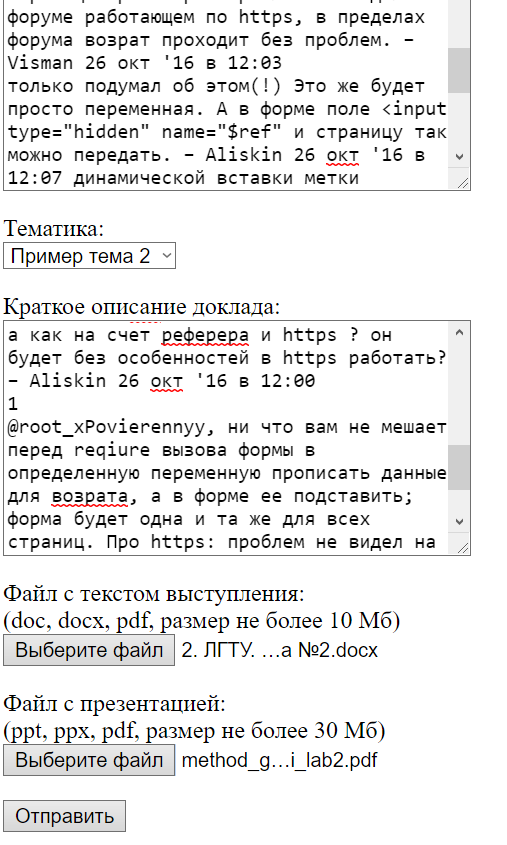
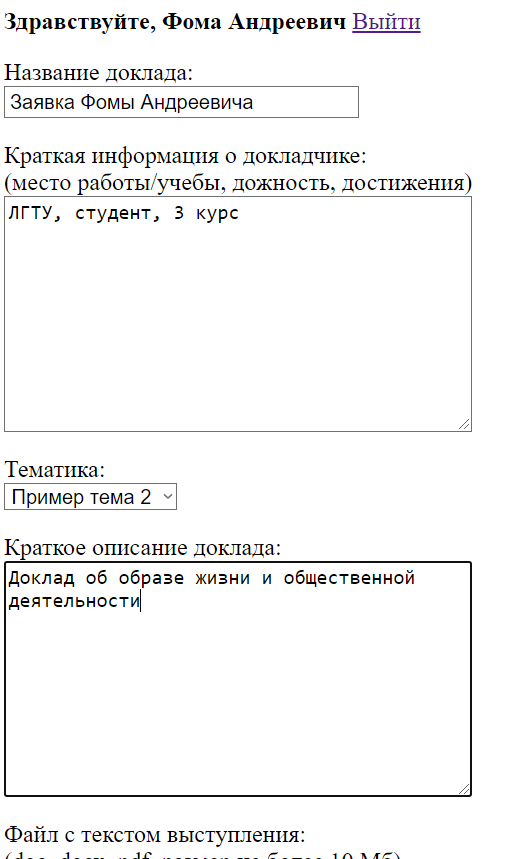
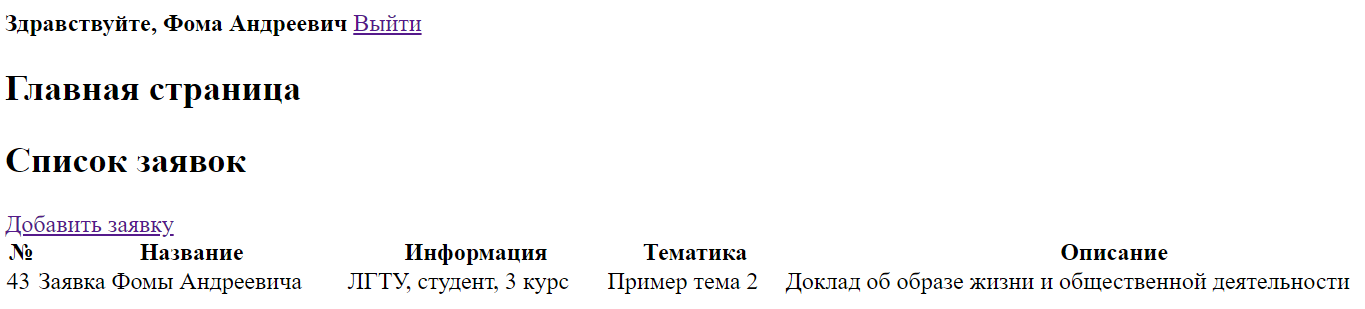
# 





# Лабораторная работа №2. Разработка веб-приложения на PHP. Авторизация. Загрузка файлов

Разработать веб-сайт в соответствии со своим вариантом.

### Требуемый функционал:

* авторизация и регистрация
* хранение записей в БД, вывод списка записей и детальной страницы записи
* отправка формы, валидация введенных значений, сохранение данных в БД
* загрузка файлов через форму
* реализация разных уровней доступа

Для визуального оформления можно использовать bootstrap или собственную верстку.

### Критерии проверки:

* аккуратный внешний вид сайта
* отсутствие ошибок проектирования БД
* отсутствие уязвимостей типа “sql-инъекция”
* безопасное хранение паролей в БД
* в закрытый раздел невозможно попасть без авторизации
* через форму невозможно загрузить вредоносный файл
* через форму нельзя отправить невалидные значения
* оптимальная работа с БД (нет запросов в цикле, не выбираются лишние данные)
* код оформлен по стандарту PSR-12
* у кода понятная структура, отсутствуют логические ошибки

### Рекомендации по выполнению для студентов

Общие рекомендации

<https://gist.github.com/daria-popova/db8b6738eaa766fd12ba775ffb60ef66>

\* Не обязательно, но будет плюсом - разобраться с библиотеками composer, использовать их в проекте.

<https://gist.github.com/daria-popova/1e9d7bc0606cea0b32bbc9235eefd708>

### Лекции по PHP

<https://github.com/intaro/php-course>

### Дополнительные материалы:

* [официальная документация](https://www.php.net/manual/ru/langref.php)
* [ошибки и исключения](https://anton.shevchuk.name/php/php-for-beginners-error-handling/)
* [PHP основы ООП](http://www.php.su/php/intro/?11)
* [работа с файлами](https://www.internet-technologies.ru/articles/rabota-s-faylami-na-php-otkrytie-zapis-chtenie.html)
* [куки и сессии](https://webformyself.com/kak-ispolzovat-sessii-v-php/)
* [работа с БД, PDO](https://p0vidl0.info/php-pdo-rabotaem-s-bazami-dannyx-pravilno.html)
* [хеширование паролей](https://www.php.net/manual/ru/faq.passwords.php)
* [регулярные выражения](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%B3%D1%83%D0%BB%D1%8F%D1%80%D0%BD%D1%8B%D0%B5_%D0%B2%D1%8B%D1%80%D0%B0%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F)
* [работа с регулярными выражениями в PHP](https://www.php.net/manual/ru/function.preg-match.php)
* [регулярные выражения онлайн](https://regex101.com/)
* [чистый код на PHP](https://github.com/peter-gribanov/clean-code-php)
* [стандарт написания кода PSR](https://www.php-fig.org/psr/)
* [SOLID](https://habr.com/ru/post/208442/)
* [безопасность](https://www.owasp.org/images/9/96/OWASP_Top_10-2017-ru.pdf)
* [хорошие практики разработки на PHP](https://phptherightway.com/)
* [инструменты автоматической проверки форматирования](https://github.com/FriendsOfPHP/PHP-CS-Fixer)

### 

### Задания

#### Вариант 1. Студенческий файлообменник

Разработать студенческий файлообменник с учебными материалами по предметам.

**На всех страницах** в шапке сайта для неавторизованных пользователей выводить ссылки на авторизацию и регистрацию, для авторизованных - приветствие, кнопку “Выход” и ссылку на добавление поста.

**На главной странице** выводятся посты, отсортированные по дате добавления.

У каждого поста выводится название (ссылка на страницу поста), дата добавления, имя автора.

**На странице поста** выводится информация о посте:

* название
* дата добавления
* текст описания
* имя автора
* список прикрепленных файлов (ссылки на скачивание)

**На странице добавления поста** располагается форма с полями

* название
* описание
* файлы (множественное поле. Допустимы файлы типов: zip, doc, docx, xls, xlsx, pdf, jpg, png)

Все поля обязательные. Если какие-то из введенных значений невалидны, сохранения в БД не происходит, на форме выводятся сообщения об ошибках. Заполненные пользователем текстовые поля не сбрасываются.

После успешной отправки выполнять редирект на страницу созданного поста.

Страница доступна только авторизованным пользователи

Реализовать авторизацию и регистрацию (см. раздел [Общие требования к авторизации и регистрации](#_7zn5kn76iye0))

#### Вариант 2. Сайт с обзорами фильмов

Разработать сайт с обзорами фильмов. Пользователи с правами модератора могут добавлять новые обзоры, прикреплять постер и ссылку на трейлер, добавлять текст отзыва.

Пользователи могут регистрироваться на сайте и оставлять комментарии к обзорам.

**На всех страницах** в шапке сайта для неавторизованных пользователей выводить ссылки на авторизацию и регистрацию, для авторизованных - приветствие и кнопку “Выход”. Если пользователь имеет права модератора, то дополнительно выводить ссылку на добавление обзора.

**На главной странице** выводятся обзоры, отсортированные по дате добавления.

У каждого обзора выводится картинка постера, название (ссылка на страницу поста), дата добавления, имя автора.

**На странице обзора** выводится:

* название фильма
* постер
* трейлер (встроенное видео с youtube.com)
* дата добавления
* текст обзора
* имя автора
* список комментариев пользователей, отсортированных по дате добавления
* форма “Добавить комментарий” (текстовое поле и кнопка “Отправить”)

**На странице добавления обзора** располагается форма с полями

* название фильма (обязательное)
* текст обзора (обязательное)
* файл с постером (обязательное)
* ссылка на трейлер (необязательное)

Если какие-то из обязательных полей не заполнены, сохранения в БД не происходит, на форме выводятся сообщения об ошибках. Заполненные пользователем текстовые поля не сбрасываются.

Форма доступна только авторизованным пользователям с правами модератора.

После успешной отправки выполнять редирект на страницу созданного поста.

Реализовать **авторизацию и регистрацию** (см. раздел [Общие требования к авторизации и регистрации](#_7zn5kn76iye0))

#### Вариант 3. Фотогалерея

Пользователь может зарегистрироваться и загрузить галерею фотографий.

Можно просматривать чужие галереи, ставить оценки фотографиям.

**На всех страницах** в шапке сайта для неавторизованных пользователей выводить ссылки на авторизацию и регистрацию, для авторизованных - приветствие, кнопку “Выход” и ссылку на страницу профиля.

**Список фотографий** выглядит следующим образом:

Каждая запись содержит

* фото
* описание
* ссылку на страницу профиля автора
* количество оценок
* рейтинг (средняя оценка)

Если пользователь авторизован, рядом с каждой записью выводится **форма оценки** (селект со значениями от 1 до 5 и кнопка “Оценить”). Фотографию можно оценить только один раз, свои фотографии оценивать нельзя.

Необходимо подключить удобный просмотрщик фотографий (например, lightbox).

**На главной странице** выводятся список из 20 последних фотографий (добавленных позже всего).

**На странице профиля пользователя** выводится список фотографий текущего пользователя, отсортированный по дате добавления.

Если это профиль текущего пользователя, то также выводить ссылку на страницу добавления фото.

**На странице добавления фото** располагается форма с полями

* описание
* файл с фотографией (допустимый формат - jpg, максимальный размер - 3 Мб)

Оба поля обязательные. Если есть какие-то ошибки валидации, сохранения в БД не происходит, на форме выводятся сообщения об ошибках. Заполненные пользователем текстовые поля не сбрасываются.

После успешной отправки выполнять редирект на страницу профиля.

Реализовать **авторизацию и регистрацию** (см. раздел [Общие требования к авторизации и регистрации](#_7zn5kn76iye0))

*\* Не обязательно, но будет плюсом. Реализовать создание уменьшенных копий фотографий. В списках выводить уменьшенные картинки, а в просмотрщике - полноразмерные. При пережатии пропорции должны сохраняться.*

*Можно использовать библиотеку* [*php gd*](https://www.php.net/manual/ru/book.image.php)

#### Вариант 4. Система обработки тикетов

Система позволяет пользователям общаться с технической поддержкой.

Пользователь может зарегистрироваться и создать тикет (сообщение о проблеме + файл скриншота), просматривать ответы на тикет.

Сотрудник техподдержки может отвечать на тикет, менять статус и ответственного, закрывать тикет.

**На всех страницах** в шапке сайта для неавторизованных пользователей выводить ссылки на авторизацию и регистрацию, для авторизованных - приветствие и кнопку “Выход”.

**На главной странице**

Для неавторизованного пользователя выводится информация о системе и предложение зарегистрироваться/войти.

Для авторизованного пользователя без прав сотрудника техподдержки выводится список незакрытых тикетов, созданных им и ссылка на форму создания тикета.

Для сотрудника техподдержки выводится список всех незакрытых тикетов.

**Форма создания тикета** содержит поля:

* Тема (обязательное)
* Описание проблемы (обязательное)
* Скриншот с описанием проблемы (необязательное. Допустимые размеры - jpg, png. Максимальный размер - 5 Мб)

Если есть какие-то ошибки валидации, сохранения в БД не происходит, на форме выводятся сообщения об ошибках. Заполненные пользователем текстовые поля не сбрасываются.

Форма доступна только авторизованным пользователям.

**Список тикетов** выглядит так:

* Тема (ссылка на страницу тикета)
* Статус
* Имя пользователя, создавшего тикет
* Имя сотрудника техподдержки, ответственного за тикет (может быть пустым, если тикет еще не взят в работу)

**На странице тикета** выводится:

* Тема (ссылка на страницу тикета)
* Статус
* Имя пользователя, создавшего тикет
* Имя сотрудника техподдержки, ответственного за тикет (может быть пустым, если тикет еще не взят в работу)
* Описание
* Ссылка на прикрепленный файл (если есть)
* Список сообщений. Для каждого сообщения выводится имя автора, дата и время отправки, текст сообщения. Сообщения отсортированы по дате добавления (от раннего к позднему)
* Форма добавления сообщения (текстовое поле и кнопка “Отправить”)
* Для сотрудника техподдержки выводится ссылка на форму редактирования тикета.

**Форма редактирования тикета** содержит поля:

* ответственный сотрудник (выбор из списка сотрудников техподдержки)
* статус (выпадающий список с вариантами). Список статусов задается в конфиге
* флаг “тикет закрыт”

Форма доступна только сотрудникам техподдержки.

Реализовать **авторизацию и регистрацию** (см. раздел [Общие требования к авторизации и регистрации](#_7zn5kn76iye0))

#### Вариант 5. Сайт конференции

Сайт предназначен для регистрации докладчиков на конференции.

**На всех страницах** в шапке сайта для неавторизованных пользователей выводить ссылки на авторизацию и регистрацию, для авторизованных - приветствие и кнопку “Выход”

**На главной странице**

Для неавторизованного пользователя выводится информация о системе и предложение зарегистрироваться/войти. Ему недоступны просмотр и добавление заявок, в т.к. по прямым ссылкам.

Для авторизованного пользователя без прав администратора выводится список его заявок и ссылка на форму создания заявки.

Для администратора выводится список всех заявок.

**Список заявок** выглядит так:

* Название доклада (ссылка на детальную страницу)
* Имя и email отправителя
* Тематика
* Краткое описание доклада

**Форма добавления заявки** содержит поля:

* Название доклада
* Краткая информация о докладчике (место работы/учебы, должность, достижения)
* Тематика (выбор из списка). Список задается в конфигурационном файле.
* Краткое описание доклада
* Файл с текстом выступления (doc, docx, pdf, размер не более 10 Мб)
* Файл с презентацией (ppt, pptx, pdf, размер не более 30 Мб)

Все поля обязательные. Если какие-то из полей не заполнены, сохранения в БД не происходит, на форме выводятся сообщения об ошибках. Введенные пользователем значения не сбрасываются.

После успешной отправки выполнять редирект на страницу созданной заявки.

**Детальная страница заявки** выглядит так:

* Название доклада
* Краткая информация о докладчике
* Тематика
* Краткое описание доклада
* Ссылка на прикрепленные файлы

Реализовать **авторизацию и регистрацию** (см. раздел [Общие требования к авторизации и регистрации](#_7zn5kn76iye0))

#### Общие требования к авторизации и регистрации

**На странице регистрации** располагается форма с полями

* имя (допустимы только русские буквы, пробелы и дефисы)
* email (можно вводить только корректный email)
* пароль (минимальная длина - 6 символов, не может состоять только из цифр)
* повтор пароля (введенное значение должно совпадать с паролем)
* флаг согласия на обработку персональных данных.

Все поля обязательные. Если какие-то из введенных значений невалидны, сохранения в БД не происходит, на форме выводятся сообщения об ошибках, введенные ранее значения сохраняются.

После успешной отправки авторизовывать пользователя и выполнять редирект на главную страницу.

\* Не обязательно, но будет плюсом: добавить проверку, что пароль не является скомпрометированным <https://symfony.com/doc/current/reference/constraints/NotCompromisedPassword.html>

\* для проверки полей можно использовать регулярные выражения

**На странице авторизации** располагается форма входа с полями

* email
* пароль

При отправке формы проверяется, что пользователь с таким email найден в базе и хеш пароля совпадает с хешем, хранящимся в базе.

Если проверка не прошла, выводим сообщение об ошибке.

Если данные верные, авторизуем пользователя и делаем редирект на главную страницу.