УДК 004.056

СИСТЕМЫ ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ

Осипов И.Н. (Санкт-Петербургский государственный университет информационных технологий, механики и оптики)

Научный руководитель – Югансон А.Н.

(Санкт-Петербургский государственный университет информационных технологий, механики и оптики)

Аннотация. Данная работа рассматривает современные системы защиты веб-приложений, такие как брандмауэр и система обнаружения вторжений. Рассмотрены различные варианты реализации и выделены наборы данных для реализации данных методов при помощи машинного обучения.

Введение. Для совершения своих действий в интернете пользователи используют веб-приложения, они подвержены многочисленным атакам как из вне, так и изнутри системы. Вследствие чего, данные приложения нуждаются в защите.

Основная часть. Статья посвящена обзору существующих методов защиты веб-приложений. Были рассмотрены основные угрозы и методы борьбы с ними, такие как брандмауэр веб-приложения (WAF – Web Application Firewall), WAF это совокупность мониторов и фильтров, предназначенных для обнаружения и блокирования сетевых атак на веб-приложение. согласно модели OSI находится на прикладном уровне и система обнаружения вторжений (IDS – Intrusion Detection System), IDS это системы, собирающие информацию из различных точек защищаемой системы (вычислительной сети) и анализирующие эту информацию для выявления реальных нарушений защиты (вторжений). Данные системы могут функционировать на основе сигнатур, аномалий и с использованием машинного обучения. Указаны достоинства и недостатки данных систем. Изучены наборы данных содержащие запросы для обучения и работы систем на основе машинного обучения.

Выводы. В данной статье рассмотрены основные методы и системы защиты веб-приложений, были выделены их достоинства и недостатки. Так системы, использующие сигнатуры, хорошо справляются с уже известными атаками, но уязвимы для атак новых атак. Системы на основе аномалий нуждаются в постоянном обновлении шаблонов поведения, но в случае корректной отладки данная система способна предотвратить атаки нулевого дня. В настоящий момент идет упор на внедрение машинного обучения в системы обнаружения вторжений.

Список использованных источников:

1. Alaoui R. L., Nfaoui E. H. Deep learning for vulnerability and attack detection on web applications: A systematic literature review //Future Internet. – 2022. – Т. 14. – №. 4. – С. 118.
2. Goutam A., Tiwari V. Vulnerability assessment and penetration testing to enhance the security of web application //2019 4th International Conference on Information Systems and Computer Networks (ISCON). – IEEE, 2019. – С. 601-605.
3. Calvo M., Beltrán M. An Adaptive Web Application Firewall. – 2022.
4. Halim H. I., Kholief M., Maghraby F. Deep Learning Methods in Web Intrusion Detection: A Systematic Review. – 2022.
5. Khraisat A. et al. Survey of intrusion detection systems: techniques, datasets and challenges //Cybersecurity. – 2019. – Т. 2. – №. 1. – С. 1-22.
6. Kruegel C., Vigna G., Robertson W. A multi-model approach to the detection of web-based attacks //Computer Networks. – 2005. – Т. 48. – №. 5. – С. 717-738.

7. Zhang M. et al. A deep learning method to detect web attacks using a specially designed CNN //International Conference on Neural Information Processing. – Springer, Cham, 2017. – С. 828-836.

Осипов И.Н. (автор) Подпись

Югансон А.Н. (научный руководитель) Подпись