Thesis Summary Report: Dynamic Analysis using a browser add-on.

Allen Varghese • 01.20.2023

Overview

Thesis focuses on creating a browser extension that tracks and logs the usage of various JavaScript API calls on a website. The extension uses "monkey patching" technique to override default behavior of certain API calls like alert(), getElementById(), and getElementsByTagName(), and keeps track of how many times they are called.The extension captures the API calls and their count in a global variable which can be exported. The data collected by the extension can be sent to a MongoDB database, where it can be analyzed, stored and queried.

- The goal of the extension is to provide developers with a tool for monitoring the usage of JavaScript API calls on their website, which can help identify potential performance bottlenecks, security issues, and areas for optimization.
- The extension can also be useful for analyzing the behavior of third-party scripts and identifying any potential conflicts or issues with the website's own scripts.
- The data collected by the extension can be sent to a MongoDB database, where it can be analyzed, stored, and queried.
- This allows developers to track the usage of API calls over time and gain insights into how their website is being used by visitors.

- Machine learning can be used to analyze patterns of API calls made on a website, and identify any anomalies that may indicate malicious activity.
- By training a model on a dataset of labeled examples, such as known attacks or benign interactions, the model can be used to identify potential vulnerabilities in the website's code and flag them for further investigation.
- Another approach is to use machine learning to analyze the behavior of users on the website and identify any suspicious or unusual activity.
- For example, a model can be trained to recognize patterns of user interactions that are typical of automated bots or scrapers, and flag any instances of such behavior for further investigation.
- By identifying potential malicious activity, the model can prevent users from navigating to malicious sites by alerting the developer or blocking access to the site.

Concepts/Topics Learned

So far, I was able to understand the key difference between properties of the object being used/created as well as creating new instance of a given function so that it can be monitored, and policies/other function calls can be embedded in them. This concept of intercepting the function call and applying/enforcing policies or other function calls helps to give users more control of their data as well as blocking unwanted redirection which prevents drive by downloads and other unwanted installations.

Next steps

Train a machine learning algorithm.

Repository:

https://github.com/isseclab-udayton/allen-thesis-s23