Аудит безопасности

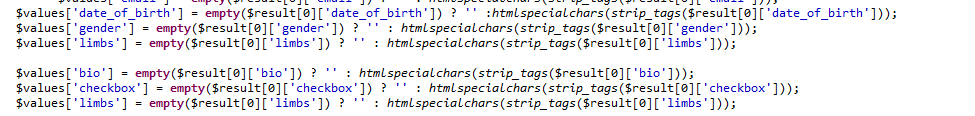
1. **XSS:**

это уязвимость системы безопасности, которая позволяет злоумышленнику размещать клиентские скрипты (обычно JavaScript) на веб-страницах. Для защиты данные, введённые пользователем, проходят валидацию данных при помощи регулярного выражения.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Также данные проходят фильтрацию.



1. **SQL INJECTION:**

Изменение SQL запроса. Для защиты используются подготовленные запросы.



1. **CSRF:**

Атака на сайт, при которой браузер заставляют выполнять действия от имени пользователя (отправка сообщений, смена паролей). Был добавлен скрытый input, содержащий в себе токен. Во время генерации токен помещается сессию, после отправки формы происходит сверка данных из сессии с данными, полученными из метода POST, если они не совпадают, то произойдёт перенаправление на страницу с ошибкой 405. Поскольку CSRF представляет опасность только для авторизованных в систему пользователей, токен будем использовать только в этом случае.

Изображение выглядит как текст, Шрифт, снимок экрана, линия

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

1. **Include:**

Вставка нежелательных данных в качестве параметров функции include. В работе не используются динамические include функции, которые могут менять подключаемые файлы.

1. **Upload:**

Возникают, когда веб-сервер позволяет пользователям загружать файлы в свою файловую систему без достаточной проверки таких параметров, как их имя, тип, содержимое или размер. В работе не используются функции загрузки файлов.