ЛАБОРАТОРНАЯ РАБОТА № 5

**Тема**: Инструменты сканирования уязвимостей

OWASP-ZAP

**Цель работы**:

1. Используйте инструменты OWASP для сканирования уязвимостей в веб-приложениях (2-3 веб-приложения).
2. Определите, какие уязвимости встречаются, и опишите их.
3. Каковы методы решения тех проблем, которые вызваны определенными уязвимостями?
4. Определите другие приложения для сканирования уязвимостей для веб-приложений.

# 1. Теоретические понятия

**OWASP** (*Open Web Application Security Project*) - это проект безопасности открытого веб-приложения. Сообщество OWASP включает корпорации, учебные заведения и частных лиц по всему миру. Сообщество работает над созданием статей, учебных пособий, документации, инструментов и технологий, которые находятся в свободном доступе. Фонд OWASP - это благотворительная организация 501 (c) (3), которая поддерживает и осуществляет управление проектами и инфраструктурой OWASP. Кроме того, Фонд был зарегистрирован как некоммерческая организация в Европе с июня 2011 года.

Члены сообщества OWASP создают приложения безопасности с учетом человеческого фактора и технологического уровня. Наиболее популярные документы, опубликованные OWASP, включают в себя: Руководство OWASP, см. Руководство OWASP для кода, а также широко используется OWASP Top 10 Project.

Наиболее распространенными инструментами являются среда обучения OWASP, анализатор **WebScarab Proxy** и инструменты **NET**. OWASP состоит из примерно 190 местных глав, которые расположены по всему миру, и тысяч участников в списках обсуждений проекта.

OWASP создает стандарты, первый из которых был опубликован под названием «Стандарт проверки безопасности приложений OWASP (ASVS)». Основная цель OWASP ASVS - стандартизировать диапазон покрытия и уровень строгости, доступные на рынке приложений, обеспечивая безопасность. Целью OWASP ASVS является предоставление набора открытых коммерчески успешных стандартов, адаптированных к конкретным веб-технологиям. Сборник для веб-приложения уже опубликован. Коллекция веб-сервисов находится в процессе разработки.

**Проекты**

OWASP - это набор связанных задач с конкретным планом развития и командой разработчиков.

Руководители проекта OWASP отвечают за определение имиджа, схемы и целей проекта, так как они участвуют в продвижении проекта и формировании команды. В настоящее время существует более 130 активных проектов OWASP, а также число проектов, растущих еженедельно. Проект является одним из самых популярных подразделений OWASP, поскольку он дает активистам возможность свободно тестировать различные теории и идеи с профессиональным сообществом поддержки OWASP. Все, что создано OWASP: инструменты, документация и библиотеки кода, распределены по следующим категориям:

• Безопасность - существуют инструменты и документация, которые можно использовать для обеспечения защиты от атак и использования системных недостатков;

• Обнаружение - это инструменты и документация, которые можно использовать для обнаружения системных атак и недостатков;

• Цикл - это инструменты и документация, которые можно использовать для добавления вещей, связанных с безопасностью, в жизненный цикл Программного обеспечения.

**Проекты OWASP:**

- OWASP Application Security Verification Standard (ASVS);
- OWASP Mantra Security Framework;
- Руководство по тестированию OWASP;
- OWASP Топ-10;
- Полная модель программного обеспечения OWASP.

**OWASP ZAP** (***Zed Attack Proxy***) - это веб-приложение с открытым исходным кодом для сканирования безопасности. Он предназначен для использования как новичками, специалистами по безопасности приложений, так и профессиональными тестерами на проникновение.

Это один из самых активных проектов OWASP, получивший статус Flagship. Он также полностью интернационализирован и переведен на более чем 25 языков.

При использовании в качестве прокси-сервера он позволяет пользователю манипулировать всем трафиком, проходящим через него, включая трафик с использованием https. Он также может быть запущен в режиме (daemon) «демон», который затем управляется через интерфейс программирования приложения REST.

Этот кроссплатформенный инструмент написан на Java и доступен во всех популярных операционных системах, включая Microsoft Windows, Linux и Mac OS X. ZAP был добавлен в технологический радар ThoughtWorks в мае 2015 года в Trial Circle.

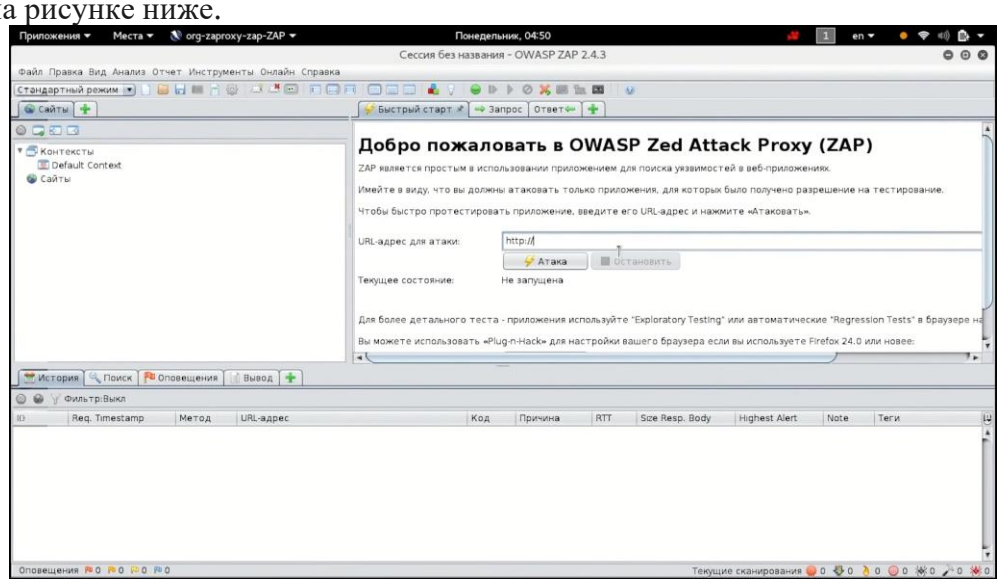
Некоторые из сборок включают в себя:

• Перехват прокси-сервера;
• Традиционный и веб AJAX crawler;
• автоматический сканер;
• пассивный сканер;
• принудительная навигация;
• Fuzzer;
• поддержка WebSocket;
• скриптовые языки;
• Plug-н-Hack.

Он имеет архитектуру плагинов и онлайн-магазин, который позволяет добавлять новые функции или обновленные функции.

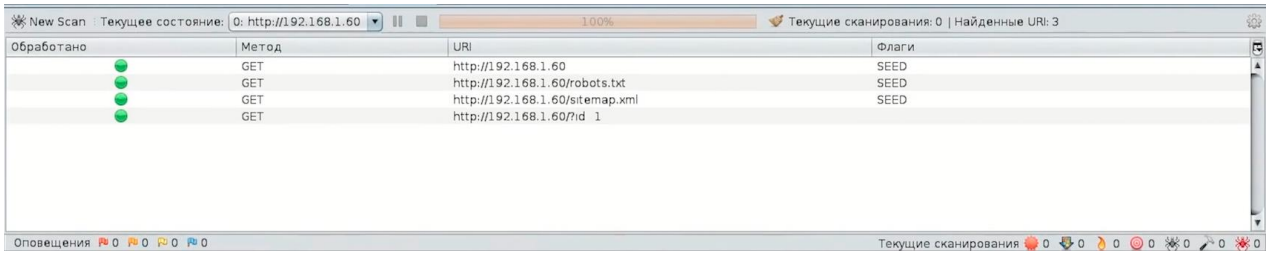
## 2. Сканирование уязвимостей

Для сканирования новой веб-страницы, используйте приложение OWASP ZAP 2.4.3, показанное на рисунке ниже.



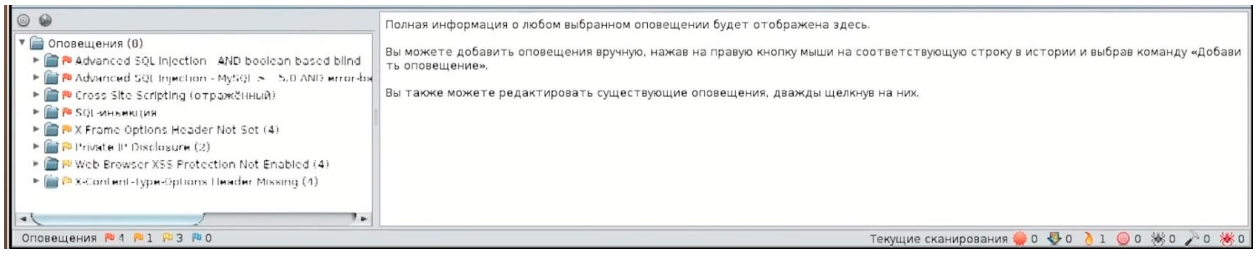

**Фигура 1**. Приложение OWASP ZAP.

Для сканирования уязвимостей веб-страницы при запуске приложения OWASP-ZAP выберите вкладку «Быстрый поиск» и в поле «UR-адрес для атаки» введите адрес страницы, которую мы хотим сканировать, и нажмите кнопку «Atack».




**Фигура 2**. Сканирование уязвимостей.

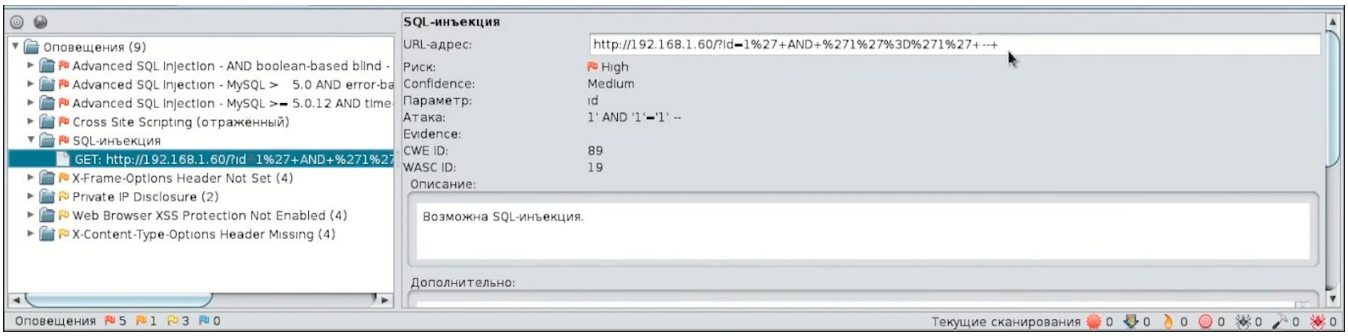
При сканировании веб-страницы определяются все типы http-запросов и параметры, которые передаются. Когда OWASP ZAP завершит сканирование, он отобразит результаты на вкладке под названием «Опавещение».




**Фигура 3.** Результаты сканирования.

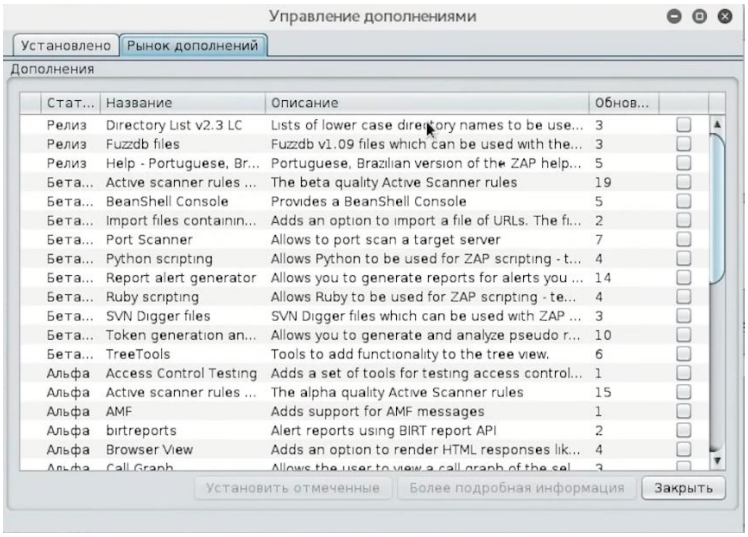
После просмотра результатов сканирования мы можем просмотреть все найденные оповещения, сгруппированные по категориям: SQL-инъекция, раскрытие частного IP-адреса, веб-браузер XSS Protection Not Enabled, отсутствует заголовок X-Content-Typ-Options и т. д.

Выбор одного из этих предупреждений справа отобразит все данные об этой уязвимости на рисунке ниже.



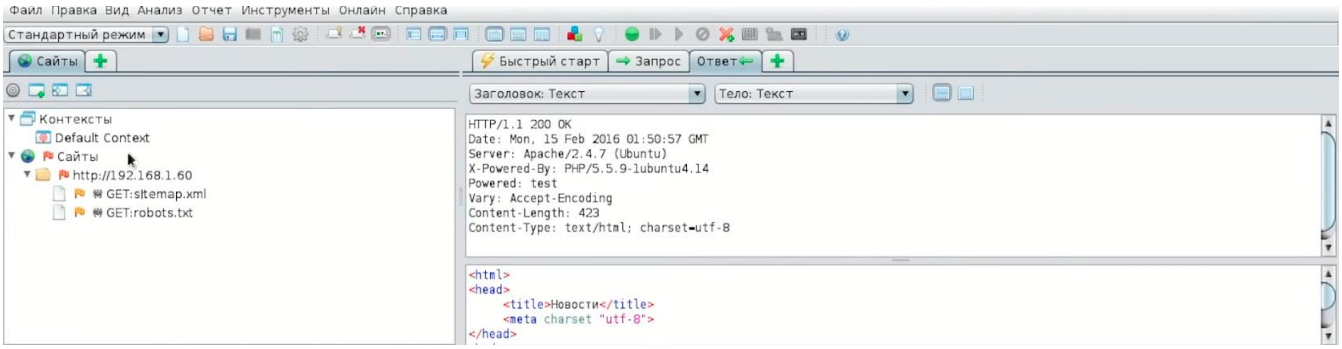

**Фигура 4.** Данные об найденых уязвимостей.

Если мы перейдем по ссылке этой уязвимости, мы сможем получить доступ к этой уязвимости. В представленных данных мы видим такие поля как: Url, Risc, Confidence, Parameter, Attack, Evidence, CWE ID, WASC ID, и т. д.



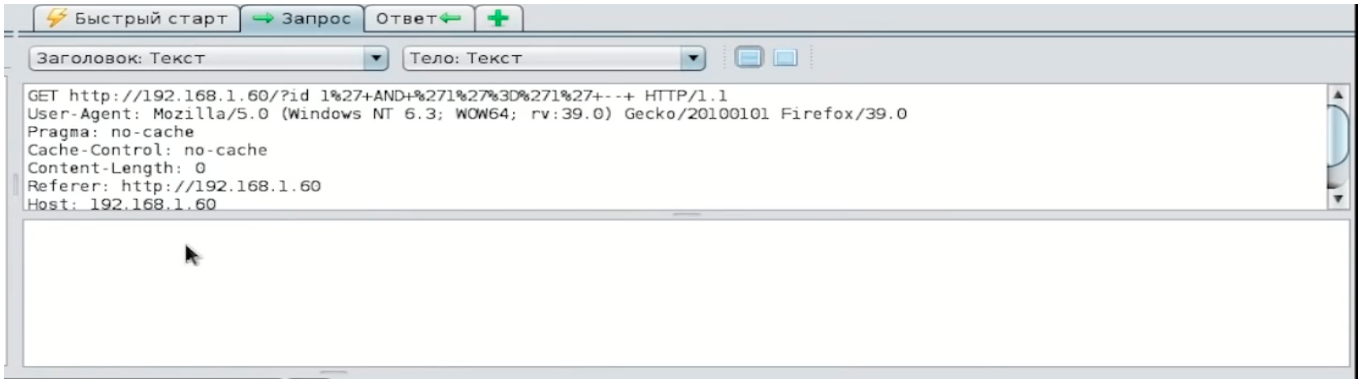

**Фигура 5.** Плагины

На рисунке 5 показаны дополнительные плагины, которые можно установить для дополнительных функций и возможностей.




**Фигура 6.** Дерево веб-страницы.

На рисунке 5 показаны дополнительные плагины, которые можно установить для дополнительных функций и возможностей.




**Фигура 7.** Менеджер запросов.

На рисунке 7 показана вкладка, в которой передается запрос, здесь мы можем изменить запрос, добавив поле или иным образом удалив один.