Threat_Model_LAB1

Owner: Student
Reviewer:
Contributors:
Date Generated: Mon Nov 24 2025

OWASP Threat Dragon

Executive Summary

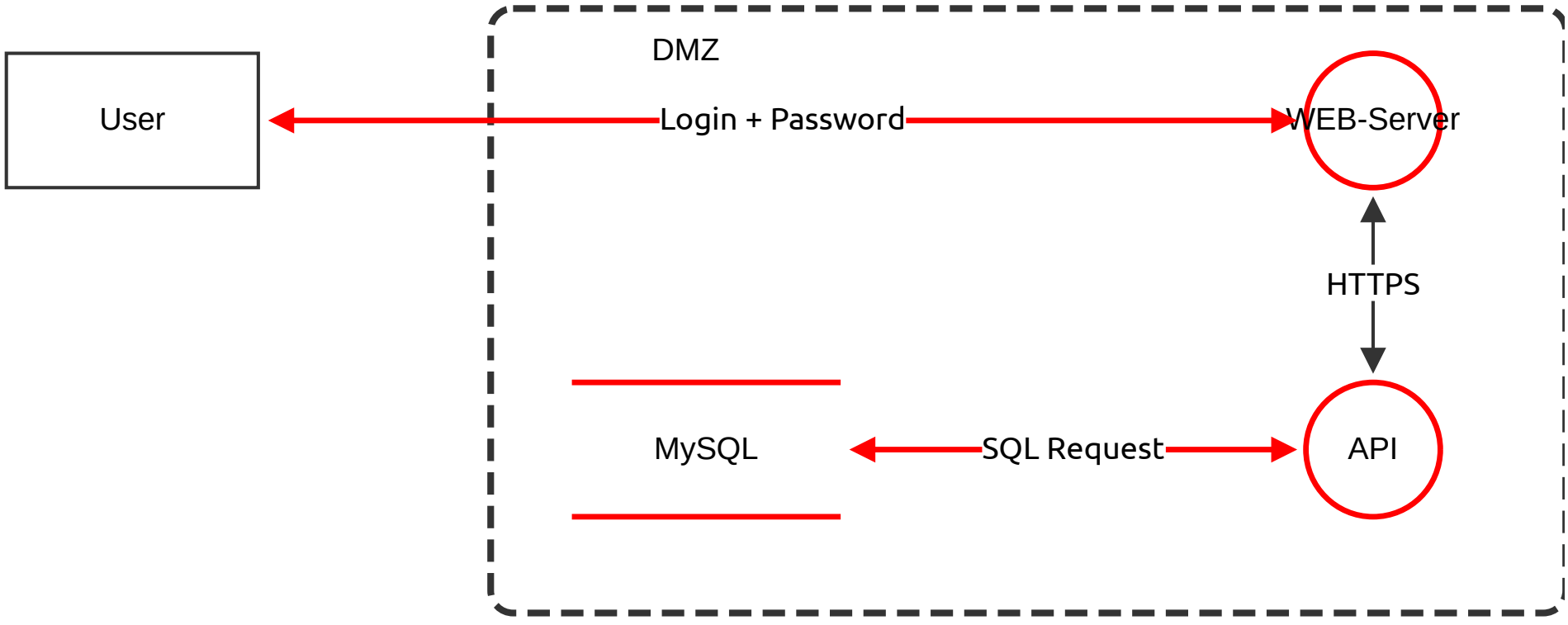
High level system description

Система адмін-панелі для управління контентом веб-сайту.
Адміністратори автентифікуються через логін/пароль + 2FA (SMS).
Доступ через HTTPS до API та бази даних.

Summary

Total Threats	5
Total Mitigated	0
Total Open	5
Open / Critical Severity	0
Open / High Severity	2
Open / Medium Severity	3
Open / Low Severity	0

STRIDE diagram



STRIDE diagram

User (Actor)

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

WEB-Server (Process)

Properties: Web Application

Number	Title	Type	Severity	Status	Score	Description	Mitigations
6	Cross-Site Scripting	Tampering	Medium	Open	6-7	Cross-Site Scripting (XSS) дозволяє атакувачу впровадити зловмисний JavaScript код на веб-сторінку WEB-Server, який виконається в браузері жертви. Типи XSS: 1. Reflected XSS - код виконується одразу через URL параметр 2. Stored XSS - код зберігається в БД і виконується для всіх користувачів 3. DOM-based XSS - маніпуляція DOM без серверної обробки Можливі наслідки: - Викрадення session cookies і токенів аутентифікації - Перенаправлення на фішингові сайти - Виконання дій від імені користувача (зміна паролю, переказ коштів) - Збір конфіденційних даних з форм - Keylogging в браузері - Модифікація контенту сторінки	Provide remediation for this threat or a reason if status is N/A

API (Process)

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations
7	Distributed Denial of Service	Denial of service	Medium	Open	6	Provide a descriptDDoS (Distributed Denial of Service) атака перевантажує API сервер величезною кількістю запитів з множини джерел, роблячи його недоступним для легітимних користувачів.	Provide remediation for this threat or a reason if status is N/A

Login + Password (Data Flow)

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Number	Title	Type	Severity	Status	Score	Description	Mitigations
5	Password interception	Information disclosure	Medium	Open	7	Хакер може перехопити пароль користувача, якщо немає HTTPS шифрування.	Provide remediation for this threat or a reason if status is N/A

HTTPS (Data Flow)

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations

SQL Request (Data Flow)

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations
4	SQL Injection	Tampering	High	Open	9	Хакер може вставити шкідливий SQL код через API і викрасти всі дані з MySQL бази даних.	Provide remediation for this threat or a reason if status is N/A

MySQL (Store)

Properties:

Number	Title	Type	Severity	Status	Score	Description	Mitigations
8	Unprotected storage	Information disclosure	High	Open	9	Незахищене зберігання виникає коли чутливі дані в MySQL базі даних зберігаються в незашифрованому вигляді або з використанням слабких механізмів захисту. При компрометації БД або доступі до backup файлів атакувач отримує повний доступ до всіх даних.	Provide remediation for this threat or a reason if status is N/A