nowsec

Säker programmering - Applikationer

Information är en värdefull tillgång i dagens värld och en effektiv hantering sätter höga säkerhetskrav på medarbetarna.

Säker programmering - .Net

Nowsec säkerhetsgranskar dagligen applikationer, plattformar och nätverk på uppdrag av svenska myndigheter och företag med mycket höga säkerhetskrav. Målet med kursen är att förmedla våra kunskaper till medverkarna på ett sådant sätt att de efter kursen tillgodogjort sig goda kunskaper inom ämnesområdet. Efter kursen kommer deltagarna vara väl förtrogna med de vanligaste misstagen i samband med programmering, både idag och i framtiden, samt hur misstagen undviks.

”Säker programmering” är en praktisk kurs i utveckling av säker mjukvara, dvs. hur ni undviker säkerhetshål när ni designar och utvecklar applikationer. Kursen innehåller cirka 20 procent teori och 80 procent praktisk. Den praktiska delen delas upp i demonstrationer och laborationer. Föreläsaren går genom verklighetsbaserade scenarier och diskuterar de säkerhetshål som det kan ge upphov till. Sedan får eleverna pröva att säkra upp sårbarheterna genom pedagogiska laborationer.

Deltagarna får:

- Insikt i hur sårbarheter och säkerhetshål ser ut i verkligheten
- Lär sig att upptäcka och säkra upp sårbarheter i programkod
- Praktiskt säkra upp sårbarheterna genom hands-on laborationer
- Förståelse för hur sårbarhet upptäcks och undviks från designfas, till utveckling och i slutändan driftsättning

- **Mål**

Målet med våra kurser är att deltagarna efter kursen ska ha erhållit goda kunskaper inom ämnesområdet och vara väl förtrogen med de vanligaste misstagen i samband med programmering, problemområden och framtida utvecklingsmöjligheter.

I våra kurser blandar vi mycket teoretiska kunskaper med praktiska övningar.

Kursen ger deltagaren en gedigen kunskapsplattform avseende alla de vanligt förekommande misstagen och hur han/hon ska försöka undvika dem.

- **Genomförande**

Kursen genomförs i Nowsec´s lokaler eller i er egna lokaler där ni får tillgång till en virtuell labbmiljö med verktyg, labbar mm. Presentationer varvas hela tiden med övningar för att garantera att ni får praktisk erfarenhet av det kursen täcker.

- **Kursmaterial**

Utförligt kursmaterial i form av kurspärm med ett teori kompendium, övningshäfte och all presentationsmaterial.

- ***Vem bör deltaga?***

Kursen vänder sig till dig som, oavsett bransch och roll är i behov av kännedom eller en heltäckande kurs inom säker programmering.

- ***Förkunskaper***

Flera års praktisk och teorisk erfarenhet av programmering är att rekommendera.

Kurs innehåll

- Buffer Overflow
- Integer Overflow
- Format String Vulnerabilities
- Signed / Unsigned Vulnerabilities
- Race Condition
- NULL Pointer Vulnerabilities
- Logical Vulnerabilities

Exempel från kurslitteratur - Teori

Typer av säkerhetsluckor

Logiska missar

Logiska missar syftar till rena misstag som oftast gjorts redan på designstadiet av ett system. Dessa finner man ganska ofta när man analyserar inloggningssystem och dylikt. De kan vara väldigt lätta att identifiera men är ofta mycket svåra att rätta till i efterhand då det kan innebära att man måste ändra hela designen av ett system. […]

Konfigurationsfel

Konfigurationsfel är sällan uppenbara, ofta vill utvecklare ha en massa trevliga debugg funktioner och detaljerade felmeddelanden påslagna för att underlätta felsökning. Detta är dock en guldgruva med information för en angripare som vill angripa en webbapplikation då han mycket lättare kan se vad hans försök till SQL-injektionsattacker och liknande leder till. […]

Programmeringsmisstag

Dessa uppstår ibland av slarv men väldigt ofta beror de på bristande förståelse hos utvecklaren. Tyvärr lärs inte säker programmering ut i skolorna, man ser faktiskt till och med att exempelkoden som används av lärare ofta har otroligt enkla säkerhetsluckor som någon som kan säker programmering kan identifiera omedelbart, bl.a. klassiska buffer overflows. För att undvika dessa krävs det dels att man känner till hur det språk man skriver sitt program i fungerar och hanterar data samt att man är mycket noggrann med hur man hanterar programmets indata.

Medvetet tagna risker /tradeoffs

Vissa säkerhetshål är väldigt kostsamma att skydda sig mot, t.ex. så är det väldigt tidskrävande och därmed dyrt att säkerhetsgranska kod. Därför måste då företaget göra en riskbedömning och en tradeoff, och bestämma sig för om man anser att det är värt pengarna att göra en säkerhetsgranskning. […]

Omdömen från tidigare deltagare

Fråga 12: Kursens styrkor? (Ange de tre viktigaste)

Praktisk/konkret
Kunnig lärare
Sympatisk lärare

Kombination teori och praktik
Kursledare
Bra diskussion / Tvåvägskommunikation

Konkreta exempel
Små grupper
Lagom takt

Att ha en IT-expert till kursledare
Bra upplägg
Höll sig till ämnet

Hands-on erfarenhet
Ger praktiska erfarenheter på tidigare teoretiska kunskap
Erfaren lärare

Upplägg (Teori, demo o labbar)
Aktuella och farliga sårbarheter
Kunnig lärare

Intressant att få inblick i hur svagheter i kod kan få stora konsekvenser
Ökad kunskap om vilka faror som finns

Praktisk information

Kursen är begränsad till minst 10 och högst 15 deltagare

Längd: 3 dagar
Pris: 14 950 kronor (exkl. moms)
Inregistrering: kl. 09:00
Kursort: Stockholm

Lunch, fika samt kursmaterial ingår

- **Information och bokning**

För mer information samt bokning vänligen kontakta oss på kurser@nowsec.se eller 08-51 984 384

Om Nowsec

På Nowsec är vi specialister inom teknisk informationssäkerhet.

Vi skapar trygghet genom att upplysa våra kunder om hot och risker samt föreslår lämpliga åtgärder och lösningar där varje detalj uppfyller kraven på högsta kvalitet.

Vi är strikt produkt- och leverantörsoberoende och strävar bara efter att ge råd och stöd som ger rätt säkerhet för våra kunders informations- och IT-system.

Vår styrka är vår personal som har mångårig erfarenhet och goda referenser från kvalificerade leveranser till Sveriges viktigaste myndigheter och även privata företag.