# Technologie pro publikování na webu 2

# Semestrální projekt – webová aplikace

**Identifikační údaje**

|  |  |
| --- | --- |
| Jméno a příjmení: | Marek Fadrný |
| Školní login: | Fadrnma1 |
| Studijní obor: | Aplikovaná informatika – Softwarové inženýrství |
| Akademický rok: | 2024/2025 |
| Cvičení: | - |

**Souhrnné informace**

|  |  |
| --- | --- |
| Název projektu: | PassOwl |
| Anotace projektu: | PassOwl je zabezpečený systém pro správu hesel a citlivých dat, zahrnující backendové API, webový frontend a budoucí desktopovou aplikaci. Klíčovým prvkem je end-to-end šifrování (E2EE) na straně klienta, kde jsou data šifrována pomocí Master Hesla (nikdy neopouštějícího klienta) s využitím symetrické šifry. Backend je postavený na Python/FastAPI s Postgres databází a frontendová (webová) část na SvelteKit. Aplikace umožňuje ukládání a kategorizaci hesel. Další funkcionalitou je možnost ukládání šifrovaných poznámek. Díky koncovému šifrování nemají ani administrátoři přístup k dešifrovaným uživatelským datům. Plánovaným rozšířením je možnost bezpečně sdílet hesla mezi uživateli a také offline desktopová verze aplikace, umožňující synchronizaci se cloudem. |

## Uživatelská dokumentace

Popište používání aplikace.

|  |
| --- |
| Při registraci si vytvoříte účet s jedním hlavním (master) heslem. Toto heslo je klíčové – je nutné si ho pamatovat, protože jen s ním se dostanete ke svým datům a nikdo ho nemůže obnovit.  Po přihlášení si do aplikace jednoduše ukládáte své přihlašovací údaje a poznámky. Všechna data se automaticky zašifrují hlavním heslem, takže je nikdo jiný nepřečte. Hesla navíc možné bezpečně i sdílet ostatním uživatelům.  Obsah obrázku text, diagram, kruh  Obsah generovaný pomocí AI může být nesprávný. |
|  |

## Dokumentace architektury

Popište klíčové koncepty a principy, na základě kterých byla navržena architektura aplikace. Popište logiku fungování aplikace.

|  |
| --- |
| Aplikace je navržena jako **client-side E2EE** systém postavený na principu **Zero-Trust**. Veškeré kryptografické operace probíhají výhradně v klientově prohlížeči (SvelteKit), zatímco backend (FastAPI) slouží pouze jako zabezpečené, ale "neznalé" API a úložiště pro šifrovaná data.  **Klíčové principy fungování:**   1. **Odvození klíče:** Hlavní šifrovací klíč je odvozen na klientovi z **master hesla** a uživatelského **saltu** pomocí **PBKDF2**. Tento klíč (AES-256-GCM) existuje pouze v paměti prohlížeče s **omezenou životností**, po které je vyžadována re-autentizace. 2. **Šifrování dat:** Všechna citlivá data (hesla, poznámky) jsou před odesláním na server šifrována na klientovi tímto odvozeným klíčem. Backend tak ukládá pouze šifrované bloby a nešifrovaná metadata. 3. **Hybridní šifrování pro sdílení:** Pro bezpečné sdílení hesel je implementováno **hybridní šifrování**. Symetrický *sharing key* je zašifrován **asymetricky (RSA)** veřejným klíčem příjemce, zatímco samotné heslo je zašifrováno tímto *sharing key* **symetricky (AES)**. Tím je zajištěn bezpečný přenos mezi uživateli bez zapojení serveru do dešifrovacího procesu.   Aplikace je nasazena na platformě [Render](Render.com) a databáze běží jako managed PostgreSQL na [Neon.tech](neon.tech). SvelteKit aplikace je hostovaná na platofrmě [Vercel](vercel.com). |

## Dokumentace API

Popište koncové body aplikace a jejich obsluhu.

|  |
| --- |
| API dokumentace je automaticky generovaná přímo frameworkem FastAPI, včetně uživatelského prostředí Swagger UI: <https://api.passowl.fadrny.com/docs> |

## Dokumentace databáze

Popište model jednotlivých zdrojů a vztahy mezi nimi.

|  |
| --- |
| V aktuální konfiguraci běží PostgreSQL databáze na serverless platformě [Neon.tech](neon.tech).  Obsah obrázku text, snímek obrazovky, diagram, design  Obsah generovaný pomocí AI může být nesprávný. |

## Kontrolní checklist

Tento protokol semestrálního projektu má obsahovat:

✔ Uživatelská dokumentace

✔ Dokumentace architektury

✔ Dokumentace API

✔ Dokumentace databáze