NTNU
Norges teknisk-naturvitenskapelige universitet

Fakultet for informasjonsteknologi, matematikk og elektroteknikk

Institutt for datateknikk og informasjonsvitenskap

BOKMÅL

AVSLUTTENDE EKSAMEN I

TDT42378
Programvaresikkerhet

Mandag 11. August 2008
Kl. 09.00 – 13.00

Faglig kontakt under eksamen:

Lillian Røstad, tlf. 994 00 628

Hjelpemidler:

Kalkulator ikke tillatt. Utover dette er ingen trykte eller håndskrevne hjelpemidler tillatt.

Sensurdato:

1. september 2008.

Resultater gjøres kjent på http://studweb.ntnu.no/ og sensurtelefon 81548014.

Det er angitt i prosent hvor mye hver deloppgave teller ved sensur. Gjør nødvendige antagelser der dette er nødvendig. Husk: *korte* og *konsise* svar er ofte de beste.

Lykke til!

Oppgave 1 (30%) – hver deloppgave teller 5%

a) Bruk pseudokode til å lage et eksempel på en kodesnutt som vil være sårbar for sql-injections. Forklar hvordan en angriper kan utnytte sårbarheten.
b) Utvid pseudokoden du laget i oppgave a) slik at den ikke lenger er sårbar for sql-injections. Forklar hvilke mottiltak du har brukt og hvordan de(t) fungerer.
c) I hvilke(n) fase(r) av et utviklingsprosjekt ville du ha brukt abuse/misuse caser? Hvorfor? Gi gjerne eksempler.
d) Hvilke hovedutfordringer har man ved bruk av code review? Hva er fordelen og ulempene ved manuell code review vs. code review med bruk av automatiserte verktøy?
e) Vil du si at input validation er sikkerhetsfunksjonalitet? Hvorfor/hvorfor ikke? Gi gjerne eksempler på hva du forstår med begrepet ”sikkerhetsfunksjonalitet” i et programvaresystem.
f) Hva inngår i touchpointet penetration testing?

Oppgave 2 (30%) – Risikoanalyse

Det skal utvikles et nytt system for overvåking av signalanlegget for T-banen i Oslo. Signalanlegget styrer togsettene og feil på anlegget kan ha store konsekvenser for mennesker og utstyr. Overvåkningssystemet skal vise en oversikt over signaler, status og hvor togsettene befinner seg. Signalanlegget er automatisert, men det skal være mulig for en operatør å gå inn og styre anlegget manuelt dersom det oppdages en feil. Det er avgjørende at informasjonen som vises til enhver tid er korrekt og oppdatert.

Systemet er bestilt av Oslo Sporveier. De ønsker seg i utgangspunktet et webbasert system. Din oppgave er å gjøre en risikoanalyse som tar for seg sikkerhetsmessige utfordringer ved systemet. Denne risikoanalysen skal brukes som grunnlag for å beslutte om man skal gå videre med prosjektet og i hvilken form dvs. hvilken teknologi som skal brukes.

Du kan gjøre bruk av tekst og/eller modeller i analysen din. Husk å forklare valgene dine, inkludert valg av metode.

Oppgave 3 (40%) - Case

Basert på risikoanalysen du utførte i forrige oppgave har Oslo sporveier bestemt seg for å gå videre med prosjektet. De har også bestemt at systemet skal være webbasert, det skal utvikles i Java med utstrakt bruk av rammeverk og eksisterende APIer der det er mulig. Etter å ha gjennomgått risikoanalysen har de valgt å sette av ekstra midler til arbeidet med sikkerhet i løsningen, for å håndtere risikoen ved en webløsning.

Din oppgave er å være ”security lead” (sikkerhetsansvarlig) i prosjektet. Du skal delta i hver fase av utviklingen og er ansvarlig for valg av metoder for modellering og utvikling med tanke på sikkerhet og generelt ansvarlig for å ivareta fokuset på sikkerhet.

Denne oppgaven er tredelt:

- Gjør først rede for hvile metoder du vil velge i hver prosjektfase og hvilke punkter du vil lekke vekt på å følge opp.
- Illustrer så valgene dine ved å gi eksempler på metodebruk i hver enkelt prosjektfase.
- Diskuter til slutt utfordringer knyttet til rollen som ”security lead”/sikkerhetsansvarlig i et utviklingsprosjekt.

Husk å gi begrunnelser for valgene dine og forklar eventuelle antagelser du gjør.

ENGLISH (transl. Dec. 2008)

Task 1 (30%) – every subtask counts 5%

g) Use pseudocode to demonstrate how code can be vulnerable to sql-injections. Explain how an attacker could exploit this vulnerability.
h) Extend the code you created in subtask a) so it is no longer vulnerable to sql-injections. Explain what mitigation-techniques our countermeasures you have used and how they work.
i) In what phases of the development process would you use abuse/misuse cases? Why? Provide examples.
j) What are the main challenges of using code review? What are the advantages and disadvantages of manual code review compared to code review using tools?
k) In your opinion – is input validation an example of security functionality in a system? Why/why not? Explain how you understand the term ”security functionality”.
l) Explain the touchpoint penetration testing.

Task 2 (30%) – Risk analysis

A new monitoring-system for the signaling system for the subway in Oslo is to be developed. The signaling system controls the subway train and errors may have fatal consequences. The monitoring system shall provide an overview of the current signals, status and where the different trains are. The signaling system is automated but an operator shall be able to control the system manually in the event that an error occurs. It is crucial that the information shown in the monitoring system is correct and up to date at all times.

Oslo Sporveier has commissioned the system and they want it to be web-base. Your task is to perform a risk analysis of the system focusing on security challenges. This risk analysis will be used to determine whether to continue with the project and also what technology to use.

You can use text and/or models in the analysis. Remember to explain your reasoning, including choice of method.

Task 3 (40%) - Case

Based on the risk analysis from the previous task, Oslo Sporveier has decided to continue the project and develop the system. They have also decided that the system shall be web-based, developed in Java and using existing frameworks and APIs where possible. After having reviewed the risk analysis, they have decided to allocate extra resources to security activities to tackle the risks of developing a web-based system.

Your task is to be ”security lead” in the development project. You will participate in all development phases and be in charge of selecting methods for modeling and development

with a focus on security, and also to maintain an overall focus on security throughout the project.

This task consists of three parts:

- Explain what methods/techniques you would use in every development phase and what you would focus on.
- Demonstrate your choices by providing examples on the use of the selected methods in each project phase.
- Discuss the main challenges of being ”security lead” in a development project.

Remember to include the reasoning behind your choices and explain any assumptions you make.