ТЕСТИРОВАНИЕ БЕЗОПАСНОСТИ

Безопасность веб-приложений: Распространенные уязвимости

- Инъекции
- XSS
- LFI/RFI
- Социальная инженерия

Инъекции

- Уязвимости подобного класса начинаются SQL-инъекциями, в различных его вариациях, и заканчивая RCE (Remote Code Execution) — удаленным выполнением кода.

  Пример:

  SQLi: http://example.com/?id=1' union select 1,2,version(),4

  RCE: http://example.com/search.php?q=;+cat+/etc/passwd

XSS

- В общем случае злоумышленник внедряет скрипт в веб-приложение, который срабатывает для каждого пользователя, посетившего вредоносную страницу.

  Пример:

  http://example.com/?search=<script>alert('xss')</script>

LFI/RFI

- Уязвимости данного класса позволяют злоумышленникам через браузер включать локальные и удаленные файлы на сервере в ответ от веб-приложения.

  Пример:

  http://example.com/?search=/../../../../../../etc/passwd

Социальная инженерия

- Психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации.

  Пример:

  Взломщик позвонил в офис в Чикаго и попросил соединить с мистером Джонсом. Секретарь в приемной спросила, знает ли он имя мистера Джонса; он ответил: «Оно где-то здесь, я ищу его. Сколько у вас работает Джонсов?». Она сказала: «Три. В каком он подразделении?» Он сказал: «Если вы зачитаете мне имена, может, я вспомню его».

  – Барри, Джозеф и Гордон.

  – Джо. Я вполне уверен, что это он. И… в каком он подразделении?

  – Развития бизнеса

  – Отлично. Соедините меня с ним, пожалуйста.

  Она соединила его. Когда Джонс взял трубку, атакующий сказал: «Мистер Джонс? Это Тони из отдела (начисления) заработной платы. Мы как раз выполняем ваш запрос о переводе ваших денег на кредитный счет».

  – ЧТО?! Вас обманули. Я не делал таких запросов. У меня даже нет счета.

  – Проклятие, я уже выполнил запрос. А какой у Вас номер счета?

  Джонс сообщил свой номер. Звонивший сказал: «Действительно, вы не делали запрос».

Учимся и защищаемся

- ## DAMN VULNERABLE WEB APPLICATION (Стенд)

Чертовски уязвимое веб-приложение (DVWA) - это веб-приложение PHP / MySQL, которое чертовски уязвимо. Его основная цель - помочь специалистам по безопасности проверить свои навыки и инструменты в среде, помочь веб-разработчикам лучше понять процессы защиты веб-приложений, узнать о безопасности веб-приложений в контролируемой среде.

Целью DVWA является практика некоторых из наиболее распространенных веб - уязвимостей , с различными уровнями сложности, с простым интерфейсом. Обратите внимание, что в этом программном обеспечении есть как задокументированные, так и недокументированные уязвимости . Это сделано намеренно. Предлагаем вам попытаться обнаружить как можно больше проблем.

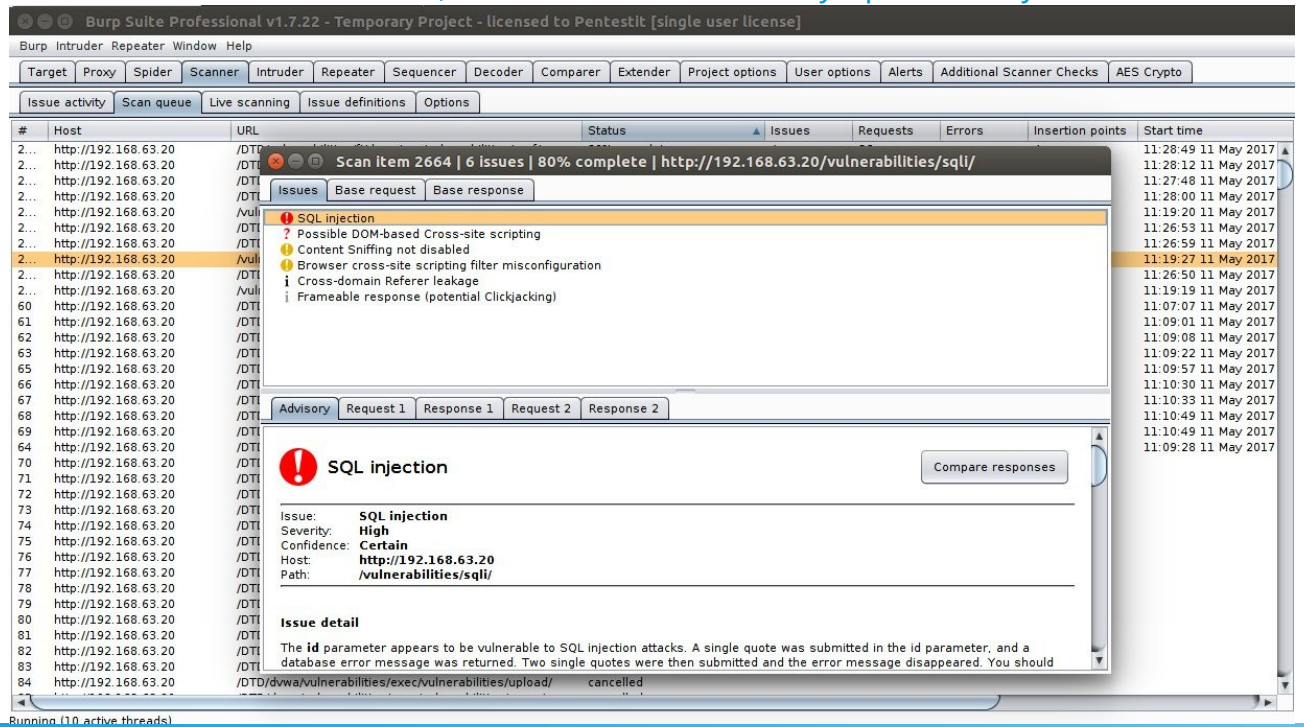
https://github.com/digininja/DVWA

!!! Не загружайте его в общедоступную html-папку вашего хостинг-провайдера или на какие-либо серверы с выходом в Интернет , так как они будут скомпрометированы. Рекомендуется использовать виртуальную машину;

Контейнер Docker

Автоматизация

Burp Suite (Professional) – интегрируемая универсальная платформа для тестирования безопасности веб-приложений и выявления уязвимостей. Разнообразные инструменты в составе ПО поддерживают всю процедуру тестирования, начиная с отображения и анализа атаки на всех ее этапах, и заканчивая поиском и устранением уязвимостей.



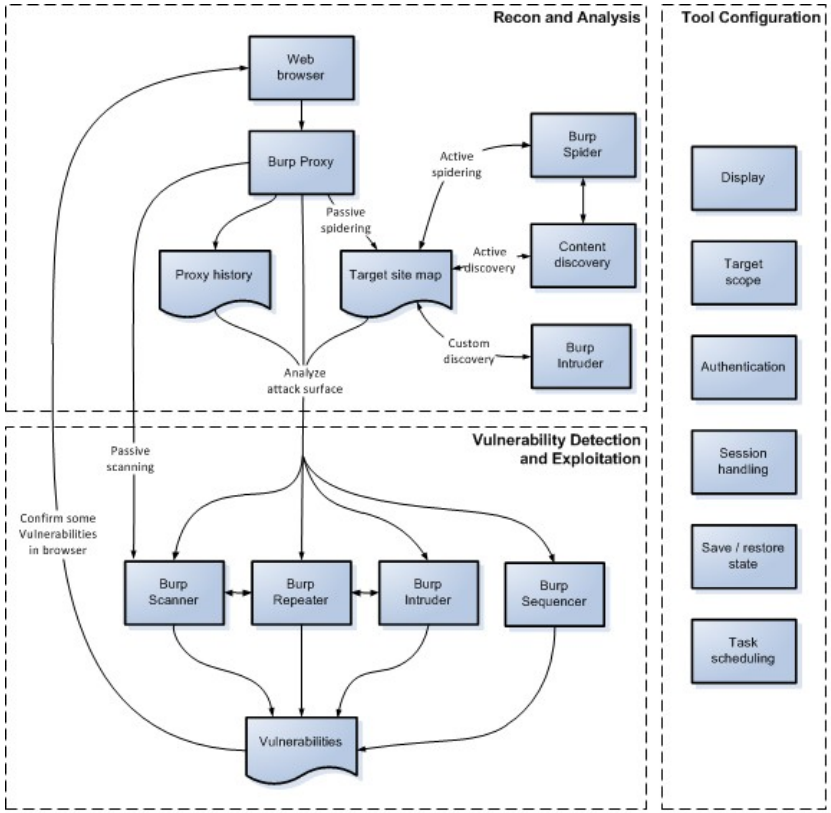
Burp Suite (Professional)

Основной функционал основан на следующих модулях:

- Proxy — перехватывающий прокси-сервер, работающий по протоколу HTTP(S) в режиме man-in-the-middle. Находясь между браузером и веб-приложением он позволит вам перехватывать, изучать и изменять трафик идущий в обоих направлениях.
- Spider — паук или краулер, позволяющий вам в автоматическом режиме собирать информацию о об архитектуре веб-приложения.
- Scanner — автоматический сканер уязвимостей (OWASP TOP 10 и т.д.) Доступен в Professional версии, в бесплатной версии только описание возможностей.
- Intruder — утилита, позволяющая в автоматическом режиме производить атаки различного вида, такие как подбор пароля, перебор идентификаторов, фаззинг и так далее.
- Repeater — утилита для модифицирования и повторной отправки отдельных HTTP-запросов и анализа ответов приложения.
- Sequencer — утилита для анализа генерации случайных данных приложения, выявления алгоритма генерации, предиктивности данных.
- Decoder — утилита для ручного или автоматического преобразования данных веб-приложения.
- Comparer — утилита для выявления различий в данных.
- Extender — расширения в BurpSuite. Можно добавлять как готовые из BApp store, так и собственной разработки.

Burp Suite (Professional)

Использование совокупности инструментов позволяет наиболее глубоко и продуктивно исследовать веб-приложение.



Web applications security assessment:

- test the authentication mechanism;
- test for username enumeration;
- test resilience to password guessing;
- test account recovery functionality;
- check for unsafe transmission of credentials;
- test the session management mechanism;
- test session tokens for meaning and predictability;
- check for insecure transmission of tokens;
- test session termination;
- check for session fixation;
- check cookie scope;
- fuzz all request parameters;
- test for SQL injection;
- test for XSS and other response injection;
- test for OS command injection;
- test for path traversal;
- test for script injection;
- test for file inclusion;
- test for function-specific input vulnerabilities;
- test for HTTP Response Splitting;
- test for Server-side request forgery (SSRF);
- test for Cross Site Request Forgery (CSRF);
- test CORS policy;
- test CSP policy;
- test for HTTP request smuggling;
- test for vulnerable and outdated components;