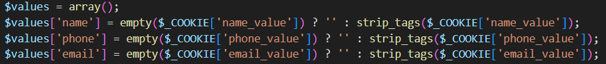
**ОТЧЕТ**

# 1 XSS

XSS - это тип атаки на веб-системы, при которой злоумышленник внедряет вредоносный код на веб-страницу, который будет выполнен на компьютере пользователя при открытии этой страницы. Этот код может взаимодействовать с сервером злоумышленника. XSS является разновидностью атаки "Внедрение кода".  
Изначально, если данные из базы не были обработаны и не были приведены к безопасному формату перед загрузкой в форму, это могло создать уязвимость и открыть возможность для проведения XSS-атаки.



Используем strip\_tags() (возвращает строку str, из которой удалены HTML и PHP тэги) для строковых данных и intval() (возвращает целое значение переменной var) для целочисленных:



# 2 SQL-INJECTION

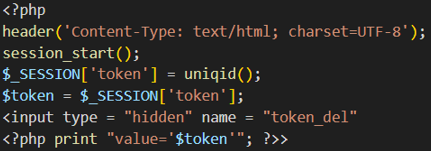
SQL-INJECTION - это один из распространенных способов взлома сайтов и программ, работающих с базами данных, который основан на внедрении в запрос произвольного SQL-кода. Для предотвращения SQL-INJECTION необходимо экранировать символы, поступающие из формы, перед записью в базу данных или использовать подготовленные запросы.

# 

# 3 CSRF

CSRF — вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP.

Защитим важные поля форм, добавив токен, привязанный к сессии пользователя и проверку токена:



# 4 Upload и Include уязвимости

Уязвимости, связанные с функциями include и upload, могут возникать в веб-приложениях из-за неправильного обращения к ним или недостаточной проверки данных, поступающих от пользователей.