Отчёта по индивидуальному проекту №5

дисциплина: Информационная безопасность

Кашкин Иван Евгеньевич

Содержание

[Цель работы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab2\Lab_2_report.docx#_Toc177202532)

[Задание](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab2\Lab_2_report.docx#_Toc177202533)

[Теоретическое введение](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab2\Lab_2_report.docx#_Toc177202534)

[Выполнение лабораторной работы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab2\Lab_2_report.docx#_Toc177202535)

[Выводы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab2\Lab_2_report.docx#_Toc177202536)

[Список литературы](file:///C:\Users\MateBook%20D15\Desktop\ИБ\lab2\Lab_2_report.docx#_Toc177202537)

# Цель работы

Целью данной работы является изучение приложения BurpSuite.

# Введение

## Burp Suite

**Burp Suite** – это набор инструментов для тестирования безопасности веб-приложений.

Этот инструмент используется для обнаружения уязвимостей, анализа трафика и

проведения различных атак на веб-приложения, таких как XSS, SQL-инъекции и другие.

## SQL Инъекции

**SQL-инъекции** – это тип уязвимости, который позволяет злоумышленникам выполнять произвольные SQL-запросы в базе данных через приложение. Это может привести к несанкционированному доступу к данным, их модификации или даже удалению.

SQL-инъекция возникает, когда приложение не корректно обрабатывает пользовательский ввод и включает его в SQL-запросы. Злоумышленники могут вставить (инъектировать) свои SQL-коды в вводимые данные, которые затем выполняются базой данных.

# Выполнение проекта

BurpSuite можно использовать для выполнения SQL инъекций. Переходим к примеру атаки SQL-инъекция.

В главном верхнем меню выбираем Proxy, а в подменю, выбираем Intercept (Перехват).

Используя браузер Burp, откроем DVWA, установим средний уровень безопасности и перейдем в раздел SQL-инъекции/

В Burp Suite и включаем перехват, нажав на Intercept is of. В DVWA и нажмем Submit (Отправить).

Если вернуться в Burp Suite, он покажет перехваченные данные.



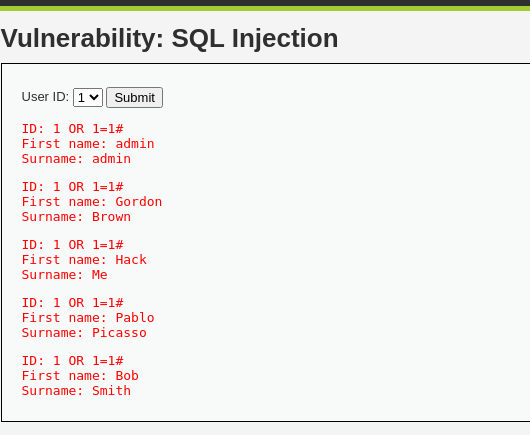
В Burp Suite изменим значение id с 1 на 2, затем нажмем Forward, чтобы посмотреть, что произойдет.

Как видите, в выпадающем списке по-прежнему отображается идентификатор

пользователя 1; однако отображается информация об идентификаторе пользователя 2. Это означает, что Burp Suite смог успешно внедрить новое значение, даже не затрагивая веб-страницы:

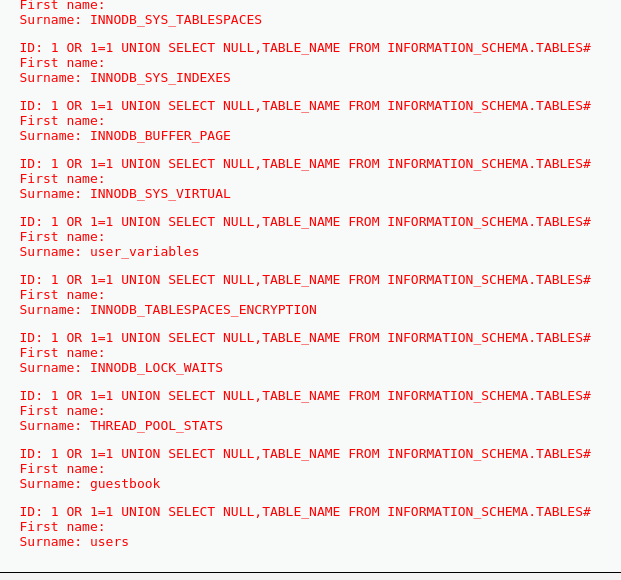
Теперь, когда мы поняли, что можно внедрять данные, давайте попробуем сделать настоящую SQL-инъекцию.







На этот раз мы получили гораздо больше информации, включая имена таблиц. Это очень серьезная уязвимость, поскольку злоумышленник может получить очень важные данные из веб-приложения.



# Вывод

Мы изучили возможности BurpSuite.