

ОПТИМИЗАЦИЯ ОБХОДА СТРАНИЦ ДИНАМИЧЕСКИХ ВЕБ-ПРИЛОЖЕНИЙ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ БИБЛИОТЕКИ REACTJS

Говорков Илья Сергеевич

Студент

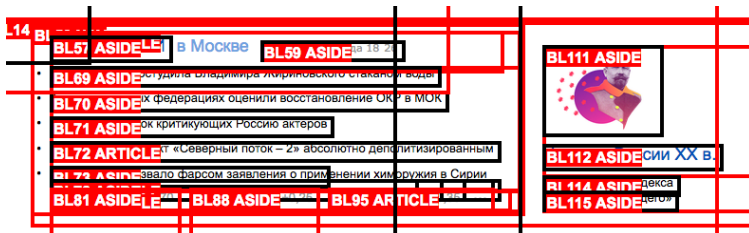
Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: govorkovmedian@yandex.ru

Данная работа посвящена исследованию возможности оптимизации процесса обхода (англ. crawling) динамических приложений с пользовательским интерфейсом, написанным с использованием современного JavaScript фреймворка — ReactJS, — за счет предварительной сегментации страниц [2][4].

При проведении проверки защищенности приложения методом «черного ящика» [5 с. 27] эксперту в первую очередь необходимо выделить так называемые входные точки — HTTP запросы (включая параметры и их возможные значения), при помощи которых происходит доступ к функциям веб-приложения. Распространенным подходом [1][3] к решению данной задачи является реализация процесса обхода приложения и моделирование поведения пользователей для создания графа состояний приложения и выделения тех переходов между состояниями, которые приводят к созданию HTTP запроса (к активации входной точки). С ростом сложности современных приложений, особенно в контексте SPA(Single Page Application), ручной анализ становится неприменимым. В то же время проблемой автоматизированных подходов, как, например [1][3], является неопределенность порядка обхода в условиях отсутствия информации о текущем состоянии серверной стороны веб-приложения.

Данная работа нацелена на оптимизацию автоматизированного обхода за счет предварительной сегментации страницы.



Пример сегментации страницы с помощью фреймворка Block-o-Matic [4]

В данной работе под «сегментом страницы» понимается некоторая ее визуально выделенная часть. В основу данной работы положено следующее предположение:

Предположение 1. *Предположение о том, что в одном сегменте страницы содержатся однородные элементы с точки зрения обхода приложения и поиска входных точек.*

В рамках указанного предположения 1 сегментация страницы может позволить принять более информированное решение о дальнейшем направлении обхода. Целью данной работы является проверка указанного предположения 1.

Данная работа находится в процессе завершения. Для достижения поставленной цели предпринимаются следующие шаги:

- разработка методики определения однородности элементов в одном сегменте страницы;
- разработка программного средства на основе [4], получающего на вход множество сегментов страницы и выделяющего с использованием разработанной методики сегменты, содержащие однородные элементы;
- создание выборки сайтов, использующих библиотеку ReactJS, для проведения практического испытания;
- проведение эксперимента над созданной выборкой сайтов и разработанным средством для проверки основного предположения 1.

На данном этапе уже реализован прототип указанного программного средства.

Литература

1. Петухов А. А., Носеевич Г. М. ПОИСК ВХОДНЫХ ТОЧЕК ДЛЯ ВЕБ-ПРИЛОЖЕНИЙ С ДИНАМИЧЕСКИМ ПОЛЬЗОВАТЕЛЬСКИМ ИНТЕРФЕЙСОМ //Безопасность информационных технологий. - 2013 - с. 13-20.
2. Cai Deng et al. Extracting content structure for web pages based on visual representation. - 2003.
3. Mesbah A. et al. BozdagE Crawling AJAX by Inferring User Interface State Changes. - 2008.
4. Sanoja A., Gancarski S. Block-o-Matic: A web page segmentation framework - 2014.

5. Open Web Application Security Project OWASP Testing Guide v4
- 2015 <https://www.owasp.org/images/1/19/OTGv4.pdf>