browsersec
Browser Security Handbook

	Search projects

Project Home   **Downloads**   **Wiki**   **Issues**   **Source**

Search | Current pages ▼ | for | | Search

☆ **Main**
Browser Security Handbook landing page
Featured

Updated Sep 7, 2010 by lcam...@gmail.com

Browser Security Handbook

- Written and maintained by Michal Zalewski <lcamtuf@google.com>.
- Copyright 2008, 2009 Google Inc, rights reserved.
- Released under terms and conditions of the CC-3.0-BY license.

Table of Contents

Introduction

Hello, and welcome to the *Browser Security Handbook*!

This document is meant to provide web application developers, browser engineers, and information security researchers with a one-stop reference to key security properties of contemporary web browsers. Insufficient understanding of these often poorly-documented characteristics is a major contributing factor to the prevalence of several classes of security vulnerabilities.

Although all browsers implement roughly the same set of baseline features, there is relatively little standardization - or conformance to standards - when it comes to many of the less apparent implementation details. Furthermore, vendors routinely introduce proprietary tweaks or improvements that may interfere with existing features in non-obvious ways, and seldom provide a detailed discussion of potential problems.

The current version of this document is based on the following versions of web browsers:

Browser	Version	Test date	Usage*	Notes
Microsoft Internet Explorer 6	6.0.2900.5512	Feb 2, 2009	16%	
Microsoft Internet Explorer 7	7.0.5730.11	Dec 11, 2008	11%	
Microsoft Internet Explorer 8	8.0.6001.18702	Sep 7, 2010	28%	
Mozilla Firefox 2	2.0.0.18	Nov 28, 2008	1%	
Mozilla Firefox 3	3.6.8	Sep 7, 2010	22%	
Apple Safari	4.0	Jun 10, 2009	5%	
Opera	9.62	Nov 18, 2008	2%	
Google Chrome	7.0.503.0	Sep 7, 2010	8%	
Android embedded browser	SDK 1.5 R3	Oct 3, 2009	n/a	

* Approximate browser usage data based on public Net Applications estimates for August 2010.

Disclaimers and typographical conventions

Please note that although we tried to make this document as accurate as possible, some errors might have slipped through. Use this document only as an initial reference, and independently verify any characteristics you wish to depend upon. Test cases for properties featured in this document are freely available for download.

The document attempts to capture the risks and security considerations present for general populace of users accessing the web with default browser settings in place. Although occasionally noted, the degree of flexibility offered through non-standard settings is by itself not a subject of this comparative study.

Through the document, red color is used to bring attention to browser properties that seem particularly tricky or unexpected, and need to be carefully accounted for in server-side implementations. Whenever status quo appears to bear no significant security consequences and is well-

carefully accounted for in server-side implementations. Whenever status quo appears to bear no significant security consequences and is well understood, but a particular browser implementation takes additional steps to protect application developers, we use green color to denote this, likewise. Rest assured, neither of these color codes implies that a particular browser is less or more secure than its counterparts.

Acknowledgments

Browser Security Handbook would not be possible without the ideas and assistance from the following contributors:

- Filipe Almeida
- Brian Eaton
- Chris Evans
- Drew Hintz
- Nick Kralevich
- Marko Martin
- Tavis Ormandy
- Wladimir Palant
- David Ross
- Marius Schilder
- Parisa Tabriz
- Julien Tinnes
- Berend-Jan Wever
- Mike Wiacek

The document builds on top of previous security research by Adam Barth, Collin Jackson, Amit Klein, Jesse Ruderman, and many other security experts who painstakingly dissected browser internals for the past few years.

(*Continue to basic concepts behind web browsers...*)

Terms - Privacy - Project Hosting Help

Powered by Google Project Hosting