УДК 004.75

Обеспечение безопасности данных в высоконогруженном веб-приложении на Java.

Верещагин Н. (ИТМО)

Научный руководитель – Ассистент Мухамеджанов С.

(ИТМО)

Введение. Высоконагруженные веб-приложения, построенные на Java, требуют тщательного подхода к обеспечению безопасности данных, так как они обрабатывают большие объемы трафика и чувствительной информации. В этой работе рассматриваются методы обеспечения безопасности данных в таких приложениях с использованием Spring Framework, который предоставляет широкий спектр инструментов для защиты от угроз, а также реализации шифрования, аутентификации и авторизации. В рамках исследования предложена методика интеграции современных методов защиты данных в высоконагруженные веб-приложения на Java с использованием Spring Security, Spring Boot и других компонентов фреймворка. [2].

Основная часть. Для веб-приложений на Java в условиях высокой нагрузки защита данных включает решение нескольких ключевых задач безопасности [4]:

1. **Обзор проблемы.** В данном разделе рассматривается актуальность темы обеспечения безопасности в высоконагруженных веб-приложениях, роль Spring Framework в разработке таких приложений и обоснование выбора темы исследования. Здесь также акцентируется внимание на повышенных требованиях к безопасности данных, которые обрабатываются в веб-приложениях, и на важности использования гибких и надёжных инструментов защиты данных.
2. **Обзор литературы.** В данном разделе проводится обзор существующих методов защиты данных в высоконагруженных приложениях и возможностей Spring Framework для обеспечения безопасности. Рассматриваются ключевые компоненты Spring, такие как Spring Security и Spring Boot, а также их применение для защиты данных. Включаются преимущества и недостатки различных методов защиты, применяемых в контексте использования Spring, и анализ актуальных теоретических подходов в области безопасности данных.
3. **Методология обеспечения безопасности данных.** Для обеспечения безопасности данных в высоконагруженных веб-приложениях описываются различные методы защиты, использующие возможности Spring Framework. Это включает в себя внедрение шифрования данных с использованием алгоритма AES-256 для защиты хранения данных и протоколов TLS/SSL для безопасной передачи. Рассматривается реализация многофакторной аутентификации через Spring Security и использование OAuth2 и JWT для авторизации с токенами. Также в этом разделе рассматриваются способы защиты от наиболее распространённых атак, таких как SQL-инъекции, XSS и CSRF, с использованием механизмов фильтрации входных данных и защиты в Spring Security. Для контроля состояния безопасности предлагается настройка системы мониторинга с использованием Spring Boot Actuator и интеграция с инструментами для анализа логов и обнаружения аномалий, такими как ELK Stack (Elasticsearch, Logstash, Kibana).[6]

4. **Реализация методики на примере приложения на Spring Framework** В этом разделе описывается процесс разработки высоконагруженного веб-приложения с использованием Spring Boot и Spring Security для обеспечения защиты данных. Представлены практические шаги по реализации шифрования, аутентификации, защиты от атак, а также мониторинга безопасности в рамках выбранного подхода. Приводятся результаты оценки производительности приложения до и после внедрения предложенной методики безопасности.
5. **Результаты и обсуждение.** В данном разделе анализируются результаты внедрения предложенной методики безопасности, включая снижение числа уязвимостей, повышение уровня защиты передачи и хранения данных, а также улучшение показателей безопасности в реальных условиях.

Использование Spring Security для внедрения шифрования данных с применением AES-256 для защиты хранения данных и TLS/SSL для защиты передачи информации обеспечивает высокий уровень безопасности. Реализация многофакторной аутентификации через Spring Security и использование OAuth2 и JWT для авторизации с токенами повышают защиту от несанкционированного доступа. Защита от SQL-инъекций, XSS и CSRF с помощью фильтров Spring Security минимизирует риски этих атак. Внедрение мониторинга безопасности с помощью Spring Boot Actuator и инструментов, таких как ELK Stack (Elasticsearch, Logstash, Kibana), позволяет оперативно выявлять аномалии и предотвращать угрозы в реальном времени.

Выводы. Проведен анализ уязвимостей высоконагруженных веб-приложений и разработана методика обеспечения безопасности данных с использованием современных технологий и подходов.

Список использованных источников:

1. Основные угрозы безопасности сайта / Хабр [Электронный ресурс]. https://habr.com/ru/articles/279787/
2. Что такое веб-угрозы? - Лаборатория Касперского [Электронный ресурс]. https://www.kaspersky.ru/resource-center/threats/web
3.Безопасность веб-приложений: анализ методов защиты от атак [Электронный ресурс]. https://habr.com/ru/articles/800017/
4. OWASP Top 10: самые распространённые уязвимости веб-приложений [Электронный ресурс]. https://skillbox.ru/media/code/owasp-top-10-samye-rasprostranyonnye-uyazvimosti-vebprilozheniy/
5. Самые опасные уязвимости веб-приложений - Noventiq Belarus [Электронный ресурс]. https://noventiq.by/about/news/samyie-opasnyie-ugrozyi-dlya-veb-prilozheniy
6. Spring Security Documentation [Электронный ресурс]. https://docs.spring.io/spring-security/reference/index.html