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

Информационная безопасность

Работа 4

Анализ уязвимостей веб-приложения с помощью OWASP ZAP

Группа: P3416

Выполнил:

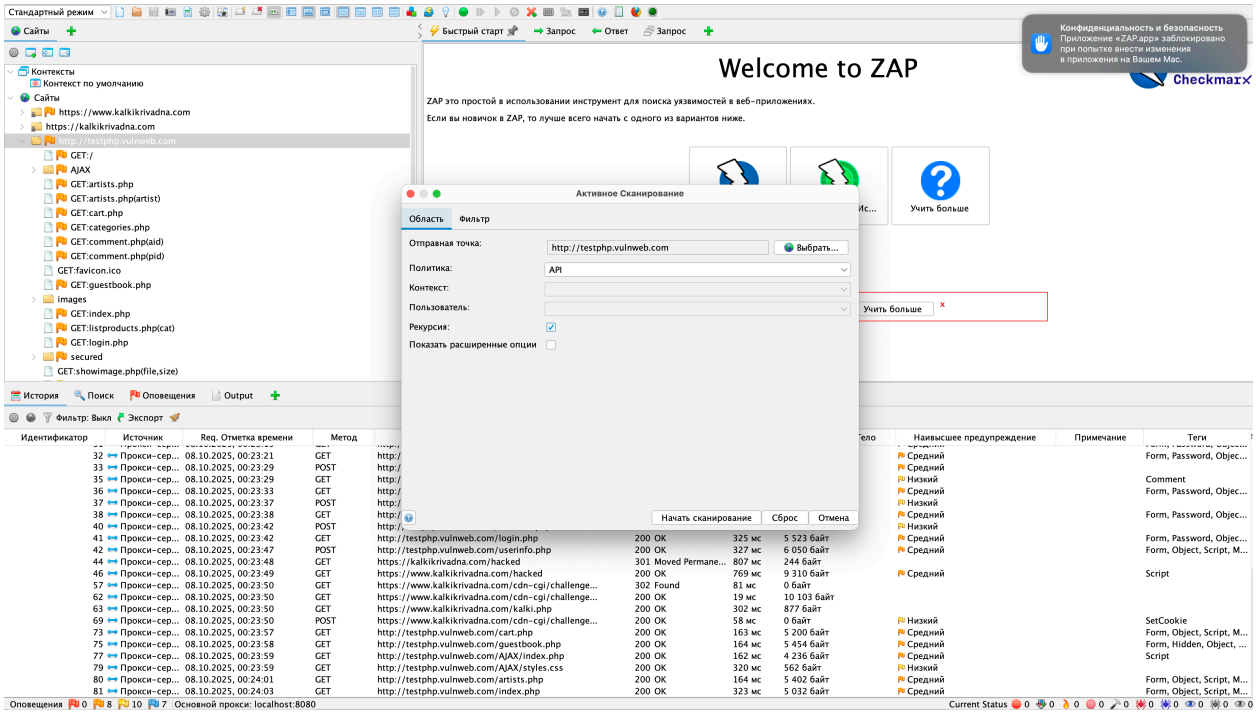
Сиразетдинов Азат Ниязович

г. Санкт-Петербург

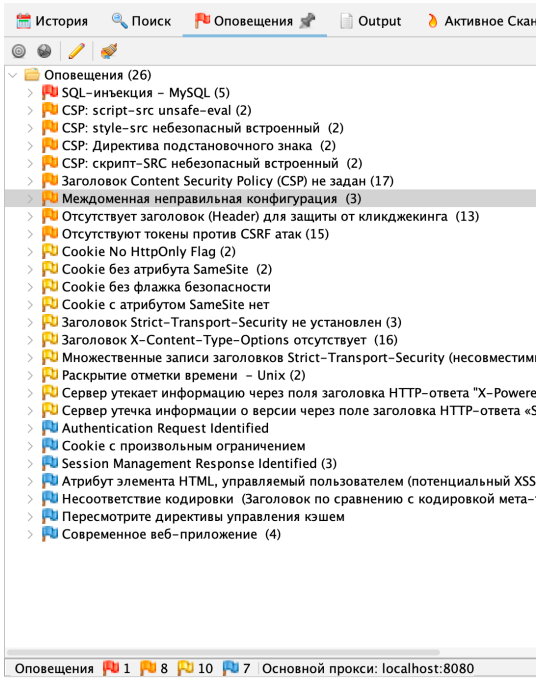
2025

Выполнение

Выполняем сканирование с помощью OWASP ZAP. Для сканирования был выбран сайт http://testphp.vulnweb.com/



В процессе сканирования были выявлены уязвимости: 1 high, 8 medium, 10 low и 7 informational



Уязвимость 1: SQL инъекция

Уровень риска

Высокий(High). Количество экземпляров – 5

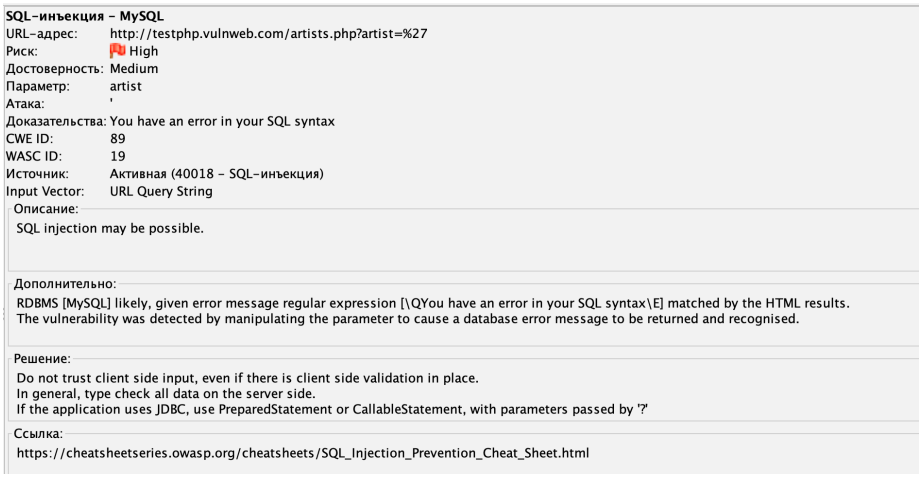
Причина

Пользовательский ввод попадает в SQL запрос без экранирования. Злоумышленник может удалять/изменять/получать данные из таблицы используя фразы SQL.

Обнаружение

Чтобы обнаружить наличие SQL инъекции можно передать невалидный SQL скрипт. Одним из вариантов является одинарная кавычка. SQL вернет ошибку, что кавычка не имеет закрывающую кавычку

Пример



При запросе http://testphp.vulnweb.com/artists.php?artist=%27 параметр artist не экранируется при запросе в базу данных, вследствие чего одинарная кавычка вызывает ошибку SQL синтаксиса

Уязвимость 2: XSLT Инъекция

Уровень риска

Средний (Medium). Количество экземляров – 2

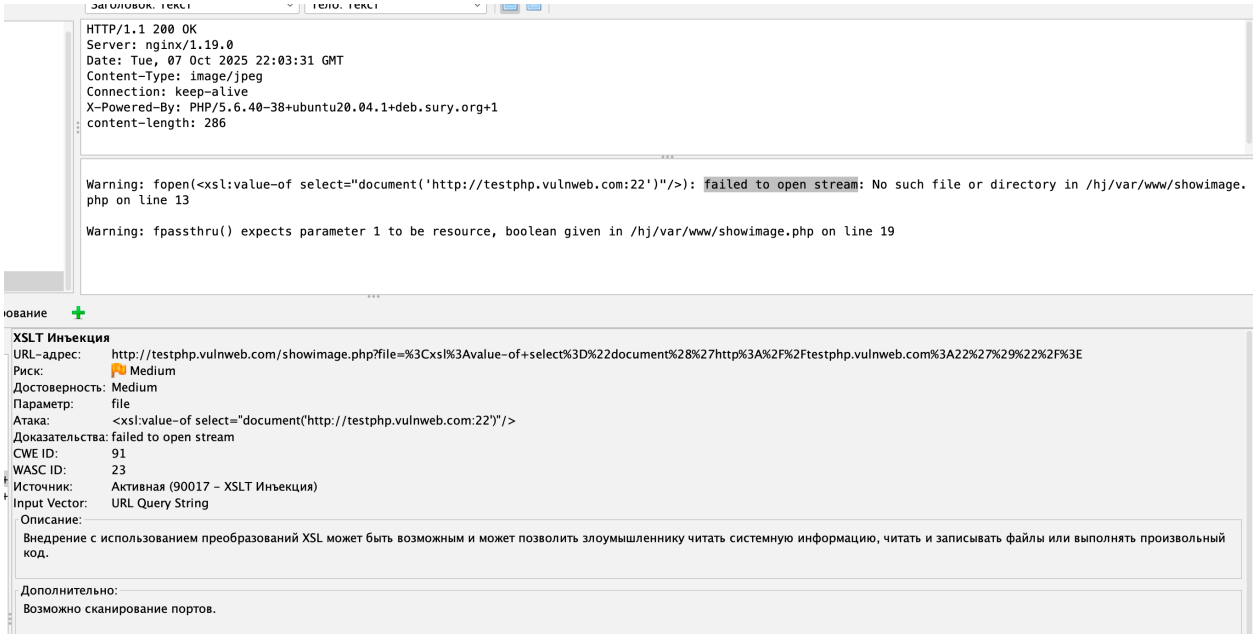
Причина

Текстовый ввод попадает в XSLT-процессор без дальнейшего форматирования. Это позволяет злоумышленнику добавлять XSL трансформации и получить содержимое системных файлов, делать запросы на внутренние порты, вызывать удаленное исполнение кода

Обнаружение

Для обнаружения XSLT инъекции можно передать невалидную XSL трансформацию. Например, двойные кавычки, одинарные кавычки и угловые скобки

Пример



При запросе http://testphp.vulnweb.com/showimage.php?file=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2Ftestphp.vulnweb.com%3A22%27%29%22%2F%3E мы передаем XSL трансформацию

<xsl:value-of select="document('http://testphp.vulnweb.com:22')"/> что вызывает ошибку XSLT-процессора

Уязвимость 3: Отсутствует заголовок (Header) для защиты от кликджекинга

Уровень риска

Средний (Medium). Количество экземляров – 21

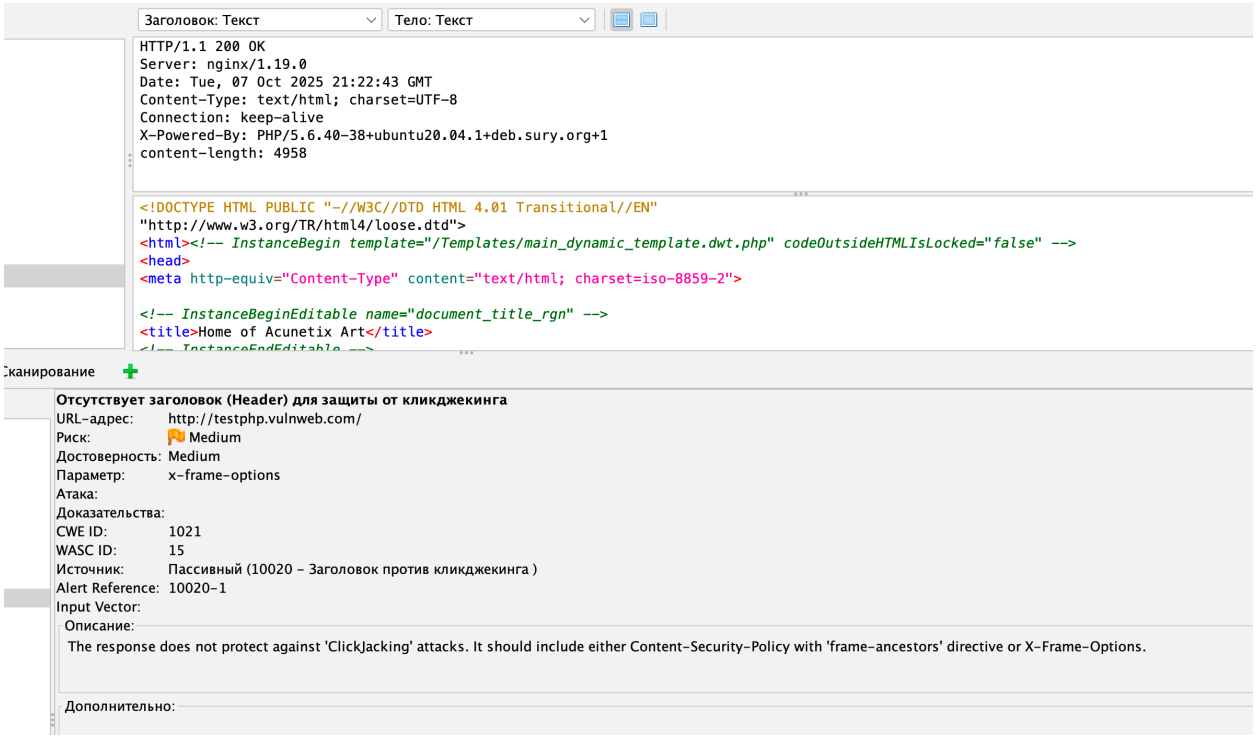
Причина

Сайт не защищен от кликджекинга. Это позволяет злоумышленнику использовать невидимые iframe для совершения действий на уязвимом сайте

Обнаружение

Для обнаружения нужно проверить наличие заголовка X-Frame-Options (позволит ограничить появление сайта в iframe) или Set-Cookie (запретит использование cookie файлов на других доменах)

Пример



При запросе на http://testphp.vulnweb.com/ отсутствуют заголовки, защищающие от кликджекинга