Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики.

Лабораторная работа №1

«Разграничение прав доступа к веб ресурсу»

Санкт-Петербург

2018

**Цель работы:** Изучение методов разграничения доступа на примере выданного веб приложения.

**Задание.** Выполнить усовершенствование системы разграничения доступа веб-приложения, в которую входят схема авторизации, алгоритмы управления сессиями, подсистема разграничения доступа на сервере и в базе данных.

**Порядок выполнения работы:**

* Залить выданные исходники на бесплатный хостинг (например, beget.ru) или поднять собственный web сервер и настроить необходимое для выполнения лабораторной работы взаимодействие сервера с базой данных;
* Импортировать выданный архив базы данных (функция авторизация в БД находится в файле initialization.php);
* Выделить недостатки и уязвимости в системе разграничения доступа веб приложения;
* Усовершенствовать веб приложение. Предлагаются следующие задания:
  + Задание 1. Модификация формы авторизации:
    - Проверки на уязвимые пароли (короткие, словарные, совпадающие с логином, заранее установленные значения);
    - Защита от брутфорса аккаунтов (ограничение попыток входа, блокирование аккаунта, система восстановления, капча);
    - Перехват данных процесса аутентификации, передаваемых на сервер (подбор хешей для паролей, перехват логина).
  + Задание 2. Управление сессиями
    - Уязвимости генерации токена для сессии
    - Время жизни сессии
    - Перехват данных сессии
    - Система управления сессиями (ведение базы данных соединений)
  + Задание 3. Разграничение доступа между аккаунтами пользователей:
    - Усовершенствовать/изменить права доступа, реализованные в веб приложении. Добавить возможность регулировать права на удаление, изменение, вставку данных.
    - Добавить новых пользователей с отличными от существующих группами прав
    - Реализация мандатной системы разграничения доступа.

**Структура отчета:**

* Титульный лист;
* Цель работы, выбранное задание;
* Порядок выполнения работы с обязательным указанием внесенных изменений в исходный код веб приложения;
* Скриншоты, демонстрирующие внесенные усовершенствования и модификации.

*Примечание:* если модификации реализованы на языке программирования, интеграция которого в выданное веб приложение затруднена или невозможна, то вместо скриншотов в отчет включается словесное описание изменений в поведении веб-приложения, которые ожидаются при успешном внедрении предлагаемых усовершенствований.

**Отправка отчета**

Отчеты высылаются на почту [serg.tvc@gmail.com](mailto:serg.tvc@gmail.com). Название файла отчета должно обязательно содержать фамилию исполнителя. В теме письма обязательно указание краткого названия предмета, номера группы, и номера лабораторной. Фильтры для тем представлены ниже:

* где «название предмета»=ЗИВИ or ЗИвИ or ZIVI or Защита информации в Интернет
* где «номер группы»=3350 or n3350 or N3350 or P3350 or p3350
* где «номер лабы»= Лаб1 or ЛР1 or лр1 or Лаб№1 or ЛР№1

Для формирования темы письма рекомендуется использовать формулировки из приведенных фильтров.