Berend-Jan Wever

berendj@nwever.nl | LinkedIn | Blog | Twitter

Senior Information Security Specialist

- Veteran of specialist security teams at both Microsoft and Google.
- Prolific vulnerability finder with a track record of discovering security issues in widely used application spanning more than 15 years impacting billions of internet users.
- Skilled security researcher with a knack for bypassing security boundaries and mitigations.
- Avid security community member contributing back through many publications and as a speaker at conferences.
- Microsoft Security Research Center Top 100 Security Researcher.

Selection of Recent Projects

BugId

Software to automatically analyze crashes and determine their security impact.

- Reduce the need for a large and costly team of specialized security engineers.
- Reduce time-to-patch and window of exploitability by prioritize important issues and speeding up analysis.
- Create detailed reports containing both concise management-level information and extensive technical details.

Browser Security Whitepaper

Whitepaper collecting all relevant information on the security of a number of different web browsers.

- Covers everything from high-level configuration management to low-level security technologies.
- Helps IT managers make an informed decision about which browser is best suited for their specific needs.
- Provides security experts with evidence based data on which browser protects best against specific risks.

Recent Work History

Owner of SkyLined Security

Company: SkyLined Security
Location: Work from home in the Netherlands
Period: 2011-2018
Position: Owner

- Developed automated security tests (fuzzers) that found a large number of issues in high-profile targets, including Microsoft Windows, Microsoft Internet Explorer, Microsoft Edge, Google Chrome, and Mozilla Firefox.
- Worked as an external consultant on a wide-range of projects from pen-testing, code-, and design-reviews, through fuzzer development and integration to writing whitepapers and guidance documents.

Google Chrome Security Team Founder

Company: Google
Location: Work from home in the Netherlands
Period: 2008-2011
Position: Senior Software Security Engineer

- Hired as an initial member of the Google Chrome Security Team. Hit the ground running to make sure the software did not ship with any mayor security issues three months later.
- Developed tools to look for and analyze security issues in nearly all parts of the codebase, which are still actively used to this date.
- Found large numbers of vulnerabilities, analyzed externally reported vulnerabilities and guided the patch process to release comprehensive fixes to customers at record speeds.

- Improved security by mitigating or preventing exploitation of issues through design and implementation changes and offered guidance and advise to Chromium project members on security related topics.
- Participated in setting up and maintaining the Google Chrome Vulnerability Reward Program.

Security Windows Initiative Attack Team member

Company: Microsoft
Location: Work from home in the United Kingdom
Period: 2005-2008
Position: Security Software Engineer

- Joined a newly formed team of two security researchers working from home in Cheltenham, UK, as the European branch of the larger SWI-AT team.
- Developed better tools to automate the detection of security issues, such as fuzzers and compiler plug-ins that detect vulnerable design and implementation patterns.
- Reviewed code and patches and analyzed external reports of vulnerabilities in Microsoft products.
- Researched new attack vectors and techniques and shared knowledge with developers working on various product teams.
- Took part in the hiring and on-boarding of additional team members in the UK.

Skills and Experience

Key skills

- Working from home for 15+ years with various teams based all over the world has resulted in good communicative skills and an ability to work both in a team and independent.
- A history of developing innovative security techniques has shown continuous initiative and creativity.
- A wide range of projects has provided experience in a large number of programming languages and applications. Programming languages include but are not limited to: ASP, x86, IA-32 & x86-64 Assembler, Batch scripting, C, C++, C#, CSS, ECMAScript, HTML, Java, JScript, PHP, Powershell, Python, SQL, SVG, VBScript, VML, and XML.
- Comfortable and experienced with learning new programming languages, applications and frameworks on the job.

Historically Notable Publications

A small selection of contributions to the information security community that have not been mentioned above:

- Developed and released various tools for security researchers as open source software.
- Released technical analysis of a large number of vulnerabilities and techniques.
- Illustrated the fragility of state-of-the-art web browser code by publishing a new way to crash a web browser - in a tweet - daily for a large part of 2016.
- Introduced heap-spraying in web browsers, a technique that facilitates exploitation of vulnerabilities in application. This technique has been widely adopted and built upon to bypass mitigations and create sophisticated and reliable exploits.
- Co-author of the world's smallest Windows shellcode and inventor of the concept of Omelette shellcode.
- Creator of the first practical alphanumeric shellcode encoder, which was ported to the Metasploit framework and author of ASCII art shellcode.
- Created the first Proof-of-Concept XSS worm in 2002 to warn of their potential danger; the first publicly released XSS worms proved they can causing serious damage 3 years later.

Spoken languages

Dutch - native
English - Fluent
German - Proficient
French - Basic