybersecurity knowledge and skills taught in capture the flag challenges" Computers & Security 102 (2021): 102154.

[14] Amin, Muhammad Ahmad and Saqib Saeed. "Role of Usability in E-Learning System: An Empirical Study of OWASP WebGoat." Human Factors in Software Development and Design, edited by Saqib Saeed, et al., IGI Global, (2015), pp. 295-312.

[15] WebGoat 8: A deliberately insecure Web Application, [Электронный ресурс]. // URL: https://github.com/WebGoat/WebGoat/blob/develop/README.MD/, (2022).

[16] Wibowo, Ripto Mukti, and Aruji Sulaksono. "Web Vulnerability Through Cross Site Scripting (XSS) Detection with OWASP Security Shepherd." Indonesian Journal of Information Systems 3, no. 2 (2021): 149-159.

[17] Manual Shepherd Setup, [Электронный ресурс]. // URL: https://github.com/OWASP/SecurityShepherd/wiki/Manual-Shepherd-Setup, (2022).

[18] OWASP Juice Shop CTF Extension, [Электронный ресурс]. // URL: https://www.npmjs.com/package/juice-shop-ctf-cli/, (2022).

[19] Chicone, Rhonda G., and Susan Ferebee. "A comparison study of two cybersecurity learning systems: facebook's open-source capture the flag and CTFd." Issues in Information Systems 21, no. 1 (2020): 202-212.

[20] FBCTF, «What is FBCTF?», [Электронный ресурс]. // URL: https://github.com/facebookarchive/fbctf/blob/master/README.md/, (2022).

[21] Magkos, Emmanouil. "An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools." Information security education. information security in action: 13th Ifip Wg 579, (2020).

[22] RootTheBox/README.md, [Электронный ресурс]. // URL: https://github.com/moloch--/RootTheBox/blob/master/README.md/, (2022).

[23] Basic Deployment, [Электронный ресурс]. // URL: https://github.com/CTFd/CTFd/wiki/Basic-Deployment/ (2022).

[24] CTFd Documentation, [Электронный ресурс]. // URL: https://docs.ctfd.io/ (2022).

Comparative analysis of CTF platforms for cybersecurity training

O.R. Laponina, V.A. Matoshenko

***Abstract*– The article discusses the procedure for introducing game mechanisms into the educational process. The main elements of gamification, the concept of the game element "Capture the flag" ("CaptureTheFlag" - CTF) are described, the basic principles of the architecture of CTF platforms and the general scheme of the organization of CTF competitions are considered. The following types of CTF competitions are considered - "Survey" ("Quiz"), "Attack-Defense" ("Attack-Defense"), "Risk Analysis" or "Problem Solving" ("Jeopardy" or "Task-Based"), "King of the Hill", "Mixed". The article defines the main requirements for CTF platforms and the criteria from the comparison. The following are highlighted as requirements for CTF platforms: ease of installation, cross-platform, ease of configuration, status monitoring, extensibility, interactivity.**

This article discusses five CTF platforms: WebGoat and Security Shepherd from OWASP, CTFd, FBCTF, RootTheBox from third-party manufacturers. The last three CTF platforms use JuiceShop from OWASP as a demonstratively vulnerable application, which is considered separately. All platforms have implemented the main vulnerabilities from the Top 10 OWASP. All platforms are open source and available on GitHub.

Keywords **– gamification, cybersecurity, CTF, CaptureTheFlag, web security, Top 10 OWASP, WebGoat, Security Shepherd, CTFd, FBCTF, RootTheBox, JuiceShop, SQL injection, broken authentication, XSS, XXE.**

REFERENCES

[1] Daniel Berube, Motivate player for better engagement and retention [Jelektronnyj resurs]. // URL: https://thinkgamedesign.com/player-retention-engagement, (2022).

[2] Verbah, Kevin, D. Hanter. "Vovlekaj i vlastvuj." Igrovoe myshlenie na sluzhbe biznesa. M.: Mann, Ivanov i Ferber (2015): 16-25, 10-50 s.

[3] Suhomlin V.A., Beljakova O. S., Klimina A.S., Poljanskaja M. S., Rusanov A. A. «Model' cifrovyh navykov kiberbezopasnosti.» (2021).

[4] S. Kucek, M. Leitner «An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments», Journal of Network and Computer Applications, Volume 151, (2020), 102470, ISSN 1084-8045.

[5] Pew Research Center, Cybersecurity Knowledge Quiz, March 22, 2017, [Jelektronnyj resurs]. // URL: https://www.pewresearch.org/internet/quiz/cybersecurity-knowledge/, (2022).

[6] S. Choi, J. Cha, S.K. "Git-based {CTF}: «A simple and effective approach to organizing in-course attack-and-defense security competition". In: 2018 {USENIX} Workshop on Advances in Security Education {ASE} 18.

[7] M. Swann, J. Rose, G. Bendiab, S. Shiaeles and F. Li, "Open Source and Commercial Capture The Flag Cyber Security Learning Platforms - A Case Study," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), (2021), pp. 198-205, doi: 10.1109/CSR51186.2021.9527941.

[8] Nakaya, Makoto, S. Akagi, and Hiroyuki Tominaga. "Implementation and trial practices for hacking competition CTF as introductory educational experience for information literacy and security learning." In Proceedings of ICIA 2016, vol. 5, pp. 57-62. (2016).

[9] Bock, Kevin, George Hughey, and Dave Levin. "King of the hill: A novel cybersecurity competition for teaching penetration testing." In 2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18).

[10] Smussenko, Diana Alexandrovna. "Cyber kill chain." Jazyk v sfere professional'noj kommunikacii. — Ekaterinburg, (2021): 569-575.

[11] M. Bach-Nutman "Understanding the Top 10 OWASP Vulnerabilities." arXiv preprint arXiv:2012.09960 (2020).

[12] Registry of all known vulnerable web applications OWASP-VWAD, [Jelektronnyj resurs]. // URL: https://owasp.org/www-project-vulnerable-web-applications-directory, (2022).

[13] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková. "Cybersecurity knowledge and skills taught in capture the flag challenges" Computers & Security 102 (2021): 102154.

[14] Amin, Muhammad Ahmad and Saqib Saeed. "Role of Usability in E-Learning System: An Empirical Study of OWASP WebGoat." Human Factors in Software Development and Design, edited by Saqib Saeed, et al., IGI Global, (2015), pp. 295-312.

[15] WebGoat 8: A deliberately insecure Web Application, [Jelektronnyj resurs]. // URL: https://github.com/WebGoat/WebGoat/blob/develop/README.MD/, (2022).

[16] Wibowo, Ripto Mukti, and Aruji Sulaksono. "Web Vulnerability Through Cross Site Scripting (XSS) Detection with OWASP Security Shepherd." Indonesian Journal of Information Systems 3, no. 2 (2021): 149-159.

[17] Manual Shepherd Setup, [Jelektronnyj resurs]. // URL:https://github.com/OWASP/SecurityShepherd/wiki/Manual-Shepherd-Setup, (2022).

[18] OWASP Juice Shop CTF Extension, [Jelektronnyj resurs]. // URL: https://www.npmjs.com/package/juice-shop-ctf-cli/, (2022).

[19] Chicone, Rhonda G., and Susan Ferebee. "A comparison study of two cybersecurity learning systems: facebook's open-source capture the flag and CTFd." Issues in Information Systems 21, no. 1 (2020): 202-212.

[20] FBCTF, «What is FBCTF?», [Jelektronnyj resurs]. // URL: https://github.com/facebookarchive/fbctf/blob/master/README.md/, (2022).

[21] Magkos, Emmanouil. "An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools." Information security education. information security in action: 13th Ifip Wg 579, (2020).

[22] RootTheBox/README.md, [Jelektronnyj resurs]. // URL: https://github.com/moloch--/RootTheBox/blob/master/README.md/, (2022).

[23] Basic Deployment, [Jelektronnyj resurs]. // URL: https://github.com/CTFd/CTFd/wiki/Basic-Deployment/ (2022).

[24] CTFd Documentation, [Jelektronnyj resurs]. // URL: https://docs.ctfd.io/ (2022).