Исследование синтаксической структуры точек отправки запросов на сервер клиентской стороны веб-приложения

Пятаков Никита Сергеевич

Студент

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

E-mail: pyatakovns@seclab.cs.msu.ru

Научный руководитель *— Хашаев Артур Акрамович*

JavaScript используется в качестве языка программирования клиентской стороны на более чем 94% всех веб-сервисов. Исходя из этого, можно с точностью сказать, что данный язык сейчас является неотъемлемой частью подавляющего большинства сайтов, поэтому для исследования сайта на наличие уязвимостей, необходимо уметь анализировать JavaScript-код [1].

Данная работа посвящена синтаксической классификации точек отправки HTTP-запросов в клиентском JavaScript-коде и реализации соответствующих инструментов статического анализа клиентского JavaScript-кода для их поиска и классификации.

Задача поиска данных точек решалась с помощью написанного статического анализатора, который по коду на языке JavaScript строит AST и предоставляет интерфейс для обхода полученного AST, включающий поиск вызовов API для отправки HTTP-запроса.

Для классификации собранных точек было решено провести анализ с точки зрения того, насколько легко поддается статическому анализу та или иная точка отправки HTTP-запроса. Было проведено экспериментальное исследование на выборке из Alexa Top 1000. Результаты эксперимента получились следующими:

Класс	Количество	%
Значения аргументов известны из вызова	5,314	18.94
Часть аргументов неизвестна из вызова	12,844	45.89
Ни один аргумент не известен из вызова	9,887	35.25

Таблица 1: Статистика по классам сложности анализа точек отправки запросов

Полученная статистика по классам показала, что большенство точек тяжело поддается анализу. Данный результат указывает на

необходимость в исследовании JavaScript-кода и разработке соответствующих анализаторов.

Публикация подготовлена при поддержке Министерства науки и высшего образования РФ в рамках Договора о предоставлении гранта на государственную поддержку центров НТИ от 15.08.2019 № 7/1251/2019.

Литература

1. An Analysis of the Dynamic Behavior of JavaScript Programs / G. Richards [и др.] // Proceedings of the 31st ACM SIGPLAN Conference on Programming Language Design and Implementation. — Toronto, Ontario, Canada : Association for Computing Machinery, 2010. — с. 1— 12. — (PLDI '10).
2. Analysis of JavaScript Programs: Challenges and Research Trends / K. Sun, S. Ryu // ACM Comput. Surv. — New York, NY, USA, 2017. — авг. — т. 50, No 4.
3. Statically Checking Web API Requests in JavaScript / E. Wittern [и др.] // 2017 IEEE/ACM 39th International Conference on Software Engineering (ICSE). — 2017. — с. 244—254.