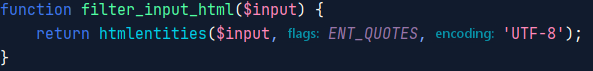
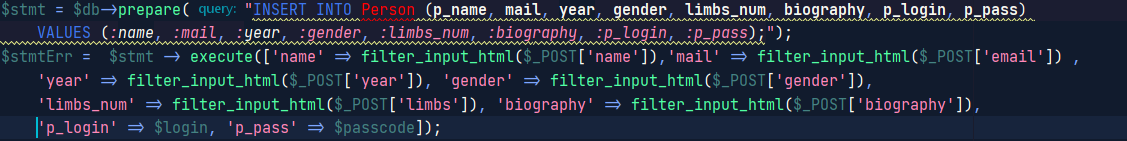
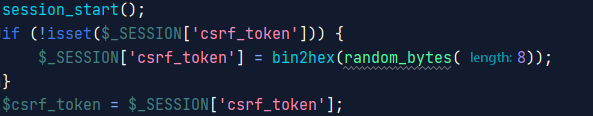
1. XSS (межсайтовый скриптинг) - защита от вставки вредоносного кода в веб-страницы, которые могут быть использованы для кражи данных пользователя. Для защиты от XSS рекомендуется использовать фильтрацию входных данных. Пример кода:

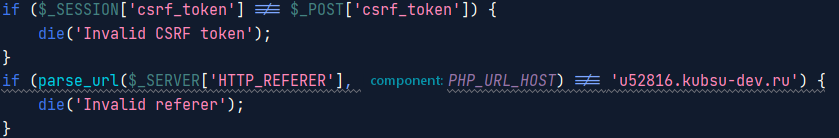


2. SQL Injection - защита от вставки вредоносного SQL-кода в запросы к базе данных, который может привести к краже данных пользователя. Для защиты от SQL Injection рекомендуется использовать подготовленные запросы и фильтрацию входных данных. Пример кода:

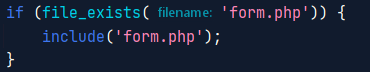


3. CSRF (межсайтовая подделка запроса) - защита от подделки запросов, которые отправляются с других сайтов и могут привести к изменению данных пользователя. Для защиты от CSRF рекомендуется использовать токены CSRF и проверку referer. Пример кода:





4. Include - защита от включения вредоносного кода из внешних файлов, которые могут привести к краже данных пользователя. Для защиты от Include рекомендуется использовать только относительные пути и проверку наличия файла. Пример кода:



5. Upload - защита от загрузки вредоносных файлов на сервер, которые могут привести к краже данных пользователя. Для защиты от Upload рекомендуется проверять тип и размер загружаемого файла, а также использовать уникальные имена файлов. В задании не требуется заливать файлы на сервер, поэтому приведу абстрактный пример. Пример кода:

// Проверка типа и размера файла

if ($\_FILES['file']['type'] !== 'image/jpeg' || $\_FILES['file']['size'] > 1000000) { die('Invalid file type or size');

}

// Генерация уникального имени файла

$filename = uniqid() . '.jpg';

move\_uploaded\_file($\_FILES['file']['tmp\_name'], 'uploads/' . $filename);