БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет радиофизики и компьютерных технологий
Кафедра интеллектуальных систем

Аннотация к дипломной работе

Исследование средств защиты веб-ресурсов

Шестак Герман Алексеевич

Научный руководитель: старший преподаватель В.А. Чуйко

Минск, 2024

РЕФЕРАТ

Дипломная работа: 51 страница, 3 рисунка, 14 источников.

ROBOTIC PROCESS AUTOMATION, ПАРСИНГ, TRANSPORT LAYER SECURITY, CROSS-SITE REQUEST FORGERY, CANVAS, DENIAL-OF-SERVICE ATTACK, ЧЕЛОВЕЧНОСТЬ, SELENIUM

Объект исследования – методы защиты веб-ресурсов от автоматизированного взаимодействия

Цель работы – анализ существующих средств защиты веб-ресурсов от автоматизированных запросов. Анализ существующих методов противодействия защитным средствам. Применение результатов анализа для разработки программного обеспечения, взаимодействующего с выбранным веб-ресурсов и наглядно демонстрирующее уязвимые к автоматизации места.

Методы исследования – анализ исходного кода и сетевого трафика

В работе исследуется сферы применения RPA и парсинга, исследуются методы обнаружения и защиты от автоматических запросов к веб-ресурсу, такие как блокировка по ASN, использования TLS и CANVAS отпечатков. Исследуются методы противодействия защитам: изменения параметров TLS-отпечатка с целью мимикрировать под реальный браузер, использование специализированных программ для изменения характеристик устройства, исследуется автоматизация веб-браузере с использованием инструментов Selenium и WebDriver.

Результатом дипломной работы является применение на практике исследованных методов противодействия защитам от автоматических запросов для обнаружения уязвимых мест в защите выбранного веб-ресурса.

Полученные результаты способствуют развитию более эффективных и удобных для пользователей стратегий защиты, что является важным шагом в направлении повышения общей безопасности и удобства использования веб-ресурсов.

РЭФЕРАТ

Дыпломная праца: 51 старонка, 3 малюнка, 14 крыніц.

ROBOTIC PROCESS AUTOMATION, ПАРСИНГ, TRANSPORT LAYER SECURITY, CROSS-SITE REQUEST FORGERY, CANVAS, DENIAL-OF-SERVICE ATTACK, ЧАЛАВЕЧНАСЦЬ, SELENIUM

Аб'ект даследавання – метады абароны вэб-рэсурсаў ад аўтаматызаванага ўзаемадзеяння

Мэта працы – аналіз існуючых сродкаў абароны вэб-рэсурсаў ад аўтаматызаваных запытаў. Аналіз існуючых метадаў процідзеяння ахоўным сродкам. Ужыванне вынікаў аналізу для распрацоўкі праграмнага забеспячэння, які ўзаемадзейнічае з абраным вэб-рэсурсаў і наглядна дэманструе ўразлівыя да аўтаматызацыі месца.

Метады даследавання – аналіз зыходнага кода і сеткавага трафіку.

У працы даследуецца сферы ўжывання RPA і парсінгу, даследуюцца метады выяўлення і абароны ад аўтаматычных запытаў да вэб-рэсурсу, такія як блакіроўка па ASN, выкарыстанні TLS і CANVAS адбіткаў. Даследуюцца метады процідзеяння абаронам: змены параметраў TLS-адбітка з мэтай мімікрыраваць пад рэальны браўзэр, выкарыстанне спецыялізаваных праграм для змены характарыстык прылады, даследуецца аўтаматызацыя вэб-браўзэры з выкарыстаннем прылад Selenium і WebDriver.

Вынікам дыпломнай працы з'яўляецца ўжыванне на практыцы даследаваных метадаў процідзеяння абаронам ад аўтаматычных запытаў для выяўлення ўразлівых месцаў у абароне абранага вэб-рэсурсу.

Атрыманыя вынікі спрыяюць развіццю больш эфектыўных і зручных для карыстальнікаў стратэгій абароны, што з'яўляецца важным крокам у напрамку павышэння агульнай бяспекі і зручнасці выкарыстання вэб-рэсурсаў.

ABSTRACT

Thesis: 51 pages, 3 figures, 14 sources.

ROBOTIC PROCESS AUTOMATION, PARSING, TRANSPORT LAYER SECURITY, CROSS-SITE REQUEST FORGERY, CANVAS, DENIAL-OF-SERVICE ATTACK, HUMANITY, SELENIUM

The object of research – Methods for protecting web resources from automated interactions.

Objectives – Analysis of existing means of protecting web resources from automated requests. Analysis of existing methods to counter protective measures. Application of the analysis results to develop software that interacts with a selected web resource and clearly demonstrates vulnerabilities to automation.

Methods – Analysis of source code and network traffic.

The works explores the application areas of RPA and parsing, and investigates methods for detecting and protecting against automated requests to web resources, such as blocking by ASN, using TLS and CANVAS fingerprints. It also examines countermeasures against these protections: altering TLS fingerprint parameters to mimic a real browser, using specialized programs to change device characteristics, and automating web browsers using Selenium and WebDriver tools.

The outcome of the work is the practical application of the studied methods to counteract protections against automated requests, aimed at identifying vulnerabilities in the protection of a selected web resource. The results contribute to the development of more effective and user-friendly protection strategies, which is an important step towards improving the overall security and usability of web resources.