

## Домашнее задание. Урок 8

1. Исследование DVWA. Попробуйте самостоятельно разобраться с интерфейсом DVWA. В разделе Security DVWA переключайте уровни сложности (low, medium, high, impossible) для каждой уязвимости. Обратите внимание, как меняется код страницы при изменении уровня сложности (используйте "View Source" или инструменты разработчика в браузере). Запишите, какие уровни сложности доступны для каждой уязвимости.
2. Задание 2. SQL Injection – базовая проверка. В разделе "SQL Injection" на уровне сложности "low" попробуйте ввести в поле "User ID" следующие значения:
  - 1 (корректный ID)
  - 1' or '1'='1
  - 1' or '1'='2
3. В разделе "XSS (Reflected)" на уровне сложности "low" попробуйте ввести в поле поиска следующий код: `<script>alert("Привет, я XSS!");</script>` Опишите, что произошло. Почему это сработало? Как можно использовать подобную уязвимость во вред пользователям? Исследуйте, как меняется поведение при переключении на уровни сложности "medium" и "high".
4. В разделе "Command Injection" на уровне сложности "low" попробуйте ввести в поле "IP Address" следующие значения:
  - 127.0.0.1 (корректный IP)
  - 127.0.0.1 && ls -l (Linux)Опишите, что происходит в каждом случае. Что делают добавленные команды ls -l и dir? Попробуйте выполнить другие простые команды. Почему это считается уязвимостью?