NTNU
Institutt for datateknikk
og informasjonsvitenskap

Eksamensoppgave i/Exam

TDT4237 – Programvaresikkerhet/Software security

Onsdag/Wednesday 9. Desember/December 2009, kl. 09:00 - 13:00

Oppgaven er utarbeidet av faglærer Lillian Røstad og kvalitetssikrer Torbjørn Skramstad.
Kontaktperson under eksamen er Torbjørn Skramstad (mobil 971 23 246)

Språkform: Bokmål/Nynorsk/Engelsk
Tillatte hjelpemidler: D
Ingen trykte eller håndskrevne hjelpemidler tillatt./No printed or hand-written materials allowed.
Bestemt, enkel kalkulator tillatt./Approved calculator allowed.

Sensurfrist (results available): Mandag 11. Januar 2010 (Monday January 11th 2010)

Les oppgaveteksten nøye. Finn ut hva det spørres etter i hver oppgave.

Dersom du mener at opplysninger mangler i en oppgaveformulering gjør kort rede for de antagelser og forutsetninger som du finner det nødvendig å gjøre.

Read each task carefully. Identify what the task asks for.

If you find that information is missing in a task you are free to make the assumptions you consider necessary, but remember to explain and clearly mark your assumptions.

BOKMÅL

Oppgave 1 (25%)

a) Hva er de ulike software security touchpoints? Gi en kort forklaring av hvert touchpoint.
b) Hva mener du er det viktigste touchpointet? Hvorfor?
c) Hva brukes et pagemap til? Illustrer med et eksempel.
d) Forklar angrepet path-traversal. Hva kan en angriper oppnå med dette angrepet?
e) Anta at du jobber på et stort utviklingsprosjekt og av ulike årsaker **ønsker** du å legge inn sårbarheter i koden. Hvordan ville du velge å gjøre dette? Fokuser på ting med maksimalt skadepotensiale og minimal sjanse for å bli oppdaget.

Oppgave 2 – Code Quiz – Spot the bug (25%)

Disse kodefragmentene illustrerer mulige sårbarheter i Java kode. Du skal gjennomføre en code review for å finne mulige sikkerhetsproblemer i hvert kodefragment.
For hvert sikkerhetsproblem du finner forventes det at du: forklarer sårbarheten som problemet kan forårsake, klassifisere feilen i henhold til McGraw sin taksonomi og foreslår en løsning. Du skal illustrere løsningen din med (pseudo)kode.

Kodefragment 1:

```
private int itemsInInventory = 100;

public int removeItem() {
  if(itemsInInventory > 0) {
    return itemsInInventory--;  // Returns new count of items in inventory
  } else {
    return 0;
  }
}
```

Kodefragment 2:

```
public Object publicLock = new Object();
synchronized(publicLock) {
  // body
}
```

Kodefragment 3:

```
class ExceptionExample {
  public static void main(String[] args) throws FileNotFoundException {
    // Linux stores a user's home directory path in the environment variable
    // $HOME, Windows in %APPDATA%
    FileInputStream fis = new FileInputStream(System.getenv("APPDATA") +
args[0]);
  }
}
```

Kodefragment 4:

```
Pattern pattern = Pattern.compile("[<>]");
String tainted = "%3C%73%63%72%69%70%74%3E"; // Hex encoded equivalent form of
<script>
if(pattern.matcher(tainted).find()) {
  throw new ValidationException("Invalid Input");
}
URI uri = new URI("http://vulnerable.com/" + tainted);
```

Oppgave 3 (20%) – Penetrasjonstesting/testplan

Du arbeider i et sikkerhetsfirma som leverer penetrasjonstesting. Dere skal levere tilbud på penetrasjonstesting til en mulig ny kunde som utvikler og drifter et system for blogging. Systemet gjør det enkelt for sine brukere å sette opp og tilpasse utseendet og funksjonalitet (gjennom valg fra standardkomponenter eller egenutviklede komponenter) i sin egen blogg.
I første omgang skal du utvikle en overordnet testplan som skal legges ved tilbudet til kunden. Forklar og demonstrer hvordan du ville gått frem for å løse denne oppgaven. Gjør antagelser der du må, men husk å forklare antagelsene dine.

Oppgave 4 – Integrasjon av ny og gammel teknologi (30%)

Som de fleste banker har B-Banken fremdeles kjernen av sine systemer, dvs håndtering av økonomiske transaksjoner, på et stormaskinsystem der koden er skrevet i Cobol. Stormaskinsystemet er raskt og pålitelig, men det har i stadig større grad blitt vanskelig å lage moderne kundeløsninger på web som snakker med disse back-end systemene. B-Banken har derfor bestemt seg for å gjennomføre et stort utviklingsprosjekt der de over tid bytter ut alle de gamle systemene til fordel for ny løsning basert på standard komponenter og web-teknologi. Prosjektet er inkrementelt og oppdelt etter funksjonalitet. Dvs. at man ikke bytter ut alt på en gang, men tar deler av funksjonaliteten av gangen. Dette innebærer at i store deler av prosjektets levetid (5 år) snakker ny og gammel teknologi sammen. Det er store ambisjoner i prosjektet om å utvikle moderne kundeløsninger med høy grad av selvbetjening for kundene.

Du er hyret inn som sikkerhetsekspert i prosjektet. I første omgang er ditt ansvar å gjøre en analyse av prosjektet og peke på hvor de viktigste sikkerhetsutfordringene ligger. Det er som alltid begrensede ressurser så det er også ønskelig at du bidrar til beslutningsgrunnlag for å gjøre en prioritering av sikkerhetstiltak. Forklar og demonstrer hvordan du ville gått frem. Gjør antagelser der du må, men husk å forklare antagelsene dine.

NYNORSK

Oppgåve 1 (25%)

a) Kva er de ulike software security touchpoints? Gi en kort forklaring av kvart touchpoint.
b) Kva meiner du er det viktigaste touchpointet? Hvorfor?
c) Kva brukas eit pagemap til? Illustrer med eit eksempel.
d) Forklar angrepet path-traversal. Hva kan en angriper oppnå med dette angrepet?
e) Anta at du jobber på et stort utviklingsprosjekt og av ulike årsaker **ønskjer** du å legge inn sårbarheter i koden. Hvordan ville du vele å gjøre dette? Fokuser på ting med maksimalt skadepotensiale og minimal sjanse for å bli oppdaga.

Oppgåve 2 – Code Quiz – Spot the bug (25%)

Disse kodefragmenta illustrerer mulige sårbarheitar i Java kode. Du skal gjennomføre en code review for å finne mulige sikkerheitsproblem i kvart kodefragment.
For kvart sikkerheitsproblem du finner forventes det at du: forklarer sårbarheita som problemet kan forårsake, klassifisere feilen i henhold til McGraw sin taksonomi og foreslå en løysning. Du skal illustrere løysningen din med (pseudo)kode.

Kodefragment 1:

```
private int itemsInInventory = 100;

public int removeItem() {
  if(itemsInInventory > 0) {
    return itemsInInventory--;  // Returns new count of items in inventory
  } else {
    return 0;
  }
}
```

Kodefragment 2:

```
public Object publicLock = new Object();
synchronized(publicLock) {
  // body
}
```

Kodefragment 3:

```
class ExceptionExample {
  public static void main(String[] args) throws FileNotFoundException {
    // Linux stores a user's home directory path in the environment variable
    // $HOME, Windows in %APPDATA%
    FileInputStream fis = new FileInputStream(System.getenv("APPDATA") +
args[0]);
  }
}
```

Kodefragment 4:

```
Pattern pattern = Pattern.compile("[<>]");
String tainted = "%3C%73%63%72%69%70%74%3E"; // Hex encoded equivalent form of
<script>
if(pattern.matcher(tainted).find()) {
  throw new ValidationException("Invalid Input");
}
URI uri = new URI("http://vulnerable.com/" + tainted);
```

Oppgåve 3 (20%) – Penetrasjonstesting/testplan

Du arbeider i et sikkerheitsfirma som leverer penetrasjonstesting. Dere skal levere tilbod på penetrasjonstesting til en mulig ny kunde som utviklar og driftar et system for blogging. Systemet gjør det enkelt for sine brukarar å sette opp og tilpasse utseendet og funksjonalitet (gjennom val frå standardkomponentar eller eigenutvikla komponentar) i sin egen blogg.
I første omgang skal du utvikle en overordna testplan som skal leggast ved tilbodet til kunden. Forklar og demonstrer hvordan du ville gått frem for å løyse denne oppgåva. Gjør antagelser der du må, men husk å forklare antagelsene dine.

Oppgåve 4 – Integrasjon av ny og gammal teknologi (30%)

Som de fleste banker har B-Banken fremdeles kjernen av sine system, dvs handtering av økonomiske transaksjonar, på et stormaskinsystem der koden er skrevet i Cobol. Stormaskinsystemet er raskt og pålitelig, men det har i stadig større grad blitt vanskelig å lage moderne kundeløysningar på web som snakkar med disse back-end systema. B-Banken har derfor bestemt seg for å gjennomføre et stort utviklingsprosjekt der de over tid bytter ut alle de gamle systema til fordel for ny løysning basert på standard komponentar og web-teknologi. Prosjektet er inkrementelt og oppdelt etter funksjonalitet. Dvs. at man ikkje bytter ut alt på en gang, men tar deler av funksjonaliteten av gangen. Dette inneberer at i store deler av prosjektets levetid (5 år) snakkar ny og gammal teknologi saman. Det er store ambisjonar i prosjektet om å utvikle moderne kundeløysningar med høy grad av sjølbetjening for kundane.

Du er hyret inn som sikkerheitsekspert i prosjektet. I første omgang er ditt ansvar å gjøre en analyse av prosjektet og peke på hvor de viktigaste sikkerheitsutfordringa ligg. Det er som alltid begrensa ressursar så det er også ønskelig at du bidrar til beslutningsgrunnlag for å gjøre en prioritering av sikkerheitstiltak. Forklar og demonstrer hvordan du ville gått frem. Gjør antagelser der du må, men husk å forklare antagelsene dine.

ENGLISH

Task 1 (25%)

a) What are the different software security touchpoints? Give a brief explanation of each touchpoint.
b) What do you think is the most important touchpoint? Why?
c) What is a pagemap used for? Illustrate with an example.
d) Explain the path traversal attack. What can an attacker accomplish using this attack?
e) Assume that you are working on a large software development project. For various reasons you **want to** add vulnerabilities to the code. How would you do this? Focus on maximum damage potential and minimal chance of getting caught.

Task 2 – Code Quiz – Spot the bug (25%)

These code snippets illustrate vulnerabilities in Java code. You shall perform a code review to identify any security-relevant issues in each snippet of code.
For each issue you identify, you are expected to: explain what vulnerability the error may cause, classify the error using McGraw's taxonomy and suggest a solution. You should illustrate your solution using (pseudo)code.

Code snippet 1:

```
private int itemsInInventory = 100;

public int removeItem() {
  if(itemsInInventory > 0) {
    return itemsInInventory--;  // Returns new count of items in inventory
  } else {
    return 0;
  }
}
```

Code snippet 2:

```
public Object publicLock = new Object();
synchronized(publicLock) {
  // body
}
```

Code snippet 3:

```
class ExceptionExample {
  public static void main(String[] args) throws FileNotFoundException {
    // Linux stores a user's home directory path in the environment variable
    // $HOME, Windows in %APPDATA%
    FileInputStream fis = new FileInputStream(System.getenv("APPDATA") +
args[0]);
  }
}
```

Code snippet 4:

```
Pattern pattern = Pattern.compile("[<>]");
String tainted = "%3C%73%63%72%69%70%74%3E"; // Hex encoded equivalent form of
<script>
if(pattern.matcher(tainted).find()) {
  throw new ValidationException("Invalid Input");
}
URI uri = new URI("http://vulnerable.com/" + tainted);
```

Task 3 (20%) –Penetration testing/test plan

You are working at a software security company that specializes on performing penetration testing. You are preparing an offer on doing penetration testing for a potential new customer. This customer develops a system for online blogging. The blogging system allows users to create and customize the look and functionality (by selecting from available standard components or creating their own custom components) of their own blogs.

You are developing a high-level test plan that will be included in the offer. Explain and demonstrate how you would do this task. Make assumptions where necessary, but remember to explain your assumptions.

Task 4 – Integrating new and old technology (30%)

As many other banks, the B-Bank still rely on old core systems, typically written in Cobol and running on large mainframes, to perform financial transactions. Mainframes are fast and reliable, but are not intended to tackle the challenge of communicating with web-based customer tools. The B-Bank has therefore decided to start a large software development project, where the goal is, over time, to replace the old mainframe system with a new system based on standard components and web technology. The project is incremental and focuses on functionality. This means that selected parts of the desired functionality is included in each release. This means that for most of the project lifetime (5 years), new and old technology together make up the core systems. The project has as an important vision to create modern customer solutions enabling customers to be as self-serviced as possible.

You have been hired to be the security expert on the project. Your first task is to perform a security analysis of the project and identify the main security challenges. As always, the resources are limited so you are also expected to contribute information to help prioritize security measures. Explain and demonstrate how you would perform this task. Make assumptions where necessary, but remember to explain your assumptions.