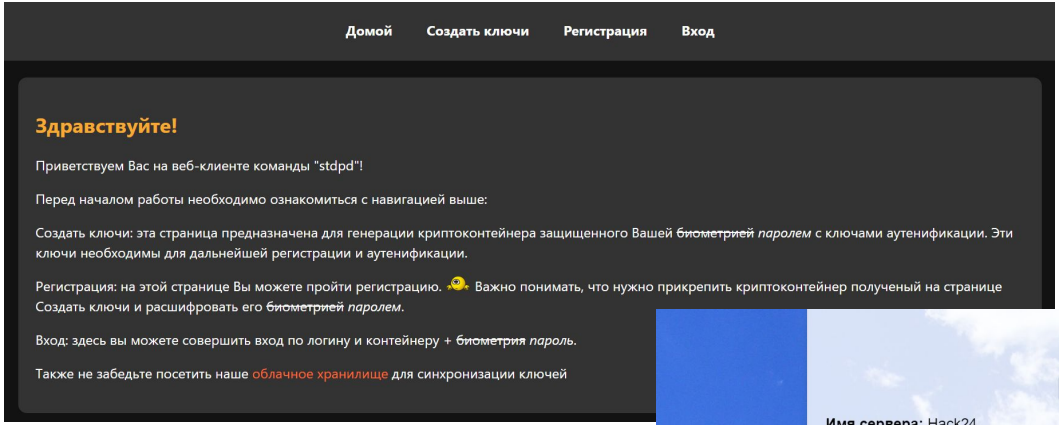
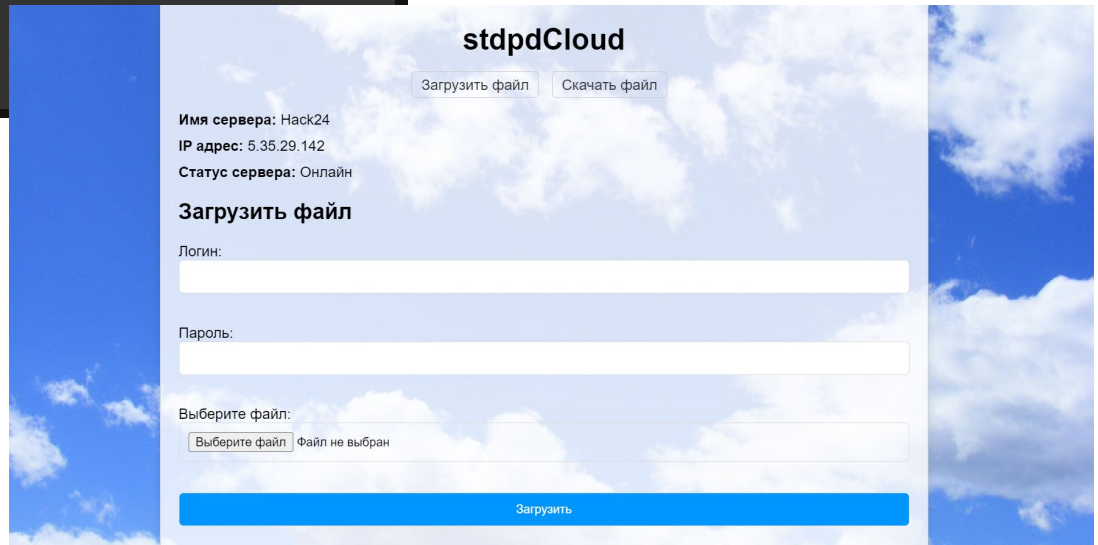
stdpd

Задание от VK

Введение


Домой
Создать ключи
Регистрация
Вход
Здравствуйте!
Приветствуем Вас на веб-клиенте команды "stdpd"!
Перед началом работы необходимо ознакомиться с навигацией выше:
Создать ключи: эта страница предназначена для генерации криптоконтейнера защищенного Вашей ~~биометрией~~ *паролем* с ключами аутенификации. Эти ключи необходимы для дальнейшей регистрации и аутенификации.
Регистрация: на этой странице Вы можете пройти регистрацию. Важно понимать, что нужно прикрепить криптоконтейнер полученый на странице Создать ключи и расшифровать его ~~биометрией~~ *паролем*.
Вход: здесь вы можете совершить вход по логину и контейнеру + ~~биометрия~~ *пароль*.
Также не забедьте посетить наше облачное хранилище для синхронизации ключей


stdpdCloud
Загрузить файл
Скачать файл
Имя сервера: Hack24
IP адрес: 5.35.29.142
Статус сервера: Онлайн
Загрузить файл
Логин:
Пароль:
Выберите файл:
Выберите файл
Файл не выбран
Загрузить

Стек технологий и протоколов

- https(+openSSL)
- sha256(хеширование, подпись, кодирование)
- Криптоконтейнеры
- SubtleCrypto, express, и т. д.
- Sqlite3
- git

Процесс разработки

Разработка плана действий
подняли сервер

Реализация шифрования
разработали правила взаимодействия

Авторизация по стандарту WebAuthn
подключили криптоконтейнеры

Клиент-серверное взаимодействие
реализовали облачное хранилище

Финал
провели ручное тестирование и дебаггинг

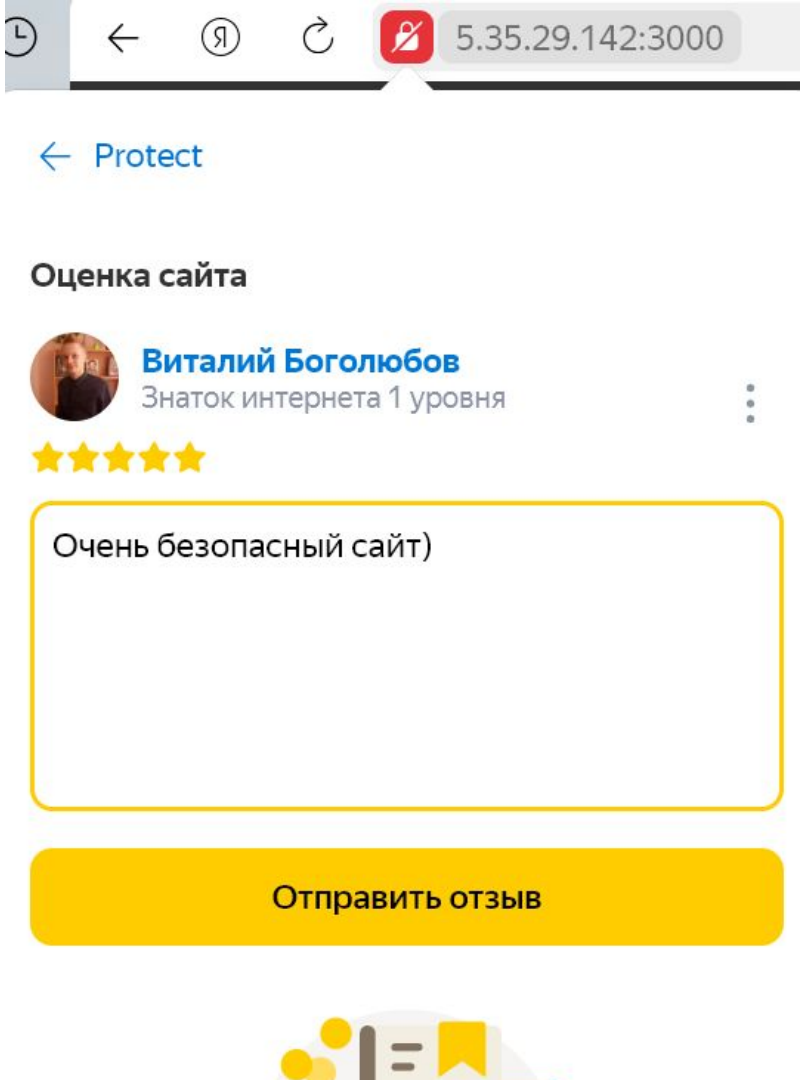
Безопасность

Использовались современные стандарты

Разработка велась на основе WebAuthn

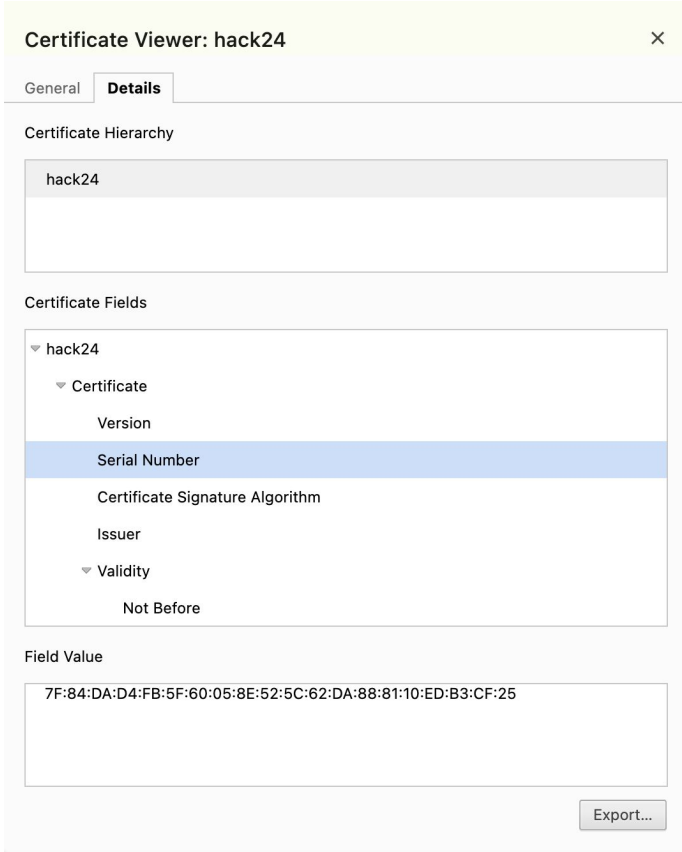
Был поднят сайт реализующий доступ по протоколу https

Все данные шифровались при помощи методов асинхронного шифрования



Как работает сайт

- был получен белый IP-адрес 5.35.29.142 и прокинуты порты 3000 и 3001 для веб-сервера и облака соответственно
- сгенерирован https-сертификат
- на каждом этапе клиент-серверного взаимодействия персональные данные передаются в защищенном виде



Как работает авторизация (WEB SERVER)

- каждый пользователь сначала генерирует себе пару ключей и защищает её паролем (подробнее о криптоконтейнерах далее)
- при регистрации он отправляет открытый ключ на сервер
- при авторизации сервер генерирует челленж (случайный набор данных на подпись), а пользователь подписывает их своим закрытым ключом
- сервер проверяет подлинность подписи и в случае успеха авторизует пользователя

Как работают криптоконтейнеры

- хешируем пароль от пользователя для доступа к контейнеру алгоритмом SHA256, для того, чтобы получить достаточно рандомизированные строки одинакового размера
- используя библиотеку cryptoContainers и полученный хеш, шифруем строку с парой ключей
- полученный контейнер скачивается на устройство
- для доступа к ключам пользователю необходимо ввести первоначальный пароль

Как работает облако

- регистрация и выгрузка криптоконтейнера на облако
- авторизация и загрузка своего криптоконтейнера с облака
- при регистрации и авторизации передается пара логин/хеш пароля зашифрованная открытым ключом облака по алгориму RSA
- пароль передается в виде хеша(SHA-256), в качестве соли используется логин.
- Для последующей авторизации пара логин/хеш пароля сохраняется в БД.

Итого

Работающий на белом IP сервис доступный по протоколу https

В процессе разработки соблюдены требования к безопасности данных и средства enterprise класса

Проведено ручное тестирование

Спасибо

Контакты:
email:
bogolyubov2003@bk.ru
telegram:
@vit_72