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

Лабораторная работа №2

«Уязвимости GFI и LFI»

Санкт-Петербург

2018

**Цель работы:** Изучить уязвимости типа GFI и LFI.

**Задание.** Выполнить усовершенствование веб-приложения с целью закрыть выявленные уязвимости типа GFI и LFI.

**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);
* Найти уязвимости типа PHP-инъекция, которые позволяют выполнить глобальное и локальное подключение файлов;
* Продемонстрировать пути эксплуатации найденных уязвимостей:
  + GFI
    - Выполнить попытку подключения внешнего ресурса
    - Выполнить попытку удаленного подключения shell-кода (2-3 действия с shell кодом по выбору)
  + LFI
    - Подключение локального текстового файла
    - Подключаем локальный файл с внедренным shell кодом (2-3 действия с shell кодом по выбору)
* Усовершенствовать веб приложение, продемонстрировать, что ранее выявленные уязвимости закрыты.

**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.