Ministerul Educaţiei şi Cercetării al Republicii Moldova
Universitatea Tehnică a Moldovei
Facultatea Electronică și Telecomunicații
Departamentul Telecomunicații și Sisteme Electronice

Admisă la susţinere

Şefă departament:

Tîrșu Valentina, conf. univ., dr.

_____
„____”_____ 2024

Evaluarea metodelor de securitate a bazelor de date și analiza implementării SQL Injection

Оценка методов обеспечения безопасности баз данных и анализ реализации SQL-инъекций

Teză de master

Student: **Parhomenco Vladislav**
MMRT-221M

Conducător: **Tîrșu Valentina**
conf. univ., dr.

Chişinău, 2024

АННОТАЦИЯ

Автор: Parhomenco Vladislav

Тема: Обеспечение безопасности баз данных от SQL-инъекций: Теоретические основы, методы анализа и практическое применение.

Структура работы: Введение, 3 раздела (Фундамент исследования и методы анализа, Проблемы безопасности в базах данных и борьба с SQL-инъекциями, Обеспечение безопасности баз данных в реальном времени от SQL-инъекций на уровне кода и ОС), Заключение, Библиография, Приложения.

Ключевые слова: SQL-инъекции, безопасность баз данных, системы аудита, методы анализа, противодействие атакам, техники безопасности, валидация данных, кодировка SQL-запросов, операционная система.

Цель работы: Исследовать методы и стратегии обеспечения безопасности баз данных от SQL-инъекций, включая анализ современных угроз, разработку и реализацию мер предотвращения атак, и обеспечение защиты в реальном времени.

Задачи работы: Анализ угроз безопасности баз данных, исследование и оценка эффективности существующих мер защиты, разработка новых подходов к обеспечению безопасности, включая управление доступом, шифрование данных, методы аутентификации и аудита, а также обучение персонала и разработка политики безопасности.

Применяемые методы: Теоретический анализ, статический анализ кода, использование систем обнаружения вторжений (IDS) и предотвращения вторжений (IPS), а также методы параметризации запросов.

Полученные результаты: Разработаны комплексные стратегии и методы защиты баз данных от SQL-инъекций, включая технические и организационные подходы, обеспечивающие повышение безопасности веб-приложений и операционных систем. Представлены практические примеры успешного применения этих стратегий для защиты от различных типов SQL-инъекций.

ADNOTARE

Autor: Parhomenco Vladislav

Titlu: Securizarea sistemelor de baze de date împotriva injecțiilor SQL: Fundamente teoretice, metode de analiză și implementare practică.

Structură: Introducere, 3 secțiuni (Fundamentul cercetării și metodele de analiză, Probleme de securitate în bazele de date și combaterea injecțiilor SQL, Securitatea bazelor de date în timp real împotriva injecțiilor SQL la nivel de cod și OS), Concluzie, Bibliografie, Anexe.

Cuvinte cheie: Injecții SQL, securitatea bazelor de date, sisteme de audit, metode de analiză, contramăsuri împotriva atacurilor, tehnici de securitate, validarea datelor, codificarea interogărilor SQL, sistem de operare.

Obiectiv: Explorarea metodelor și strategiilor de securizare a bazelor de date împotriva injecțiilor SQL, inclusiv analiza amenințărilor moderne, dezvoltarea și implementarea contramăsurilor și asigurarea protecției în timp real.

Sarcini: Analiza amenințărilor de securitate ale bazelor de date, investigarea și evaluarea eficacității măsurilor de protecție existente, dezvoltarea de noi abordări ale securității, inclusiv managementul accesului, criptarea datelor, metodele de autentificare și audit, precum și formarea personalului și dezvoltarea politicilor de securitate.

Metode utilizate: Analiză teoretică, studii de caz, analiză statică a codului, utilizarea Sistemelor de Detectare a Intruziunilor (IDS) și Sistemelor de Prevenire a Intruziunilor (IPS), și metode de parametrizare a interogărilor.

Rezultate: Au fost dezvoltate strategii și metode cuprinzătoare de protecție a bazelor de date împotriva injecțiilor SQL, cuprinzând abordări tehnice și organizaționale care îmbunătățesc securitatea aplicațiilor web și a sistemelor de operare. Sunt prezentate exemple practice de implementare reușită a acestor strategii pentru protecția împotriva diferitelor tipuri de injecții SQL.

ANNOTATION

Author: Parhomenco Vladislav

Title: Securing Database Systems Against SQL Injections: Theoretical Foundations, Analytical Methods, and Practical Implementation.

Structure: Introduction, 3 sections (Foundation of Research and Methods of Analysis, Security Issues in Databases and Combating SQL Injections, Real-Time Database Security Against SQL Injections at the Code and OS Level), Conclusion, Bibliography, Appendices.

Keywords: SQL injections, database security, audit systems, analytical methods, countermeasures against attacks, security techniques, data validation, SQL query encoding, operating system.

Objective: To explore methods and strategies for securing databases against SQL injections, including analyzing modern threats, developing and implementing countermeasures, and ensuring real-time protection.

Tasks: Analyze database security threats, investigate and evaluate the effectiveness of existing protection measures, develop new approaches to security including access management, data encryption, authentication and audit methods, as well as staff training and policy development.

Methods Used: Theoretical analysis, case studies, static code analysis, use of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), and query parameterization methods.

Results: Comprehensive strategies and methods for protecting databases from SQL injections have been developed, incorporating both technical and organizational approaches that enhance the security of web applications and operating systems. Practical examples of successful implementation of these strategies to protect against various types of SQL injections are presented.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В современном мире, где информация стала центральным активом для многих организаций, обеспечение безопасности данных является ключевым вызовом. Основной угрозой в этой сфере являются SQL-инъекции, которые позволяют злоумышленникам получать несанкционированный доступ к конфиденциальной информации, подрывая целостность данных. Эта проблема возникает из-за недостаточной обработки входных данных в приложениях, что позволяет манипулировать SQL-запросами. Угрозы SQL-инъекций присутствуют не только в веб-приложениях, но и в многочисленных системах, связанных с базами данных.

Мотивация и актуальность исследования по теме SQL-инъекций обусловлены постоянным развитием и эволюцией в области программных языков и технологий. Несмотря на то, что тема SQL-инъекций уже хорошо изучена в научной литературе и существует множество методов защиты, непрерывное появление новых языков программирования, фреймворков и технологий баз данных поддерживает актуальность этой проблемы. Новые технологии могут вносить уникальные уязвимости или особенности, которые требуют специфических методов защиты и подходов к безопасности. Кроме того, постоянное обновление и развитие существующих систем также может приводить к появлению новых уязвимостей. Все это делает исследование в области защиты от SQL-инъекций не только актуальным, но и необходимым для поддержания безопасности информационных систем в меняющемся технологическом ландшафте.

Сложность также усугубляется недостаточным пониманием разработчиками важности вопросов безопасности и распространением устаревших или неправильных методик обучения. Настоящее исследование направлено на комплексный анализ угрозы SQL-инъекций и оценку эффективности существующих мер защиты. Основной целью является разработка новых подходов к обеспечению безопасности баз данных.

Задачи исследования включают анализ современных технологий защиты от SQL-инъекций, изучение реальных случаев успешного и неудачного применения защитных мер, а также разработку рекомендаций по улучшению безопасности в разнообразных средах разработки. Результаты работы предполагается использовать для улучшения понимания угрозы SQL-инъекций и формирования эффективных стратегий ее минимизации.

Работа призвана служить ценным ресурсом в области информационной безопасности, разработчиков и менеджеров проектов, занимающихся проектированием и поддержкой информационных систем.

БИБЛИОГРАФИЯ

1. SQL, Wikipedia. [Online]. Доступно: https://en.wikipedia.org/wiki/SQL
2. SQL: 2023 is finished: Here is what's new [Online]. Доступно: https://peter.eisentraut.org/blog/2023/04/04/sql-2023-is-finished-here-is-whats-new
3. Shar, Lwin Khin, Hee Beng Kuan Tan. "Defeating SQL injection." *Computer* 46, no. 3 (2012): 69-77.
4. Stonebraker, Michael. "SQL databases v. NoSQL databases." Communications of the ACM 53, no. 4 (2010): 10-11.
5. Ludmila Peca, Dinu Țurcanu. Network security: Practical examples solved to be introduced in network security. Chișinău, Publisher „Tehnica-UTM”, 2023, pp. 7-232.
6. Жалолов, Озод Исомиддинович, Хуршид Усманович Хаятов. "Понятие SQL и реляционной базы данных." Universum: технические науки 6-1 (75) (2020): 26-29.
7. Дьяков, И. А. "Базы данных. Язык SQL." (2012): 81-81.
8. Болябкин, М. В., А. И. Панов, and Н. А. Башмуров. "Разработка и внедрение общего анализатора SQL." *Международный журнал гуманитарных и естественных наук* 1-1 (2022): 55-91 [Online]. Доступно: https://cyberleninka.ru/article/n/razrabotka-i-vnedrenie-obschego-analizatora-sql/viewer
9. Стандарты и руководства по безопасности данных, включая публикацию Gentile, Deutsch, Donald R. "The SQL standard: how it happened." IEEE Annals of the History of Computing 35.2 (2013): 72-75.
10. Беликов Г. В., Крылов И. Д., Селищев В. А. "SQL-инъекция как способ обхода авторизации". Известия Тульского государственного университета. Технические науки. (2021). [Online]. Доступно: https://cyberleninka.ru/article/n/sql-inektsiya-kak-sposob-obhoda-avtorizatsii
11. Александр А. “SQL injection для начинающих. Часть 1” [Online] Доступно: https://habr.com/ru/articles/148151/