Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.777:004.056.5:004.054

Пузеева
Александра Юрьевна

Методика тестирования безопасности инфраструктуры веб-приложений

АВТОРЕФЕРАТ
на соискание ученой степени магистра технических наук
по специальности 1-98 80 01 Информационная безопасность

_____

Научный руководитель
Белоусова Елена Сергеевна,
кандидат технических наук, доцент

_____

Минск 2021

ВВЕДЕНИЕ

В современном мире, с развитием сети Интернет, наиболее популярными становятся веб-приложения, доступ к которым пользователи получают удаленно с помощью различного программного обеспечения.

Использование веб-приложения несёт с собой различные угрозы безопасности. Каждое приложение различно и может содержать уникальные уязвимости. Большинство приложений разрабатываются недостаточно квалифицированными специалистами в области информационной безопасности, многие разработчики имеют лишь частичное представление уязвимостях, которые могут присутствовать в создаваемом ими коде, из-за этого могут возникать различные недостатки в веб-приложениях.

Из-за наличия уязвимостей, которые могут содержать веб-приложения происходят утечки конфиденциальных данных, что может нанести достаточный ущерб, как пользователям, так и владельцу веб-приложения.

В настоящее время проблема безопасности веб-приложений весьма актуальна, т. к. более 60 % от всех обнаруживаемых уязвимостей относятся к веб-приложениям. Одним из широко распространенных методов обеспечения безопасности веб-приложений является обнаружение уязвимостей с целью последующего их устранения.

В связи с этим особенно актуальным становится вопрос о наличии единой методики для обнаружения уязвимостей в веб-приложениях. Существуют множество международных методик и стандартов, которые содержат ряд недостатков и недочетов, таким образом целью является разработать собственную актуальную методику.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью диссертационной работы является совершенствование методики тестирования безопасности инфраструктуры веб-приложений для идентификации уязвимостей, приводящих к нарушению работы систем аутентификации и авторизации пользователей, а также получению прав доступа и полномочий администратора.

Для достижения поставленной цели необходимо было решить следующие задачи:

1 Изучить принципы построения инфраструктуры веб-приложений.

2 Провести анализ существующих уязвимостей в веб-приложениях.

3 Осуществить сравнительный анализ методик тестирования веб-приложения.

4 Разработать методику тестирования безопасности инфраструктуры веб-приложений.

5 Разработать методику сбора информации о тестируемом приложении.

6 Разработать методику анализа механизмов аутентификации и авторизации пользователей.

7 Сформировать структуру отчета по результатам тестирования веб-приложения по разработанным методикам.

8 Привести рекомендации по использованию разработанной методики тестирования безопасности инфраструктуры веб-приложений.

Тема диссертации соответствует приоритетным направлениям научных исследований в Республике Беларусь на 2021–2025 годы, установленным Указом Президента Республики Беларусь от 7 мая 2020 г. № 156 «О приоритетных направлениях научной, научно-технической и инновационной деятельности на 2021–2025 годы» п. 6.3 «Средства технической и криптографической защиты информации, криптология и кибербезопасность».

Личный вклад соискателя

Результаты исследований получены автором самостоятельно. Научный руководитель принимал участие в определении целей и задач исследования, интерпретации промежуточных результатов.

Апробация результатов диссертации

По теме диссертации опубликовано 2 тезиса доклада в сборниках материалов конференции.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе определена и изучена структура веб-приложений. Определены основные уязвимости веб-приложений из списка OWASP Top 10, влияющие на потерю конфиденциальных данных, изучен анализ распространенных угроз, их влияние, а также рассмотрены существующие методики, а именно NIST SP 800-115, OWASP Web Security Testing Guide, стандарт PTES, OSSTMM и BSI – Study a Penetration Testing Model, для проведения тестирования на безопасность.

Во второй главе проведен сравнительный анализ и разбор существующих методик анализа уязвимостей, для разработки нашей собственной методики для веб-приложений. Проведен разбор программного обеспечения для выполнения тестирования безопасности инфраструктуры веб-приложений, таких как Wapiti, BurpSuite, OWASP ZAP, w3af, nmap и dirb.

Для анализа уязвимостей при тестировании безопасности инфраструктуры веб-приложений была разработана методика, которая включает следующие этапы:

1 Выбор перечня инструментов для проведения тестирования, настройка виртуальной среды, в которой будут делаться тесты.

2 Сбор информации о тестируемом приложении.

3 Анализ уязвимостей веб-приложения, посредством следующих видов тестирований:

– тестирование приложения к различному виду инъекций (SQL, SOAP, LDAP, XPATH и т.д.);

– тестирование приложения к XSS-уязвимостям;

– проверка возможности реализации CSRF.

4 Анализ механизмов аутентификации и авторизации пользователей.

5 Проверка найденных уязвимостей путем попытки их эксплуатации.

6 Составления отчета о результатах тестирования.

На втором этапе разработанной методики для сбора информации о тестируемом приложении была разработана дополнительная методика, включающая следующие основные этапы:

1 Сбор информации о веб-приложении из открытых источников.

2 Анализ уязвимостей инфраструктуры веб-приложения приложения.

3 Сканирование портов веб-приложения.

4 Исследование видимого контента.

5 Поиск скрытого контента.

6 Определение платформы и веб-окружения.

7 Определение форм ввода.

8 Проверка перенаправлений и переадресаций.

9 Проверка содержания HTTP заголовков.

Для тестирования механизмов аутентификации и авторизации пользователей на четвертом этапе разработанной методики также была разработана дополнительная методика, которая включает следующие этапы:

1 Тестирование аутентификации.

2 Тестирование авторизации.

3 Проверка возможности подбора учетных данных.

4 Тестирование восстановления учетной записи.

5 Тестирование функций сохранения сессии.

6 Тестирование полномочий и прав доступа.

7 Тестирование возможности подмены идентификатора пользователя при отправке сообщений.

8 Проверка возможности подмены параметров сессии.

В третьей главе была произведена апробация разработанных методик для тестирования веб-приложения RailsGoat. Был проведен выбор инструментов для выполнения тестирования, а именно BurpSuite, nmap и dirb. Реализован сбор информации о веб-приложении RailsGoat. Проведен анализ уязвимостей веб-приложения, таких как тестирование приложения к SQL-инъекциям, к XSS-уязвимостям и к возможности реализации CSRF. Был сделан анализ механизмов аутентификации и авторизации пользователей. В таблице 1 приведены основные результаты тестирования.

Таблица 1 – Результаты проверок

Тип проверки	**Результат**
Поиск скрытого контента	Выявлено
Проверка перенаправлений и переадресаций	Выявлено
Тестирование приложения на возможность внедрения SQL-инъекции	Выявлено
Тестирование приложения на Reflected XSS-уязвимости	Выявлено
Тестирование приложения на Stored XSS-уязвимости	Выявлено
Тестирование приложения на DOM XSS уязвимости	Выявлено
Проверка возможности реализации CSRF	Выявлено

Продолжение таблицы 1

Тип проверки	Результат
Проверка средств аутентификации и авторизации	Выявлено
Тестирование подбора учетных данных	Выявлено
Тестирование восстановления учетной записи	Не выявлено – функции восстановления учетной записи не предусмотрено в приложении RailsGoat
Тестирование функций сохранения сессии	Выявлено
Проверка полномочий и прав доступа	Выявлено
Исследования сессии	Выявлено

Был составлен отчет о результатах тестирования который содержит не только конечные результаты, но и рекомендуемые действия по устранению уязвимостей и рисков. В отчете представлены следующие разделы:

– введение;
– реферат;
– перечень используемых для тестирования инструментов;
– результаты тестирования;
– рекомендации.

Были сформированы рекомендации по использованию написанной методики, для ее актуальности и востребованности, такие как:

– обновление методики раз в 3-6 месяцев;
– следование актуальным направлениям в области защиты информации;
– быстрое обновление методики при объявлении новой уязвимости;
– информирование сотрудников о новых уязвимостях в виде статей на внутреннем ресурсе компании;
– повышение квалификации для специалистов, проводящих тестирование;
– обсуждения внутри команды на предмет актуальности методики.

ЗАКЛЮЧЕНИЕ

На основе изучения существующих методик тестирования веб-приложений, был произведен сравнительный анализ NIST SP 800-115, OWASP Web Security Testing Guide, стандарт PTES, OSSTMM и BSI и выявлены их достоинства и недостатки. Было установлено, что изученные методологии тестирования устарели и ориентированы на подробные тестирования определенной области веб-приложений. Следовательно, была поставлена цель разработки новой методики тестирования безопасности инфраструктуры веб-приложений, учитывая достоинства и недостатки существующих методологий. Также в диссертационной работе подробно изучены уязвимости веб-приложений из списка OWASP Top 10, такие как внедрение, недостатки аутентификации, разглашение конфиденциальных данных, внешние сущности XML, недостатки контроля доступа и т.д.

На основе изучения статистических данных по наиболее распространенным угрозам веб-приложений было установлено, что 84 % веб-приложений подвержены угрозам из-за некорректной настройки параметров безопасности, 53 % подвержены XSS-атакам, из-за недостатка аутентификации – 37 % веб приложений, а возможность реализации инъекциям (SQL, SOAP, LDAP, XPATH и т.д.) подвержены 29 % веб-приложений.

Разработанная методика тестирования безопасности инфраструктуры веб-приложений включает такие этапы как сбор информации о тестируемом приложении и анализ механизмов аутентификации и авторизации пользователей, которые являются довольно объемными, поэтому для них были разработаны отдельные методики.

В рамках диссертационной работы была произведена апробация разработанных методик на веб-приложении RailsGoat. На первом этапе методики осуществлен выбор перечня инструментов для проведения тестирования, а именно Mozila Firefox, BurpSuite Community, Nmap, Zenmap, Dirb. При апробации методики сбора информации о веб-приложение было выявлено, что веб-приложение RailsGoat реализовано на фреймворке Ruby on Rails с версией 2.6.5 и базе данных MySQL на сервере с ОС Linux 2.6.32.

В результате реализации 3 этапа методики тестирования безопасности инфраструктуры веб-приложений были выявлены уязвимости веб-приложения к следующим атакам: SQL-инъекции, Reflected, Stored и DOM XSS, CSRF.

При апробации методики тестирования механизмов аутентификации и авторизации пользователей были обнаружены уязвимости в процессе аутентификации и авторизации пользователя, возможности подбора учетных

данных, функции сохранения сессии, полномочиях и правах доступа, возможности подмены идентификатора пользователя и параметров сессии при отправке сообщений.

На основе проведенной апробации методики тестирования безопасности инфраструктуры веб-приложений была разработана форма отчета, в которой четко указаны результаты тестирования на каждом этапе.

Разработанная методика тестирования безопасности инфраструктуры веб-приложений рекомендуется для проведения тестирования безопасности инфраструктуры клиент-серверных веб-приложений, использующих различные технологии и построенные на основе различных языков программирования.

Данная методика несет методические рекомендации по тестированию безопасности веб-приложений.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1. Пузеева, А.Ю. Методика тестирования безопасности инфраструктуры веб-приложений. / Пузеева А.Ю., Белоусова Е.С. // XVII Международная научно-практическая конференция «Управление информационными ресурсами» Академия управления при Президенте Республики Беларусь, РИВШ. Минск, 12 марта 2021 г. – Минск, 2021. – С. 232–233.

2. Пузеева, А.Ю. Методика анализа уязвимостей при тестировании безопасности инфраструктуры веб-приложений / Пузеева А.Ю. // Технические средства защиты информации : материалы XIX Белорусско-Российской научно-технической конференции, 8 июня 2021 г., Минск. – Минск, 2021. – С. 78.