Resumen

Hoy en día muchas empresas adoptan la arquitectura cliente-servidor para manejar la lógica de su negocio. El principal problema de estos sistemas, es que se utilizan herramientas que requieren la intervención humana y procesos manuales para encontrar vulnerabilidades, afectando de manera directa al tiempo requerido para parcharlas. Una vulnerabilidad que los hackers pueden explotar son las cookies generadas por los sitios web, porque de acuerdo a la literatura, contienen información sensible del usuario que puede ser robada mediante ataques de tipo Cross-Site Scripting (XSS). Por otro lado, la creación de bots maliciosos ha provocado que las empresas apliquen sistemas CAPTCHA para contrarrestar estos ataques, pero con la aplicación de técnicas de visión artificial se podrían vulnerar estos sistemas. En este contexto, el objetivo del presente trabajo es diseñar e implementar bots para automatizar las tareas de búsqueda y análisis de vulnerabilidades en sistemas web, utilizando herramientas RPA. Para el desarrollo del bot para vulnerar sistemas CAPTCHA, se utilizó la herramienta UiPath y técnicas de visión artificial para su análisis. Mientras que para el bot de análisis de vulnerabilidades XSS se utilizó la herramienta UI.Vision y scripts desarrollados en Python para su análisis. Con los resultados se demostró que las páginas webs pueden ser vulneradas mediante ataques de tipo XSS por medio del análisis de sus cookies, y que los sistemas CAPTCHA basados en imágenes pueden ser vulnerados utilizando técnicas de visión artificial. Nuestro aporte es el estudio comparativo realizado entre las herramientas UiPath y UI.Vision para mejorar la automatización de procesos repetitivos. Además de un modelo para el testeo automatizado de sistemas web, mejorando la velocidad de detección de las vulnerabilidades (CAPTCHA y XSS) y proporcionando datos que contribuyan a futuras investigaciones.

Palabras claves: vulnerabilidades web, Cross-Site Scripting, CAPTCHA, RPA.

Abstract

Many companies today adopt client-server architecture to handle their business logic. The main problem with these systems is that tools that require human intervention and manual processes are used to find vulnerabilities, directly affecting the time required to patch them. A vulnerability that hackers can exploit is the cookies generated by websites because, according to the literature, they contain sensitive user information that can be stolen through Cross-Site Scripting (XSS) type attacks. On the other hand, creating malicious bots has caused companies to apply CAPTCHA systems to counteract these attacks, but these systems could be violated with artificial vision techniques. In this context, this work aims to design and implement bots to automate search and vulnerability analysis tasks in web systems using RPA tools. For the development of the bot to violate CAPTCHA systems, the UiPath tool and artificial vision techniques were used for its analysis. While for the XSS vulnerability analysis bot, the UI.Vision tools and scripts developed in Python were used for its analysis. The results showed that XSS-type attacks can violate web pages by analyzing their cookies and that CAPTCHA systems based on images can be violated using artificial vision techniques. Our contribution is the comparative study carried out between the UiPath and UI.Vision tools to improve the automation of repetitive processes. In addition to a model for the automated testing of web systems, improving the speed of detecting vulnerabilities (CAPTCHA and XSS) and providing data that contributes to future research.

Keywords: web vulnerabilities, Cross-Site Scripting, CAPTCHA, RPA.