Дисциплина «Этичный хакинг и противодействие взлому»

Лекция 4

Анализ уязвимостей

Преподаватель: **Батыргалиев Асхат Болатканович, PhD,**
ассоц.проф. кафедры «Кибербезопасность, обработка и хранение информации»

askhat.b.b@gmail.com

Содержание

1. Общее понятие анализа уязвимостей и угрозы
2. Особенности анализа уязвимостей в сфере кибербезопасности
3. Виды анализируемых угроз в информационной безопасности
4. Методы анализа уязвимостей в сфере информационной безопасности
5. Сканеры уязвимостей

По завершению урока Вы будете знать:

1. Общее представление об анализе уязвимостей и угроз
2. Особенности анализа уязвимостей в сфере кибербезопасности
3. Виды анализируемых угроз в информационной безопасности
4. Методы анализа уязвимостей в сфере информационной безопасности
5. Виды сканеров уязвимостей

Анализ уязвимостей

Анализ уязвимостей – процесс, направленный на обнаружение всевозможных угроз, уязвимых мест и рисков вероятного несанкционированного проникновения третьих лиц в информационную систему. Уязвимость выступает в качестве слабого места информационной системы.

Угроза – фактор оказания отрицательного воздействия со стороны потенциального противника (киберпреступника), которое потенциально становится причиной компрометации конфиденциальных и других видов защищаемых данных.

При анализе уязвимостей в сфере кибербезопасности в качестве третьих лиц рассматриваются злоумышленники, использующие уязвимости, чтобы реализовать различные угрозы.

Если в информационной системе компании присутствуют уязвимости, то подобное отрицательно сказывается на ее профессиональной деятельности, потому что она является незащищенной перед недобросовестными конкурентам. Наличие уязвимостей в системе кибербезопасности облегчает деятельность преступников по нанесению вреда, позволяя посторонним лицам заполучить доступ к конфиденциальной информации. Источники киберугроз могут быть намеренными или случайными. Также в качестве источников угроз часто рассматриваются природные и техногенные факторы. Каждая угроза имеет собственный перечень уязвимостей, при помощи которых третьи лица могут реализовать свои планы.

Особенности анализа уязвимостей в сфере кибербезопасности

Правильно организованная и высокоэффективная система информационной безопасности способна обеспечить защиту от несанкционированного доступа к информации из корпоративной, внутренней сети компании. Компании, которые заинтересованы в получении эффективной системы информационной безопасности, постоянно работают над тем, чтобы предотвратить:

- утечки различных видов корпоративной, внутренней информации;
- удаленного изменения защищаемых данных;
- изменения уровня защиты от киберугроз, способных потенциально спровоцировать утрату доверия поставщиков, контрагентов, инвесторов и т. п.

У киберугроз может быть несколько источников, поэтому крайне важно иметь их четкую классификацию и иметь схему их анализа по каждому источнику. С помощью такого подхода можно получить максимальный охват вероятных уязвимостей в информационной инфраструктуре компании.

Виды анализируемых угроз в ИБ

Для проведения эффективного анализа уязвимостей информационной безопасности существующей информационной инфраструктуры, требуется различать типы угроз, возникающих в информационных системах компаний. Подобные угрозы классифицируются по следующим категориям:

1. Потенциальный источник киберугроз, находящийся прямо в информационной системе, в пределах ее видимости или вне зоны видимости.
2. Воздействие на информационную систему, несущее активную угрозу (вредоносное ПО), пассивную угрозу (копирование защищаемых данных киберпреступниками).
3. Способ обеспечения доступа, реализуемый: напрямую (кража учетных данных) или с помощью нестандартных каналов связи (к примеру, уязвимости используемого программного обеспечения).

При проведении атак на IT-инфраструктуру организации злоумышленники обычно преследуют несколько целей – получение контроля над наиболее важной информацией и ресурсами, обеспечение полного доступа к внутренней сети организации, ограничение работы предприятия в определенной сфере.

Методы анализа уязвимостей в сфере ИБ

Можно выделить несколько методов, с помощью которых есть возможность проведения анализа уязвимостей информационной системы. Первый базируется на вероятностной методике. При его эксплуатации необходимо опираться на некоторые факторы:

- потенциал киберпреступника (устанавливается за счет экспертных оценок); источник угрозы (где может быть проведена атака – в зоне видимости или за пределами видимости информационной системы);
- методика воздействия (социальная, аппаратная, сетевая);
- объект угрозы (конфиденциальная информация, средства для шифрования и т.п.).

При анализе уязвимостей информационных систем требуется учесть вероятные зоны дислокации. Для реализации подобного требуется своевременно найти и убрать ошибки в используемом программном обеспечении, а затем периодически проводить установку обновлений безопасности от разработчиков. Анализ уязвимостей информационных систем, связанных с неграмотной настройкой средства защиты, должен осуществляться систематически. Оптимальный вариант в этом случае – настройка беспрерывного мониторинга информационной системы на предмет появления уязвимостей. Отдельно от описанного выше анализа обязательно требуется проведение некоторых мероприятий с сотрудниками организации – выдача прав доступа к конфиденциальной информации и ресурсам с минимальными привилегиями, прав на установку специального ПО, прав на копирование защищаемых данных и использование внешних носителей информации.

Сканер уязвимостей

Сканер уязвимостей (vulnerability scanner) – программный или аппаратный продукт для поиска угроз в инфраструктуре. Сканер используется для обнаружения брешей в сетевой защите, операционной системе, базах данных, приложениях и т.д. Основная задача – оценивать информационную безопасность, выявлять уязвимости и предоставлять отчеты.

Основные функции сканера уязвимостей:

- ищет различные типы уязвимостей сети и анализирует их в режиме реального времени;
- проверяет ресурсы сети, ОС, подключенные устройства, порты;
- анализирует все активные процессы, поведение запущенных приложений;
- создает отчеты, в которых прописывает тип уязвимости.

Принципы работы сканера

Принципы работы сканера

- Зондирование. Эффективный, но медленный способ поиска и анализа уязвимостей. Суть его заключается в том, что решение инициализирует виртуальные атаки и мониторит сетевую инфраструктуру на поиск уязвимых точек. По окончании процесса сканирования предоставляется подробный отчет с указанием найденных проблем и рекомендации по их устранению.
- Сканирование. В таком режиме сканер работает с максимально возможной скоростью, но анализирует сетевую инфраструктуру на поверхностном уровне. То есть обнаруживает очевидные уязвимости и анализирует общую безопасность инфраструктуры. По сравнению с предыдущим методом, данный способ только предупреждает о найденных проблемах администратора, но не более того.

Работа сканера базируется на косвенных признаках уязвимостей. Если программное обеспечение анализирует протоколы прикладного уровня или API, то он детерминирует их параметры и сравнивает с приемлемыми показателями, заданными администратором. Если он обнаружит расхождение значений, администратор получит уведомление о потенциальной уязвимости. После этого нужно проверить найденные потенциальные угрозы каким-либо другими инструментами.

Действия сканера уязвимостей

Сканер уязвимостей выполняет следующие действия:

- Собирает информацию со всей инфраструктуры: активные процессы, запущенные приложения, работающие порты и устройства, службы и т. д.
- Поиск потенциальных уязвимостей разными методами.
- Использует специальные способы имитации атак, чтобы найти возможные уязвимости (функция доступна не в каждом сканере).
- Формирует подробный отчет с информацией о найденных уязвимостях.

Сканеры могут быть «дружественными» или «агрессивными». Первый тип просто собирает информацию и не моделирует атаку. Второй пользуется уязвимостью, чтобы вызвать сбой в работе программного обеспечения.

Сканеры уязвимостей

Sn1per – фреймворк для автоматического анализа безопасности цели. Сканер позволяет собирать базовую информацию (IP цели, ping, whois, DNS); запускает Nmap для поиска открытых портов и определения сервисов, в том числе и с помощью NSE; ищет часто встречающиеся уязвимости и автоматически эксплуатирует их; пробует получить доступ к различным файловым ресурсам (FTP, NFS, Samba); запускает Nikto, WPScan и Arachni для всех найденных веб-приложений и многое другое. Поддерживает интеграцию с Hunter.io, OpenVAS, Burp Suite, Shodan, Censys и Metasploit.

Сканеры уязвимостей

Wapiti – сканер веб-уязвимостей. Сканер умеет обнаруживать следующее:

- раскрытие содержимого файла (local file inclusion), в том числе бэкапов и исходного кода сайта;
- SQL-инъекции и внедрение кода PHP/ASP/JSP;
- отраженные и хранимые XSS;
- инъекции команд ОС;
- XXE Injection;
- неудачные конфигурации .htaccess;
- Open Redirect.

Wapiti3 поддерживает прокси, аутентификацию на целевом сайте, умеет не реагировать на сторонние сертификаты SSL и может вставлять в запросы любые заголовки (в том числе кастомный User-Agent).

Nikto – сканер веб-приложений, изначально встроенный в Kali Linux. Умеет находить:

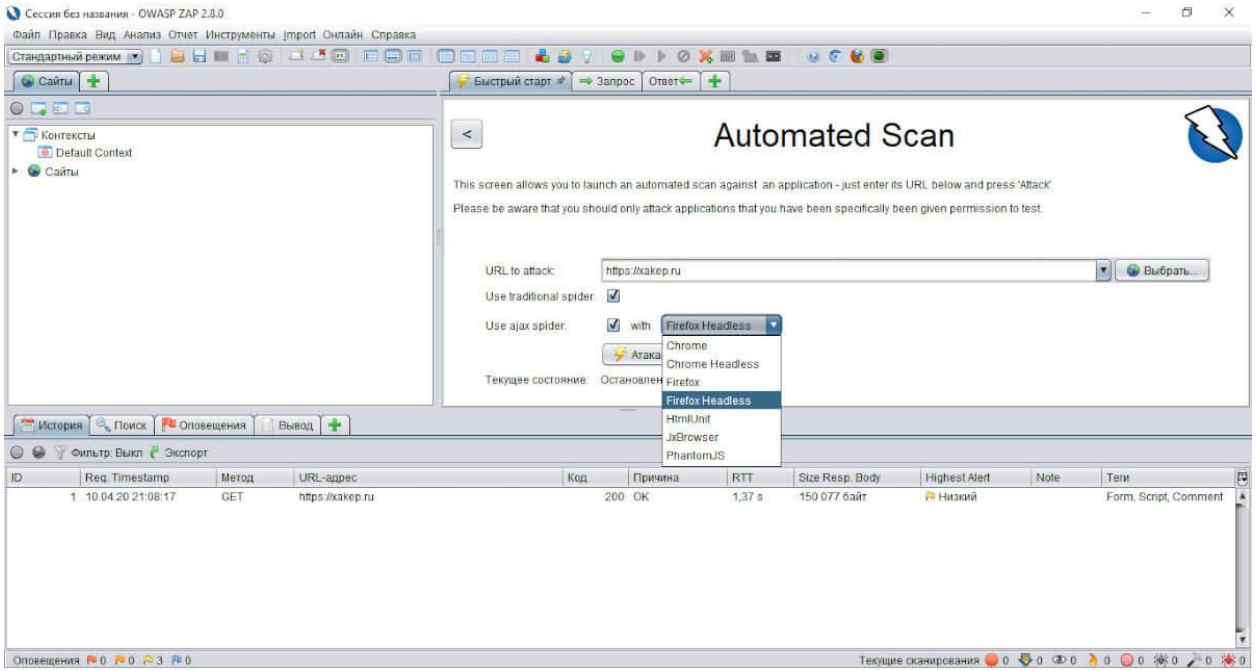
- странные и необычные заголовки;
- утечки inode через заголовок ETag;
- использование WAF;
- множество интересных файлов, к которым не стоило бы открывать доступ.

Имеет много параметров. Самый главный из них – -h [HOST], задающий цель. Также есть формат вывода (-Format) и возможность работать с Metasploit.

Сканеры уязвимостей

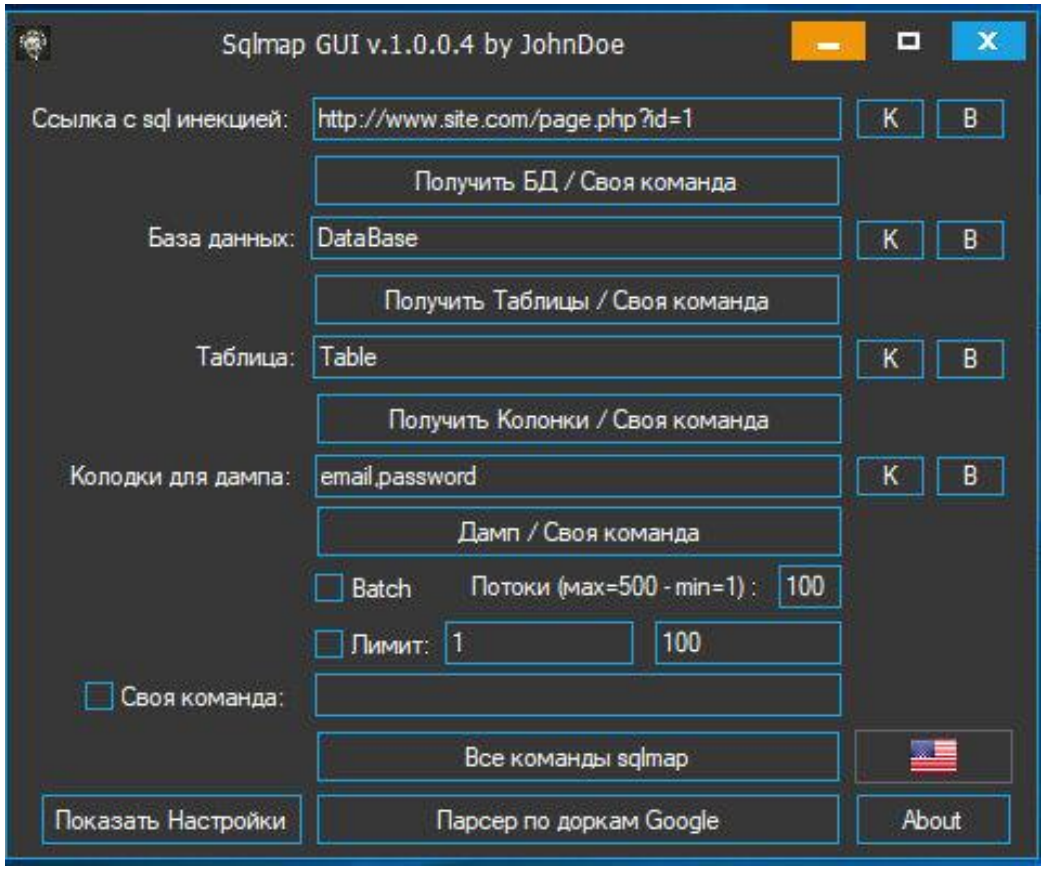
OWASP ZAP (Zed Attack Proxy) – бесплатный инструмент для тестирования на проникновение и поиска уязвимостей в веб-приложениях. Основные возможности:

- MITM-прокси для захвата трафика браузера;
- пассивный и активный сканеры уязвимостей;
- паук-краулер, который может работать даже с AJAX;
- фаззер параметров;
- поддержка плагинов;
- поддержка WebSocket.



Сканеры уязвимостей

Sqlmap – сканер для поиска SQL-инъекций. Особенность этого сканера в том, что он может не только найти ошибку, но и сразу эксплуатировать ее, причем в полностью автоматическом режиме. Умеет работать с БД MySQL, MS SQL, PostgreSQL и Oracle.



Сканеры уязвимостей

Acunetix WVS – сканер представляет собой веб-приложение, и его можно ставить на сервер без графической оболочки. Есть поддержка и Windows, и Linux. Сканирование требует только указать адрес цели (на вкладке Targets) и нажать кнопку Scan, опционально задав время начала. Сканер имеет несколько профилей сканирования, может сканировать только в рабочее или нерабочее время, умеет находить большое количество уязвимостей:

- XSS, в том числе DOM;
- SQL-инъекции, кроме слепых (blind);
- CSRF;
- обход директории;
- XXE Injection;
- небезопасная сериализация;
- проблемы с SSL-сертификатами (скорое истечение срока годности, слабые шифры);
- проблемы с CORS.

Сканеры уязвимостей

Vega – сканер с открытым исходным кодом. Сканер ищет следующие уязвимости:

- SQL-инъекции;
- XSS;
- XXE Injection;
- Integer Overflow/Underflow (кстати, единственный сканер, который их нормально ищет);
- раскрытие содержимого файла (local file inclusion);
- внедрение кода;
- path traversal;
- внедрение HTTP-заголовков;
- плохие настройки CORS.

Сканеры уязвимостей

Nessus – сканер безопасности, позволяющий ищет следующие проблемы:

- раскрытие версий ПО на хостах;
- активная малварь;
- уязвимость к брутфорсу;
- слабые методы авторизации;
- открытые данные на целях (возможность перечислить учетные записи и группы, удаленный реестр и сетевые папки);
- некорректные разрешения и политики безопасности.

Может работать как краулер.

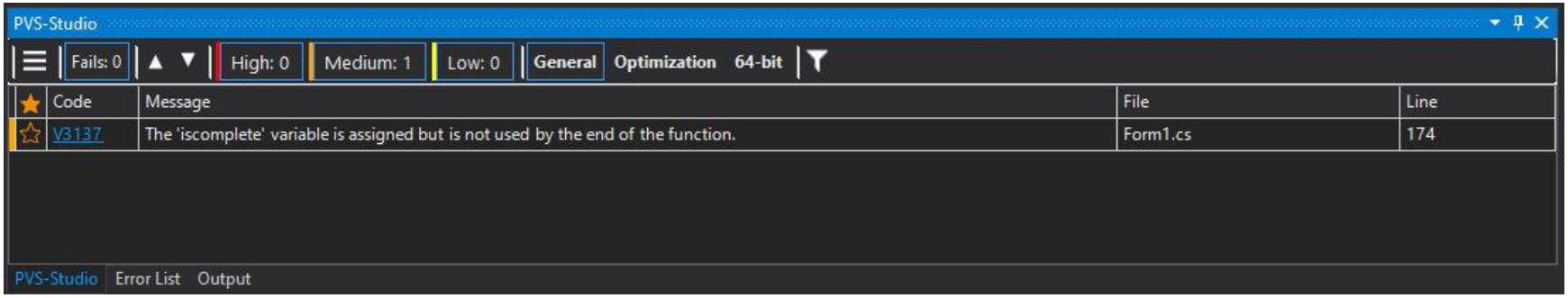
Поисковый робот (**веб-краулер** *Web crawler*; «*веб-паук*») – программа, являющаяся составной частью поисковой системы и предназначенная для перебора страниц Интернета с целью занесения информации о них в базу данных поисковика.

Сканеры уязвимостей

Kube-hunter – специализированный сканер уязвимостей для анализа безопасности кластеров Kubernetes. Сканер проводит поиск уязвимостей в удаленных кластерах, после чего позволят использовать их. Очень удобная функция, которой нет в других сканерах, – возможность просматривать результаты работы на онлайн дашборде, даже если сканер работает за NAT или еще как-то отгорожен от сети. Kube-hunter можно использовать не только против удаленной цели. Еще его можно установить как pod и сканировать изнутри.

Trivy – сканер безопасности контейнеров. Для bug bounty менее пригоден по сравнению с Kube-hunter, но довольно точен и быстр. Специализируется конкретно на Docker.

PVS-Studio – статический анализатор, позволяющий анализировать программный код на наличие уязвимостей.



Сканеры уязвимостей

Gitleaks – сканер открытых репозиториев, который позволяет:

- проверять локальные изменения до коммита, чтобы избежать утечек данных еще на стадии разработки;
- проверять любые репозитории GitHub/GitLab, в том числе приватные репозитории, если есть ключ доступа;
- проверять все репозитории заданного пользователя или организации;
- выдавать отчет в JSON для последующего автоматического анализа;
- интегрироваться с Git, для предотвращения непреднамеренной утечки.

Burp Suite – универсальный инструмент, включающий в себя прокси, сканер уязвимостей, паук-краулер, репитер запросов или платформу для множества плагинов.

Имеется GUI с удобными вкладками, автоматические модули для подбора паролей, идентификаторов, фаззинга, кодировщики и раскодировщики данных в разных форматах.

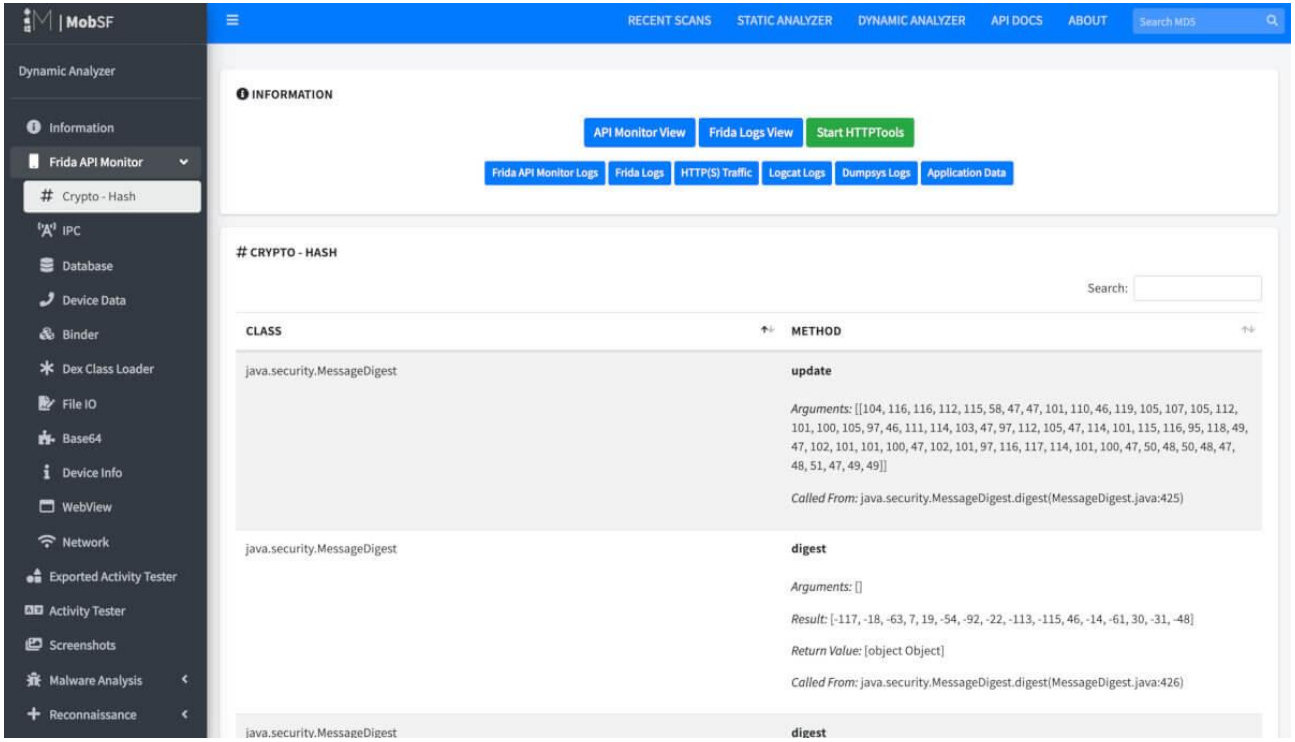
Сканеры уязвимостей

QARK – инструмент, для быстрого анализа APK на некоторые уязвимости:

- некорректно экспортируемые элементы или неправильные права доступа к экспортируемым объектам;
- уязвимые интенты;
- неправильная работа с сертификатами X.509;
- создание файлов, которые доступны другим приложениям, и работа с такими файлами;
- уязвимости activity;
- использование приватных ключей;
- слабые шифры;
- tapjacking;
- приложение разрешает бэкап своей приватной папки или имеет флаг android:debuggable=true.

Сканеры уязвимостей

MobSF – сканер-статический анализатор мобильных приложений. Формирует отчет о найденных багах с указанием возможности эксплуатации. Сканер умеет анализировать код, сертификат, которым подписано приложение, его манифест (AndroidManifest.xml) и позволяет выгрузить декомпилированный код для последующего анализа в других программах. Анализ выполняется как статически (декомпиляция и анализ полученного кода), так и динамически (запуск в виртуальном окружении).



Сканеры уязвимостей

Сканер	Категория	Цена	Интерфейс	Комментарии
Sn1per	Web / Recon	Бесплатно / 150+ долларов	Консольный	Универсальный комбайн
wapiti3	Web	Бесплатно	Консольный	
Nikto	Web	Бесплатно	Консольный	Немного устарел
OWASP ZAP	Web	Бесплатно	GUI	Быстрый и удобный
sqlmap	Web	Бесплатно	Консольный + GUI	Только SQL-инъекции
Acunetix	Web	4500+ долларов	Web-приложение	
Vega	Web	Бесплатно	GUI	Хорошая замена Acunetix
Kube-hunter	Kubernetes	Бесплатно	Консольный	
Trivy	Docker	Бесплатно	Консольный	
PVS-Studio	Анализ кода	Бесплатно / ~5250 евро	Дополнение к VS	Умеет в C/C++/C#/Java
Gitleaks	Git	Бесплатно	Консольный	
QARK	Анализ кода	Бесплатно	Консольный	Слабоват по сравнению с MobSF
Burp Suite	Web	Бесплатно / 400+ долларов	GUI	
MobSF	Анализ кода	Бесплатно	Web-приложение	
Nessus	Анализ сети	Бесплатно / 3120+ долларов	Web-приложение	