

WTCS402 Web Technologies Lab

Lab Project: JavaScript Mischief

Due: Tuesday, March 6, 2018

Browsers provide a rich set of features that enable interactive, compelling web applications. Unfortunately, these features are also open to abuse. This project demonstrates how web sites can spy on the user, steal sensitive information, and render the browser inoperable.

- É This is an individual project.
- É Use the Firefox browser for this project, and for all projects in this class.
- É you're pretending to be an attacker for this project, so your HTML files do not have to pass validation.
- É Unless noted otherwise, avoid the use of external scripts and stylesheets. Everything should be included in the HTML file.

Part 1. Denial of service

1a. Endless alert

Create a HTML document that, when opened, displays a JavaScript alert dialog box. Each time the user dismisses the dialog box, a new, identical dialog box should appear. As a result, the user will be unable to interact with the browser window.

- É You can put whatever text you want in the alert. (Be creative!)
- É To recover from this attack, it may be necessary to terminate your browser process. On Windows, you can use Task Manager (Ctrl+Alt+Del). On Mac OS, you can use Force Quit (Option-⌘-Esc)
- É Note that some browsers, such as Opera and Google Chrome, provide mitigations for this attack. Firefox does not.

1b. Whack-a-mole

Create an HTML page that contains a single button, which has the text "Click here" on it. When the button is clicked, the browser should open an infinite number of popup windows.

- É You can put whatever content you want in the popup windows.
- É Use a [data: URL](#) to give the popup window some content without making a network request.
- É Do not wait for the first window to be closed before opening the next one.
- É Your solution will be graded with the popup blocker **on** (the default setting).
- É The windows need to actually open visually; it doesn't count if the browser simply hangs.
- É You need to open windows, not tabs.

1c. Sticky page

Create a HTML document that the user cannot navigate away from. If the user tries to enter a URL into the address bar, click a bookmark, or use the search box, the browser should remain

at the same location. The browser should stay at this location no matter how many times the user tries to navigate away.

- É **You can put whatever content you want in the page.**
- É **The attack should work regardless of the URL where the page is located.**
- É **[Hint #1](#): Try navigating the page in `onunload` or `onbeforeunload` handler. Be sure to remove your handler to avoid creating an infinite loop.**
- É **[Hint #2](#): Try using `setTimeout` to delay your navigation by a few milliseconds.**
- É **It is acceptable (but not required) if the browser's "throbber" (progress indicator) spins for a brief moment before stopping. It should not keep spinning forever, however.**