PHYSICS AND MATHEMATICS

УДК 004.4'234

Кинтонова А.Ж.,
Баенова Г.М.,
Урынбасарова А.Ж.
Евразийский национальный университет им.Л.Н.Гумилева
DOI: 10.24411/2520-6990-2020-11848

ВОПРОСЫ БЕЗОПАСНОСТИ ВЕБ ПРИЛОЖЕНИЙ

Kintonova A.Zh.,
Baenova G.M.,
Urynbassarova A.Zh.
Eurasian National University named after L.N. Gumilyov

SECURITY ISSUES OF WEB APPLICATIONS

Аннотация.
В статье показана актуальность вопросов безопасности веб – приложений. В работе дано понятие веб-приложению, описана обобщенная трехуровневая архитектура веб-приложения, показаны типы тестов для сканеров веб-приложений, общие принципы тестирования, меры безопасности веб-приложений, сканеры защищенности, ориентированные на веб-приложения.

Abstract.
The article shows the relevance of web application security issues. The concept of a web application is given in the paper, a generalized three-level architecture of a web application is described, types of tests for web application scanners, general principles of testing, security measures of web applications, security scanners focused on web applications are shown.

Ключевые слова: *веб-приложение, архитектура, безопасность веб-приложения, сканер веб-приложения, принципы тестирования, меры безопасности.*
Keywords: *web application, architecture, web application security, web application scanner, principles of testing, security measures.*

Сейчас многие компании имеют свое представительство в интернете. В современном мире работа большинства компаний тесно связана с веб-приложениями. Бизнес-процессы осуществляются через веб-приложения. Раньше в области безопасности больше акцент ставился на безопасность сетей и хостов. Но сейчас все больше внимания уделяется безопасности веб-приложений. Безопасность web-приложений отличается и от защиты традиционного ПО.

Веб-приложение - это программа, которая доступна через веб-браузер и работает на веб-сервере. Обновляя веб-приложения на сервере, все пользователи получают доступ к обновленной версии.

Веб – технологии, с одной стороны позволяют компаниям для ведения бизнеса эффективно связываться с поставщиками, клиентами и другими заинтересованными сторонами, с другой стороны это породило множество ранее неизвестных угроз безопасности. Веб-приложения, которые не проходят регулярный аудит с использованием сканера веб-приложений, являются сегодня наиболее уязвимыми элементами ИТ-инфраструктуры организации.

С точки зрения архитектуры веб-приложение представляет собой трёхуровневую систему. Обычно первый уровень представляет собой веб-браузер, второй уровень - инструмент технологии создания контента, такой как Java-сервлеты или ASP (страницы активных серверов), а третий уровень - базу данных компании.

Веб-браузер отправляет начальный запрос на средний уровень, который, в свою очередь, после обработки запроса, обращается к базе данных для выполнения запрошенной задачи, либо получая информацию из базы данных, либо обновляя ее. Поскольку веб-приложения находятся на сервере, они могут обновляться и модифицироваться в любое время без необходимости установки программного обеспечения на клиентских компьютерах. Это является основной причинной широкого распространения веб-приложений в современных организациях[2].

Благодаря различным механизмам обнаружения и защиты от вторжений, разработанным компаниями, занимающимися сетевой безопасностью, получение несанкционированного доступа к локальной сети организации стало намного более сложной задачей чем раньше.

Сегодня межсетевые экраны, сканеры безопасности и антивирусное программное обеспечение защищают практически все корпоративные сети. В связи с этими мерами безопасности, злоумышленники изучают альтернативные способы взлома инфраструктуры.

К сожалению, злоумышленникам удалось довольно быстро найти новый способ проникновения в корпоративную инфраструктуру – проникновение через веб-приложения. Веб-приложения по своей природе доступны в Интернете круглосуточно и без выходных. Это обеспечивает злоумышленникам легкий и постоянный доступ к ним и предоставляет практически неограниченное количество попыток взлома.

Меры безопасности веб-приложений: 1) регулярно выполнять *выполнять процесс обнаружения уязвимостей веб-приложения на протяжении жизненного цикла разработки программного обеспечения (SDLC)*, а не только в процессе эксплуатации. *Тестирование на ранних стадиях разработки имеет первостепенное значение*, поскольку в дальнейшем может быть очень сложно или вовсе невозможно обеспечить безопасность приложения, не переписав его. *2) Технологии обнаружения уязвимостей в веб-приложениях:* автоматическое сканирование по принципу белого ящика (white box); проверка исходного кода вручную; тест на проникновение (penetration test); автоматическое сканирование по принципу черного ящика. (black box). Лучшего из них не существует — каждый имеет свои плюсы и минусы. По версии *Виды тестирования:* 1) статическое тестирование (SAST, Static Application Security Testing); 2) динамическое тестирование (DAST); 3) интерактивное тестирование (IAST); 4) тестирование мобильных приложений (MAST)[1].

Для решения задач безопасности веб-приложений на рынке существуют сканеры безопасности, осуществляющие анализ состояния защищенности как информационной системы в целом, так и отдельных ее компонентов (операционных систем, СУБД, веб-приложений и т. д.).

Сканеры информационной безопасности (сканеры уязвимостей) — это средства мониторинга и контроля, с помощью которых можно проверять компьютерные сети, отдельные компьютеры и установленные на них приложения на наличие проблем защищенности. Не все сканеры веб-приложений обладают одинаковым набором сканирующих модулей[3].

Сканеры защищенности веб-приложений: Web Application Scanning (WAS), Web Application Security Scanner (WASS), Web Application Vulnerability Scanners (WAVS), Web Application Security Vulnerability Scanners (WASVS). Также возможны другие наименования: например, на Западе сейчас также используется наименование Application Security Testing (AST), являющееся более емким классом продуктов (включает в себя несколько методов тестирования, а также выполняет сканирование веб-приложений, облачных решений и мобильных приложений). Продукты Application Security Testing выполняют анализ и тестирование приложений с использованием нескольких методов: Static AST (SAST): статическое сканирование безопасности приложений, при котором осуществляется анализ исходников веб-приложения (кода), как правило, на стадиях его программирования и тестирования; Dynamic AST (DAST): динамическое сканирование безопасности приложений, при котором осуществляется анализ рабочего приложения; Interactive AST (IAST): интерактивное сканирование безопасности приложений, при котором осуществляется анализ приложений с помощью комбинированного подхода (с использованием SAST и DAST)[4].

Типы тестов для сканеров веб-приложений: 1) базовые функциональные (smoke) тесты(должны проверять работоспособность основных низкоуровневых узлов сканера: работу транспортной подсистемы, подсистемы конфигурации, подсистемы логирования и т. п.); 2) функциональные (functional) тесты (должны реализовать проверку основных сценариев для проверки технических требований); 3) тесты на сравнение (compare) функциональности (в ходе которых выполняется сравнение качества и средней скорости поиска объектов выбранным модулем сканера с аналогичными по функционалу модулями в продуктах-конкурентах); 4) тесты на сравнение показателей оценочных критериев (criteria) (в ходе которых проверяется, что скорость и качество поиска объектов каждым сканирующим модулем в каждой новой версии тестируемого сканера — не ухудшились по сравнению с предыдущей версией).

Общие принципы тестирования: 1)подготовить необходимый тестовый контент для функциональной проверки всех технических требований и развернуть тестовые стенды; 2) инициализировать тесты, получить все необходимые настройки для тестов; 3) сконфигурировать сканируемое веб-приложение и выбрать для него тип уязвимости и уровень защиты; 4) запустить сканер с выбранными настройками на тестируемом веб-приложении и пройти набор функциональных тестов; 5) подсчитать и классифицировать найденные сканером веб-объекты (уникальные ссылки, уязвимости, векторы атаки и т. п.); 6) повторить шаги 2—5 для каждого типа уязвимостей и уровней защиты[2].

Вопросы безопасности и конфиденциальности в настоящее время очень актуальны. Сейчас все больше внимания уделяется безопасности веб-приложений. Безопасность web-приложений отличается от защиты традиционного ПО. В данной статье мы рассмотрели типы тестов для сканеров веб-приложений, общие принципы тестирования, меры безопасности веб-приложений, сканеры защищенности, ориентированные на веб-приложения.

Список литературы:

1. Богдан Тоболь. Защита веб-приложений: мифы и реальность. https://www.anti-malware.ru/analytics/Technology_Analysis/web-security-myths-and-reality

2. Яковлев Георгий Олегович, Батетников Илья Андреевич. Обеспечение безопасности сторонних компонентов веб приложений. https://cyberleninka.ru/article/n/obespechenie-bezopasnosti-storonnih-komponentov-veb-prilozheniy

3. Тимур Гильмуллин. Тестирование сканеров безопасности веб-приложений: подходы и критерии. https://habr.com/ru/company/pt/blog/187636/

4. Александр Хонин. Сканеры защищенности веб-приложений (WASS) – обзор рынка в России и в мире.https://www.anti-malware.ru/reviews/web_application_security_scanners_market_russia_