МЕТОДИКА АНАЛИЗА УЯЗВИМОСТЕЙ ПРИ ТЕСТИРОВАНИИ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ ВЕБ-ПРИЛОЖЕНИЙ

А.Ю. Пузеева

Проведение тестирования на проникновение регулируется стандартами и методиками, которые упорядочивают этапы тестирования, устанавливают последовательность действий для выявления различных угроз и уязвимостей и прочее. Наиболее распространенными методиками на сегодняшний день являются стандарт NIST SP 800-115, OWASP Web Security Testing Guide, методика OSSTMM, стандарт PTES и другие. Методика OSSTMM и стандарты NIST SP 800-115, BSI носят больше теоретический характер, при этом NIST SP 800-115 и BSI фактически являются стандартами стран-разработчиков, которых необходимо придерживаться, проводя тестирование на проникновение в этих странах. Стандарт PTES является практико-ориентированными и содержат широкий набор технических рекомендаций и конкретных уязвимостей, которые необходимо проверять в ходе тестирования на проникновение. Методика OWASP является узконаправленной на тестирование веб-приложений. Подробное изучения и анализ вышеперечисленных методик позволил приступить к разработке методики анализа уязвимостей при тестировании безопасности инфраструктуры веб-приложений. Данная методика включает следующие этапы: выбор перечня инструментов для проведения тестирования, настройка виртуальной среды; сбор информации об тестируемом приложении, а именно сканирование портов, исследование видимого контента и др.; анализ уязвимостей веб-приложения, посредством тестирования приложения на возможность реализации инъекций (SQL, SOAP, LDAP, XPATH и т.д.), XSS-уязвимостей, XML-сущностей и др.;

анализ механизмов аутентификации и авторизации пользователей; проверка найденных уязвимостей путем попытки их эксплуатации; составления отчета о результатах тестирования.

Данная методика была апробирована на веб-приложении Railsgoat, в результате чего был получен подробный отчет, содержащий не только информацию о выявленных уязвимостях, но и подробные рекомендации по их ликвидации. Таким образом, данную методику можно рекомендовать для тестирования безопасности инфраструктуры клиент-серверных веб-приложений, использующих различные технологии и построенные на основе различных языков программирования [1–4].

Литература

1. Technical Guide to Information Security Testing and Assessment [Электронный ресурс]. – Режим доступа: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf – Дата доступа: 29.04.2021.

2. OWASP Web Security Testing Guide [Электронный ресурс]. – Режим доступа: https://owasp.org/www-project-web-security-testing-guide/v42/ – Дата доступа: 29.04.2021.

3. The Open Source Security Testing Methodology Manual [Электронный ресурс]. – Режим доступа: https://www.isecom.org/OSSTMM.3.pdf – Дата доступа: 29.04.2021.

4. PTES Technical Guidelines [Электронный ресурс]. – Режим доступа: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines – Дата доступа: 29.04.2021.