Выпускная квалификационная работа на тему:

«Разработка сервиса приватных сообщений без логирования»

Бурмистров С. А

Студент гр. АИБ-4-031

Соколова О.И.

Руководитель д.п.н., профессор

Исходные данные. Введение

Сегодня с каждым днем растет количество каналов, потенциально уязвимых для утечек информации в сети, в обиход приходят новые сервисы доставки мгновенных сообщений, многие из которых используются компаниями для передачи важных данных. Такое обилие способов передачи информации в сети порождает все большее количество ухищрений в виде способов воровства информации.

В июне 2017 года стало известно о том, что объем утечек конфиденциальной информации в России за год вырос в 100 раз. Данные привела компания InfoWatch, специализирующаяся на корпоративной информационной безопасности.

Анализ утечек информации

Источников, через которые информация уходит из компании, предостаточно: различные мессенджеры (Skype, ICQ и пр.), электронная почта, открытые источники (социальные сети, форумы), бумага, флешки, диски, резервные копии. Причем и в случае со случайными утечками, и в случае с умышленным сливом источники одни и те же.

Существующие разработки

В дипломной работе проанализирован ряд современных аналог, для доставки приватных сообщений.

Ни один сервис в полной мере не удовлетворяет требованиям, достаточным для обеспечения безопасности передаваемых данных.

Некоторые из них не шифруют текст сообщения, некоторые не могут предоставить данные о наличии или отсутствии логирования.

Постановка задач сервиса

Из первого пункта мы можем сделать вывод, что проблема является актуальной в нашей стране.

Кроме того, существующие аналоги не в полной мере удовлетворяют потребностям.

На основании этого решено:

Разработать сервис, для безопасной передачи данных в сети.

Сервис должен обладать следующими качествами:

- **Шифрование передаваемых данных;**
- **Отсутствие логирования;**
- **Функция дополнительной защиты информации с помощью пароля и таймера;**
- **Исходный код;**
- **Кроссплатформенный веб-интерфейс**

Выбор языка программирования

Веб-интерфейс разработан на языках: **HTML, CSS, JS** с использованием фреймворка **Bootstrap**.

Фреймворк направлен на создание макета под различные устройства,
планшеты, смартфоны, так как масштабируется в зависимости от ширины.

Для серверной части:

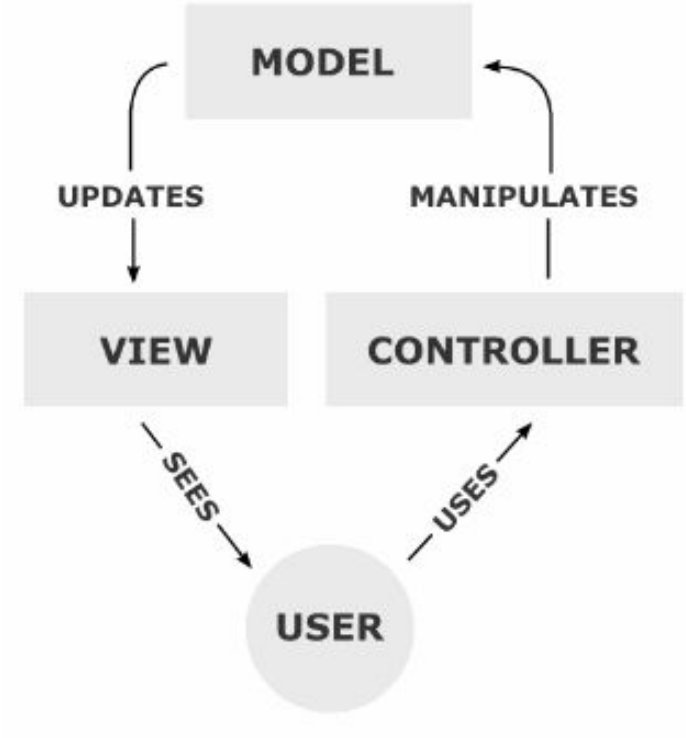
- **PHP 5.4**
- **Yii2.0 Framework**
- **Nginx**
- **Mysql**

Схема разделения данных:

MVC

Структура проекта

Как говорилось ранее в разработке используется Yii2 фреймворк.
Yii использует паттерн проектирования Модель-Представление-Контроллер (MVC, Model-View-Controller), который широко применяется в веб-программировании.



Функция пароля для сообщения

Контроллер, реализующий основную часть функционала по работе с сообщениями -**NoteController**.

Для просмотра заметки по ссылке необходимо, чтобы в запросе был передан GET-параметр hash

При его наличии производится его разбиение по разделителю ! на два параметра - uid и password функцией php list:

В случае если модель найдена по уникальному идентификатору uid производится проверка правильности пароля методом validatePassword

Функция таймера сообщения

Реализация данной задачи требуется для удаления сообщений, при создании которых был выбран параметр определенного срока жизни сообщения, то есть сообщений, которые не удаляются непосредственно при прочтении.

Эта задача должна выполняться с определённой периодичностью (по расписанию), в противном случае существует риск того, что заметки, которые так и не были просмотрены, так и не будут удалены по истечении срока хранения.

Непосредственно за удаление заметок отвечает консольный контроллер **DeleteNotesByLifetimeController**, находящийся в папке commands.

Отправка уведомления об удалении сообщения

Ранее упоминалось, что одной из задач сервиса является отправка email-сообщений автору заметки о факте удаления заметки из базы данных.

За отправку сообщений отвечает консольный контроллер SendMailController, находящийся в папке commands.

Получение уникальной ссылки.

После создания сообщения задается uid сообщения вида:

http://whispr.in/**GIO7IqbXjjdlwi4F**!**A03qf5Cq**

Красным выделена генерация уникального ключа записи, а синим, автоматический пароль, если пользователь не ввел свой.

Делается это, чтобы нельзя было найти другие записки пользователей методом перебора 1...1000 например если бы у нас была ссылка типа http://whispr.in/1

Шифрование пароля

Хеширование паролей - методы generatePasswordHash и validatePassword - в их основе лежат актуальные на данный момент функции php password_hash() и password_verify() соответственно . На данный момент в функции password_hash по умолчанию используется алгоритм CRYPT_BLOWFISH как достаточно сильный для данных целей

Помимо этого, функция шифрования, при хешировании пароля, замешивает еще один сгенерированный ключ из 10 символов который называется “соль”

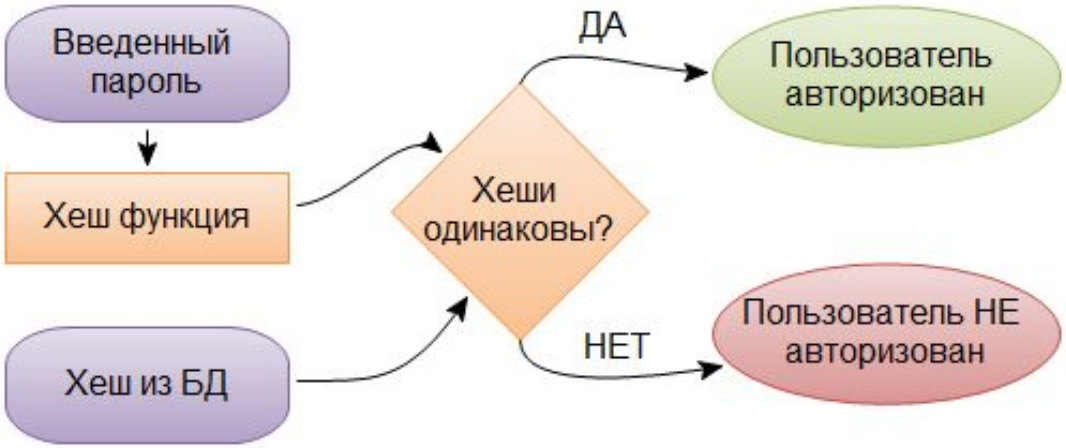
То есть у двух пользователей с паролем «123456» будут разные соли «соль1» и «соль2», а соответственно и хеш-функции от «123456соль1» и «123456соль2» в базе тоже будут разные.

Шифрование текста сообщения

Для реализации дополнительной защиты информации в виде утечки базы данных,
Решено хранить текст сообщения в зашифрованном виде по алгоритму AES128.
Для этого мы используем методы **encryptByKey** и **decryptByKey** соответственно. Ранее упоминалось, что в их основе лежит алгоритм AES (Advanced Encryption Standard), симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит)

Дешифрование сообщения и вывод данных

В базе данных пароли хранятся в виде хеша. Производится обратная процедура хешрования - переданное из http-запроса значение хешируется с применением того же алгоритма и сравнивается со значением из базы данных.



Прикрепление файлов.

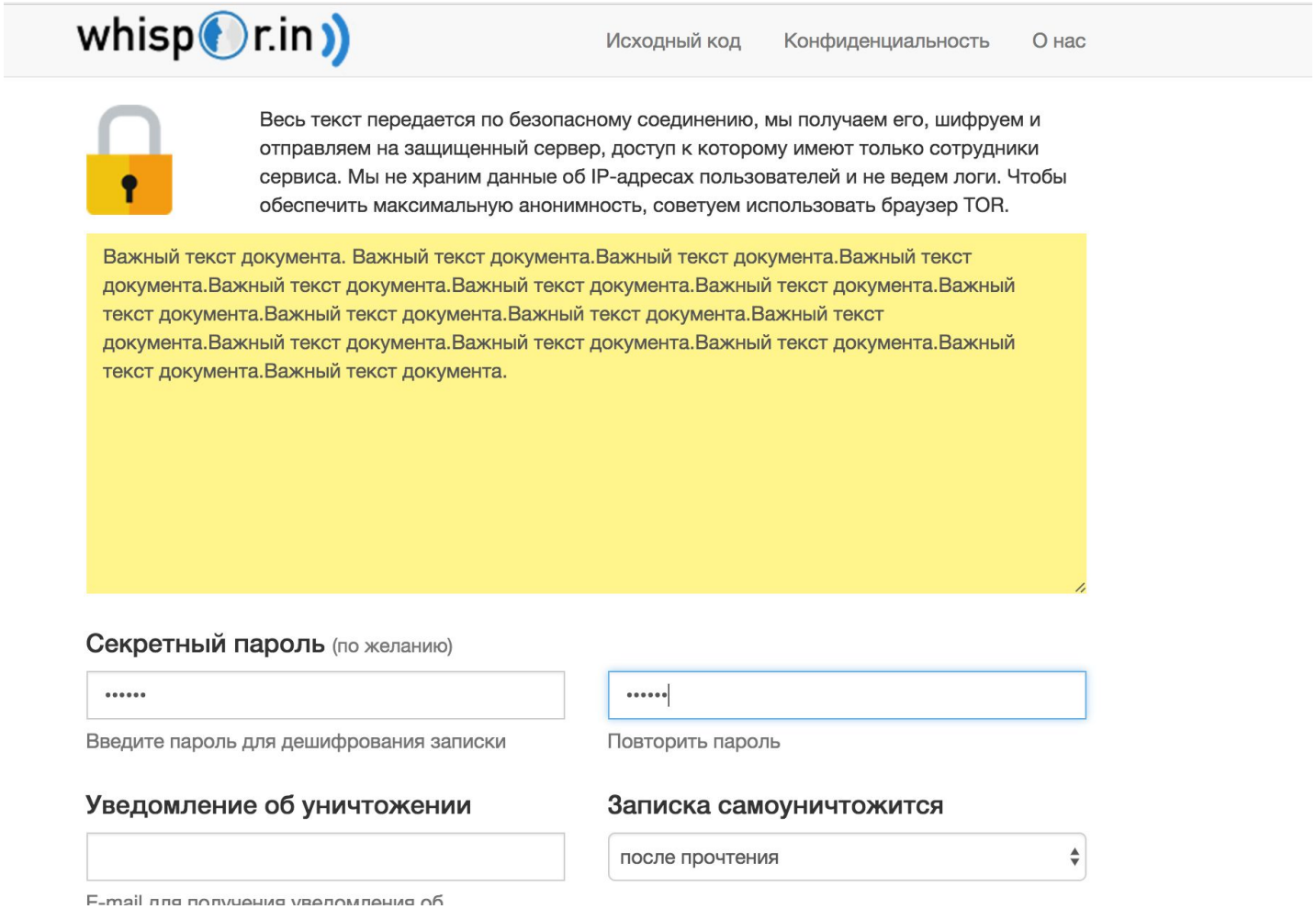
Поскольку сервис предлагает возможность прикрепления к заметке файлов, был реализован контроллер **FileController** для работы с файлами.

Файлы загружаются в папку web/uploads. Тип загружаемых файлов ограничен расширениями pdf, doc, docx (задается конфигурационным массивом при подключении **actionUpload.**

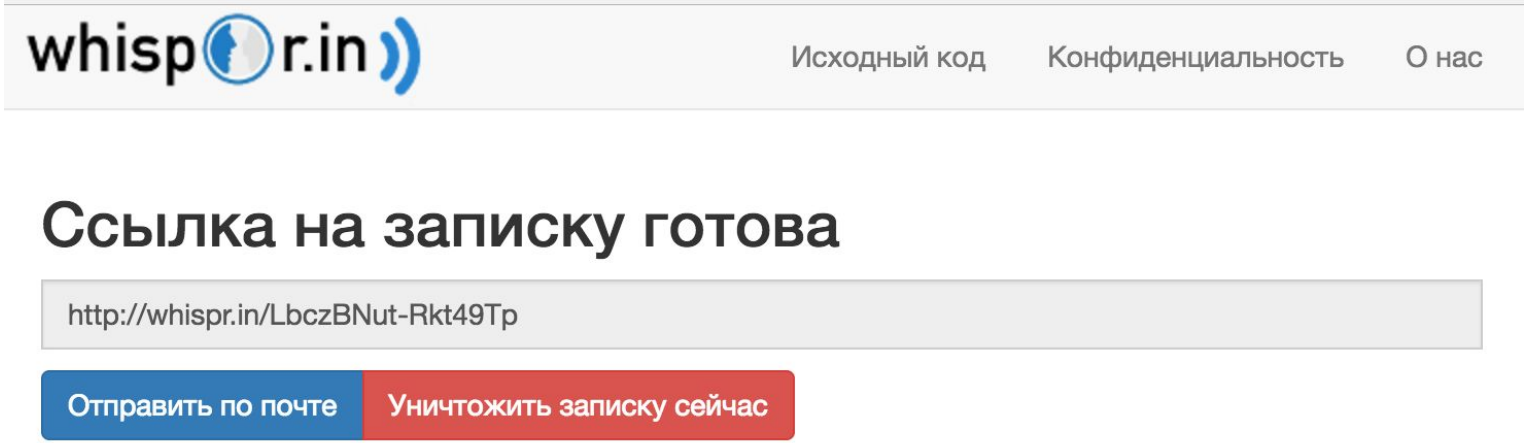
Подведение итогов

- В данной квалификационной работе были проанализированы каналы утечки информации.
- Разработан веб-сервис отправки приватных сообщений.
- Разработанный сервис удовлетворяет всем требованиям заданным на этапе проектирования и описания.

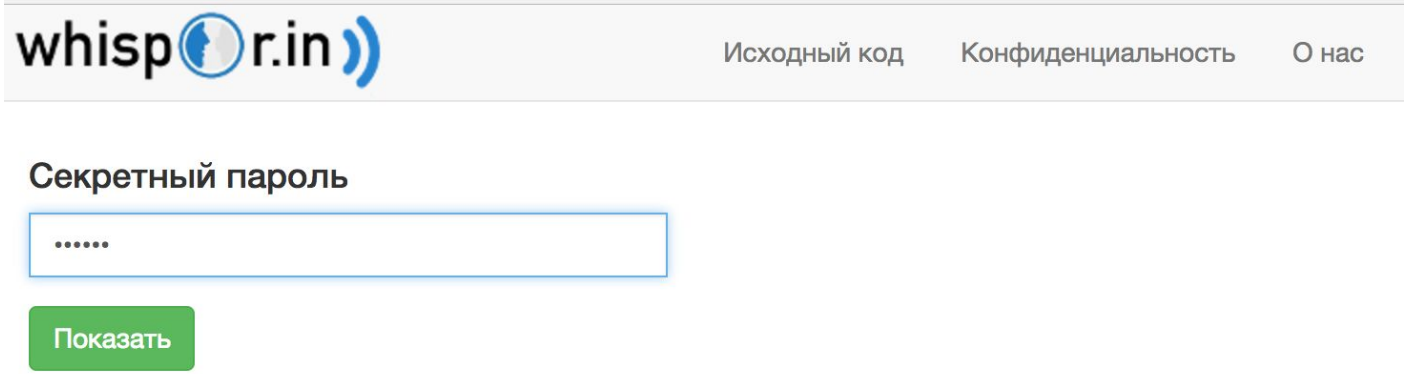
Демонстрация работы сервиса



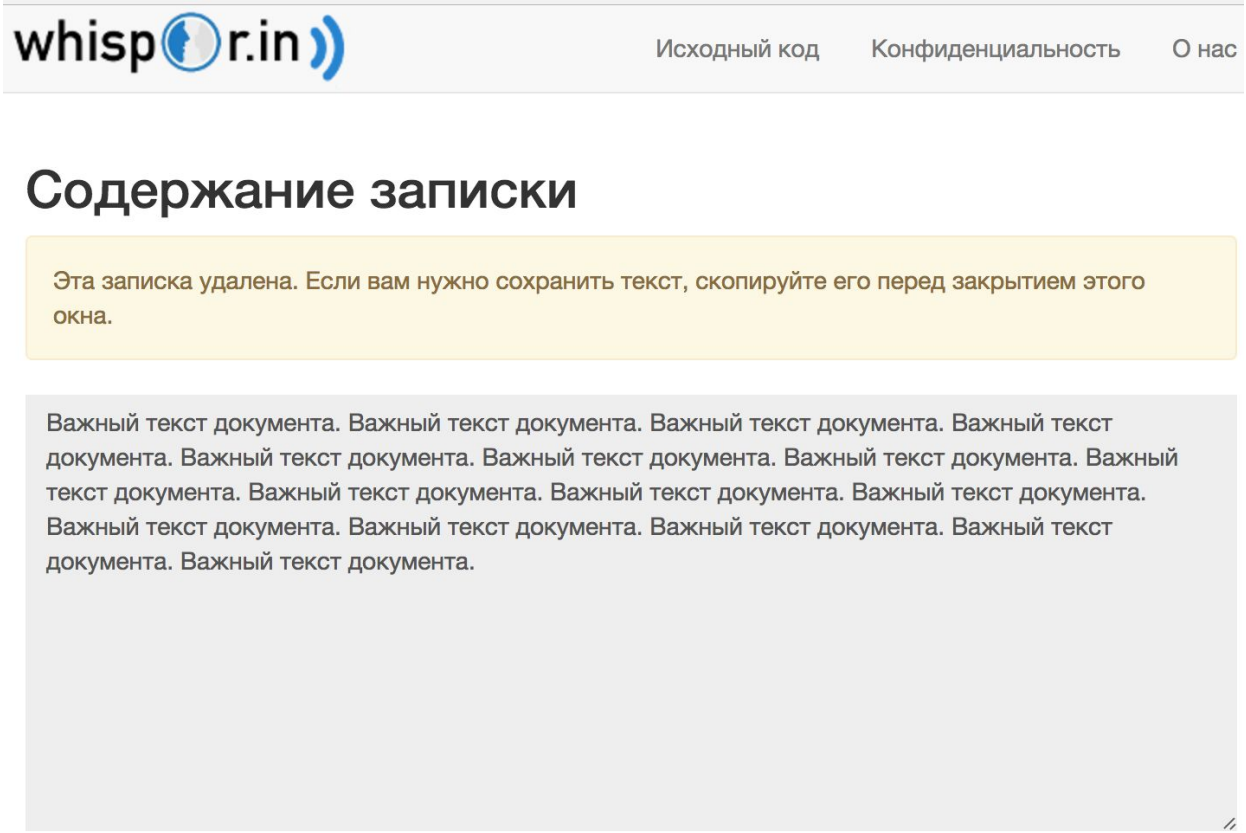
Демонстрация работы сервиса



Демонстрация работы сервиса



Демонстрация работы сервиса



Демонстрация адаптивного интерфейса