NTNU

Department of (Computer and Information Science)

Examination paper for (TDT4237) (Software Security)

Academic contact during examination: Jingyue Li

Phone: 9189 7446

Examination date: 16-December-2016

Examination time (from-to): 9.00-13.00

Permitted examination support material: D

Other information:

Language: English

Number of pages (front page excluded): 7

Number of pages enclosed: 1

Informasjon om trykking av eksamensoppgave
Originalen er:
1-sidig X **2-sidig ☐**
sort/hvit ☐ **farger ☐**
skal ha flervalgskjema ☐

Checked by: Per Håkon Meland

_____

Date Signature

Students will find the examination results in Studentweb. Please contact the department if you have questions about your results. The Examinations Office will not be able to answer this.

Introduction

In this course, the written exam will count 70% of the final grade and the remaining 30% of the final grade comes from the compulsory exercises. So, your final grade of this course will be:
(Points you get from this written exam) * 70% + your grade of compulsory exercises.

If you feel that any of the problems require information that you do not find in the text, then you should

- Document the necessary assumptions
- Explain why you need them

Your answers should be brief and to the point.

Problem 1 – (45 points)

1) (5 points) Explain what SQL injection attack is and its vulnerability exploited by this attack. List at least three countermeasures of this attack.
2) (5 points) Explain what buffer overflow is, and list at least three methods/strategies to defend against buffer overflow.
3) (5 points) List the three general ways of authentication and discuss their advantages and disadvantages.
4) (5 points) Explain encryption and decryption algorithm of One Time Pad (OTP), and explain why it is insecure to use the same key to encrypt two or several messages using OTP.
5) (5 points) Explain what digital signature is and how digital signature is used in the SSL/TLS handshake process to exchange the secret key.
6) (5 points) List software security touchpoints in order of effectiveness.
7) (5 points) Explain why Biba model can help protect data integrity.
8) (5 points) Explain what “protection level” is in Android platform. What are the Normal, Dangerous, and Signature protection levels?
9) (5 points) Explain what BSIMM is, what OpenSAMM is, and the main differences between them.

Problem 2 – (20 points)

For each of the code snippets listed below, your task is to:

- Identify what you think is the main security vulnerability
- Explain why these are security vulnerabilities/issues
- Fix the code (You may use pseudo-code for this. Remember to explain your solution).

Code snippet 1 (5 points)

Source: https://www.htbridge.com/vulnerability/

```
1. <?php
2.     $SessionID = SHA256($UserName);
3.     if (empty($_COOKIE["SESSION_ID"])){
4.         setcookie("SESSION_ID",$SessionID);
5.     }
6. ?>
```

Code snippet 2 (5 points)

Source: http://shiflett.org/articles

HTML form

```
1. <form action="buy.php" method="POST">
2. <p>Symbol: <input type="text" name="symbol" /></p>
3. <p>Shares: <input type="text" name="shares" /></p>
4. <p><input type="submit" value="Buy" /></p>
5. </form>
```

buy.php

```
1. <?php
2.     session_start();
3.     if (isset($_REQUEST['symbol'] && isset($_REQUEST['shares'])) {
4.         buy_stocks($_REQUEST['symbol'],$_REQUEST['shares']);
5.     }
6. ?>
```

Note: buy_stocks () is a user defined function to trade stocks based on value of variables “symbol” and “shares”.

Code snippet 3 (5 points)

Source: https://www.wordfence.com/

```
1.  <html><body>
2.  <form action="signup.php" method="POST">
3.  <p><input type = "text" size = "20" value = "" name = "user"></p>
4.  <p><input type="submit" value="Sign Up" /></p>
5.  </form>
6.  <?php
7.      If($_POST[‘user’]{
8.          file_put_contents(‘userlist.txt’, $_POST[‘user’]. "\n", FILE_APPEND|LOCK_EX);
9.      }
10. ?>
11. <h2> All users signed up:</h2>
12. <?php>
13.    $ list = file_read_contents (‘userlist.txt’);
14.    foreach (split ("\n", $list) as $re){
15.    echo $re. "<br />";
16.    }
17. ?>
18. </body></html>
```

Note: file_put_contents () is a PHP function to write a string to a file.

File_get_content () is a PHP function to read entire file into a string.

Code snippet 4 (5 points)

Source: https://www.htbridge.com/vulnerability/

HTML form

```
1.  <form action="upload_picture.php" method="post" enctype="multipart/form-data">
2.  <input type="file" name="filename"/>
3.  <input type="submit" name="submit" value="Upload"/>
4.  </form>
```

upload_picture.php

```
1. <?php
2. $picture = "pictures/". basename($_FILES["uploadedfile"]["name"]);
3.  if(move_uploaded_file($_FILES["uploadedfile"]["tmp_name"], $picture)){
4.     echo "You have successfully uploaded you picture.";
5. }
6. else{
7.     echo "Error!";
8. }
9. ?>
```

Note: move_uploaded_file() is a PHP function to move file to a new location.

Problem 3 – (35 points)

Case description:

Company A is developing a web application to help people rent out their private cars in a period when they do not need to use their cars.

The owner of the car needs to open an account on the website and register their personal information (including social security number, name, home address, email, phone number), car information, car availability, the account for receiving the deposit, and the account for receiving the rent. The possible renter of the car also needs to open an account and register their personal information.

When the renter wants to rent a car, he or she can search for availability of cars, compare prices, make a reservation, and pay the deposit using a credit card to the deposit account. After the car is returned, the owner and renter need to log into the system and agree on the amount of deposit to be returned. After the agreement, the rent will be transferred to the car owner and the rest of the deposit will be returned to the renter. Company A will receive 0.1% of the rent from the car owner as expense of using the web application. Company A also gets paid by other companies, such as auto repair shops, insurance companies, and road

rescue companies, who advertise their services in the web site.

Your task is to make a risk-based assessment of this web application based on RMF (Risk Management Framework).
Your tasks include:

- Identify business goals and business assets (5 points).
- Identify and prioritize business risks (5 points).

  You should use the risk matrix below to prioritize business risks.

		Probability		
Consequence	Risk matrix	Low	Medium	High
	Low	L	L	M
	Medium	L	M	H
	High	M	H	H

- Make an overall misuse case diagram (10 points)
- Draw an attack tree for at least one of the threats in the misuse case diagram (10 points)
- Discuss possible legal issues to be considered in the contract if you are hired as penetration tester to test this application (5 points)