Саммари урока 9. Инъекции

Что мы узнали?

На этом уроке мы погрузились в мир веб-уязвимостей и познакомились с тремя основными типами инъекций:

- Command Injection: Уязвимость, позволяющая злоумышленнику выполнять произвольные команды на сервере через уязвимое приложение. Это достигается путем внедрения команд операционной системы в пользовательский ввод.
- SQL Injection: Атака, при которой злоумышленник внедряет SQL-код в запросы к базе данных, что может привести к утечке, изменению или удалению данных.
- Reflected XSS (Cross-Site Scripting): Атака, при которой вредоносный JavaScript код внедряется на веб-страницу через пользовательский ввод и выполняется в браузере жертвы.

Команды:

- знак && позволяет выполнять команды последовательно одну за другой. Например: pwd && ls

Что мы делали на уроке?

- Повторили основные команды CLI (Command Line Interface).
- Изучили принципы работы и примеры Command Injection, SQL Injection и Reflected XSS атак с помощью DVWA (Damn Vulnerable Web Application).
- Обсудили потенциальные последствия этих уязвимостей.
- Рассмотрели базовые команды Linux, которые могут быть использованы при Command Injection.