Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский университет ИТМО»

Информационная безопасность

Работа №4

«Анализ уязвимостей веб-приложения с помощью OWASP ZAP»

Барсуков Максим Андреевич

Группа: P3415

2025

Выполнение

Сканирование было выполнено с помощью встроенного функционала OWASP ZAP. Был запущен режим «Quick Scan» для целевого URL http://testphp.vulnweb.com/. Инструмент автоматически выполнил разведку (spidering) сайта, обнаружил его структуру и провел активное сканирование на наличие распространенных уязвимостей. В результате был сгенерирован подробный отчет, содержащий 25 типов найденных проблем, сгруппированных по уровню риска: 4 критических (High), 5 средних (Medium), 7 низких (Low) и 9 информационных (Informational), как показано на рисунке 1.

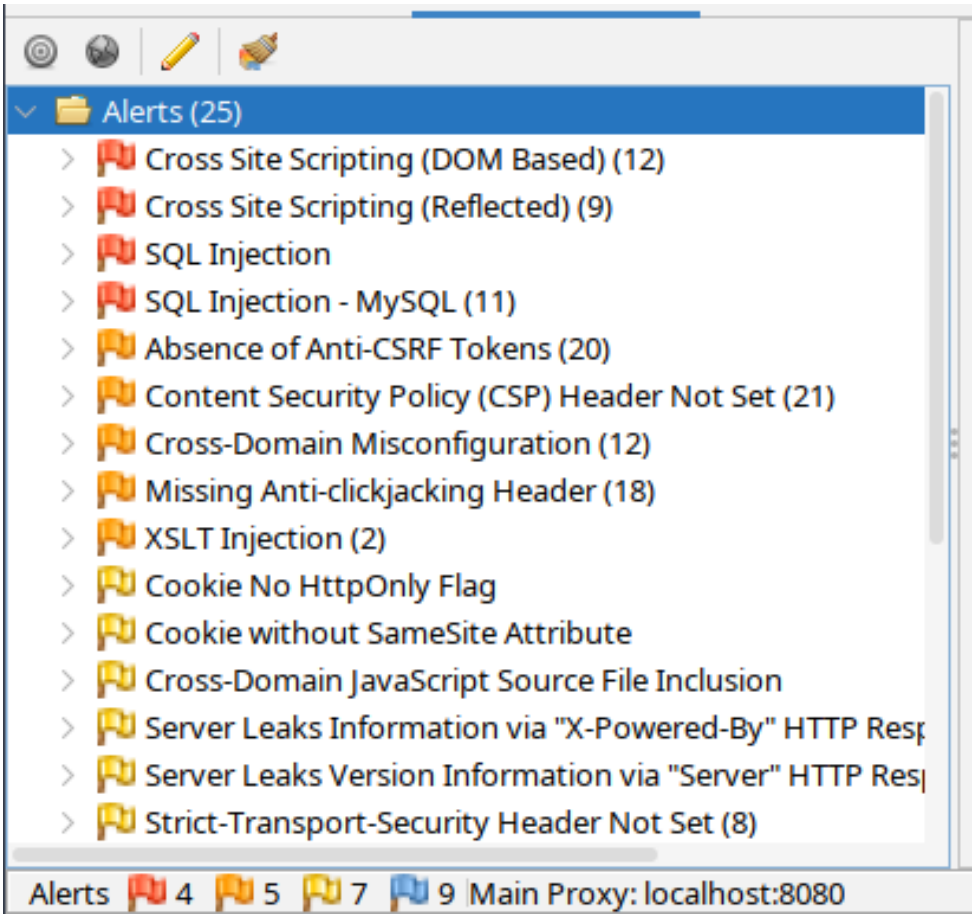

Рисунок 1 — Предупреждения ZAP

Ниже представлены три наиболее критичных типа уязвимостей, обнаруженных в ходе сканирования, с описанием их сути и потенциального воздействия.

Уязвимость 1: Межсайтовый скриптинг (Cross Site Scripting)

Уровень риска: Высокий (High), **количество экземпляров:** 12.

Это тип атаки, при котором вредоносный скрипт внедряется и выполняется в браузере жертвы, используя объектную модель документа (DOM) или полученные из HTTP-запроса данные. Уязвимость возникает из-за того, как клиентский JavaScript обрабатывает данные из источников, контролируемых злоумышленником (например, фрагмент URL или параметры формы) или выполняет скрипт из возвращенной сервером модифицированной страницы. В отчете показано, что ZAP успешно внедрил полезную нагрузку (например, *#jaVasCript:/*-/*/`/'/"/**/(/ */oNcliCk=alert(5397))//...*), которая вызвала всплывающее окно *alert* в браузере, что подтверждает возможность выполнения произвольного кода, как показано на рисунках 2 и 3.

Рисунок 2 — Найденная ZAP уязвимость Cross Site Scripting, DOM Based

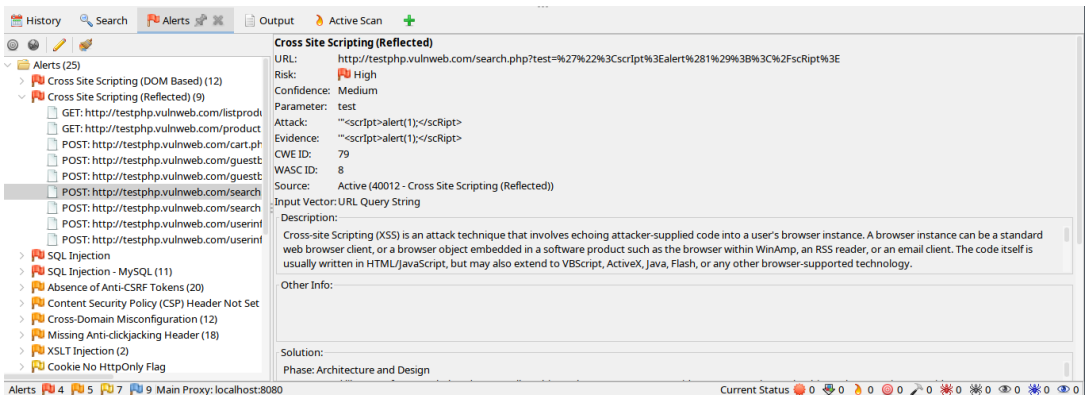

Рисунок 3 — Найденная ZAP уязвимость Cross Site Scripting, Reflected

Так, злоумышленник может украсть сессионные куки пользователя, перенаправить его на фишинговый сайт или выполнить любые действия от его имени в рамках текущей сессии.

Уязвимость 2: SQL-инъекция (SQL Injection - MySQL)

Уровень риска: Высокий (High), **количество экземпляров:** 11.

Уязвимость возникает, когда приложение небезопасно включает пользовательский ввод в SQL-запросы, отправляемые в базу данных. Сканирование показало, что передача одинарной кавычки (') в различных параметрах (например, *id*, *cat*, *pic*) вызывает ошибки синтаксиса MySQL (*You have an error in your SQL syntax*), что можно заметить на рисунке 4. Это явный признак того, что ввод не экранируется должным образом, и злоумышленник может манипулировать структурой запроса. Более того, в одном из случаев была подтверждена возможность слепой SQL-инъекции через функцию *sleep(15)*, что позволяет извлекать данные из базы данных по времени ответа, что видно из рисунка 5.

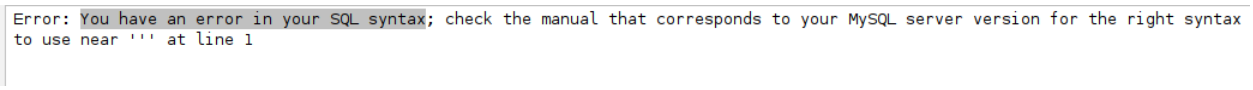

Рисунок 4 — Возможность выполнения SQL-инъекции

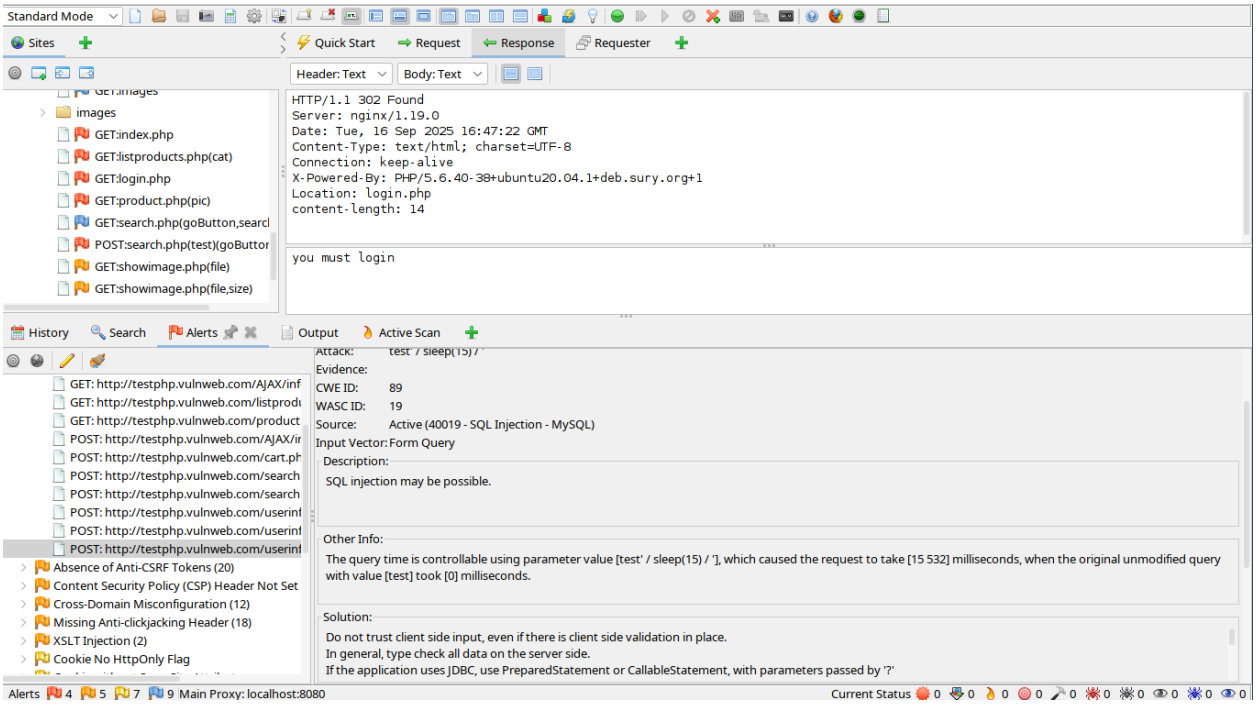

Рисунок 5 — Переданная команда влияет на время выполнения запроса

Злоумышленник может получить несанкционированный доступ ко всей базе данных, включая конфиденциальную информацию (логины, пароли, персональные данные), изменить или удалить данные, а также выполнить команды операционной системы в случае уязвимостей на уровне сервера.

Уязвимость 3: Отсутствие токенов защиты от CSRF (Absence of Anti-CSRF Tokens)

Уровень риска: Средний (Medium), **количество экземпляров:** 20.

Уязвимость CSRF (Cross-Site Request Forgery) позволяет злоумышленнику заставить аутентифицированного пользователя выполнить нежелательное действие на веб-сайте, на котором он вошел в систему. ZAP обнаружил, что ни одна из HTML-форм на сайте (например, формы входа, добавления в корзину, поиска) не содержит скрытых полей с уникальными токенами (такими как *CSRFToken* или *anticsrf*). Это означает, что злоумышленник может создать поддельную веб-страницу, которая автоматически отправит POST-запрос на целевой сайт, и браузер жертвы выполнит его, так как запрос будет сопровождаться действительными сессионными cookie, как показано на рисунке 6.

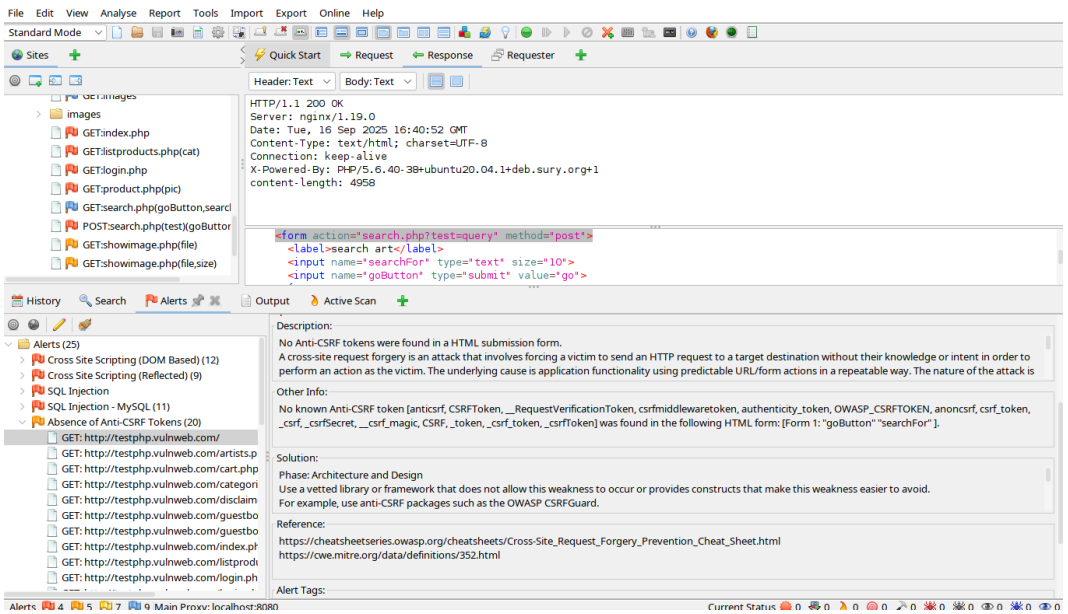

Рисунок 6 — В HTML-форме отправки не обнаружено токенов Anti-CSRF

Злоумышленник может выполнить действия от имени жертвы, такие как изменение пароля, перевод денег, размещение заказа или отправка сообщений.