УСТАНОВКА DVWA

Для того чтобы работать с приложением DVWA, необходимо выполнить следующие действия: установить локальный сервер XAMPP, проект DVWA поместить в каталог XAMPP под названием “htdocs”. В XAMPP запускаем Apache и MySQL. Далее работаем.

УЯЗВИМОСТИ

Brute Froce (Грубая сила)

Brute force – это метод поиска комбинации пароля и имени пользователя. В таком случае нужно перебрать все возможные комбинации. Чаще всего используется ПО, которое занимается этим самостоятельно.

Command injection

Внедрение команд ОС (также известное как внедрение команд) — **это** уязвимость веб-безопасности, которая позволяет злоумышленнику выполнять произвольные команды операционной системы (ОС) на сервере, на котором выполняется приложение, и, как правило, полностью скомпрометировать приложение и все его данные.

File upload

Уязвимости загрузки файлов — это когда веб-сервер позволяет пользователям загружать файлы в свою файловую систему без достаточной проверки таких параметров, как их имя, тип, содержимое или размер. Неспособность должным образом обеспечить соблюдение ограничений на них может означать, что даже базовая функция загрузки изображений может быть использована для загрузки произвольных и потенциально опасных файлов.

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)

SQL-инъекция называется слепой (англ. blind SQL injection) в том случае, когда результат выполнения запроса недоступен злоумышленнику. При этом уязвимый веб-сайт по-разному реагирует на различные логические выражения, подставляемые в уязвимый параметр.

Weak Session IDs

Знание идентификатора сеанса часто является единственным, что требуется для доступа к сайту в качестве конкретного пользователя после входа в систему, если этот идентификатор сеанса можно вычислить или легко угадать, тогда у злоумышленника будет простой способ получить доступ к учетной записи пользователей без необходимости подбора паролей или поиска других уязвимостей, таких как межсайтовый скриптинг.

XSS (DOM)

DOM based XSS, или XSS на основе DOM (или, как его называют в некоторых текстах, «Xss типа 0») — это XSS-атака, при которой полезная нагрузка атаки выполняется в результате изменения «среды» DOM в браузере жертвы, используемом исходной клиентской стороной.

XSS (Reflected)

Отраженный XSS – это атака, выполняемая через веб-сервер, но не хранящаяся в коде или базе данных. Так как она нигде не хранится, хозяин сайта может и не подозревать, что его атакуют.

XSS (Stored)

Тип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода и взаимодействии этого кода с веб-сервером злоумышленника. Является разновидностью атаки «Внедрение кода».

CSP Bypass

CSP расшифровывается как Content Security Policy, которая определяет, какие ресурсы могут быть извлечены и выполнены веб-страницей. Еще один способ понять это — определить, какие скрипты, изображения и iframe могут быть вызваны или запущены на определенной странице из разных мест в Интернете. Bypass - всяческие обходы этой системы.

JavaScript

уязвимость, которая заключается во внедрении кода, исполняемого на стороне клиента (JavaScript) в веб-страницу, которую просматривают другие пользователи. Уязвимость возникает из-за недостаточной фильтрации данных, которые пользователь отправляет для вставки в веб-страницу.

CSRF

Опаснейшая атака, которая приводит к тому, что хакер может выполнить на неподготовленном сайте массу различных действий от имени других, зарегистрированных посетителей.

ПРИМЕР ДЕЙСТВИЙ

Command Injection

Для начала выберем пункт Command Injection в dvwa (сложность - low) после чего в поле ввода введём команду “/?” нажимаем на кнопку и получаем полную информацию об адресе (Рисунок 1).

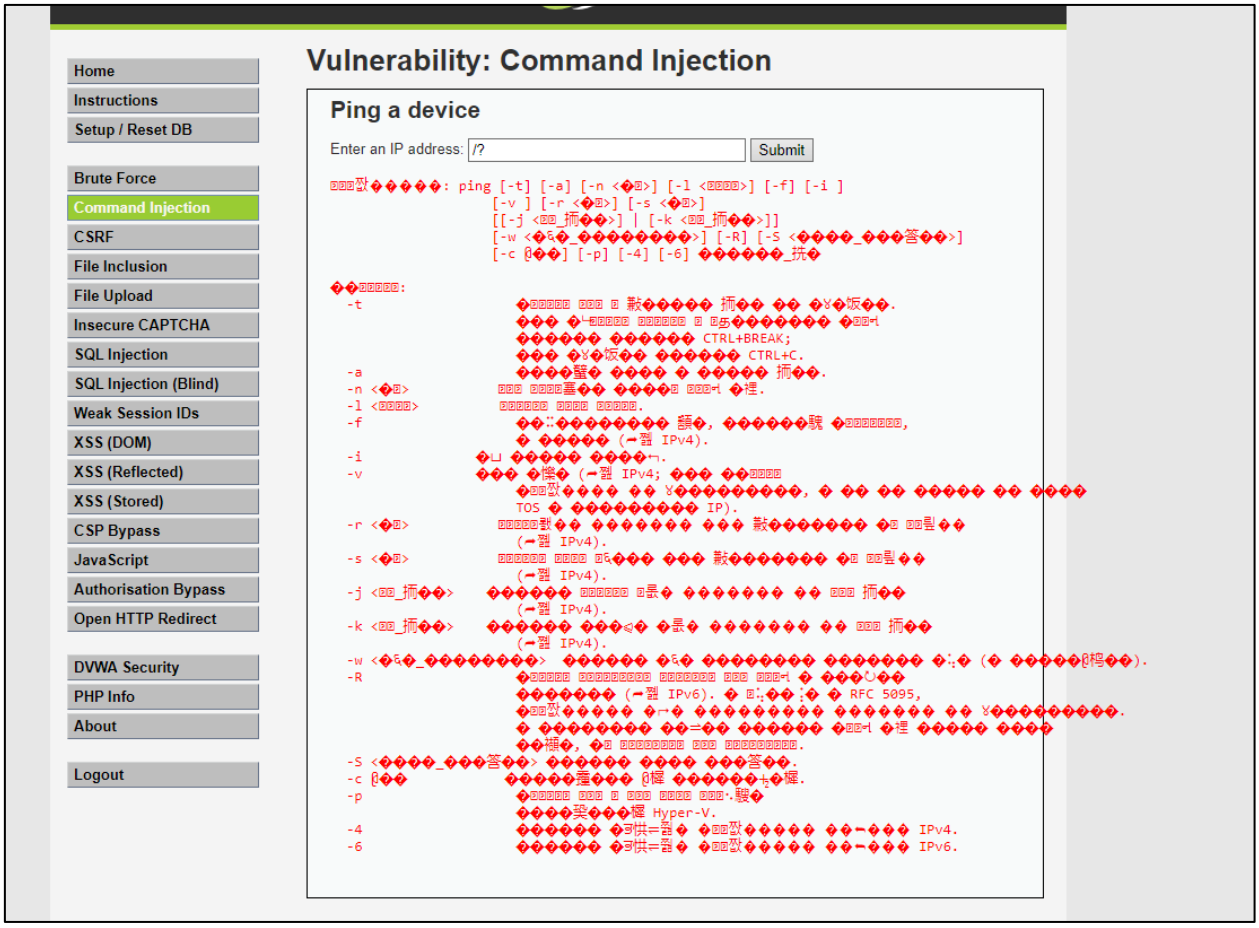

Рисунок 1 - Command Injection

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).

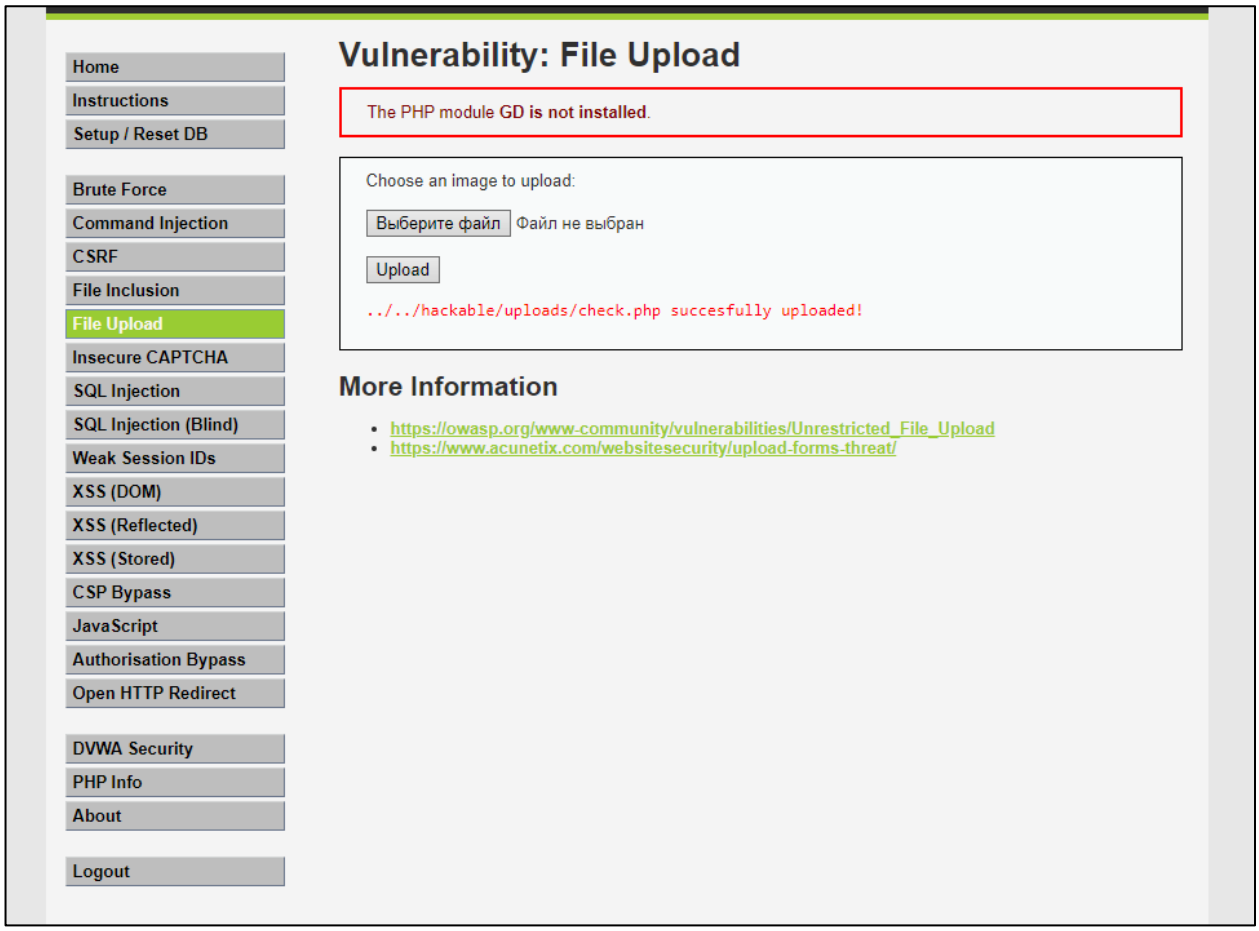

Рисунок 2 - File Upload

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).

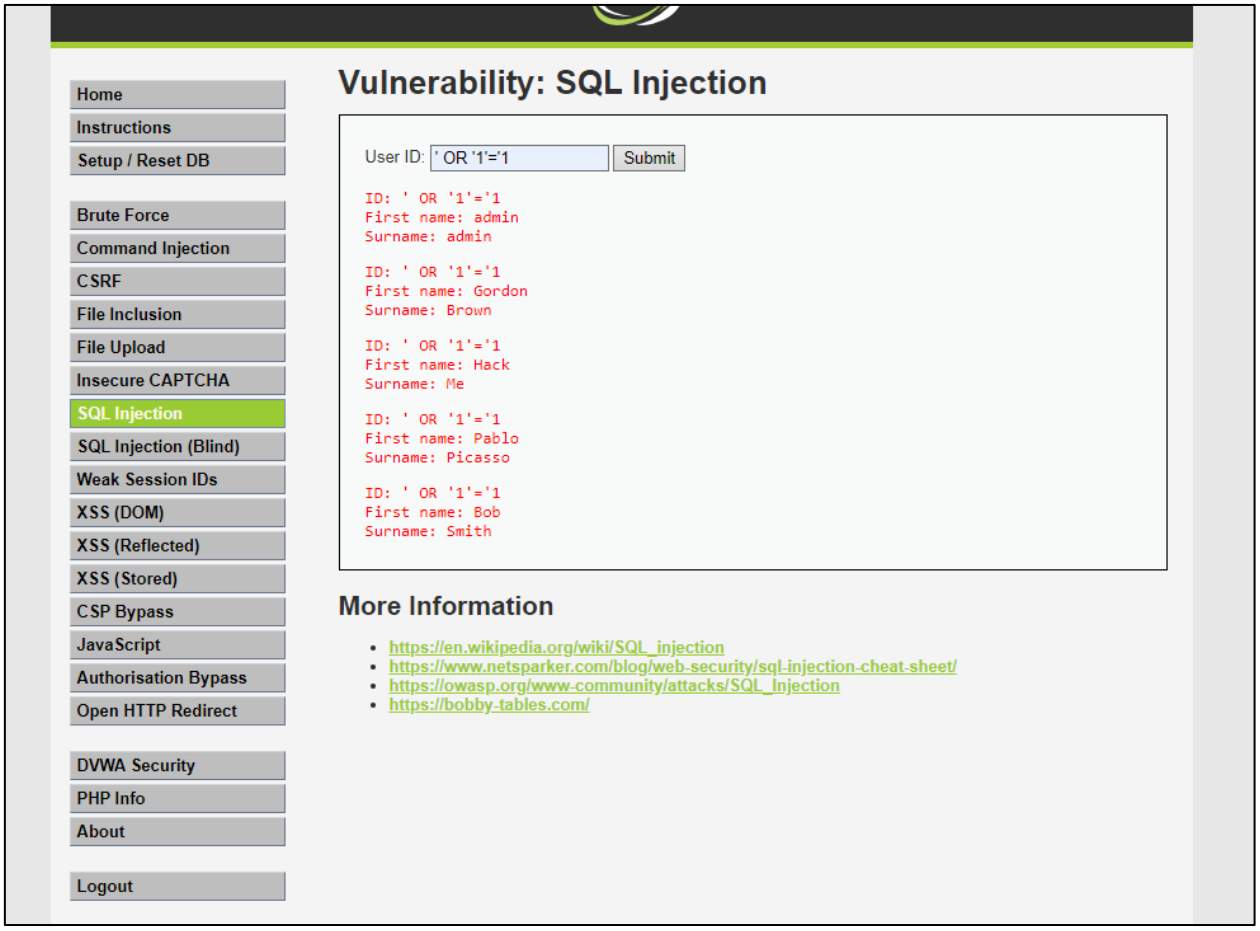

Рисунок 3 - SQL injection

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).

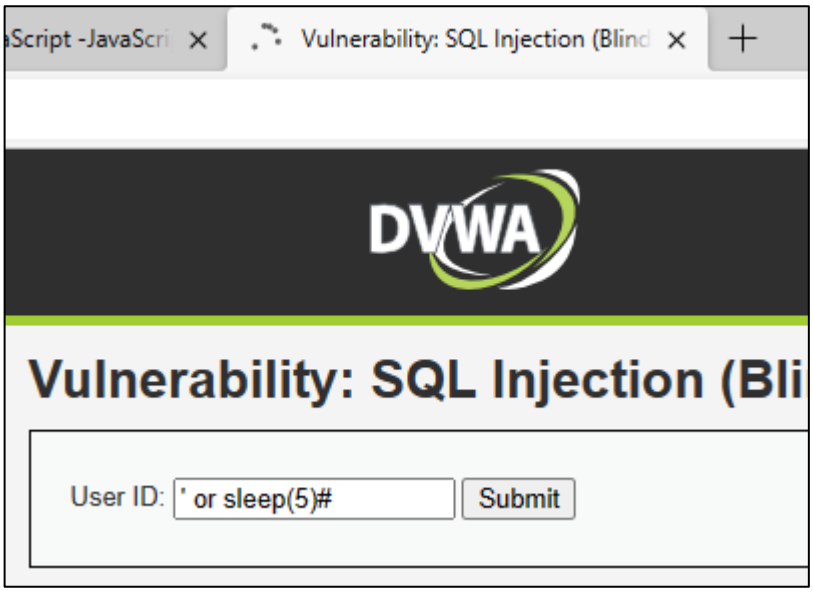

Рисунок 4 - SQL injection (Blind)

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).

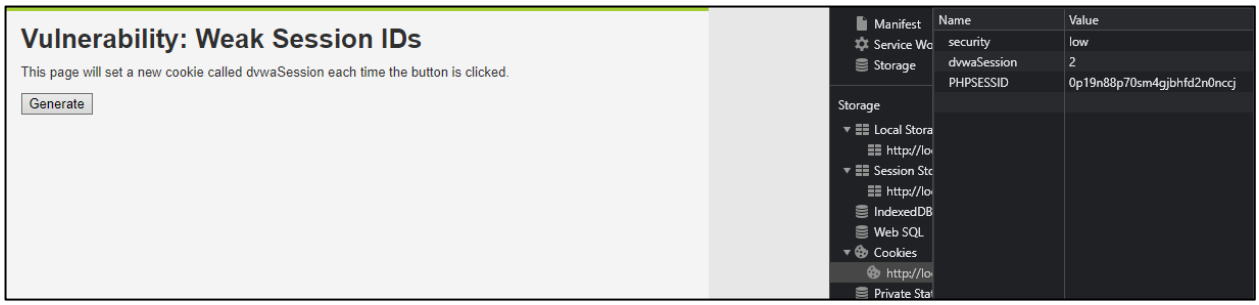

Рисунок 5 - Weak Session IDs

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).

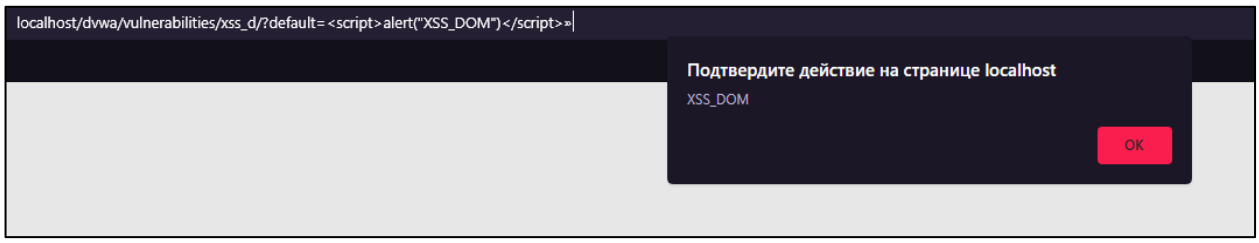

Рисунок 6 - XSS (DOM)

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