

Securing the Code

Underleverantör: IP-Solutions

Kurslängd: 4 dagar

Kursort: Stockholm

Kursdatum: 13-16 juni

Detta är en avancerad kurs för dig som behöver djup förståelse om hur man når en avancerad nivå på testlösningar ur ett säkerhetsperspektiv, lär dig om olika säkerhets testverktyg på marknaden och du lär dig också hur målinriktade säkerhetsattacker mot kod utförs.

Målgrupp

Denna utbildning riktar sig till ingenjörer (designers, testare etc.) som behöver djup förståelse för hur man bygger lösningar och säkerhetskvalificerar koden vid applikationsutveckling.

Förkunskaper

Grundläggande kunskaper om datakommunikation samt säkerhet inom utveckling av lösningar och applikationer. Du bör även ha grundläggande kunskaper om C programmering.

Övrigt

Denna kurs finns som schemalagd utbildning och presentationen ges på svenska eller engelska. Under kursen blandas teoretiska presentationer med praktiska övningar. Vi kan även hålla denna kurs företagsintern. Kontakta oss för att få reda på hur vi kan hjälpa er med anpassade kurser.

Agenda

Introduction Exploit

- Application in memory
- Assembler
- CPU Registers and functions
- Overflow
- Policy
- Stack/Heap
- Format Strings

Shellcode

- Understand shellcode
- Inject shellcode
- Tools for shellcode

OS – Know your system

- Windows and UNIX OS
- File Permissions and User Privileges
- Different UID's
- Locking
- Core Files
- Memory – Virtual memory

- Linked in libraries and other trusted external code
- Built in protections against attacks and how to handle them
- Rootkits

Finding Vulnerability

- Reading Design Spec
- Toolbox
- Create shellcode
- Inject faults
- Fuzzing
- Vulnerability discovery with source available
- Vulnerability discovery without source -blackbox-

Exploit Vulnerability

Crypto

- Symmetric
- Public Key
- Choose encryption
- Handle the Key
- Random Numbers
- Hashing
- Message Authentication
- Weaknesses

Labs

Hacking

- Assembler stage 2, shellcodes, jumpslides, registers etc
- Breaking the code
- Finding and exploiting Vulnerability

Network + Hacking

- Sniffer
- Injecting on the network
- Flooding – DOS – DDOS – SYN
- Man in the middle
- Spoofing

Tools

- Sniffers
- Scanners
- Exploit Creating Frameworks
- Debugger
- Compiler
- Memdissectors
- Writing your own
- Penetration / Exploit testers
- Finding / Creating the tools