**ФИО**

Морозов А. П., Ченцов Д. А. (100503D-6114)

**Topic**

SQL; Scripting; Web Application

**Описание предметной области**

Данный топик рассматривает исследования в области разработки Web приложений (Web Application) с использованием языка запросов SQL. Web приложения - это компьютерная программа, которая запускается прямо в веб-браузере. Scripting — это процесс написания скриптов, которые выполняются компьютером для автоматизации определенных задач. В веб-разработке скрипты часто используются для создания динамического поведения на веб-страницах. Язык запросов SQL — это язык, который применяют, чтобы работать с базами данных, структурированных особым образом. Базы данных – это огромное количество информации, разбитое на несколько таблиц для удобства использования.

**Недостаток (Gap)**

Несмотря на широкое распространение методов защиты от SQL Injection, таких как использование параметризованных запросов и фильтрация ввода данных, существует проблема обнаружения и мониторинга новых вариантов атак. Злоумышленники постоянно находят новые методы обхода существующих механизмов защиты, что оставляет веб-приложения уязвимыми к SQL Injection.

**Идея**

Одним из возможных подходов к решению этого недостатка может быть разработка и внедрение алгоритмов машинного обучения для обнаружения аномалий в SQL-запросах. Это позволит выявлять необычные или подозрительные образцы запросов, которые могут указывать на потенциальные атаки SQL Injection.

**Краткий текст обзор**

Область безопасности веб-приложений и поиска уязвимостей привлекает значительное внимание, особенно в контексте атак SQL-инъекций (SQLi) и методов защиты от них[[1]](https://www.zotero.org/google-docs/?ZI37U3),[[2]](https://www.zotero.org/google-docs/?qKnnmQ). В данном обзоре литературы представлены различные подходы и инструменты для анализа безопасности веб-приложений, включая статический анализ кода[[3]](https://www.zotero.org/google-docs/?x38roJ), гибридные методы статического и динамического анализа[[4]](https://www.zotero.org/google-docs/?1z3N20), а также использование контекстно-чувствительного анализа и метрик безопасности[[1]](https://www.zotero.org/google-docs/?aFba0t). Новые исследования рассматривают проблемы комбинирования инструментов статического анализа для удовлетворения потребностей разработчиков[[5]](https://www.zotero.org/google-docs/?bgYija), в том числе анализ производительности и эффективности этих инструментов на реальных веб-приложениях, таких как WordPress, Joomla и Drupal. Другие работы предлагают инновационные методы защиты от атак SQLi, такие как гибридный статический и динамический анализ для ограничения доступа PHP-функций к базе данных[[6]](https://www.zotero.org/google-docs/?VKf7sM) или использование алгоритмов верификации веб-приложений с применением реляционных баз данных и SQL-запросов[[7]](https://www.zotero.org/google-docs/?E3684X),[[8]](https://www.zotero.org/google-docs/?hg4iTy). Предложенные подходы не только успешно предотвращают атаки SQLi, но и демонстрируют незначительное влияние на производительность веб-приложений[[9]](https://www.zotero.org/google-docs/?inLZW2). Также в литературе рассматриваются проблемы безопасности других видов атак, включая межсайтовый скриптинг (XSS), с предложением интегрированных моделей для их предотвращения и обнаружения[[6]](https://www.zotero.org/google-docs/?no4t5H),[[9]](https://www.zotero.org/google-docs/?twbKUD),[[10]](https://www.zotero.org/google-docs/?AQS9Wc). Несмотря на разнообразие инструментов защиты, злоумышленники постоянно находят новые методы её обхода, что представляет существенную угрозу безопасности веб-приложений. Мы предлагаем в нашей статье разработку и использование механизмов машинного обучения для обнаружения аномалий в работе приложения и своевременного их устранения, что может являться решением этой проблемы.

References

[1] R. Jahanshahi, A. Doupé, и M. Egele, «You shall not pass: Mitigating SQL Injection Attacks on Legacy Web Applications», в Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, Taipei Taiwan: ACM, окт. 2020, сс. 445–457. doi: 10.1145/3320269.3384760.

[2] A. Algaith, P. Nunes, F. Jose, I. Gashi, и M. Vieira, «Finding SQL Injection and Cross Site Scripting Vulnerabilities with Diverse Static Analysis Tools», в 2018 14th European Dependable Computing Conference (EDCC), Iasi: IEEE, сен. 2018, сс. 57–64. doi: 10.1109/EDCC.2018.00020.

[3] S. Itzhaky и др., «On the automated verification of web applications with embedded SQL». arXiv, 6 октябрь 2016 г. Просмотрено: 22 февраль 2024 г. [Онлайн]. Доступно на: http://arxiv.org/abs/1610.02101

[4] L. K. Shar, H. Beng Kuan Tan, и L. C. Briand, «Mining SQL injection and cross site scripting vulnerabilities using hybrid program analysis», в 2013 35th International Conference on Software Engineering (ICSE), San Francisco, CA, USA: IEEE, май 2013, сс. 642–651. doi: 10.1109/ICSE.2013.6606610.

[5] P. Sharma, R. Johari, и S. S. Sarma, «Integrated approach to prevent SQL injection attack and reflected cross site scripting attack», Int J Syst Assur Eng Manag, т. 3, вып. 4, сс. 343–351, дек. 2012, doi: 10.1007/s13198-012-0125-6.

[6] R. Johari и P. Sharma, «A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation and Security Engine for SQL Injection», в 2012 International Conference on Communication Systems and Network Technologies, Rajkot, Gujarat, India: IEEE, май 2012, сс. 453–458. doi: 10.1109/CSNT.2012.104.

[7] S. F. Hidhaya, «Intrusion Protection against SQL Injection Attacks Using a Reverse Proxy», в Computer Science & Information Technology (CS & IT), Academy & Industry Research Collaboration Center (AIRCC), июл. 2012, сс. 129–144. doi: 10.5121/csit.2012.2314.

[8] B. Smith и L. Williams, «Using SQL Hotspots in a Prioritization Heuristic for Detecting All Types of Web Application Vulnerabilities», в 2011 Fourth IEEE International Conference on Software Testing, Verification and Validation, Berlin, Germany: IEEE, мар. 2011, сс. 220–229. doi: 10.1109/ICST.2011.15.

[9] M. H. Alalfi, J. R. Cordy, и T. R. Dean, «WAFA: Fine-grained dynamic analysis of web applications», в 2009 11th IEEE International Symposium on Web Systems Evolution, Edmonton, AB, Canada: IEEE, сен. 2009, сс. 141–150. doi: 10.1109/WSE.2009.5631226.

[10] M. S. Lam, M. Martin, B. Livshits, и J. Whaley, «Securing web applications with static and dynamic information flow tracking», в Proceedings of the 2008 ACM SIGPLAN symposium on Partial evaluation and semantics-based program manipulation, San Francisco California USA: ACM, янв. 2008, сс. 3–12. doi: 10.1145/1328408.1328410.

[11] Z. Su и G. Wassermann, «The Essence of Command Injection Attacks in Web Applications».