1. Защита от XSS (Cross-Site Scripting)

В формах отображения данных использована функция htmlspecialchars. Это исключает возможность внедрения JavaScript-кода со стороны пользователя. Пример применения: .

2. Защита от Information Disclosure

При ошибке подключения к базе данных в config.php выводится нейтральное сообщение. Подробности ошибки логируются в error_log(). Это предотвращает раскрытие конфигурации сервера.

3. Защита от SQL Injection

Все SQL-запросы выполняются через PDO с использованием prepare + execute. Данные пользователей не подставляются напрямую в запрос. Пример: $stmt = $pdo->prepare('SELECT * FROM users WHERE login = ?');

4. Защита от CSRF (Cross-Site Request Forgery)

В POST-формы добавлен токен CSRF, который сохраняется в сессии. Перед выполнением запроса происходит его проверка. Таким образом предотвращается отправка формы с внешнего сайта.

5. Защита от Include / Upload

Функции include/require не принимают пользовательский ввод. Загрузка файлов отсутствует, что исключает соответствующие риски.