Отчет

XSS (межсайтовый скриптинг) возникает, если программа принимает информацию, которую затем отображает без должного контроля и фильтрации.

Плохой код

Изображение выглядит как текст, Шрифт, линия, белый

Автоматически созданное описание

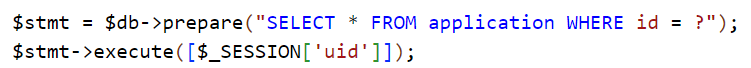
Исправленный код

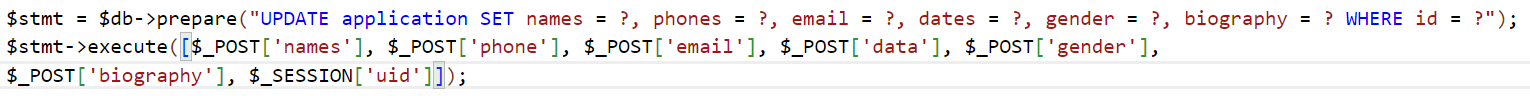
Изображение выглядит как текст, Шрифт, линия, снимок экрана

Автоматически созданное описание

Information Disclosure уязвимости возникают тогда, когда система допускает разглашение конфиденциальных данных, которые могут быть использованы злоумышленниками для вредоносных целей. В данном коде не обнаружено конкретных случаев утечки информации.

SQL Injection уязвимости возникают, если приложение допускает внедрение произвольного SQL-кода в запросы к базе данных через пользовательский ввод. Данный код безопасен от таких угроз, поскольку использует подготовленные запросы.





Уязвимости CSRF (межсайтовое подделывание запросов) позволяют злоумышленнику вынудить пользователя совершить нежелательные действия на веб-сайте, где он авторизован. В начальной версии моего кода отсутствовала защита от таких атак, поэтому было решено внедрить CSRF-токены в формы.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, линия, снимок экрана

Автоматически созданное описание

Уязвимости, связанные с include, возникают, когда приложение подключает внешние файлы без должной проверки, что может позволить злоумышленнику загрузить произвольные файлы. Для устранения данной уязвимости в моем коде было внесено следующее изменение:

Изображение выглядит как текст, Шрифт, снимок экрана, линия

Автоматически созданное описание

Функциональность Upload, которая может создать уязвимость, возникает, когда злоумышленник может загрузить свой собственный файл на сервер через определенный механизм загрузки файлов. Однако в этом коде нет возможности для пользователя загружать файлы на сервер, что исключает вероятность такой атаки.