МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ярославский государственный университет имени П. Г. Демидова»

Кафедра компьютерной безопасности и математических методов обработки информации

Сдано на кафедру
«_____» _____ 2024 г.
Заведующий кафедрой,
к. ф.-м. н., доцент

_____ Мурин Д.М.

Выпускная квалификационная работа

Анализ уязвимостей веб-приложений

по направлению
10.03.01 Информационная безопасность

Научный руководитель
к. ф.-м. н., доцент

_____ Власова О. В.
«_____» _____ 2024 г.

Студент группы ИБ-41БО

_____ С. И. Штанько
«_____» _____ 2024 г.

Ярославль, 2024

1. Реферат

Объем 8 с., 2 гл., 0 рис., 0 табл., 6 источников, 0 прил.

Ключевые слова: **Уязвимости веб-приложений, анализ безопасности сайтов**

Содержание

Введение

Современный мир характеризуется стремительным развитием информационных технологий, все большей интеграцией цифровых решений в различные сферы жизни и деятельности. Веб-приложения стали неотъемлемой частью повседневности, обеспечивая доступ к услугам, информации и коммуникации. С ростом их популярности и сложности возрастает и актуальность обеспечения их безопасности. Уязвимости веб-приложений представляют собой лазейки, которые могут быть использованы злоумышленниками для нанесения ущерба пользователям, организациям и системам.

Актуальность темы дипломной работы обусловлена возрастающей угрозой кибербезопасности, связанной с уязвимостями веб-приложений. Кибератаки становятся всё более изощрёнными и масштабными, а их последствия могут быть катастрофическими, приводя к утечке конфиденциальной информации, финансовым потерям и репутационному ущербу.

Цель дипломной работы – комплексное изучение и анализ наиболее распространенных уязвимостей веб-приложений, а также методов их обнаружения, предотвращения и устранения.

Задачи дипломной работы:

- Рассмотреть основные виды уязвимостей веб-приложений, такие как инъекции SQL, межсайтовый скриптинг (XSS), подделка межсайтовых запросов (CSRF) и другие.
- Изучить причины возникновения уязвимостей, их потенциальные последствия и угрозы для безопасности веб-приложений.
- Проанализировать методы и инструменты для обнаружения и предотвращения уязвимостей веб-приложений.
- Изучить практические примеры и рекомендации по обеспечению безопасности веб-приложений.
- Провести анализ конкретных случаев уязвимостей и рассмотреть методы их устранения.

Объектом исследования дипломной работы являются веб-приложения, а предметом исследования – уязвимости веб-приложений и методы обеспечения их безопасности.

Методологической основой дипломной работы служат методы анализа, синтеза, сравнения и обобщения информации из различных источников, включая научные статьи, техническую документацию, отчеты по безопасности и практические руководства.

Практическая значимость дипломной работы заключается в возможности использования полученных знаний и рекомендаций для повышения безопасности веб-приложений, разработки защищенных программных продуктов и снижения рисков кибератак.

Результаты данной работы могут быть полезны разработчикам веб-приложений, специалистам по информационной безопасности, студентам и всем, кто интересуется вопросами кибербезопасности.

2. Инъекции SQL

2.1. Определение и примеры инъекций SQL.

2.1.1. Сущность инъекции SQL

Инъекция SQL (SQL Injection) – это тип атаки, направленной на веб-приложения, использующие базы данных. Принцип ее действия заключается во внедрении вредоносного SQL-кода в поля ввода данных приложения. Цель такой атаки – исказить логику выполнения SQL-запросов, отправляемых к базе данных. В результате злоумышленник может получить несанкционированный доступ к чувствительным данным, манипулировать ими, нарушать работу приложения и даже получить полный контроль над сервером базы данных.

2.1.2. Механизм атаки

2.1.3. Классификация инъекций SQL

2.1.4. Механизм атаки

Заключение

Список литературы

[1] Гупта, Арун. Java EE 7. Основы. [Текст] / Арун Гупта. — Новосибирск : Издательство Вильямс, 2014.

[2] Герберт, Шилдт. Java. Руководство для начинающих. Современные методы создания, компиляции и выполнения программ на Java [Текст] / Шилдт Герберт. — Новосибирск : Издательство Диалектика, 2018.

[3] W3C Recommendation: Extensible Markup Language (XML) [Electronic resource]. — Режим доступа: `https://www.w3.org/TR/REC-xml` (online; accessed: 28.11.2008).

[4] Java API for XML Processing (JAXP) [Electronic resource]. — Режим доступа: `https://docs.oracle.com/javase/8/docs/technotes/guides/xml/index.html` (online; accessed: 01.12.2009).

[5] About XStream [Electronic resource]. — Режим доступа: `https://x-stream.github.io/` (online; accessed: 20.04.2020).

[6] Simple XML [Electronic resource]. — Режим доступа: `https://simple.sourceforge.net/` (online; accessed: 20.04.2020).