УДК 004.4

Є.О. Рудич

С.М. Довгалець

РОЗРОБКА БЕЗПЕЧНОГО ВЕБ-ДОДАТКУ З КЛІЄНТ-СЕРВЕРНОЮ АРХІТЕКТУРОЮ

Вінницький національний технічний університет

Анотація

Розглянуто та проаналізовано метод створення безпечного каркасу веб-додатку з клієнт-серверною архітектурою. Запропонований метод обгрунтований поширеними підходами використання універсального фреймворку з відкритим вихідним кодом Spring для мови програмування Java.

Ключові слова: веб-додаток, клієнт-серверна архітектура.

Abstract

The method of creating a secure framework of a web application with a client-server architecture is considered and analyzed. The proposed method is based on common approaches to using the universal open source framework Spring for the Java programming language.

Keywords: web application, client-server architecture.

Вступ

При створенні програмних систем перед розробниками часто постає завдання вибору тих чи інших проектних рішень. Ефективним рішенням в таких випадках є каркаси – існуючі добре продумані рішення, створені іншими розробниками. Вони, по-перше, істотно спрощують розробку і скорочують її час, і, по-друге, зменшують ймовірність появи помилок в розроблюваних додатках. Таким чином, якісні рішення доступні менш досвідченим розробникам, які можуть використовувати такі каркаси як основу для своїх додатків.

Для створення клієнт-серверних додатків також можна скористатися готовими каркасами, але, на жаль, не всі доступні рішення приділяють належну увагу безпеці, що може піддати додаток ризиків випадкового або навмисного втручання в його роботу, що призводить до збитків.

Аналіз загрози безпеки клієнт-серверних додатків

Безпека веб-додатків – один з найбільш гострих питань в контексті інформаційної безпеки. Як правило більшість веб-сайтів, доступних в Інтернеті, мають різного роду вразливості і постійно піддаються атакам. При використанні веб-додатків інформація може піддаватися різним атакам з боку порушників. Далі будуть розглянуті основні загрози інформаційній безпеці веб-додатків.

Виділяють наступні класи атак:

- порушення захищеності інформації на стороні клієнта (Client-side Attacks);
- виконання потенційно небезпечного коду на стороні сервера (Command Execution);
- «маскарад» (Authentication Attacks);
- перевищення повноважень (Authorization Attacks);
- витік інформації (Information Disclosure);
- логічні атаки (Logical Attacks).

Атаки для порушення захищеності інформації на стороні клієнта. Після встановлення з'єднання між користувачем і сервером виникають довірчі відносини: користувач очікує, що сайт або портал надасть йому запитане обслуговування. В силу цього порушник отримує можливість застосування різних сценаріїв атак для реалізації своїх цілей на стороні клієнта.

Атаки, спрямовані на виконання потенційно небезпечного коду на веб-сервері, засновані на тому, що для обробки запитів клієнтів сервери застосовують дані, передані користувачами разом зі своїми запитами. Ці дані можуть застосовуватися для складання команд сервера, які керують формуванням динамічного вмісту веб-сторінки. В ході такої атаки порушник може отримати можливість змінювати виконувані на стороні сервера команди.

Атаки «маскараду» використовують уразливості застосовуваних в веб-додатку методів і засобів аутентифікації (підтвердження автентичності імені) користувача, служби або додатки.

Атаки перевищення повноважень використовують недоліки методів авторизації, застосовуваних веб-сервером для визначення прав користувача, служби або програми на доступ до запитуваною об'єктів сервера. Безпечні клієнт-серверні додатки повинні дозволяти тільки певним користувачам отримувати доступ до захищених об'єктів на стороні сервера. В ході атаки перевищення повноважень порушник намагається отримати відсутні у нього права доступу.

Атаки класу «витік інформації» спрямовані на отримання потрібної порушнику інформації про атакується клієнт-серверному додатку. Використовуючи наявні вразливості, порушник може визначити які застосовуються дистрибутиви програмного забезпечення, номера версій клієнтської і серверної частин і встановлені (або невстановлені) поновлення. Також порушник може отримати інформацію про розташування на стороні сервера тимчасових або резервних файлів.

Логічні атаки спрямовані на використання функцій програми або його логіки, яка представляє собою очікувану поведінку програми при обробці запитів користувачів. Прикладами є відновлення паролів, реєстрація користувачів. Для виконання конкретної функції програми користувач повинен правильно виконати певну послідовність дій.

Шляхи зменшення загрози безпеки клієнт-серверних додатків

Найочевидніший методом створення безпечного каркасу веб-додатку – додавання переліку компонентів, що мінімізують можливість атак. З огляду на можливі атаки, які можуть виникнути при використанні клієнт-серверних додатків, визначимо наступний перелік компонентів, необхідних для створення додатку:

- модуль реєстрації користувача,
- модуль перевірки прав користувача,
- модуль створення захищеного з'єднання,
- модуль ведення аудиту.

Вибір даного набору компонентів зумовлений низкою причин:

На прикладному рівні взаємодії мережевих додатків захист в основному пов'язана із захистом веб-сторінок, що виключає їх перегляд неавторизованими користувачами. Кожний веб-додаток повинен мати форми реєстрації користувача при його першому вході на сайт і авторизації при подальшій роботі користувача з сайтом. Додаток повинен містити модуль реєстрації користувача та може бути реалізований у вигляді сукупності класів - класів, що визначають побудову об'єктів «Суб'єкт», «Об'єкт системи», «Дозвіл на доступ суб'єкта до об'єкта», і класів, які містять методи, які виконують роботу з базою даних додатки. Класи, що реалізують взаємодію з базою даних, включають класи, які містять методи по додаванню, вибору, оновленню і видаленню користувачів і об'єктів, і клас, який реалізує призначення і збереження прав користувачів.

Будь-яка система, що припускає кілька користувачів, вимагає розмежування прав суб'єктів системи по відношенню до її об'єктів. Тому будь-який безпечний веб-додаток повинен мати механізм управління доступом до його ресурсів. Вирішувати цю задачу буде модуль перевірки прав користувача. Даний зручно реалізувати використовуючи аспекти. Запропонований підхід допоможе запобігти атакам класу «Перевищення повноважень».

Будь-які відомості про дії суб'єктів при роботі з ресурсами веб-додатки повинні бути записані в журнали (файли аудиту, «лог-файли»), інакше дії порушника в разі несанкціонованого доступу або спроби такого доступу, наприклад, в ході атаки класу «Логічні атаки», залишаться непоміченими.

Висновки

Використання запропонованого підходу дозволить розробнику створювати безпечні каркаси клієнт-серверних додатків з необхідними властивостями і в короткі терміни. Після створення запропонованих

модулів, що забезпечують безпеку додатка та мінімізують можливість атак, розробник зможе доповнити створюваний веб-додаток необхідною бізнес-логікою і отримати безпечне клієнт-серверне програмне забезпечення з потрібними функціоналом.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Web Application Security Consortium [Електронний ресурс]:[Веб-сайт] – Електронні дані. — Режим доступу: http://www.webappsec.org/
2. Основні загрози безпеки сайту [Електронний ресурс]:[Веб-сайт] – Електронні дані. — Режим доступу: https://habr.com/ru/post/279787/
3. Аспектно-орієнтоване програмування [Електронний ресурс]:[Веб-сайт] – Електронні дані. — Режим доступу: https://dic.academic.ru/dic.nsf/ruwiki/71104/

Рудич Єлизавета Олександрівна — студентка групи 1АКІТ-17б, факультет комп'ютерних систем і автоматики, Вінницький національний технічний університет, м .Вінниця, e-mail: liza79682@gmail.com

Довгалець Сергій Михайлович — професор кафедри автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, м. Вінниця

Rudych Elizabeth O. — student of group 1AKIT-17b, faculty of computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia.

Dovgalets Sergeiy M. — Professor of Automation and Intelligent Information Technology department, Vinnytsia National Technical University, Vinnytsia.