Introductory Special Topics in Security and Privacy<Web Mobile Service Security: Practice & Case studies> Project proposal

Antoine RONDELET (20176461) and Ndeye Khady NGOM (20176440)

Abstract

With the growing use of the world wide web, web browsers become more and more sophisticated. Many companies want to develop their own browser and try to dethrone the leading actors of this market. As web browsers embed more and more features, some security flaws are likely to appear in some of them. While XSS attacks target websites or web applications, Universal XSS attacks exploit vulnerabilities in the web browser or in its extension to engender an XSS condition and affect the browser's behavior and security. The goal of this project is to try to find Universal XSS vulnerabilities in the Brave web browser developed by Brave Software Inc.[†]

1. Description of the browser Brave (extracted from Wikipedia):

Brave is a free and open-source web browser based on the Chromium web browser and its Blink engine, announced by the co-founder of the Mozilla Project and creator of JavaScript, Brendan Eich. It claims to block website trackers and remove intrusive Internet advertisements, while inserting its own. The browser also claims to improve online privacy by sharing less data with advertising customers. As of 2017, it is currently in beta testing for Windows, macOS, and Linux and available as a stable release for iOS and Android.

2. Project title

Try to find Universal Cross Site Scripting (UXSS) vulnerabilities in the Brave web browser.

2.1. Objectives

The objectives of this project is to find UXSS vulnerabilities in Brave through the study of previous UXSS attacks against other web browsers.

2.2. Proceedings

In order to achieve our objectives, we plan to proceed step by step until the discovery of UXSS vulnerabilities. Here are the steps we plan to follow:

- Do some additional research on UXSS to fully understand the potential breach we could use later on.
- Study previous UXSS attacks.
- Become familiar with part of the code base of Brave and try to find vulnerabilities to UXSS using knowledge acquired in previous steps
- If some patterns can be deduced from previous UXSS attacks payloads, then develop a tool that generates potential payloads for UXSS attacks, based on the patterns we detected

2.3. What if we fail to find vulnerabilities ?

We think that this project is quite ambitious for two persons that have no experience in web security. However, we truly feel motivated by trying to find vulnerabilities in the browser. UXSS is a hot topic. Moreover, Brave is based on Chromium, and the community reports its findings on a day to day basis for the companies to develop patches. That is why it is possible that we do not manage to find any UXSS vulnerabilities in Brave. Even if we are going to do our best to come up with vulnerabilities, the risk of failure is real. If this is the case, our deliverable would be a report tracing all the reflections we made to try to find breaches in Brave coupled with the code we wrote.