Кущ Александр, 23

**ОТЧЕТ ОБ АУДИТЕ**

# 1 Цель работы

Провести аудит безопасности приложения и исправить уязвимости. В нем должны быть разделы, посвященные уязвимостям XSS, SQL Injection, CSRF, Include, Upload. В отчете указать по каждой уязвимости примененные методы защиты с примерами вашего кода.

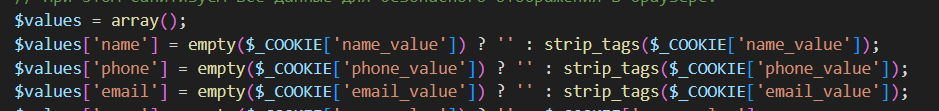
# 2 Защита от XSS

XSS — тип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода (который будет выполнен на компьютере пользователя при открытии им этой страницы) и взаимодействии этого кода с веб-сервером злоумышленника. Является разновидностью атаки «Внедрение кода».

Изначально, при загрузке в форму данные из базы не приводились к безопасному формату и была возможность провести XSS-атаку:



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:



# 3 Защита от SQL-INJECTION

SQL-INJECTION — один из распространённых способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода.

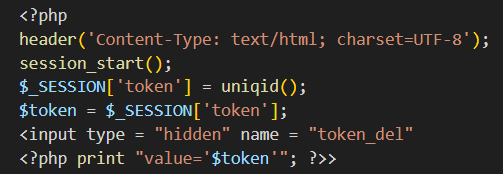
Необходимо экранировать символы, поступающие из формы, записать в базу данных (DBO::quote) или использовать подготовленные запросы:

# 

# 4 Защита от CSRF

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

Защитим важные поля форм, (изменение записи в базе данных и удаление записи) добавив токен, привязанный к сессии пользователя и проверку токена:



# 5 Защита от Upload и Include уязвимости

PHP-include — уязвимость, которая позволяет «принудить» произвольный файл и выполнить PHP код в любом файле на сервере.

Upload уязвимостей нет, т. к. пользователь не загружает на сервер файлы. Include уязвимостей нет, т. к. пользователь не дает данные для подключения модулей обработчиков.

# 6 Вывод

Защитили сайт от различного рода уязвимостей в коде, атак типа внедрения SQL и атак на посетителей веб-сайта. Теперь при загрузке в форму данные из базы приводятся к безопасному формату.