Browser Exploitation

5-Day Security Training on Advanced Browser Exploitation

Course Description:

Web browsers are among the most utilized consumer facing software products on the planet. As the ubiquitous gateway to the internet, browsers introduce significant risk to the integrity of personal computing devices. In the race to protect users while advancing web technology, premiere browsers have become increasingly complex targets to compromise.

Over the course of this training, students will receive a thorough introduction to vulnerability research as it pertains to modern web browsers. This includes identifying, evaluating, and weaponizing the latest vulnerability patterns via the exploitation of several recently patched vulnerabilities. Through this, students will experience the end to end process of developing memory corruption based exploits against these high value targets. This course will focus specifically on Google Chrome and Apple Safari.

Learning Outcomes:

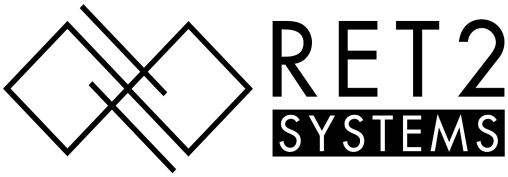
- Identify contemporary vulnerability patterns in web browsers
- Develop an understanding of target-specific exploit techniques
- Weaponize a diverse selection of real-world vulnerabilities
- Execute renderer-only attacks to hijack user sessions
- Clone, build, and debug properly versioned browser engines
- Learn tooling for vulnerability discovery against massive codebases
- Become familiar with the architecture of modern web browsers
- Build an in-depth understanding of browser internals and JavaScript engines
- Obtain a high level overview of browser sandboxing

Prerequisites:

- Familiar with modern exploitation subjects (DEP, ASLR, ROP)
- Working knowledge of C++ and JavaScript
- Some exposure to AMD64 assembly or low level systems
- Linux command line proficiency
- A Laptop capable of connecting to the internet (SSH, VNC)

Course Registration:

For more information on how to register for our next public training event, please visit our website at https://ret2.io/trainings. If you can't make it, we would be happy to offer private versions of this training at a location of your choice. Please inquire at contact@ret2.io



Course Syllabus:

1. **Browser Architecture (General, Chrome, Safari/Webkit)**
    - Breaking down modern browser architectures, major components
    - Setting up a browser research environment, building, debugging
    - Interfacing with different components of the browser (DOM, JS)
    - Introduction to JavaScript engines
    - JavaScript + DOM interaction, past issues

2. **JavaScript Internals in Exploitation (General, V8, JSC)**
    - A deepdive into JavaScript engine internals
    - Low-level JavaScript types and natives
    - Garbage collection implementations
    - Current vulnerability pattern found in JS engines
    - Introduction to exploit building blocks (Primitives)

3. **JavaScript JIT Compilers (General, V8)**
    - Overview of JavaScript JIT compiler pipelines
    - Exploring JIT debugging tools
    - Optimizations and typing
    - Type cache and speculation
    - JIT vulnerability classes, contemporary exploits

4. **Exploiting JavaScript Engines (General, V8, JSC)**
    - Layering exploit primitives
    - Locating interesting structures
    - Overwriting JIT structures
    - Control flow hijacking
    - Continuation of execution

5. **Applied Exploit Engineering (General)**
    - Bypassing browser-specific mitigations
    - SOP bypasses and renderer-only attacks
    - N-Day exploitation exercises
    - Performing independent browser vulnerability research
    - Time permitting: Intro to sandboxing / sandbox escapes