nowsec

Kurs
Säker programmering

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

Säker programmering

Nowsec säkerhetsgranskar dagligen applikationer, plattformar och nätverk på uppdrag av svenska myndigheter och företag med mycket höga säkerhetskrav. Målet med utbildningen är att förmedla våra kunskaper till medverkarna på ett sådant sätt att de efter utbildningen tillgodogjort sig goda kunskaper inom ämnesområdet. Efter utbildningen 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 ett utbildning i utveckling av säker mjukvara, dvs. hur ni undviker säkerhetshål när ni designar och utvecklar applikationer. Utbildningen innehåller cirka 20 procent teori och 80 procent praktisk.

Deltagarna får:

- Insikt i hur sårbarheter och säkerhetshål ser ut i verkligheten
- Förståelse för hur sårbarhet upptäcks och undviks från designfas, till utveckling och i slutändan driftsättning

Mål

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

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

Genomförande

Utbildningen genomförs i Nowsec´s utvalda lokaler eller i er egna lokaler. Presentationer varvas hela tiden med demostratiner för att garantera att ni får praktisk erfarenhet av det utbildningen täcker.

Vem bör deltaga?

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

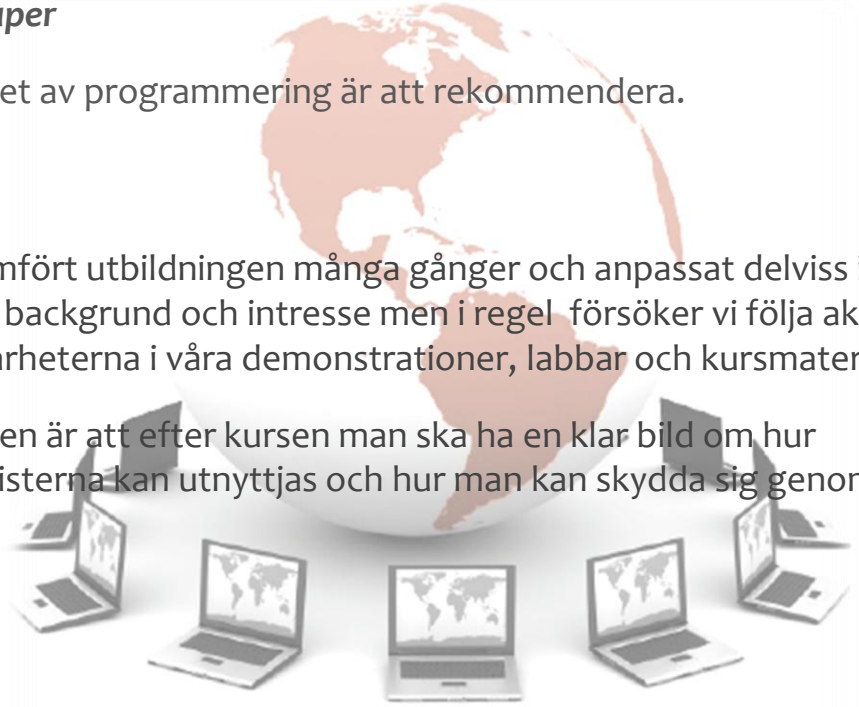
Förkunskaper

Viss erfarenhet av programmering är att rekommendera.

Innehåll

Vi har genomfört utbildningen många gånger och anpassat delviss innehållet efter deltagarnas backgrund och intresse men i regel försöker vi följa aktuella OWASP Top 10 sårbarheterna i våra demonstrationer, labbar och kursmaterial .

Målsättningen är att efter kursen man ska ha en klar bild om hur säkerhetsbristerna kan utnyttjas och hur man kan skydda sig genom tekniker och processer.



OWASP Top 10 – 2013 Edition

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Known Vulnerable Components – New (previously part of "Security Misconfiguration")
- A10 Unvalidated Redirects and Forwards

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.