OWASP

The Open Web Application Security Project

OWASP Netherlands Meeting Anouncement:

March 11th 2010: Database Security

Summary: The main goal of the upcoming OWASP-NL meeting is to provide information to managers, architects, designers, developers and security and risk professionals. The speakers will give specific examples and there will be time to ask questions.

ASR Nederland

MD0.60 - Auditorium

Smallepad 30

3811 MG Amersfoort

18:00 - 18:30 Check-In (catering included)

18:30 - 18:45 Introduction (OWASP organization, projects, sponsor)

18.45 - 19.45 Oracle Database Security (by Alexander Kornbrust)

Alexander Kornbrust is the founder of Red-Database-Security a company specialized in Oracle security. He provides Oracle security audits, security training and consulting to customers worldwide. Alexander is also the co-author of the book "SQL Injection Attacks and Defense ".

Alexander has worked since 1992 with Oracle and his specialties are the security of Oracle databases and secure software architectures. In the last 6 years Alexander has reported more than 400 security bugs to Oracle and gave various presentations on security conferences like Black Hat, Defcon, Bluehat, HITB, ...

Alexander holds a masters degree in computer science from the University of Passau, Germany.

Oracle Database Security: The presentation will show the most common security problems found in Oracle based web applciation

- Introduction
- Common hacker techniques ()
- Tools for detecting SQL Injection
- Using database trigger to detect SQL Injection attacks
- Security Problems in Oracle APEX (SQL Injection, XSS, Authentication, ...)
- How to fix the problems

19.45 – 20.00 Break

20. 00 – 20.30 VAC Insecure Direct Object Reference (By Marinus Kuivenhoven)

Marinus Kuivenhoven is a Senior Technology Specialist with Sogeti Nederland B.V. specializing in service oriented architectures and secure application development. His experience include developing and administrating Oracle-based systems. At Sogeti Nederland B.V. he is also an active member of the PaSS -Software(Proactive Security Strategy) taskforce focusing on secure application development. Marinus also developed and teaches several application security courses both within and outside Sogeti. In the past years he has written for magazine such as Computable and We Love IT. And he has spoken on a number of conferences and events like OWASP, Recent OO Trends, Open Source Developer Conference and Engineering World.

Vulnerability: Insecure Direct Object Reference is when a web application exposes an internal implementation object to the user. Some examples of internal implementation objects are database records, URLs, or files.

Assessment: An attacker can modify the internal implementation object in an attempt to abuse the access controls on this object. When the attacker does this they may have the ability to access functionality that the developer didn't intend to expose access to.

Countermeasure: Reference should be validated for authorization and accessed through reference maps. How this should be done will be shown.

20.30 – 21.30 SQL Injection - How far does the rabbit hole go? (By Justin Clarke)

Justin Clarke is a co-founder and Director at Gotham Digital Science, based in the United Kingdom. He has over twelve years of experience in assessing the security of networks, web applications, and wireless networks for large financial, retail, technology and government clients in the United States, the United Kingdom and New Zealand.

Justin is the the technical editor and lead author of "SQL Injection Attacks and Defense" (Syngress 2009), co-author of "Network Security Tools: Writing, Hacking, and Modifying Security Tools" (O'Reilly 2005), a contributing author to "Network Security Assessment: Know Your Network, 2nd Edition" (O'Reilly 2007), as well as a speaker at a number of conferences and events on security topics, including Black Hat USA, EuSecWest, OSCON, ISACA, RSA, SANS, OWASP, and the British Computer Society. He is the author of the open source SQLBrute blind SQL injection testing tool, and is the Chapter Leader for the London chapter of OWASP.

SQl Injection - How far does the rabbit hole go? SQL Injection has been around for over 10 years, and yet it is still to this day not truly understood by many security professionals and developers. With the recent mass attacks against sites across the world it has again come to the fore of vulnerabilities under the spotlight, however many consider it to only be a data access issue, or parameterized queries to be a panacea.

This talk starts from what was demonstrated last year at Black Hat in Las Vegas, where a self propagating SQL Injection worm was demonstrated live on stage. Explore some of the deeper, darker areas of SQL Injection, hybrid attacks, and exploiting obscure database functionality

21.30 – 22:00 Discussion, questions and social networking