Крістіна Шатц, студентка
Науковий керівник – Воронкова В.Г., д. філос. н., проф.,
зав. каф. менеджменту організацій та управління проектами
Запорізька державна інженерна академія.

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВЕБ – ДОДАТКІВ

Актуальність дослідження. Безпека веб-додатків знаходиться в першій десятці трендів і загроз інформаційної безпеки вже понад 10 років. Дійсно, сучасні бізнес-процеси та повсякденне життя - все більше і більше залежить від використання веб-додатків, в найрізноманітніших аспектах: від складних інфраструктурних систем до IoT пристроїв. Проте, навіть з використанням цих засобів безпечніше веб не став, більш того, майже усі уразливості "класичного інтернету" практично в незмінному вигляді мігрували в мобільну розробку.

З чого складалася захист веб-додатки раніше? З грамотної настройки сервера, чищення сайту від непотрібних файлів і ділянок коду з мінімальним контролем. Дійсно, канали були слабкі, DDoS не був поширен, вразливостей було мало, додатки були простими, дії користувачів були передбачені декількома сценаріями.

Згодом ускладнювалися веб-додатки, серверна інфраструктура і взаємодія, код ставав все більш об'ємним і громіздким - це набагато збільшило "поверхню атаки". Веб став дуже популярним, в ньому з'явилися можливості фінансового зростання - що природно привернуло в цю сферу бажаючих незаконно скористатися чужою працею.

Експоненціально стала рости кількість і різновид атак на веб-додатки, які умовно можна розділити на дві категорії (виходячи з концепції інформаційної безпеки):

• загрози спрямовані на порушення конфіденційності інформації;

• загрози спрямовані на порушення доступності інформації.

В першу чергу це стосується експлуатації вразливостей, в другу атак на відмову в обслуговуванні. І якщо частина атак можна спробувати уникнути на етапі планування та розробки програми (використовуючи інструменти тестування, налагодження, аналіз коду і т.д.), то при розміщенні веб-додатку у мережі інтернет сайт (особливо популярною сфери діяльності або компанії) починає піддаватися атакам практично в усіх напрямках.

Проблемна ситуація. Хоча проблема безпеки стоїть дуже гостро спеціалізованих засобів захисту веб-додатків досить мало, здебільшого це завдання покладають на розробників. Це і використання різних фреймворків, засобів санації, очищення даних, нормалізації і багато чого іншого. Проте, навіть з використанням цих засобів безпечніше веб, не став, більш того, майже усі уразливості "класичного інтернету" практично в незмінному вигляді мігрували в мобільну розробку.

Завдання дослідження. Метою роботи є проектування і розробка системи захисту та аналізу можливих загроз для веб-додатку. Подібне завдання включає в себе захист веб-додатку від найбільш популярних та небезпечних загроз.

Мета дослідження. Метою роботи є проектування і розробка системи захисту та аналізу можливих загроз для веб-додатку. Подібне завдання включає в себе захист веб-додатку від найбільш популярних та небезпечних загроз.

Методи дослідження. Методи аналізу атак на застосунки, методи захисту через нейронну мережу.

Висновки. Після дослідження предметної області та детального аналізу поставленої проблеми було встановлено актуальність розробки системи пошуку та усунення вразливостей на веб-ресурсі. Шляхом аналізу різних видів атак та проведення теоретичних і практичних досліджень було сформовано набір методів для дослідження, проведено їх порівняння та аналіз, а також було визначено стек технологій та інструментів розробки, визначено їх відносну продуктивність, ступінь інтеграції та зручність використання.

Дослідження також показали, що на ринку відсутня подібна комплексна і загальнодоступна система. Отже, програмний комплекс, що розроблюється, має широкі можливості для розвитку і великі шанси зайняти своє місце на ринку.

Ключові слова: JavaScript, front-end, web, веб-додаток, захист, безпека.

Список літератури:

1. *Жуков Ю.В. Основы веб-хакинга. Нападение и защита / Юрий Викторович Жуков, 2012. – 206 с. Знай сложности алгоритмов.*
2. *Dafydd Stuttard, Marcus Pinto The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2 edition Wiley; 2011. 912c.*