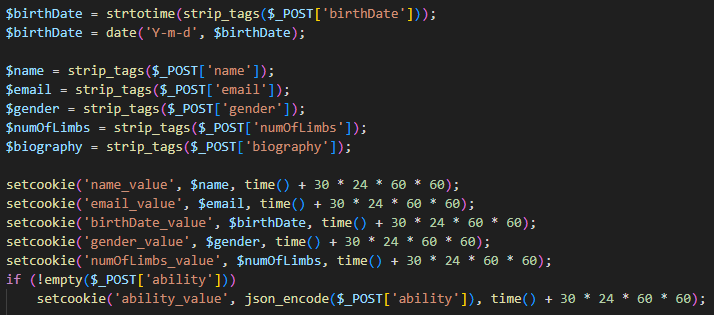
**Отчёт о безопасности**

**Защита от XSS** **(Cross-Site Scripting)**

Это тип атаки, при которой злоумышленник внедряет вредоносный скрипт в веб-страницу или приложение, которые затем выполняются на стороне клиента.

strip\_tags() в PHP используется для удаления HTML и PHP тегов из строки, используется при выводе пользовательского ввода из формы. Это помогает предотвратить внедрение HTML-кода



**Защита от SQL Injection**

Это вид атаки, при котором злоумышленник пытается внедрить злонамеренный SQL-код в запросы к базе данных.

Чтобы избежать SQL-инъекций, используются параметризованные запросы и подготовленных выражения ->prepare() и ->execute() для выполнения запросов к базе данных для корректной обработки параметров запроса

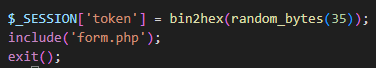


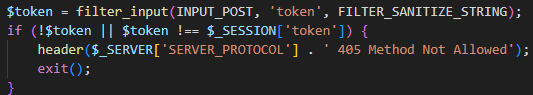


**Защита от CSRF** **(Cross-Site Request Forgery)**

Это вид атаки, при которой злоумышленник заставляет авторизованного пользователя совершить нежелательные действия на веб-сайте, к которому у пользователя есть доступ.

Чтобы предотвратить такие атаки, генерируется токен в сессии и проверяется его наличие и соответствие при обработке запросов. Так сервер понимает, что запрос был отправлен именно от меня





**Защита от Include и Upload уязвимости**

Уязвимость "Include" возникает, когда веб-приложение использует ненадежные или некорректно проверенные данные, например, пользовательский ввод, для формирования пути к файлам, которые должны быть включены в исполняемый код. Злоумышленник может внедрить злонамеренный код или получить доступ к конфиденциальным файлам на сервере.

Уязвимость "Upload" возникает, когда веб-приложение позволяет пользователям загружать файлы на сервер без должной проверки и контроля. Это может привести к загрузке вредоносных файлов, которые могут выполняться на сервере или быть доступными для скачивания другими пользователями.

Указывается путь к файлу в операторе include() вручную мы предотвратить включение нежелательных файлов

С уязвимостью "Upload" в нашей работе мы не сталкиваемся



.