Автор:
Сулима Дмитро Олександрович,
студент 41 ПІ групи
Науковий керівник:
Франчук Василь Михайлович,
кандидат педагогічних наук,
професор кафедри комп'ютерної інженерії та освітніх вимірювань

СИСТЕМА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ФАКУЛЬТЕТУ. БЕЗПЕКА ДАНИХ

Анотація. Метою дослідження є забезпечення безпеки даних користувача для web-орієнтованої системи електронного документообігу в межах навчального підрозділу університету, а саме факультету. Завданням дослідження є порівняння та вибір підходів забезпечення безпеки даних, що підвищує захист даних в системі. Об'єктом дослідження є методи забезпечення захисту даних. У дослідженні використано метод інтерв'ювання та роботи з документацією. Дослідження проводиться з метою покращення безпеки в системі електронного документообігу(СЕД) факультету.

Ключові слова: система електронного документообігу, web-орієнтовані технології, документообіг, робота факультету, хмарні технології, безпека даних, безпека сайтів, забезпечення безпеки.

Вступ. Дуже важливою частиною будь-якого багатокористувацького проекту є безпека. Безпека включає в себе організаційну та інформаційну частини. Використання організаційної частини відповідає за те, щоб користувача наперед проінструктували щодо правил безпеки на підприємстві, при роботі з комп'ютером тощо. Під інформаційною безпекою розуміється захищеність даних в системі, тобто технічна реалізація методів захисту. Потреба в оптимальному методі захисту даних в СЕД факультету, призвела до дослідження існуючих підходів для забезпечення інформаційної безпеки.

Постановка задачі. Визначення оптимального набору методів захисту даних в СЕД факультету. Методи повинні мінімально впливати на продуктивність системи та перекривати максимальну кількість вразливостей (в тому числі й потенційних).

Для вирішення цієї проблеми потрібно визначити вразливості СЕД факультету та об'єднати їх у групи (наприклад, група пов'язана з введенням даних користувачем). На основі створених груп визначити набір методів, які можуть виправити вразливість.

Метою дослідження є визначення оптимального набору методів забезпечення інформаційної безпеки в СЕД факультету.

Основна частина. Користувач працює з системою за допомогою web-інтерфейсу, який складається з полів вводу та можливістю роботи с Google Drive. Оскільки СЕД факультету повністю встановлюється в каталог на Google Drive, то користувачі можуть побачити структуру та модифікувати її. Таким чином, можна виокремити вразливості пов'язані з даними, що вводить користувач та доступ до даних, які має користувач.

Оскільки система працює на платформі Google Cloud, щоб модифікувати вихідний код системи необхідно отримати доступ до Google-аккаунту розробника. Але є можливість отримати доступ до коду, призначеного для клієнтської частини системи. Зазвичай це JavaScript-файли, в яких прописано перевірки простих помилок користувача, наприклад, не заповнено необхідні поля вводу.

З перерахованих вразливостей можна виокремити дві групи, пов'язаних з введенням даних та доступом до певних частин системи (структура системи та код клієнтської частини).

Проблему введення даних можна вирішити за допомогою додаткових перевірок полів вводу на стороні клієнта та сервера. Але велика кількість перевірок може призвести до зниження продуктивності системи, та зі сторони клієнта можна вимкнути виконання скриптів (але після цього система не повинна функціонувати). Тому найкращим підходом в

такій ситуації буде те, щоб залишити найпростіші перевірки (наприклад, заповнення необхідних полів вводу), а перевірки конкретних даних проводити на сервері.

Для вирішення проблеми доступу до коду клієнтської частини, в коді необхідно залишити тільки функції пов'язані з візуальними ефектами, оповіщення, очищення та збір необхідних даних з полів вводу. Опрацювання даних необхідно повністю перенести на сторону сервера. Організувати взаємодію з сервером за допомогою асинхронних викликів.

Щоб виправити вразливість пов'язану з доступом та можливістю модифікування структури системи, необхідно змінити підхід до зберігання даних (від налаштувань системи до особистих даних користувача). Замість збереження всіх даних в файлах на Google Drive, необхідно створити нормалізовану базу даних (БД). Використання нормалізованої БД, може суттєво підвищити швидкодію системи, оскільки в більшості СУБД використовуються внутрішні механізми безпеки та з SQL-запитами легше працювати, чим з файлами. Але виникає питання забезпечення підключення до БД без відома для користувача, тобто необхідно приховати IP-адресу сервера БД та пароль до неї. Але оскільки ці відомості текстові та мають невеликий обсяг, їх можна зашифрувати.

Якщо використовувати для збереження даних MySQL на окремому локальному сервері виникає потреба в окремому налаштуванні параметрів безпеки сервера (наприклад, порти), та при достатньо високому рівню навантаження сервер може не відповідати на запити.

Google Cloud Platform включає в себе CloudSQL, який підтримує роботу з MySQL та PostgreSQL в хмарному середовищі. Тому можна використовувати CloudSQL, MySQL як звичайну базу даних але на серверах компанії Google, та питання захисту серверів не залежить від розробника СЕД факультету. Але ця послуга є платною, тому в цьому разі система стає умовно-безкоштовною. Ще варто враховувати можливість технічних робіт на серверах Google, які можуть призвести до того, що системи не буде відповідати.

Висновки. З досліджених вразливостей СЕД виокремлено дві групи, пов'язаних з введенням даних та доступом до певних частин системи (структура системи та код клієнтської частини). В оптимальний набір методів захисту даних в СЕД факультету було визначено:

1. На стороні клієнта залишити найпростіші перевірки (наприклад, заповнення необхідних полів вводу), функції пов'язані з візуальними ефектами, оповіщення, очищення та збір необхідних даних з полів вводу, опрацювання та перевірки конкретних даних проводити на сервері.
2. Запити до сервера виконувати за допомогою асинхронних викликів.
3. Замість зберігання даних в файлах на Google Drive, необхідно створити нормалізовану базу даних (БД). Вибір СУБД залежить від конкретних вимог.

Список використаних джерел

1. Document automation [Electronic resource] / en.wikipedia.org. – 2017. – Mode of access : https://en.wikipedia.org/wiki/Document_automation.
2. Захист інформаційних ресурсів / Василь Франчук. - К.:Редакції газет природничо-математичного циклу, 2012. - 112 с. - (Бібліотека «Шкільного світу»).
3. Франчук В.М. Використання хмарних технологій у ВНЗ. Служби Google// Хмарні технології в освіті : матеріали Всеукраїнського науково-методичного Інтернет-семінару (Кривий Ріг – Київ – Черкаси – Харків, 21 грудня 2012 р.). – Кривий Ріг : Видавничий відділ КМІ, 2012. – С. 99-100