OWASP-NL Chapter Meeting announcement
May 20th 2010: Web Application Firewalls

Program:

18:00 - 18:30 Check-In (catering included)
18:30 - 18:45 Introduction (OWASP organization, projects, sponsor)
18.45 - 19.45 Web Application Firewalls in dynamic environments(by Alexander Meisel)

Alexander Meisel is the CTO of 'art of defence' (AOD), a German based software vendor. The company specializes in high performance deployments of Web Application Firewalls in very dynamic environments all over the world.

Abstract:

The current trend towards cloud computing forces everybody to deploy services in a virtual environment. In current dedicated environments WAFs or Web Application Firewalls are mostly deployed as a hardware (black) box which is easy at first but limits them to only low performance web cluster architectures. Moving those systems virtualized into a cloud environment makes almost no sense because of the resource limitations.

The is solution is a redesign which enables WAFs to be part of a true message based cloud system. This talk explains how truly virtualized and distributed web applications are architected, work and scale in high performance environments

19.45 – 20.00 Break
20.00 - 21:00 Bypassing Web Application Firewalls (by Sandro Gauci).

Sandro Gauci is the owner and Founder of EnableSecurity (www.enablesecurity.com) where he performs R&D and securityconsultancy for mid-sized companies. Sandro has over 9 years experience in the security industry and is focused on analysis of security challenges and providing solutions to such threats. Hispassion is vulnerability research and has previously worked together with various endors such as Microsoft and Sun to fix security holes. Sandro is the author of the free VoIP security scanning suite SIPVicious (sipvicious.org) and VOIPPACK for CANVAS.

Abstract:

WAFs or Web Application Firewalls are being deployed to fix security issues in your web applications. The question is, are they?

In this presentation we take a look at some of the issues related to making use of this solution and how it may affect the overall security posture of your web application. Finally we will describe tools to automate detection of WAFs, and also tools to help identify ways to bypass WAFs. This presentation will include updates to the open source WAF security testing tools - WAFFIT.

21.00 – 21:30 Discussion, questions and social networking

Location: http://www.setuputrecht.nl/

SETUP is gevestigd aan het Neude plein in Utrecht (Neude 4) in het nieuwe kantoor van de Dutch Game Garden (entrance at the back of the ABNamro building on “het Neude”).

If you want to attend, please send an email to Netherlands@owasp.org