

SAST for JavaScript

A Brief Overview of Commercial Tools

Achim D. Brucker
achim.brucker@sap.com

SAP AG, Central Code Analysis Team

June 30, 2014

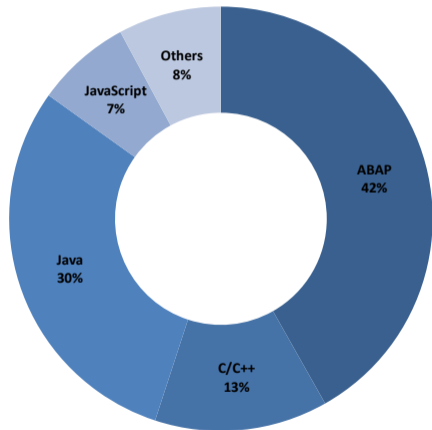
SAST for JavaScript: A Brief Overview of Commercial Tools

Abstract

Static application security testing (SAST) is a widely used technique that helps to find security vulnerabilities in program code at an early stage in the software development life-cycle. Since a few years, JavaScript is gaining more and more popularity as an implementation language for large applications. Consequently, there is a demand for SAST tools that support JavaScript.

We report briefly on our method for evaluating SAST tools for JavaScript as well as summarize the results of our analysis.

Static Code Analysis at SAP



Analyzed Languages (LoC) in 12/2013

- Since 2010, mandatory for all products
- Multiple billions lines analyzed (several thousands of products/projects)
- JavaScript:
 - Will overtake C/C++ in 2014
 - Average size ca. 200 kLoC (up to several mLoC)
- Also important: SQLScript, Python, Ruby
We also use: Perl, TCL, R, ...
- Mainly used tools:

Language	Tool	Vendor
ABAP	CVA (SLIN_SEC)	SAP
C/C++	Coverity	Coverity
Others	Fortify	HP

Initial Observation and Assessment of Situation



Initial Situation:

- Increasing adoption of scripting languages (client-side and server-side, large frameworks, etc.)
- High false negative rate (in contrast to most other languages)

Market Analysis:

- Only three tools
 - commercially supported
 - with broad security scope
- Many other tools
 - specialized (e.g., only DOM-based XSS)
 - failed already on parsing our code

Evaluation and Assessment Approach

Evaluation:

- We used most sensitive “default” configuration (no SAP specific template/filters)
- We used the same evaluation targets
 - library of JavaScript “challenges” (own examples, test cases from IBM Research)
 - three SAP applications of different size (including one with server-side JavaScript using the XS Engine)

Assessment:

- Overall analysis:
 - how many findings in total
 - reported categories
- Detailed comparison for
 - XSS-variants
 - All findings of the two topmost priorities (high)

Result Overview (Test Library)

	X	Z	Y
Scan duration (in s)	246	246	1147
Findings (all)	111	118	242
Findings (high)	52	80	119
True positive	+	+++	++
False negatives	-	+	+

We also tested three SAP applications

- Rather small (less than 100kLoC)
- Scalability is not a (big) problem (nightly scans are acceptable)
- Identified many aspects currently missing in test library

Observations:

- Only Z allows for
 - modifying existing checks
 - write own checks
- Y and Z have a better understanding of core JavaScript (they are very close)
- X and Z each have one check that reports most of the findings (false positives)
- Z includes checks for
 - use of outdated libraries (e.g., JQuery)
 - RegExp injection / RegExp DoS
- X includes checking of J2EE configurations
- Y mainly reports OWASP Top Ten

Conclusion and Outlook

“

- There is no good static analysis tool for JavaScript (applied) security available
- Static analyzers should be understood as frameworks (instead of off-the shelf tools)
- Frameworks and lack of modules creates as hard challenges as core JavaScript
- Good benchmark/evaluation libraries (similar to SAMATE) are needed

Response from tool vendors:

- Unsatisfactory results confirmed
- Fourth tool currently under development

And finally

- if you have questions (or want to discuss example libraries), please approach me
- want to see code examples, see my talk on Wednesday

Bibliography



Achim D. Brucker and Uwe Sodan.

Deploying static application security testing on a large scale.

In Stefan Katzenbeisser, Volkmar Lotz, and Edgar Weippl, editors, *GI Sicherheit 2014*, volume 228 of *Lecture Notes in Informatics*, pages 91–101. GI, March 2014.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company.

Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase, Inc. Sybase is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

The information in this document is proprietary to SAP. No part of this document may be reproduced, copied, or transmitted in any form or for any purpose without the express prior written permission of SAP AG.

This document is a preliminary version and not subject to your license agreement or any other agreement with SAP. This document contains only intended strategies, developments, and functionalities of the SAP® product and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development. Please note that this document is subject to change and may be changed by SAP at any time without notice.

SAP assumes no responsibility for errors or omissions in this document. SAP does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intent or gross negligence.

The statutory liability for personal injury and defective products is not affected. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages.