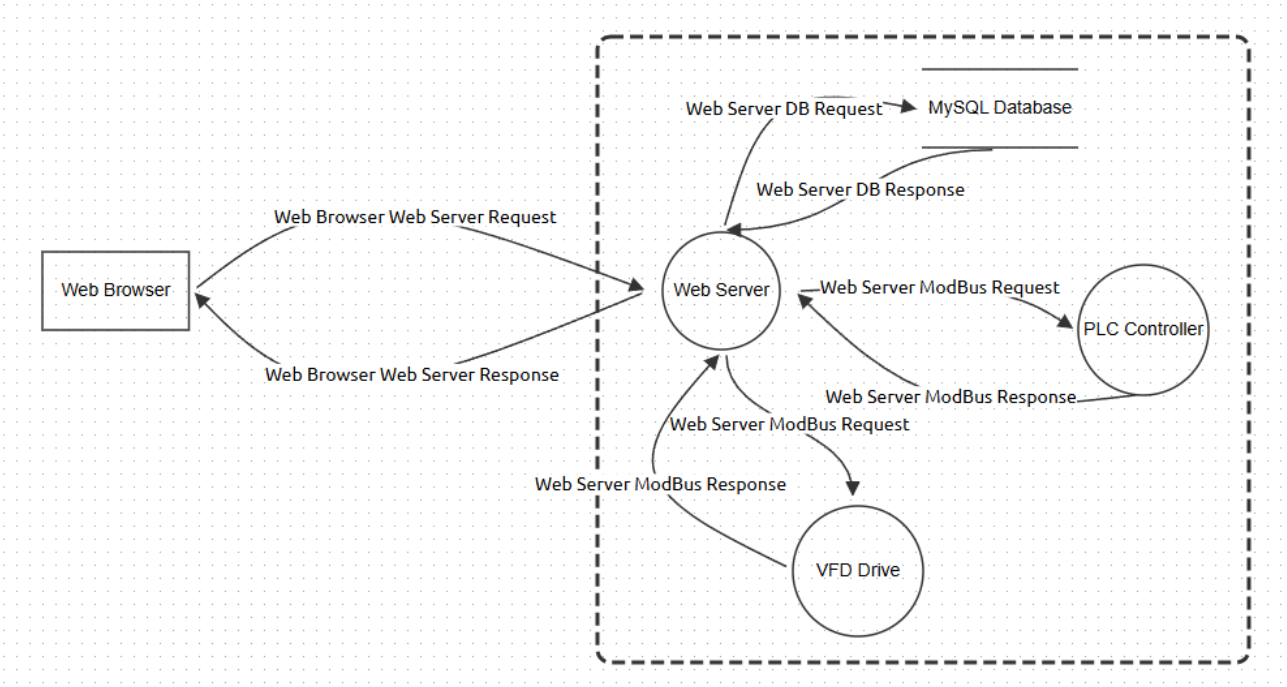

Рисунок 1 – Вигляд схеми в OWASP Thread Dragon

Система представляє собою веб-застосунок для віддаленого керування промисловим обладнанням з веб-сервером та базою даних. Веб-браузер взаємодіє із веб-сервером, котрий в свою чергу обробляє запити, оновлює базу даних та керує ПЛК і частотними перетворювачами.

Опис зв'язків між сутностями:

1. Web Browser ↔ Web Server
    - Тип зв'язку: HTTPS запити через веб-інтерфейс.
    - Напрямок: Двосторонній.
    - Опис:
        - Користувач здійснює взаємодію з веб-застосунком (вхід у систему, перегляд параметрів ПЛК, виконання команд керування).
        - Web Server приймає вхідні дані та повертає результат роботи або інформацію про стан обладнання.

2. Web Server ↔ MySQL Database
    - Тип зв'язку: SQL запити до бази даних.
    - Напрямок: Двосторонній.

• Опис:

o Веб-сервер виконує CRUD-операції (Create, Read, Update, Delete) для роботи з конфігураціями ПЛК, історією операцій та обліковими записами користувачів.

o База даних обробляє запити та повертає результат.

3. Web Server ↔ PLC Controller

• Тип зв'язку: Modbus TCP команди.

• Напрямок: Двосторонній.

• Опис:

o Web Server може надсилати команди керування до ПЛК для зміни параметрів або читання стану.

o PLC Controller повертає дані про поточний стан та результати виконання команд у форматі Modbus TCP.

4. Web Server ↔ VFD Drive

• Тип зв'язку: Modbus TCP команди.

• Напрямок: Двосторонній.

• Опис:

o Web Server надсилає команди до частотного перетворювача для управління частотою обертання двигуна.

o VFD Drive повертає параметри роботи двигуна та стан пристрою.

Таблиця загроз:

№	Назва зв'язку	STRIDE-клас	Назва загрози	Опис загрози
1	Web Browser Web Server Request	Spoofing	Spoofing the Web Server Process	Web Server may be spoofed by an attacker and this may lead to information disclosure by Web Browser

2	Web Browser Web Server Request	Tampering	Potential Lack of Input Validation for Web Server	Data flowing across Web Browser Web Server Request may be tampered with by an attacker
3	Web Browser Web Server Request	Repudiation	Potential Data Repudiation by Web Server	Web Server claims that it did not receive data from a source outside the trust boundary
4	Web Browser Web Server Request	Information Disclosure	Data Flow Sniffing	Data flowing across Web Browser Web Server Request may be sniffed by an attacker
5	Web Browser Web Server Request	Denial of Service	Potential Process Crash or Stop for Web Server	Web Server crashes, halts, stops or runs slowly; in all cases violating an availability metric
6	Web Browser Web Server Request	Elevation of Privilege	Web Server May be Subject to Elevation of Privilege Using Remote Code Execution	Web Browser may be able to remotely execute code for Web Server
7	Web Server DB Response	Spoofing	Spoofing of Source Data Store MySQL Database	MySQL Database may be spoofed by an attacker and this may lead to incorrect data delivered to Web Server

8	Web Server DB Response	Information Disclosure	Weak Access Control for a Resource	Improper data protection of MySQL Database can allow an attacker to read information not intended for disclosure
9	Web Server ModBus Request	Elevation of Privilege	Elevation Using Impersonation (PLC)	PLC Controller may be able to impersonate the context of Web Server in order to gain additional privilege
10	Web Server ModBus Request	Elevation of Privilege	Elevation Using Impersonation (VFD)	VFD Drive may be able to impersonate the context of Web Server in order to gain additional privilege

Опис наведених загроз:

1. Підробка веб-сервера дозволяє атакувальнику видавати себе за легітимний сервер та отримувати конфіденційну інформацію від користувачів, які вводять свої облікові дані.

2. Відсутність валідації вхідних даних дозволяє атакувальникам надсилати шкідливі дані, що може призвести до SQL-ін'єкцій, XSS-атак або порушення роботи сервера.

3. Відсутність адекватного логування призводить до неможливості забезпечити підзвітність, що дає змогу атакувальникам уникнути відповідальності за свої дії.

4. Перехоплення незашифрованого трафіку дозволяє атакувальникам отримати доступ до конфіденційної інформації, такої як паролі, параметри ПЛК або технологічні дані.

5. Відмова в обслуговуванні може бути викликана перевантаженням сервера або цілеспрямованими DDoS-атаками, що призводить до недоступності системи керування.

6. Віддалене виконання коду дозволяє атакувальнику повністю контролювати веб-сервер та отримати доступ до всіх підключених промислових пристроїв.

7. Підробка бази даних може призвести до отримання сервером некоректних або підроблених конфігураційних даних, що може вплинути на роботу промислового обладнання.

8. Слабкий контроль доступу до бази даних може дозволити несанкціонований доступ до конфіденційної інформації, включаючи паролі користувачів та критичні параметри ПЛК.

9. Імперсонація ПЛК дозволяє зловмисному пристрою видавати себе за легітимний контролер та надсилати підроблені дані або команди до веб-сервера.

10. Імперсонація частотного перетворювача може призвести до отримання сервером хибної інформації про стан двигунів або несанкціонованого керування швидкістю обертання.