УНИВЕРСИТЕТ ИТМО

Факультет Информационных Технологий и Программирования

Кафедра Информационных Систем

**Лабораторная работа №6.**

**Защита интернет-ресурсов от распространенных атак**

Информационная безопасность

Выполнили: Ратникова А.М., гр. М3300

Синкевич Е.В., гр. М3300

Санкт-Петербург

2017

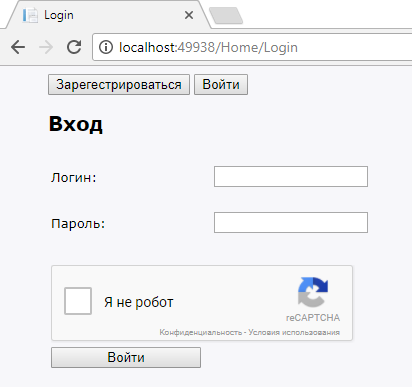
Рассматриваемые вопросы:

* Распространенные уязвимости в интернет-ресурсах.
* Методы защиты от распространенных видов атак.

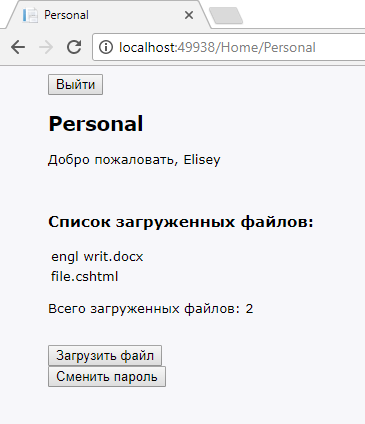
Лабораторная работа была выполнена с помощью технологии **Microsoft** **ASP.NET MVC 5** (язык программирования C#) с использованием базы данных **MySQL**.

Задание на лабораторную работу:

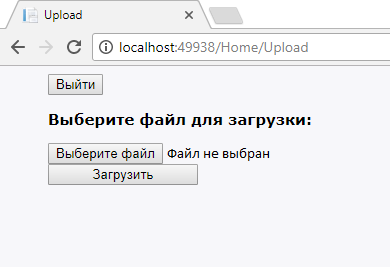
1. Разработать интернет-ресурс, состоящий из:
   * Страницы входа в систему.



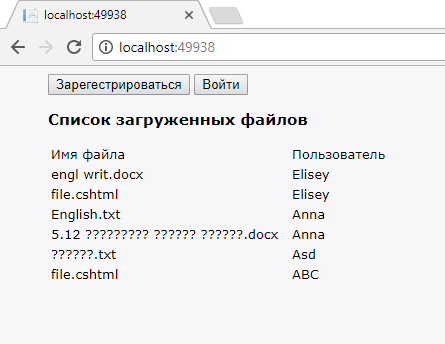
* + Страницы профиля пользователя.



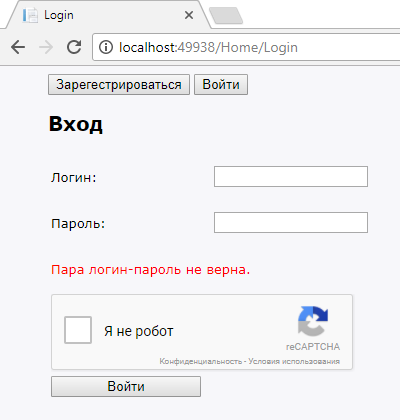
* + Страницы загрузки файла на сервер.



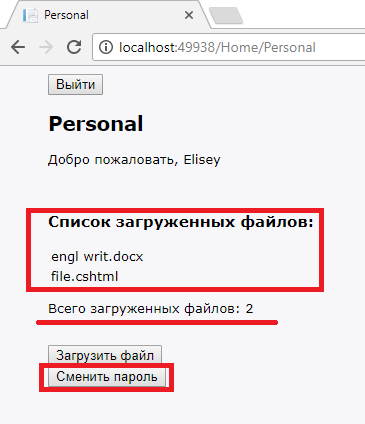
* + Страницы, содержащей список всех загруженных на сервер файлов.



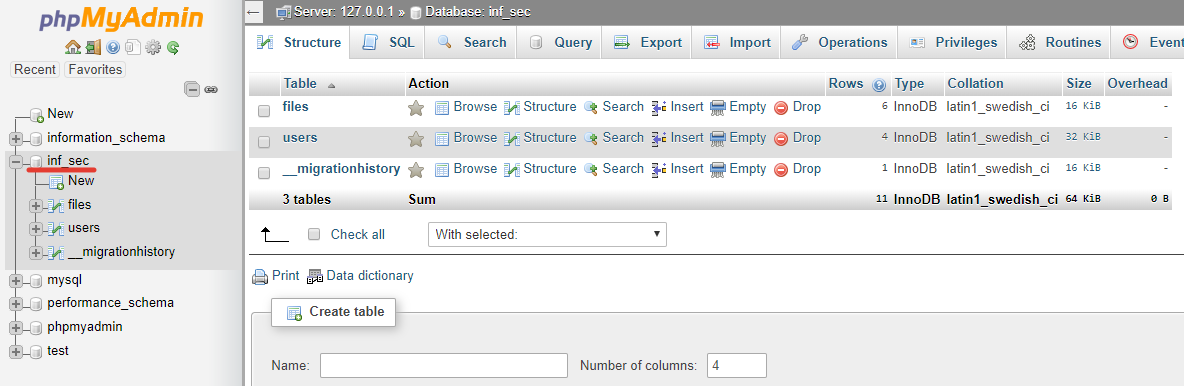
1. Вход на ресурс должен осуществляться только после удачной авторизации посредством ввода пары "логин-пароль".



1. Страница профиля должна отображать список всех, загруженных пользователем, файлов, их количество, а также поле для смены пароля.

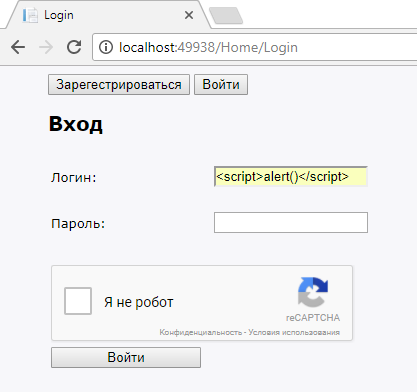


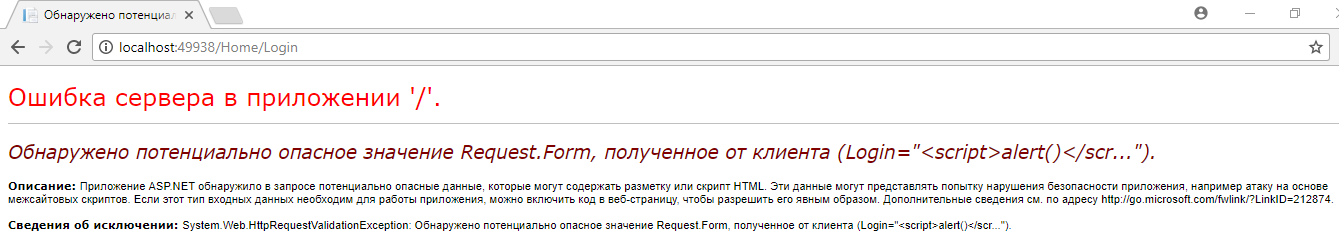
1. Ресурс должен использовать СУБД MySQL.



1. Ресурс должен быть защищен от распространенных видов атак, таких как:
   * XSS (Cross Site Scripting)

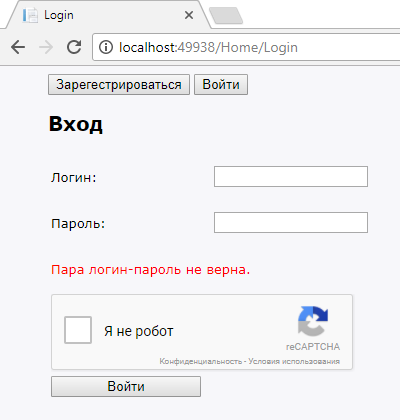
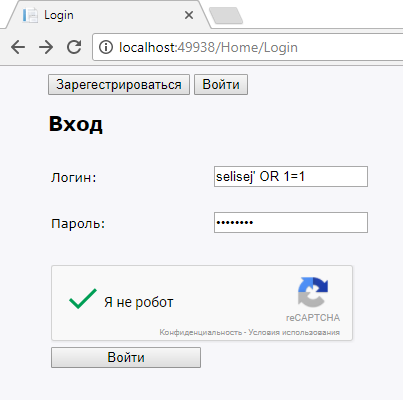
Платформа ASP.NET предоставляет разработчику базовые механизмы защиты от XSS. В частности, при попытке ввести вредоносный код в поле ввода, генерируется исключение, которое может быть обработано в коде пользователя.





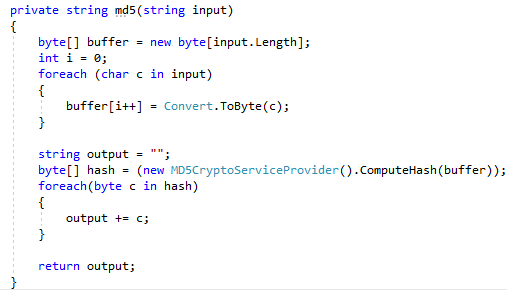
* + SQL инъекция (SQL Injection)

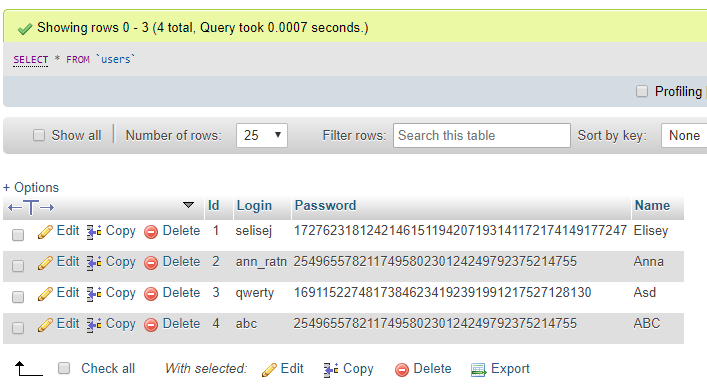
Платформа ASP.NET предоставляет разработчику базовые механизмы защиты от SQL инъекций. Все значения, передаваемые с сервера/на сервер, параметризуются и не могут быть внедрены в код, так как представляют собой строки.



* + Утечка информации (Information Leakage)

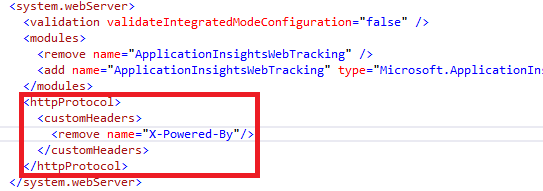
Для защиты от утечки информации все пароли пользователей хранятся в базе данных в виде хэша. Для хэширования паролей в приложении используется алгоритм MD5.



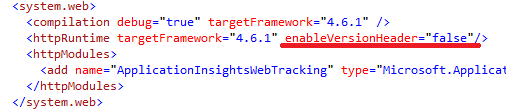


Для защиты данных о сервере, его конфигурации, версии платформы и т.д. выполнены следующие действия:

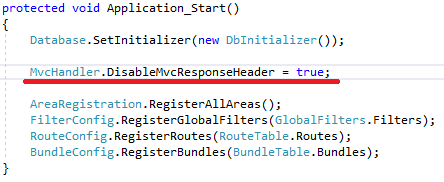
* Удален заголовок X-Powered-By



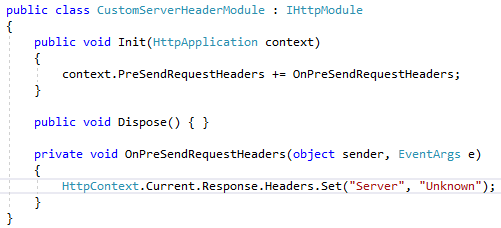
* Удалена версия ASP.NET

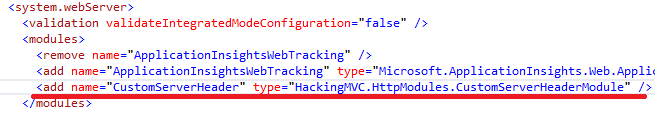


* Удалена версия MVC



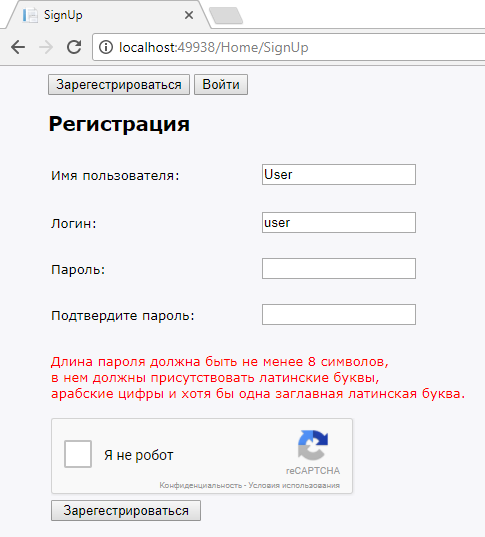
* Удалена информация о сервере





* + Brute Force

Для защиты от подбора пароля наложены условия на длину и состав пароля, а также в форму входа на ресурс добавлена система Google ReCAPTCHA.



* + DoS-атака

Для защиты от DoS на страницу входа в систему добавлена система Google ReCAPTCHA.