Тип работы: Курсовая работа

Предмет: Информационные системы и процессы

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ
С развитием интернета и информационных технологий, веб-приложения стали неотъемлемой частью современного общества. Они используются для различных целей, таких как интернет-банкинг, онлайн-торговля, социальные сети, управление личными данными и деловыми процессами. Однако, с распространением таких систем возросли и заботы о безопасности, так как множество веб-приложений стали целью злоумышленников, желающих получить несанкционированный доступ к информации или нарушить ее целостность.
Одной из главных уязвимостей веб-приложений являются SQL-инъекции, позволяющие атакующему внедрить вредоносный SQL-код в запросы к базе данных, получить доступ к конфиденциальной информации, а также модифицировать или удалить данные. Это может привести к серьезным последствиям для компаний и пользователей.
Цель данной курсовой работы – исследовать проблему SQL-инъекций как одной из основных угроз безопасности веб-приложений, проникнуть в сущность этой уязвимости, изучить механизмы успешных атак и возможные способы защиты от них.
В рамках работы будут рассмотрены следующие основные аспекты. В курсовой работе в первом разделе будут рассмотрены теоретические основы SQL- инъекций: проведен обзор теоретических аспектов SQL-инъекций, рассмотрены основные уязвимости веб приложений, связанные SQL- инъекциями, перечислены методы предотвращения и защиты от SQL- инъекций.
Во втором разделе курсовой работы рассмотрены SQL- инъекции с помощью Burp Suite на DVWA: запуск и настройка Burp Suite на Kali Linux, уровни безопасности DVWA, SQL инъекция с помощью Burp Suite на DVWA, исправление ошибки Burp Suite и DVWA.

1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ SQL-ИНЪЕКЦИЙ
1.1 Обзор теоретических аспектов SQL-инъекций
QL-инъекция (SQL Injection) – это один из самых распространенных и опасных видов атак на веб-приложения, который заключается во внедрении вредоносного SQL-кода через пользовательский ввод, контроль форм или URL-параметры. Обычно SQL-инъекции используются злоумышленниками для доступа, кражи или изменения данных в базе данных, нарушения конфиденциальности и доступа к другим ресурсам и системам.
Теоретические аспекты SQL-инъекций включают следующие основные концепции:
1. Внедрение SQL-кода: Злоумышленники используют различные методы и инструменты для формирования вредоносного SQL-кода, который может быть внедрен в пользовательский ввод или вовлечен при обработке данных, поступающих из ненадежных источников.

2. Недостатки безопасности в веб-приложениях: SQL-инъекции возможны из-за недостатков безопасности в разработке веб-приложений. Наиболее распространенные ошибки включают использование строки конкатенации для формирования SQL-запросов, отсутствие должного экранирования и проверки пользовательского ввода, а также неправильную обработку ошибок.
3. Типы SQL-инъекций: Существует несколько типов SQL-инъекций, включая
a) Ошибочные (Error-based) SQL-инъекции, при которых злоумышленник использует сообщения об ошибках, возникающих при обработке некорректных SQL-запросов, чтобы определить структуру и содержимое базы данных.
b) Тайминг (Time-based) SQL-инъекции, при которых злоумышленник вводит специальные условия в SQL-запросы, которые требуют определенного времени для выполнения, что позволяет определить наличие уязвимостей или извлечь данные из базы данных.
c) Булевы (Boolean-based) SQL-инъекции, при которых злоумышленник выполняет SQL-запросы с условиями, возвращающими истину (true) или ложь (false), чтобы определить информацию о базе данных или получить доступ к данным.
d) Batched (также известные как множественные или стековые) SQL-инъекции, при которых злоумышленник отправляет несколько SQL-запросов одновременно для выполнения различных действий с базой данных.
4. Методы предотвращения SQL-инъекций: Существуют различные методы и практики безопасности для предотвращения SQL-инъекций в веб-приложениях, включая параметризированные запросы, экранирование и проверку пользовательского ввода, использование непривилегированных пользователей базы данных, обработку ошибок и лимитирование вывода сообщений об ошибках.
5. Обнаружение и тестирование SQL-инъекций: Существует множество инструментов, как автоматических, так и ручных, которые используются для обнаружения уязвимостей, связанных с SQL-инъекциями, и тестирования веб-приложений на наличие таких уязвимостей. Одним из таких инструментов является OWASP Zed Attack Proxy (ZAP), который является свободно доступным инструментом для тестирования на проникновение и обнаружения уязвимостей.
1.2. Основные уязвимости веб-приложений, связанные с SQL-инъекциями

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ
1. Белоусов В. К. SQL-инъекции. Превосходный подход к кибербезопасности. // Хакер. – 2018. – № 9. – С. 14-17.
2. Карлов А. О. Основы безопасности веб-приложений: защита от SQL-инъекций. // Материалы III Международной научно-практической конференции «Современные информационные технологии и IT-образование». – Москва, 2017. – С. 60-65.
3. Руцкая Е. В. Противодействие SQL-инъекциям в веб-приложениях. // Материалы VI Международной научно-практической конференции «Современные информационные технологии и IT-образование». – Москва, 2020. – С. 60-65.
4. Соболев А. В. SQL-инъекции в практике тестирования веб-приложений. // Материалы Всероссийской научно-практической конференции «Интернет-технологии и образование». – Томск, 2016. – С. 92-96.
5. Хрусталев И. А. Проектирование безопасных веб-приложений с учетом уязвимостей SQL-инъекций. // Материалы V Международной научно-практической конференции «Информационные технологии и математическое моделирование». – Красноярск, 2019. – С. 52-57.
6. Шестакова Т. А. SQL-инъекции как одна из основных уязвимостей веб-приложений. // Материалы IV научно-практической конференции «Современные информационные технологии и образование». – Тула, 2018. – С. 77-81.
7. Кривохатский А.В. SQL-инъекции: угроза веб-приложений // Безопасность информационных технологий. – 2015. – № 3. – С. 40-43.
8. Мартыненко Н. Анализ защиты от SQL-инъекций в веб-приложениях // Научный журнал КубГАУ. – 2015. – № 107(03). – С. 1319-1335.
9. Гребенчук А.А. Особенности SQL-инъекций в современных веб-приложениях // Информационные технологии и техника. – 2018. – № 2 (2). – С. 107-112.
10. Городеник М.С. Анализ уязвимостей веб-приложений, связанных с SQL-инъекциями // Современные проблемы науки и образования. – 2017. – № 2. – С. 92-98.
11. Кель А.А. SQL-инъекции в приложениях на платформе .NET // Сборник научных трудов XXIII Международной молодежной научной конференции «Ломоносов-2016». – 2016. – С. 183-185.
12. Российский центр компетенций по кибербезопасности. SQL-инъекции. URL:

https://www.cyber.mil.ru/docs/m/6/0/42_Infocenter_empy_2016_138_R_T_Z1333.pdf (дата обращения: 21.05.2021).
13. Суйков А.Н. Система предотвращения и обнаружения SQL-инъекций в веб-приложениях // Проблемы защиты информации. – 2017. – № 3. – С. 31-38.
14. Филимонов В.В. Методы защиты от SQL-инъекций в веб-приложениях // Современные информационные технологии и IT-образование. – 2016. – № 1. – С. 79-82.
15. SQL-инъекции: определение, причины и способы предотвращения. URL: https://kaspersky.ru/blog/sql-injekcii-opredelenie-prichiny-i-sposoby-predotvrashcheniya (дата обращения: 21.05.2021).
16. Про SQL-инъекции в веб-приложениях. URL: https://habr.com/ru/post/131973/ (дата обращения: 21.05.2021).