**Теоретичні відомості FortNotes**

FortNotes – онлайн менеджер паролів.

Технологія в основі цього проекту – BlackBox , чорна скринька або зашифрований контейнер. Всі записи, створювані на цьому сайті, негайно шифруються прямо у браузері за допомогою AES (Симетричний алгоритм блочного шифрування, прийнятий як стандарт шифрування урядом США) і тільки після цього відправляються на сервер вже в зашифрованому вигляді. Це означає, що ніхто, крім власника даних, не має доступу до них. Чорна скринька розшифровується в реальну інформацію лише при вході на сайт FortNotes та введення пароля. FortNotes зберігає лише зашифровані чорні скриньки і нічого більше, жодної інформації у відкритому вигляді. Далі комп'ютера користувача і браузера не йде навіть логін, під яким проходить реєстрація у системі. Абсолютно все шифрується перед надсиланням на сервер. Коли потрібні дані – надсилається запит, закачується крипто-контейнер і відбувається розшифровка. Процес автоматизований і прозорий: потрібне лише попереднє введення пароля.

**Реєстрація**

Для реєстрації в системі потрібно лише логін та пароль, які перед відправкою на сервер перетворюються на sha256-хеш, що по суті робить реєстрацію анонімною. Замість імен користувачів та їх паролів у базі зберігаються символьні послідовності виду «a9dc602f9d82bc6720b2b4bb016edcacf7da4b2b453a466b742da743f3cba15d». На сервері не зберігаються жодні дані, які б ідентифікувати користувачів. З цієї ж причини не запитується e-mail користувача, так що відновлення логіну та пароля неможливе. Високий рівень безпеки накладає певні вимоги: немає жодних бекдорів, жодних відновлень забутих паролів. Це означає, що втрата цього пароля рівнозначна втраті всієї бази секретних даних користувача.



Для верифікації реєстрації використовується капча:



Після успішної реєстрації відбувається редирект в секцію користувача. При кожному вході в цю закриту секцію запитується пароль, який потрібний для всіх операцій шифрування та розшифрування даних. Пароль зберігається в оперативній пам'яті обмежений (настроюється) час, після якого очищається і знову запитується у користувача.



Перед очищенням пароля (після закінчення часу його зберігання), всі дані, які ще не були збережені, шифруються і тимчасово зберігаються в браузері без відправлення на сервер. Після того, як користувач введе пароль, ці дані будуть відновлені, і користувач зможе продовжити роботу.

У правому верхньому куті екрана доступні дві команди:

**Lock** дозволяє негайно зашифрувати всі відкриті дані, стерти з пам'яті пароль та заблокувати екран доти, доки не буде введено пароль. Важливо пам'ятати, що якщо в цей момент редагувалися будь-які дані нотатки і вони не були збережені, то при цьому блокуванні ці зміни так і залишаться тільки в браузері і не потраплять на сервер, поки користувач явно не збереже нотатку.

**Exit** виконує повний вихід із системи з очищенням пароля з пам'яті, видаленням всіх кешів і сесії на сервері, після чого перенаправляє на домашню сторінку проекту.

**Створення та редагування нотаток**

Основна одиниця інформації у системі це note – замітка. Нотатки можуть бути різних типів. Для створення нотаток є десяток основних типів, оформлених у вигляді шаблонів. З їх допомогою в один клік можна отримати замітку типу «поштова скринька», «сайт», «jabber аккаунт», «ssh/ftp сервер» і т.д. Список типових шаблонів для нотаток:



Кожна нотатка складається з набору полів (entry), які являють собою кінцеві поля введення інформації, і списку тегів, розділених пробілом. Так, наприклад, замітка типу «skype» складається з трьох полів: skype name (ім'я скайп-акаунта), password (пароль), comments (необов'язкове поле коментарів) і виглядає так:



Поля, своєю чергою, теж діляться за типами: простий однорядковий текст, e-mail, URI (для адрес типу сайтів), пароль, багаторядковий текст, html.

Поділ за типами для полів дозволяє додавати різні допоміжні операції: наприклад, для поля типу «пароль» стає доступною функція генерації випадкового пароля заданої довжини, для поля адреси під час введення URL робиться спроба отримати опис сайту та іконки для подальшого використання.

Як уже було згадано вище, поля у нотатках не статичні. У замітці типу «скайп» можна в будь-який момент додати нове поле будь-якого типу (наприклад, e-mail) і спозиціонувати його в бажаному місці, можна видалити будь-яке вже існуюче поле (відновити віддалене), перемістити вище або нижче, змінити тип або просто відредагувати текст поля та заголовок.

При наведенні курсору миші на будь-яке поле спливають додаткові елементи управління:



Тип будь-якого поля може бути змінений у будь-який момент за допомогою відповідного пункту. Текст заголовка (якщо він був змінений) і дані зберігаються.



Окремо варто відзначити перегляд історії змін кожного поля з можливістю відкотитись до раніше збережених значень. Відновлюються дані поля і заголовок. При виборі відповідного пункту у спливаючому меню з'являється таблиця з десяти останніми значеннями історії та посиланням для відновлення:



При зміні заголовка або даних вже існуючої нотатки модифіковані дані підсвічуються:



Після внесення змін при збереженні нотатки, візуально відображається які поля були додані, а які оновлені (плюс – нове поле, галочка – оновлене): При редагуванні нотатки можна виконати швидке збереження за допомогою комбінації клавіш Ctrl + Enter .



Крім збереження доступні дві спеціальні команди – дублювання поточної нотатки та створення нової нотатки аналогічної поточної, але з порожніми полями. Це буде зручно під час створення серії однотипних нотаток.

**Пошук та фільтрація**

Пошук на серверній стороні здійснюється за допомогою тегів, перерахованих через пропуск у рядку пошуку. Використання пошуку тега зі знаком мінус перед ним виводить список нотаток, де такий тег не зустрічається. Крім користувацьких тегів, що створюються при додаванні нотаток, є набір системних тегів для отримання списку віддалених нотаток, нотаток без тегів або фільтрації за часом останнього доступу. Такі теги доступні в рядку пошуку після введення символу двокрапки. У прикладі нижче показаний результат пошуку записів за останній місяць, де зустрічаються теги site , work та dev , але не зустрічається тег php :



Результуючий список відображає всі нотатки, що відповідають умовам, де кожен рядок відповідає одній нотатці з коротким зазначенням вмісту полів, датою останніх змін і повним списком тегів. При натисканні мишею на тегу можна додати його в умови пошуку або прибрати його з пошуку, якщо він там вже був. При одночасно затиснутій клавіші Ctrl можна додати у пошук вибраний тег зі знаком мінус.

Поле пошуку підтримує інтелектуальне автодоповнення. Достатньо почати вводити ім'я тега і відразу буде відображено список можливих варіантів з урахуванням уже введених тегів. Тобто. відображаються лише ті теги, які зустрічаються у парі з уже вказаними.



Пошук за тегами повертає перші 20 нотаток. При необхідності отримати повний список можна скористатися відповідним посиланням load all . Там же є посилання для виділення всіх нотаток, зняття виділення та інвертування. Щоб розпочати роботу з нотаткою, достатньо клацнути по ній мишею, після чого рядок буде позначений галочкою і підсвічений зеленим кольором, а нотатка буде відкрита в режимі редагування. Також можна відзначити галочкою одну і більше нотаток, клацнувши по потрібному рядку із кнопкою Ctrl . Аналогічно роботі у файлових менеджерах працює виділення нотаток при натиснутій клавіші Shift – виділяє всі елементи між двома клацаннями мишею. Над виділеними галочками нотатками можна проводити загальні операції: видалення чи відновлення віддалених. Для переходу в режим відновлення віддалених нотаток можна скористатися системним тегом : deleted. Також можливість перейти до відновлення присутня у підказці, що спливає відразу після видалення вибраних нотаток.

Якщо у рядку пошуку будуть виявлені слова, які не є тегами, то вони будуть використані для додаткової фільтрації всіх завантажених до списку нотаток.

