3. Формы и методы контроля знаний студентов знаний [Электронный ресурс]. – Режим доступа: https://infourok.ru/formy-i-metody-kontrolya-znanij-studentov-4340906.html. – Дата доступа: 24.03.2023.

УДК 004.42

Анализ инструментария для автоматического тестирования веб-приложений с использованием технологии искусственного интеллекта

Андреев М. А., студент
Вагин Д. И., студент
Белорусский национальный технический университет
Минск, Республика Беларусь
Научный руководитель: ст. преподаватель Астапчик Н. И.

Аннотация.
В данной статье рассматривается инструментарий для обнаружения и предотвращения атак на веб-приложения на основе машинного обучения, что позволяет повысить безопасность веб-приложений и защитить конфиденциальную информацию в различных сферах.

В современном мире информационная безопасность является одной из наиболее важных проблем, и безопасность веб-приложений не является исключением. Существует множество угроз, связанных с безопасностью веб-приложений, включая атаки типа SQL-инъекций, кросс-сайт скриптинга, подделки параметров.

Традиционные подходы к обнаружению атак на веб-приложения включают правила и эвристики, которые основываются на известных методах атаки и позволяют выявлять аномалии в поведении пользователей. Однако такие подходы могут быть неэффективными против новых и неизвестных атак. С другой стороны, использование методов машинного обучения может значительно повысить эффективность обнаружения атак и предотвращения их последствий.

Для разработки алгоритма обнаружения и предотвращения атак на веб-приложения, основанного на машинном обучении, необхо-

димо использовать данные, собранные в процессе работы приложения. Для этого могут быть использованы различные методы, включая логирование, мониторинг сетевого трафика, анализ журналов аутентификации и другие.

Эти данные могут быть обработаны и использованы для выявления признаков, характерных для атак на веб-приложения.

Существует множество таких методов машинного обучения. К ним относятся нейронные сети, метод опорных векторов, деревья решений, градиентный бустинг и другие. При выборе метода необходимо учитывать специфику веб-приложения, в том числе его архитектуру, тип данных и другие факторы.

Рассмотрим один из методов машинного обучения, который может быть применен для обнаружения атак на веб-приложения, а именно нейронные сети.

Нейронные сети являются мощным инструментом для классификации и анализа данных, включая данные, собранные в процессе работы веб-приложений. Эти методы машинного обучения могут быть использованы для обнаружения аномалий, которые могут указывать на наличие атак.

Нейронные сети – это компьютерные системы, которые пытаются эмулировать работу человеческого мозга. Они состоят из множества связанных нейронов, которые принимают и обрабатывают данные. Обучение нейронных сетей происходит путем подачи на вход нейронной сети множества данных, которые уже размечены (имеют метки классов). Нейронная сеть обучается таким образом, чтобы минимизировать разницу между ее выходом и правильным ответом на входных данных.

Одним из преимуществ использования нейронных сетей для обнаружения атак на веб-приложения является их способность к обнаружению неизвестных атак. В отличие от традиционных подходов, которые основываются на известных методах атак, нейронные сети могут обнаружить атаки, которые не были известны ранее. Нейронные сети также могут использоваться для обработки больших объемов данных, что делает их подходящими для обнаружения атак на веб-приложения, которые происходят на высокой скорости.

Одним из основных недостатков нейронных сетей является необходимость в большом количестве данных для их обучения, что мо-

жет быть проблематично в случае, если у веб-приложения недостаточно трафика. Кроме того, для эффективной работы нейронных сетей необходимо правильно настроить параметры модели, что требует определенных знаний и опыта в области машинного обучения.

Для эффективной работы нейронных сетей в задаче обнаружения атак на веб-приложения необходимо правильно выбирать признаки, которые будут использоваться для обучения модели. В качестве признаков могут использоваться различные характеристики HTTP-запросов и ответов, такие как адрес, метод, параметры, заголовки и др. Также можно использовать информацию о поведении пользователей, такую как частота запросов, время ответа и другие.

Одним из наиболее популярных подходов к обучению нейронных сетей для обнаружения атак на веб-приложения является использование архитектуры «рекуррентные нейронные сети» (RNN). Эта архитектура позволяет учитывать контекст при анализе последовательности запросов и ответов, что может повысить точность обнаружения атак.

В целом, разработка алгоритма обнаружения и предотвращения атак на веб-приложения на основе машинного обучения является актуальной и важной задачей в области информационной безопасности. Это может помочь повысить эффективность защиты веб-приложений и обеспечить их безопасность в условиях растущих угроз со стороны злоумышленников.

Список использованных источников

1. Чумаченко, М. А. Обзор методов машинного обучения / А. М. Чумаченко, А. В. Кудрявцев, А. А. Яковлев // Компьютерные технологии в образовании. – 2021. – № 1(22). – С. 37–40.

2. Шананин, А. А. Обнаружение атак на веб-приложения с использованием машинного обучения / А. А. Шананин // Компьютерные технологии в образовании. – 2020.– № 3. – С. 87–94.

3. Азаренко, Ю. М. Обнаружение атак на веб-приложения с помощью методов машинного обучения / Ю. М. Азаренко, А. М. Турчин // Компьютерные технологии в образовании. – 2021. – № 2. – С. 53–64.