УЯЗВИМОСТИ

Brute Froce (Грубая сила)

Command injection

File upload

SQL injection

Внедрение кода SQL — это атака, во время которой вредоносный код вставляется в строки, которые позже будут переданы на экземпляр SQL Server для анализа и выполнения. Любая процедура, создающая инструкции SQL, должна рассматриваться на предмет уязвимости к внедрению кода, так как SQL Server выполняет все получаемые синтаксически правильные запросы. Даже параметризованные данные могут стать предметом манипуляций опытного злоумышленника.

SQL injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

CSRF

ПРИМЕР ДЕЙСТВИЙ

Command Injection

File upload

Для начала выберем пункт Command Injection в dvwa (сложность - low) после чего добавим php файл со скриптом и нажмём на кнопку. Файл успешно добавлен теперь можно с ним работать (Рисунок 2).

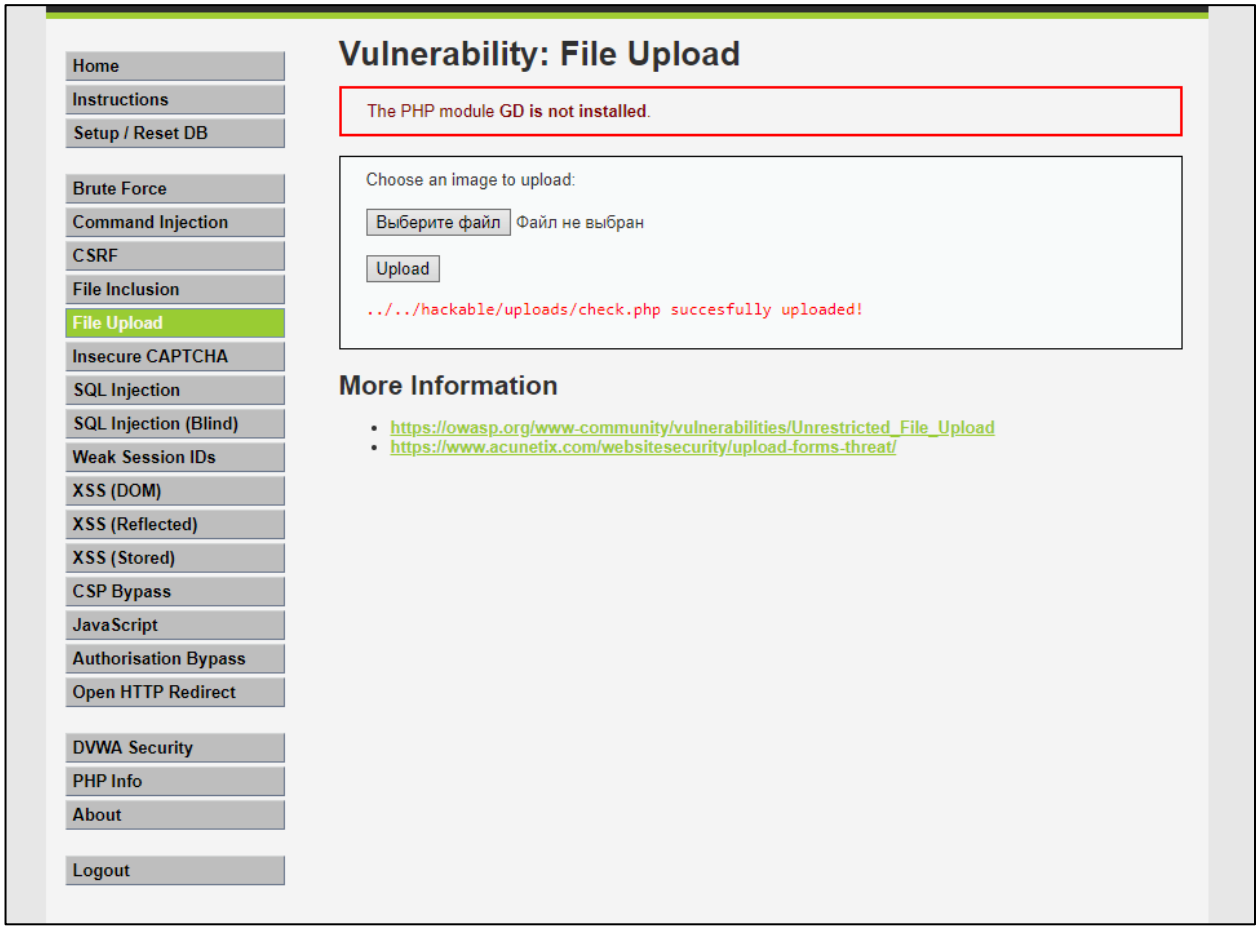

Рисунок 2 - File Upload

SQL injection

Для начала выберем пункт SQL injection в dvwa (сложность - low) после чего напишем в поле ввода строку “ ' OR '1'='1” и получим весь список данных (Рисунок 3).

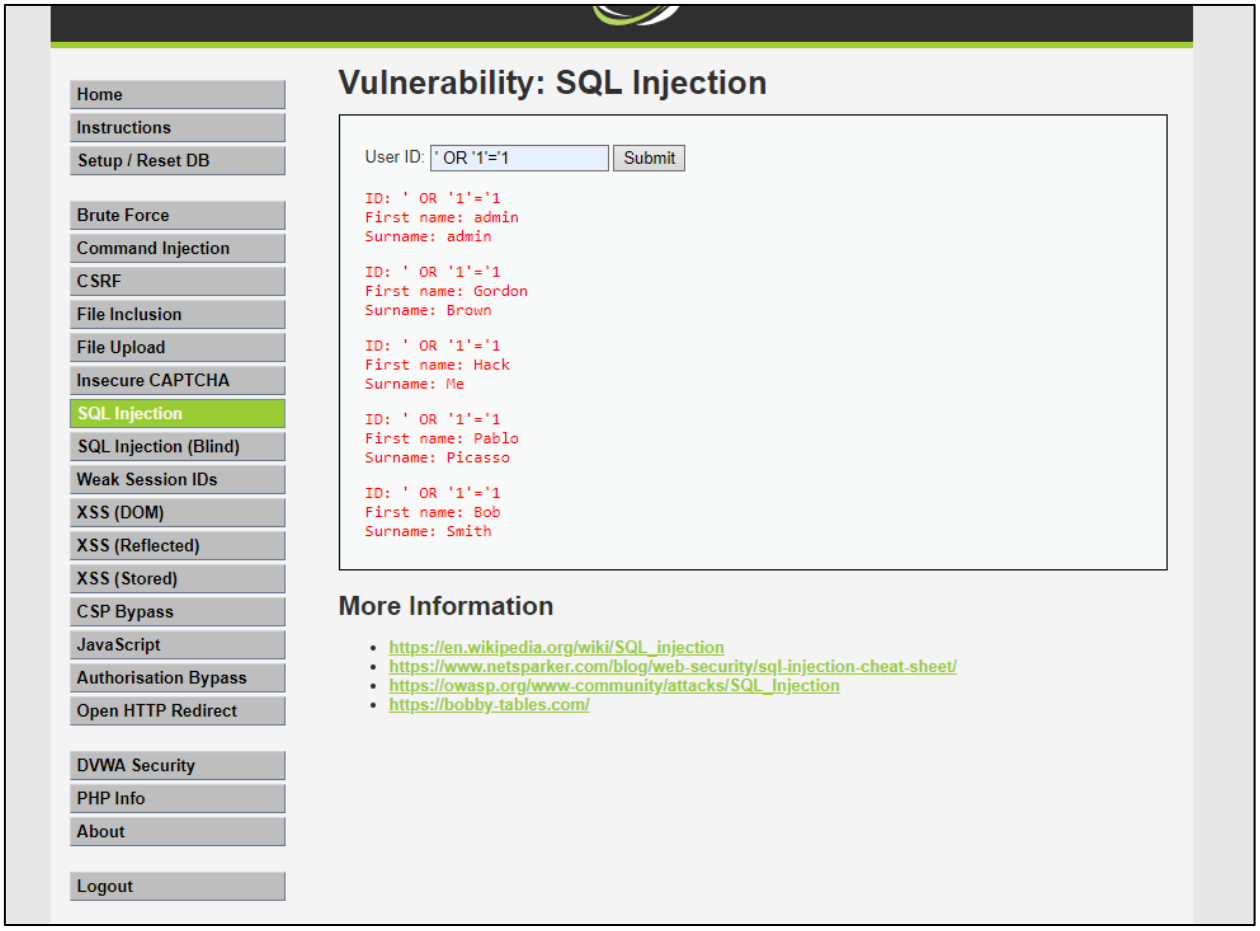

Рисунок 3 - SQL injection

SQL injection (Blind)

Для начала выберем пункт SQL injection (Blind) в dvwa (сложность - low) после чего напишем в поле ввода строку “ ' OR SLEEP (5) #” и получим то, что сайт перестанет работать на некоторое время (Рисунок 4).

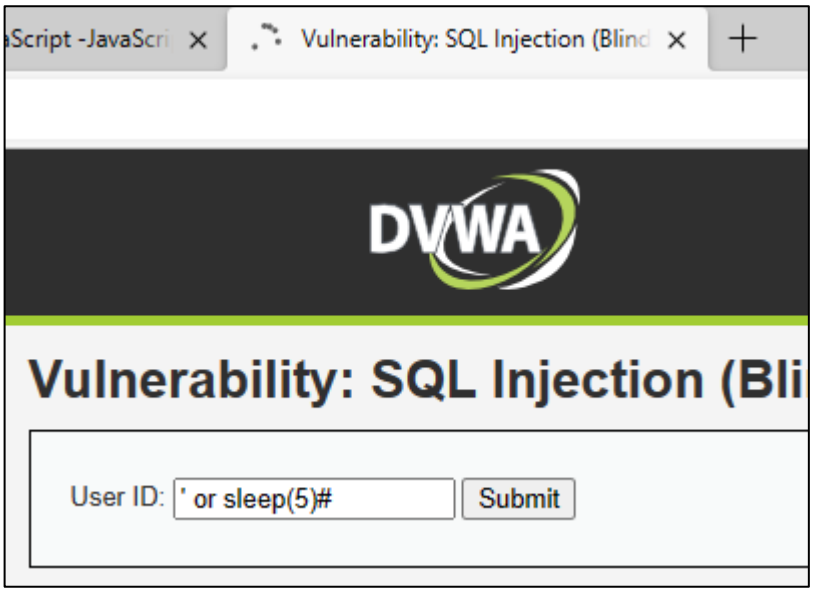

Рисунок 4 - SQL injection (Blind)

Weak Session IDs

Для начала выберем пункт Weak Session IDs в dvwa (сложность - low) после чего нажмём кнопку “Generate”, заходим в Application в браузере и видим id dvwaSession (Рисунок 5).

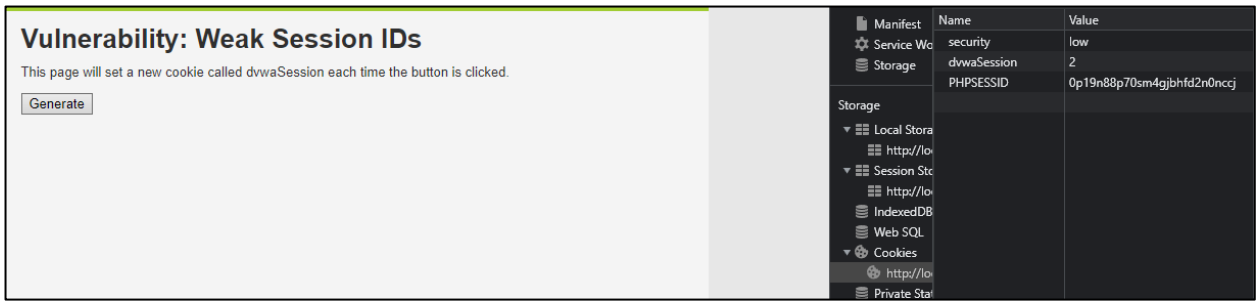

Рисунок 5 - Weak Session IDs

XSS (DOM)

Для начала выберем пункт XSS (DOM) в dvwa (сложность - low) после чего вводим в параметр ссылки default “<script>alert(“XSS DOM”)</script>” и у нас появляется уведомление с заданным текстом так и в XSS Reflected (Рисунок 6).

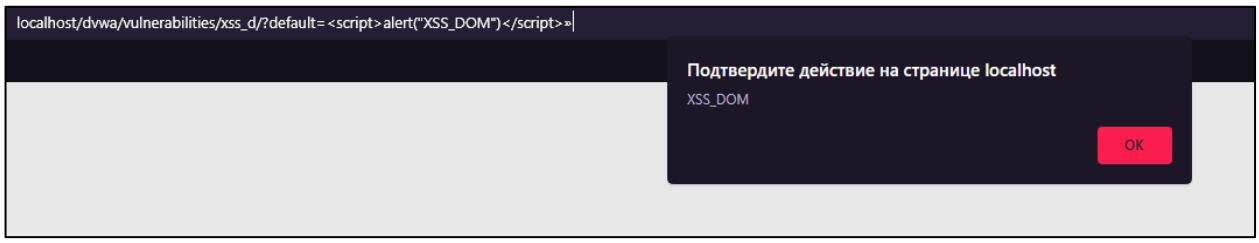

Рисунок 6 - XSS (DOM)

XSS (Stored)

Для начала выберем пункт XSS (Stored) в dvwa (сложность - low) после чего вводим в поле Message “<script>alert(“XSS Stored”)</script>” в итоге получаем такое же уведомление с заданным текстом и пустой отзыв (Рисунок 7).

Рисунок 7 - XSS (Stored)

JavaScript

Для начала выберем пункт JavaScript в dvwa (сложность - low) после чего вводим в поле “success” и нажимаем кнопку далее снова вводим “success”, открываем консоль вводим функцию “generate_token()” и снова нажимаем кнопку (Рисунок 8).

Рисунок 8 - JavaScript