Усванова Д.Р. Исследование методов защиты ВЕБ-приложений от атак типа SQL-ИНЪЕКЦИЯ // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 12(50) с. 5–7

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.736

ИССЛЕДОВАНИЕ МЕТОДОВ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ ОТ АТАК ТИПА SQL-ИНЪЕКЦИЯ

Усванова Д.Р.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: dusvanova@gmail.com

В статье рассмотрены методы защиты веб-приложений от атак типа SQL-инъекция, которые остаются одной из наиболее серьёзных угроз информационной безопасности. Приведён анализ основных типов SQL-инъекций, их механизма действия и возможных последствий, включая угрозу конфиденциальности, целостности и доступности данных. В работе выделены три ключевых подхода к защите: использование подготовленных выражений (Prepared Statements), валидация входных данных и применение объектно-реляционного отображения (ORM).

Ключевые слова: SQL-инъекции, защита веб-приложений, Prepared Statements, валидация данных, ORM, информационная безопасность, методы защиты, анализ атак.

INVESTIGATION OF METHODS FOR PROTECTING WEB APPLICATIONS FROM SQL INJECTION ATTACKS

Usmanova D.R.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: dusvanova@gmail.com

The article examines methods for protecting web applications against SQL injection attacks, which remain one of the most significant threats to information security. An analysis of the main types of SQL injections, their mechanisms of operation, and potential consequences, including risks to data confidentiality, integrity, and availability, is presented. The study highlights three key approaches to protection: the use of prepared statements (Prepared Statements), input data validation, and object-relational mapping (ORM).

Keywords: SQL injection, web application protection, Prepared Statements, data validation, ORM, information security, protection methods, attack analysis.

Атаки типа SQL-инъекция представляют собой одну из наиболее серьёзных угроз для безопасности современных веб-приложений. Уязвимости SQL-инъекций неизменно занимают верхние строчки в ежегодных отчётах о киберугрозах, таких как OWASP Top 10. Например, в 2020 году атака на авиакомпанию EasyJet привела к утечке данных более 9 миллионов клиентов, включая финансовую информацию. SQL-инъекция является одним из наиболее распространенных типов атак на веб-приложения, и ее можно предотвратить путем использования параметризованных запросов и валидации пользовательского ввода [1]. Особую опасность SQL-инъекций представляет их универсальность. Они могут быть использованы не только для получения доступа к конфиденциальным данным, но и для

нарушения их целостности или доступности, что влечёт значительные финансовые и репутационные потери. По данным исследований, на долю SQL-инъекций в 2022 году пришлось около 40% всех зарегистрированных уязвимостей веб-приложений [3]. Цель данной работы — исследовать эффективные методы предотвращения атак типа SQL-инъекция.

Понимание механизмов SQL-инъекций играет ключевую роль. Одним из эффективных методов защиты от SQL-инъекций является использование механизмов обнаружения и предотвращения инъекций [4]. Эти атаки основаны на внедрении вредоносного кода в SQL-запросы, что позволяет злоумышленникам изменять их логику. Наиболее распространённые типы SQL-инъекций включают:

- **Ошибка-сообщения:** использование сообщений об ошибках базы данных для извлечения её структуры.
- **Объединение запросов (UNION):** выполнение дополнительных запросов через оператор UNION.
- **Булевые атаки:** анализ ответов сервера на условия, возвращающие истину или ложь.
- **Замедление выполнения:** использование временных задержек в запросах для определения успеха атаки.

К основным методам защиты относятся подготовленные выражения (Prepared Statements), валидация входных данных и объектно-реляционное отображение (ORM). Подготовленные выражения исключают возможность внедрения кода в запросы, так как параметры передаются отдельно от структуры SQL-запроса, гарантируя, что все входные данные обрабатываются только как параметры. Валидация входных данных добавляет дополнительный уровень защиты, ограничивая или фильтруя ввод пользователя в соответствии с заданными правилами. ORM-инструменты упрощают процесс разработки, автоматически генерируя SQL-запросы, что снижает вероятность ошибок, связанных с ручным кодированием.

При использовании Prepared Statements обеспечивается высокая надежность благодаря защите от SQL-инъекций и других угроз безопасности, а также достигается универсальность, поскольку один и тот же подготовленный запрос может применяться для различных типов данных без необходимости переписывания кода. Однако внедрение Prepared Statements в существующий код может потребовать дополнительных усилий. Валидация данных характеризуется простотой реализации и низкими затратами, но она не способна защитить от сложных атак, таких как XSS и CSRF. Наконец, использование ORM упрощает разработку, автоматизирует защиту от SQL-инъекций, однако может привести к потенциальной потере производительности из-за добавления дополнительных уровней абстракции.

Сравнительный анализ этих подходов показал, что подготовленные выражения являются наиболее надёжным методом предотвращения атак. Валидация данных эффективна для защиты от простых атак, но не всегда достаточна в более сложных случаях. ORM-решения облегчают разработку, но могут увеличивать нагрузку на систему и требуют точной настройки, особенно в условиях высокой производительности. Для максимальной защиты рекомендуется использовать комплексный подход, комбинируя несколько методов. Регулярное обновление и патчинг веб-приложения и базы данных также является важной мерой по предотвращению SQL-инъекций [2].

Правильная конфигурация базы данных и использование безопасных протоколов аутентификации также являются важными мерами по предотвращению SQL-инъекций [5].

Список литературы

1. Котенко, И.В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров / Котенко И.В., Левшун Д.С., Чечулин А.А., Ушаков И.А., Красов А.В. // Вопросы кибербезопасности. 2018. № 3 (27). С. 29-38.
2. Красов, А.В. Обеспечение безопасности передачи multicast-трафика в ip-сетях / Красов А.В., Сахаров Д.В., Ушаков И.А., Лосин Е.П.// Защита информации. Инсайд. 2017. № 3 (75). С. 34-42.
3. Сахаров Д.В., Левин М.В., Фостач Е.С., Виткова Л.А. "Исследование механизмов обеспечения защищённого доступа к данным, размещённым в облачной инфраструктуре" // Наукоёмкие технологии в космических исследованиях Земли, 2017. Т. 9. № 2. С. 40–46.
4. Сахаров Д.В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6 / Сахаров Д.В., Красов А.В., Ушаков И.А., Бирих Э.В. // Защита информации. Инсайд. 2020. № 1 (91). С. 51-57.
5. Штеренберг С.И. Синхронизированное использование систем защиты информации для контроля учёта рабочего времени / Штеренберг С.И., Щеголева Д.И., Виноградова О.М. // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2019. № 4. С. 3-8.

References

1. Kotenko, I.V. An integrated approach to ensuring the security of cyber-physical systems based on microcontrollers / Kotenko I.V., Levshun D.S., Chechulin A.A., Ushakov I.A., Krasov A.V. // Issues of cybersecurity. 2018. No. 3 (27). pp. 29-38.
2. Krasov, A.V. Ensuring the security of multicast traffic transmission in IP networks / Krasov A.V., Sakharov D.V., Ushakov I.A., Losin E.P.// Information protection. Inside. 2017. No. 3 (75). pp. 34-42.
3. Sakharov D.V., Levin M.V., Fostach E.S., Tsvetkova L.A. "Research of mechanisms for ensuring secure access to data hosted in cloud infrastructure" // High-tech technologies in Earth space research, 2017. Vol. 9. No. 2. pp. 40-46.
4. Sakharov D.V. Modeling of a secure scalable enterprise network with dynamic routing based on IPv6 / Sakharov D.V., Krasov A.V., Ushakov I.A., Birikh E.V. // Information Protection. Insider 2020. No. 1 (91). pp. 51-57.
5. Shterenberg S.I. Synchronized use of information security systems for monitoring working hours / Shterenberg S.I., Shchegoleva D.I., Vinogradova O.M. // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. 2019. No. 4. pp. 3-8.