



ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВЕБ-СЕРВІСУ ДЛЯ ХМАРНОГО ЗБЕРІГАННЯ ТА ОБМІНУ ФАЙЛІВ

ВИКОНАЛА: СТУДЕНТ ГР. КІТ-М119Б ЩЕРБІНІНА Є.М.

КЕРІВНИК: ПРОФ. ФІЛОНЕНКО А.М.

ПОСТАНОВКА ЗАДАЧІ

Метою дипломної роботи є: формування методів захисту інформації та впровадження їх у веб-сервіс хмарного зберігання та обміну файлів.

Задачі розробки:

- проведення дослідження та аналізу існуючих методів захисту інформації та вибір використовуваних методів;
- проведення аналізу і вибір використовуваних технологій;
- розробка веб-сервісу хмарного зберігання файлів;
- впровадження обраних методів захисту в розроблений продукт;
- оцінка ефективності виконаної розробки.

СПИСОК НАЙБІЛЬШ ЧАСТИХ 10 ЗАГРОЗ ВЕБ-ЗАСТОСУНКІВ

- ін'єкції (Injections);
- недоліки системи аутентифікації і зберігання сесій (Broken Authentication and Session Management);
- незахищеність критичних даних (Sensitive Data Exposure);
- впровадження зовнішніх XML-сутностей (XXE);
- порушення контролю доступу (Broken Access Control);
- похибки в конфігуруванні (Security Misconfiguration);
- міжсайтовий скриптинг - XSS (Cross Site Scripting);
- небезпечна десериалізація (Insecure Deserialization);
- використання компонентів з відомими вразливостями (Using Components with Known Vulnerabilities);
- недостатнє логування та моніторинг.

MD5

- Append Padding Bits
- Append Length
- Initialize MD Buffer
- Process Message in 16-Word Blocks
- Output

ПОРІВНЯННЯ SHA1 З MD5

Схожість:

- чотири етапи;
- кожна дія додається до раніше отриманого результату;
- розмір блоку обробки становить 512 біт;
- обидва алгоритми виконують складання по модулю 2^{32} , вони розраховані на 32-х бітну архітектуру.

Відмінності:

- у SHA-1 на четвертому етапі використовується та ж функція f , що і на другому етапі;
- в MD5 у кожній дії використовується унікальна адитивна константа. У SHA-1 константи використовуються повторно для кожної із чотирьох груп;
- у SHA-1 додана п'ята змінна;
- SHA-1 використовує циклічний код виправлення помилок;
- в MD5 чотири різних елементарних логічних функції, в SHA-1 – три;
- в MD5 довжина дайджесту становить 128 біт, в SHA-1 - 160 біт;

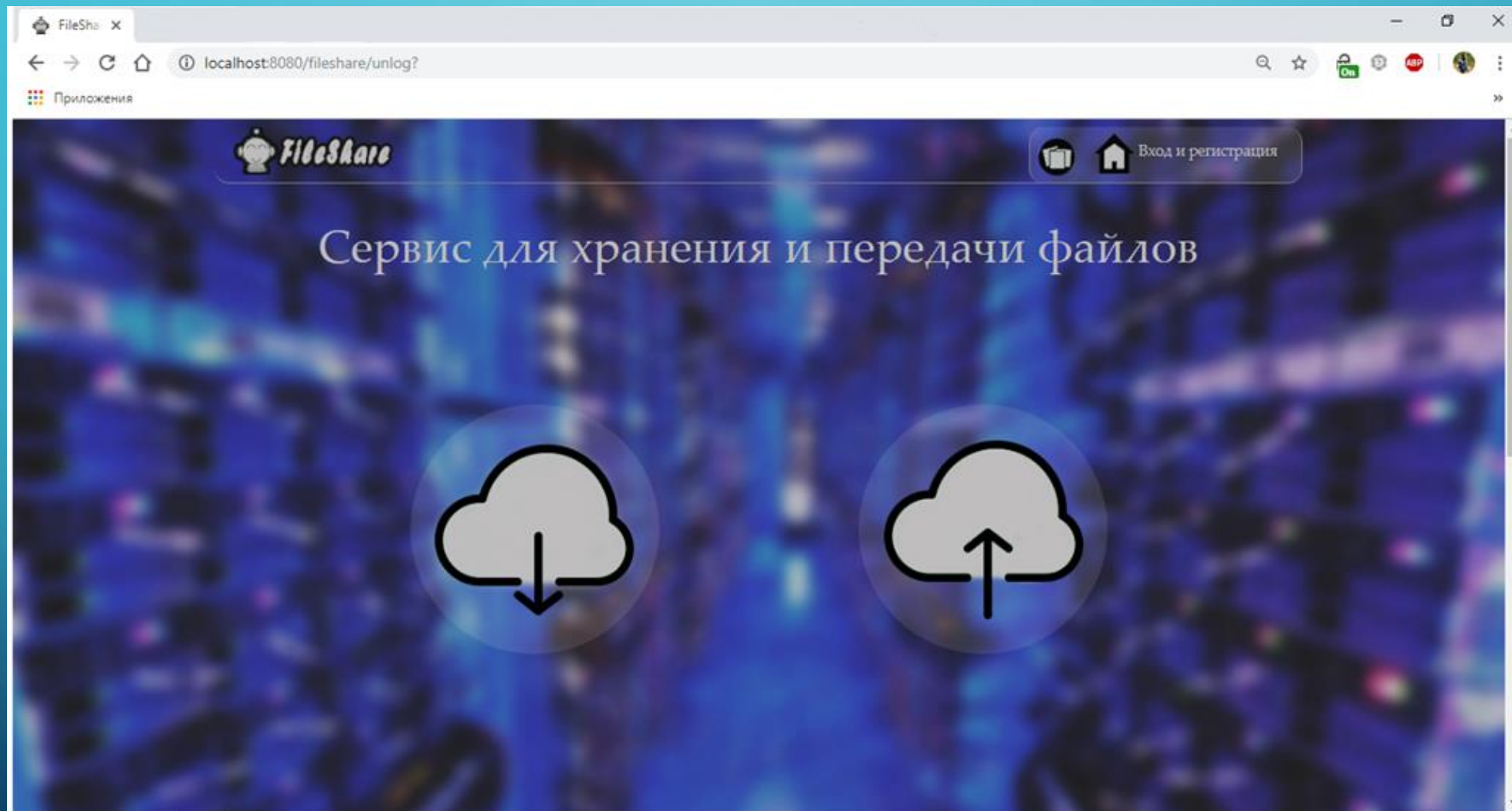
SCRIPT

MD5: 16000 M/s
SHA-1: 5900 M/s
SHA256: 2050 M/s
SHA512: 220 M/s
NTLM: 28400 M/s
Script: 8,5 k/s

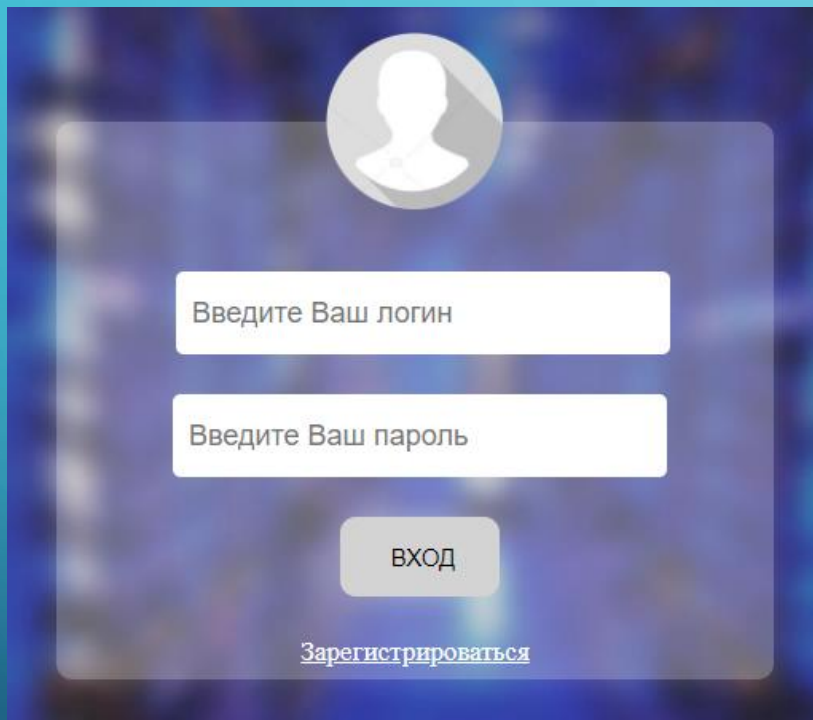
ОБРАНІ ТЕХНОЛОГІЇ ДЛЯ ПРОЕКТУВАННЯ



ГОЛОВНА СТОРІНКА ВЕБ-СЕРВІСУ



ФОРМИ ВХОДУ ТА РЕЄСТРАЦІЇ

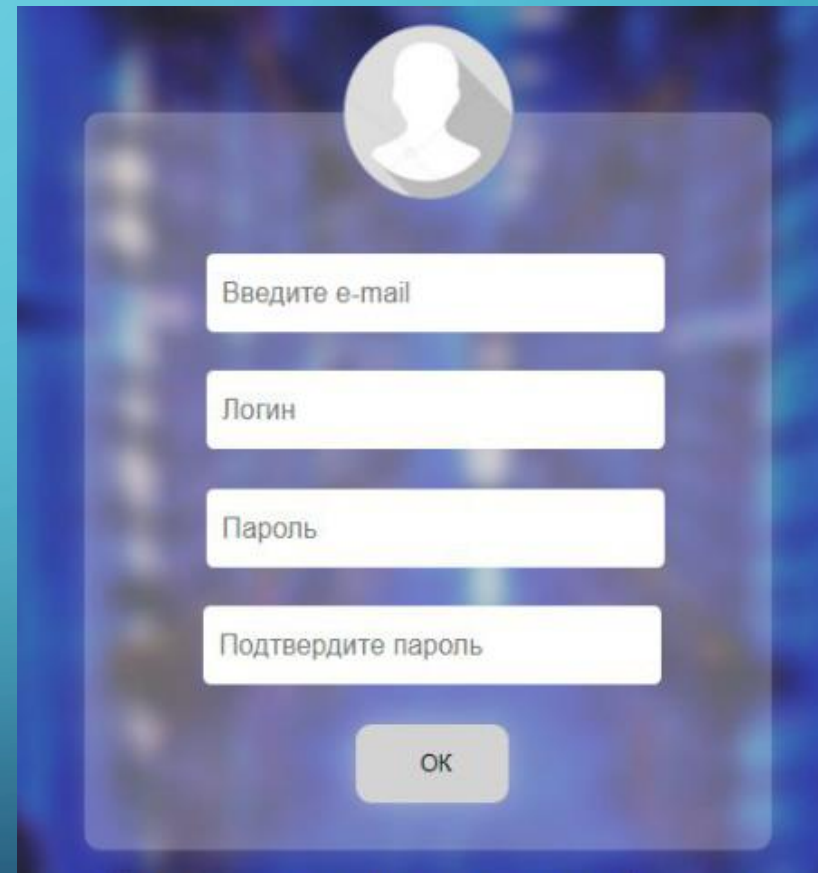


Введіть Ваш логін

Введіть Ваш пароль

ВХОД

[Зареєструватися](#)



Введіть e-mail

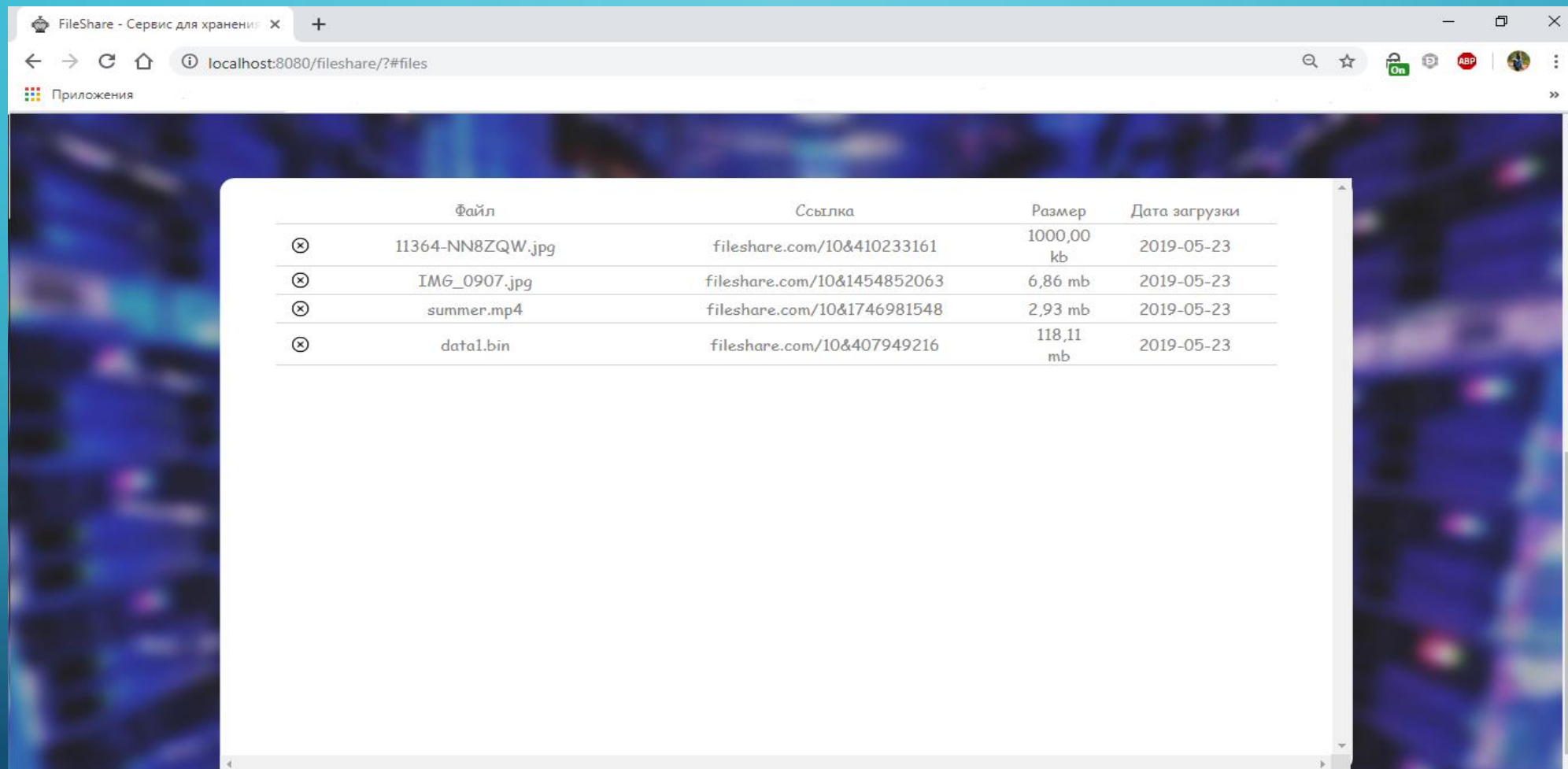
Логін

Пароль

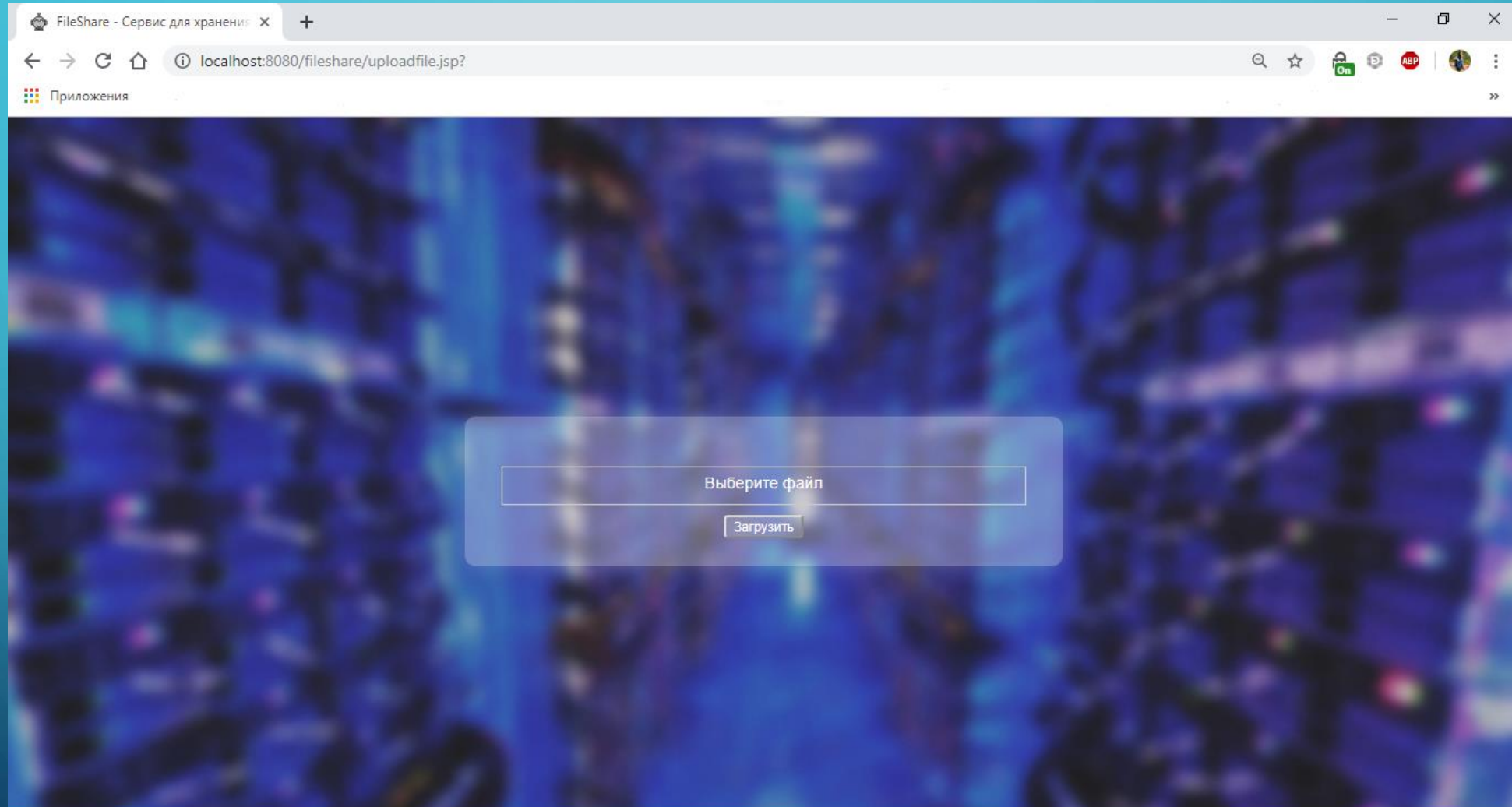
Підтвердіть пароль

ОК

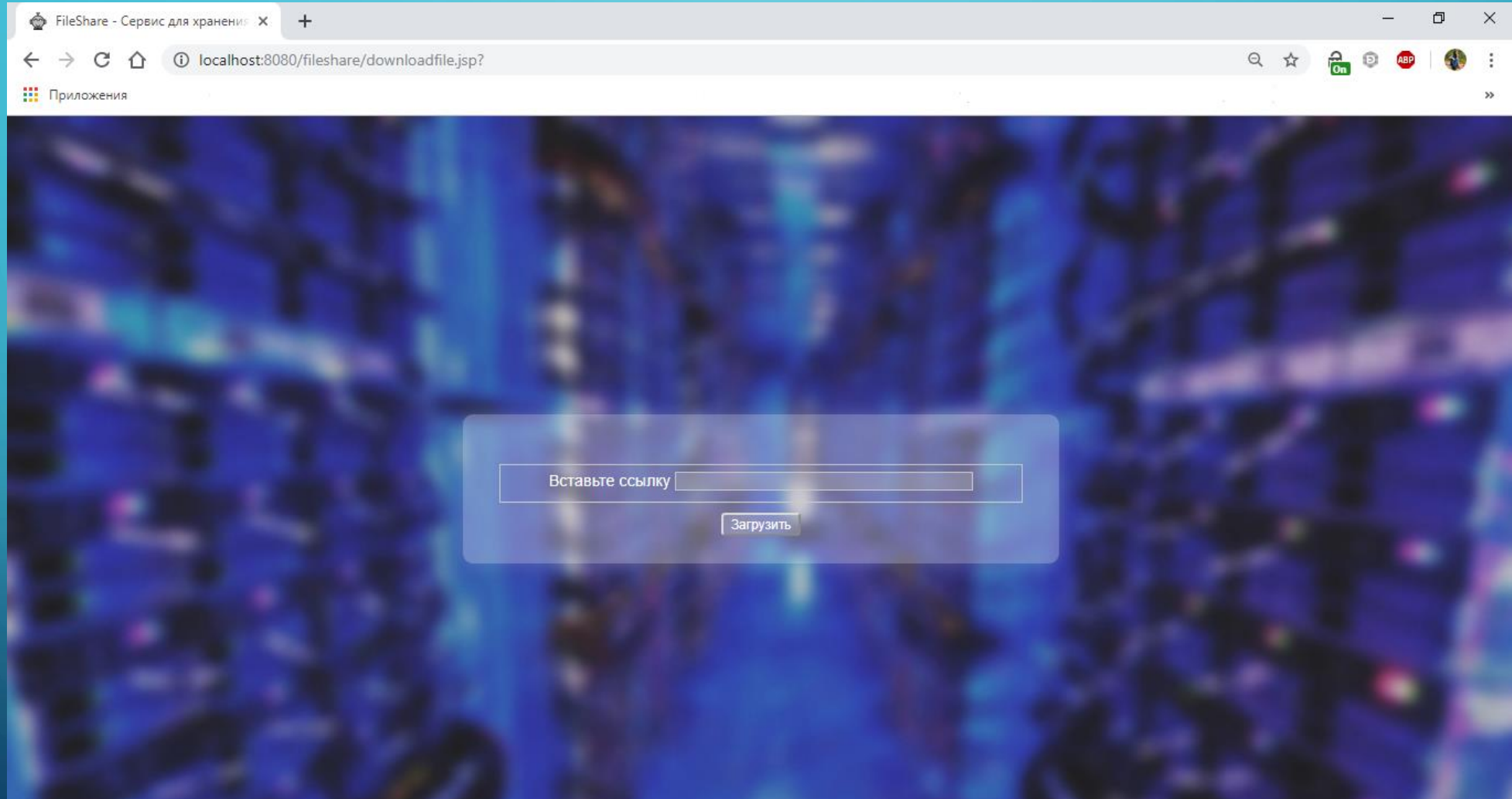
СТОРІНКА ПЕРЕГЛЯДУ ВЛАСНИХ ФАЙЛІВ



СТОРІНКА ЗАВАНТАЖЕННЯ ФАЙЛУ



СТОРІНКА ПОШУКУ ФАЙЛУ



ВИСНОВОК

У роботі розглянуті найпоширеніші загрози веб-застосунків за версією OWASP, проведено аналіз найпоширеніших методів хешування паролів, описані переваги та недоліки кожного метода, виділено найбезпечніший та найбільш актуальний метод. Проведено огляд існуючих методів шифрування бази даних. Розроблено базу даних для зберігання інформації користувача, обрано спосіб зберігання файлів у сховищі. Створено веб-сервіс для хмарного зберігання та інтегровано до нього обраний спосіб захисту.

The background is a blue gradient. In the corners, there are decorative white line art elements resembling circuit boards or neural networks, with lines and small circles.

ДЯКУЮ ЗА УВАГУ

Yelyzaveta Shcherbinina

16.12.2020р