OWASP
The Open Web Application Security Project

Announcement meeting March 26th:

Software Vulnerability assessment

Summary

The main goal of the upcoming OWASP-NL meeting is to provide information to developers and security professionals involved in creating secure (web-)applications. The main focus will be on software vulnerability assessment. The speakers will give specific examples and of course there is time to ask questions about your own experiences.

Location

The location and catering is provided by the sponsor of this meeting:

Mercure Utrecht Nieuwegein
Buizerdlaan 10
3435 SB NIEUWEGEIN
Tel : (+31)30/6044844
Fax : (+31)30/6038374

FORTIFY SOFTWARE

Fortify Software products protect companies from today's greatest security risk: the software applications that run their businesses. Combining deep application security expertise with extensive software development experience, Fortify Software has defined the market with award-winning products that span the software development cycle. Today, Fortify Software fortifies the software for the most demanding customer deployments, including the world's largest, most varied code bases.

For more information please visit:
www.fortify.com

Program

17.30 - 18.30 **Check-In** (catering included)

18.30 – 18:50 **Introduction** (OWASP, sponsor)

18.50 - 19.30 **Complex(ity) matters** (Dutch) Mario de Boer

Various methods exist to locate specific vulnerabilities in software. In the presentation we will look at static analysis of binaries, and the problems we face when trying to locate vulnerabilities. Several ideas will be discussed to make the search easier, but at the same time less exact. The first idea is trivial:

automate as much as possible. The second idea is nearly trivial: don't aim at exact vulnerabilities but relax the search to locating potential vulnerabilities. We will give examples that illustrate the results.

Mario de Boer is a senior security consultant at Logica, and as such focuses on security management aspects like security frameworks, compliance, monitoring and control and risk management. Before joining Logica, Mario worked at the Dutch ministries of Defense and Justice, he co-founded a security company and worked as a project manager in the financial sector. For several years he taught courses in software security analysis and secure software development. Besides security management, Mario has interest in software security, reverse engineering and cryptography. Within Logica Netherlands, he is knowledge manager application security. Mario holds a PhD in Mathematics and is CISA and CISSP.

19.30 – 19:50 **Break**

19:50 – 20:20 **V.A.C. SQL injection** (Dutch) Marinus Kuivenhoven

Vulnerability:
An application which uses a database for its information needs, communicates with it trough SQL. SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of a Database for parsing and execution.
Assessment:
SQL injection can threaten the confidentiality, availability and integrity of the data. The various types of SQL injection and their impact will be shown.
Countermeasure:
Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because a database will execute all syntactically valid queries that it receives. How this should be done will be shown for the most popular languages.

Marinus is a Technology Specialist with Sogeti Nederland B.V. specializing in service oriented architectures and secure application development. His experience includes developing and administrating Oracle-based systems.

20.20 - 21.00 **Secure Programming with Static Analysis** (English) Brian Chess

Creating secure code requires more than just good intentions. Programmers need to know how to make their code safe in an almost infinite number of scenarios and configurations. Static source code analysis gives users the ability to review their work with a fine tooth comb and uncover the kinds of errors that lead directly to vulnerabilities. This talk frames the software security problem and shows how static analysis is part of the solution.
We will look at how static analysis works, how to integrate it into the software development processes, and how to make the most of it during security code review. Along the way we'll look at examples taken from real-world security incidents, showing how coding errors are exploited, how they could have been prevented, and how static analysis can rapidly uncover similar errors.

Brian Chess is a founder of Fortify Software and serves as Fortify's Chief Scientist, where his work focuses on practical methods for creating secure systems. His book, Secure Programming with Static Analysis, shows how static source code analysis is an indispensable tool for getting security right. Brian holds a Ph.D. in computer engineering from the University of California at Santa Cruz, where he studied the application of static analysis to the problem of finding security-relevant defects in source code.
Before settling on security, Brian spent a decade in Silicon Valley working at huge companies and small startups. He has done research on a broad set of topics, ranging from integrated circuit design all the way to delivering software as a service.

21.00 – 21:30 **Discussion, questions and social**

Registration

If you want to attend, please send an email to: owasp@irc2.com.

All OWASP chapter meetings are free of charge and you don't have to be an OWASP member to attend. There are never any vendor pitches or sales presentations at OWASP meetings.

NOTE TO CISSP's: OWASP Meetings count towards CPE Credits.