

# Säker applikationsutveckling | 3 dagars grundkurs

Kursen vänder sig till dig som idag är verksam inom systemutveckling i allmänhet och webbutveckling i synnerhet. Kursen är utformad för tilltala att alla som på något sätt är delaktiga i utvecklingsprojekt såsom arkitekter, tekniska projektledare, testare, systemförvaltare, säkerhetsspecialister m.fl.

Dagens verktyg och plattformar har gett systemutvecklaren en oöverträffad frihet och flexibilitet när det kommer till att utveckla innehållsrika och användarvänliga applikationer. Genom användning av dessa sofistikerade verktygslådor i kombination med en kort och intensiv utvecklingscykel blir det också lättare att missa de små detaljerna innebärande att sårbarheter smyger sig in i applikationerna.

I denna grundläggande och språkoberoende kurs lär vi ut principerna i säker applikationsutveckling och går igenom ett antal verktyg och exempel i både .NET och Java där vi kommer att trycka på vikten av säkerhet i förhållande till rådande hotbild.

## UTBILDNINGSMÅL

Målet med kursen är att ge en förståelse för hur sårbarheter i applikationer och tjänster kan exploateras och utnyttjas samt hur man medelst olika tekniker kan skydda sig mot detta.

Efter utbildningen ska eleven:

- kunna beskriva aktuell hotbild avseende webbapplikationer och distribuerade tjänster
- kunna beskriva och tillämpa "best practises" för utveckling av säkra webbapplikationer
- kunna tillämpa grundläggande kunskap om testning för att hitta svagheter i applikationer
- ha grundläggande kunskap om kryptering och autentisering



## KURSLEDARE

**Janne Haldesten** har lång erfarenhet av både teknisk IT-säkerhet och strategiskt informationssäkerhetsarbete med ett antal uppdrag inom både privat och offentlig sektor.

Med bakgrund som systemutvecklare och arkitekt likväl som säkerhetsrådgivare på nationell nivå förmedlar han ett antal insikter och erfarenheter som alla som arbetar med applikationsutveckling i någon form borde känna till. Han sitter i Myndigheten för Samhällsskydd och Beredskaps referensgrupp för framtagning av det nya nationella informationssäkerhets-ramverket SVISA, svenska tekniska kommittén för tjänster i molnet, SIS TK 542.

Han är även rådgivare i European Network and Information Security Agency's Awareness Raising-gruppering (ENISA/AR-community).



SSTC

## Om kursen och om oss

Kursen utgår i stora stycken från The Open Web Application Security Project, OWASP, och delar som inte täcks av OWASP kompletteras från noga utvald referenslitteratur och kursledarens egen forskning och erfarenhet. .

Vår pedagogik bygger på en väl beprövad lärandemodell bestående av fyra steg; din förståelse, föreläsningar, gruppövningar och teknikträning.

## Förkunskaper

Grundläggande kunskaper i systemutveckling, Viss grundläggande förståelse om SQL-injektioner och Cross-Site Scripting (XSS). Grundläggande kunskaper i engelska

## Omfattning

Kursen omfattar tre (3) arbetsdagar.

## Nivå

Kursen är en grundkurs som syftar till att ge eleven en introduktion till tekniker för säker applikationsutveckling.

# Utbildningens innehåll

## HOTBILD

Ett effektivt skydd ska vara avvägt mot de hot som det ämnas att motverka. Genom att titta på trender och attackvektorer liksom aktörer och bakomliggande drivkrafter får vi en förståelse om hur hotbilden ser ut.

## KRAVHANTERING

Utformningen av krav spelar en central och viktig roll i alla utvecklingsprojekt. Säkerhet är ofta ett område som inte får tillräcklig uppmärksamhet från start utan tillkommer i bästa fall i slutskedet av projektet där kostnaderna för åtgärdande av brister blir mycket högre och projektet riskerar att försenas. Här tittar vi konkret på hur vi kan få in säkerhetsaspekterna tidigt i projektet och hur vi säljer in säkerhet kopplat till nytta.

## ATTACKTYPER

Anfall är bästa försvar. Här förmedlas ett antal exempel på hur en angripare kan exploatera en webbapplikation. Vi går igenom sross-site scripting (både persistenta och inpersistenta attacker), Cross-site request forgery (CSRF), SQL-injektioner och skadlig kod

## SESSIONSHANTERING OCH ACCESSKONTROLL

Genom att använda sig av rätt tekniker i sin utveckling kan många av de sårbarheter som vanligen exploateras undvikas och risker därmed minimeras. Vi går igenom cookie-hantering (replay och poisoning) autentisering i applikationer (authentication bypass) och filhantering och filanrop.

## SÄKER DESIGN OCH IMPLEMENTATION

Kallas också konsten att göra rätt från början. Här går vi igenom ett webbutvecklingsprojekt från början till start där vi fokuserar på säkerhetsaspekterna kopplat till varje del i projektet.

Vi går igenom...

- Designprinciper
- Datamodellering och arkitektur
- Distribuerade tjänster
- Datatrafik
- Validering av indata
- Konsistent loggning
- Saltning
- Hashning
- Verktyg (OWASP m.m.)
- Rutiner och checklistor

... och tar tar även upp:

- Mobila tillämpningar
- Testning
- Förvaltning
- Policyer och styrning
- Risker med tredjepartsapplikationer
- Lösningaspekter (lokalt vs. molnbaserat)



### Kursdatum

Aktuella kursdatum annonseras på [www.sstc.se](http://www.sstc.se)

Utbildningen ges även som kundanpassad uppdragsutbildning

### Pris

12 900:- per deltagare (exklusive moms).

### I priset ingår

- Kursdokumentation
- Lunch
- Fika
- Frukt

### Anmälan

Anmälan sker via [www.sstc.se](http://www.sstc.se) alternativt genom att kontakta kundservice på telefon: 08-663 34 56.

### Avbokning

Avbokning måste ske skriftligt till [avbokning@sstc.se](mailto:avbokning@sstc.se) senast 14 dagar före kursstart. Efter 14 dagar före kursstart kan om möjligt kursplatsen överlåtas till annan deltagare.

*Vi reserverar oss för ev. förändringar i utbildningsinnehållet.*

## Trygghet och säkerhet genom utbildning

STOCKHOLM - GÖTEBORG - NORRKÖPING

[www.sstc.se](http://www.sstc.se) - 08-663 34 56