



VICTORIA UNIVERSITY OF
WELLINGTON
TE HERENGA WAKA

EXAMINATIONS – 2022

TRIMESTER 2

CYBR 271

SECURE PROGRAMMING

Time Allowed: TWO HOURS

CLOSED BOOK

Permitted materials: Only silent non-programmable calculators or silent programmable calculators with their memories cleared are permitted in this examination.

Printed foreign to English language dictionaries are permitted.

No other material is permitted.

Instructions: Attempt ALL questions.

There are 100 marks total.

Write answers in the spaces provided in the examination booklet.

Hand in the examination booklet.

Questions	Marks
1. Security Principles	[10]
2. Security Threat Modelling	[20]
3. Security Testing	[20]
4. Privilege escalation	[20]
5. Buffer Overflow	[20]
6. Format String	[10]
7. Web security	[15]

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

1. Security Principles.

(10 marks)

- (a) Consider an Internet banking application where the application allows users to query their balance and transfer money between accounts:

- i. **(2 marks)** Define the security principle *secure data at rest* and give a simple example of the principle in the context of the Internet banking application.

- ii. **(2 marks)** Define the security principle *separation of duty* and give a simple example of the principle in the context of the Internet banking application.

- (b) You have been hired to review the security of a new smartwatch that has been designed to detect severe heart arrhythmia. A condition characterized by abnormal heart rhythm. The smartwatch will vibrate when the condition is detected giving them time to seek emergency care.

- i. **(3 marks)** The smartwatch collects extra information such as GPS location that is not necessary for its functionality. *Identify the security principle being violated and justify your answer.*

- ii. **(3 marks)** When the smartwatch fails, it doesn't indicate that there is an error to user and the display looks the same as if it is working correctly. *Identify the security principle being violated and justify your answer.*

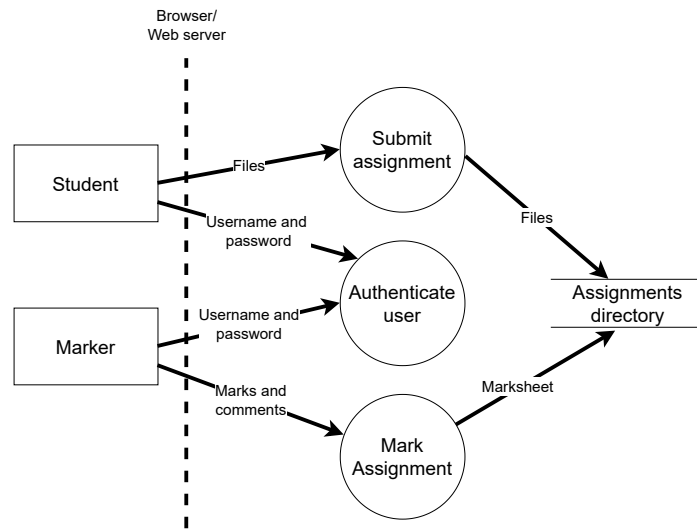
SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

2. STRIDE and Security Cards

(10 marks)

Consider the following data flow diagram for the ECS submission system. Note that all communications between the browser and web server are encrypted..



- (a) **(2 marks)** Name an external entity, process, data store and dataflow shown in the diagram.

- (b) **(2 marks)** Name two categories of threats that are applicable to an external entity and give a brief description of each.

- (c) **(2 marks)** Describe an example of a threat applicable to any of the data flows shown in the diagram and an appropriate **mitigation**.

- (d) **(4 marks)** Compare using security cards with the STRIDE methodology in terms of coverage and creativity, and explain why STRIDE is considered more suitable for inexperienced secure programmers. Make sure that you justify your answers.

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.

Specify the question number for work that you do want marked.

3. Libraries and Addressing Threats

(10 marks)

(a) Consider the Common Vulnerabilities and Exposures (CVE) standard.

i. **(2 marks)** Define the term *vulnerability* and give a simple example.ii. **(2 marks)** Define the term *exposure* and give a simple example.

Provide a concise example of each concept.

iii. **(2 marks)** What is the relationship between a CVE and the US National Vulnerability Database (NVD).

(b) Consider Open Web Application Security Project (OWASP) top 10 risks.

i. **(2 marks)** List four risks from the 2021 edition.ii. **(2 marks)** Briefly discuss the process that helps keep the list both based upon what has been observed as well as what are new emerging threats.

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

4. Ranking Threats

(10 marks)

- (a) **(2 marks)** Briefly explain why Microsoft has moved away from using DREAD to using Bug Bars?

- (b) **(4 marks)** Briefly explain the relationships between assets, vulnerabilities, threat, security controls and risk.

- (c) **(4 marks)** A colleague recommends that you purchase cyberinsurance for your company to transfer the risk associated with ransomware attacks. What are **TWO** new risks that might arise from taking our cyberinsurance? Assume that you **do not** publicise that you have taken out cyberinsurance.

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.

Specify the question number for work that you do want marked.

5. Reviews and Security Testing

(5 marks)

- (a) **(3 marks)** Briefly explain why it is considered best to use a combination of manual and automated security testing?

- (b) **(2 marks)** Compare and contrast ordinary software testing with security testing.

SECTION A Privilege escalation**[20 marks]**

6. Unix uses the “9-bit permission mechanism” and groups users into different groups where access permission can be managed per group. Using the `ls -l` command, you have got the following output. Identify the different groups and their corresponding permissions regarding this file. **(3 marks)**

```
-r-xrwxr-- 1 john staff 290 12 Oct 15:03 script
```

7. What values should be used with the `chmod` command to grant the following permissions to the script file? **(3 marks)**

- **Others:** Cannot read, write and execute.
- **Owner:** Can read and execute but cannot write.
- **Group:** Only allowed to write

```
$chmod __ __ __ script
```

8. Converting a program to be a Set-UID program requires setting the Set-UID bit and changing the ownership of the program. After executing the following two commands on the `stack` program, the system is not showing it is a privileged program. Explain what could be the reason. **(5 marks)**

```
seed@VM$ sudo chmod 4755 stack
seed@VM$ sudo chown root stack
```

9. A developer created the following privileged program to display the calendar by invoking the `cal` program using the `system()` function. Briefly explain how Environment Variables can be used to execute a `cal` program developed by the attacker instead of the one provided by the system. **(5 marks)**

```
#include <stdlib.h>
int main()
{
    4 system("cal");
    5 return 0;
}
```

10. Briefly explain the Principle of Isolation

(4 marks)

SECTION B Buffer Overflow**[20 marks]**

11. Draw the stack frame for the following function.

(7 marks)

```
int func(int g, int x, int f)
{
    int d, b, a;
    static str;
    static y=5;
    a = g - x;
    d = a + x;
    return d;
}
```

12. Calculate the memory address of the “Return Address” field if the offset between the start of the buffer and
- `ebp`
- is 73 bytes, and
- `ebp`
- is pointing to the address
- `0xbffea130`
- .

(3 marks)

13. For each of the following variables, specify on which part of the memory it will be located.
- (5 marks)**

1. Initialised local variable
2. `static ver_foo = 7`
3. Uninitialised global variable
4. `int *ptr = (int *) malloc(5*sizeof(int)); //(*ptr)`
5. `static hello;`

- 1.
- 2.
- 3.
- 4.
- 5.

14. An attacker has identified a vulnerable program that reads from a file and has created `abadfile` with the aim of getting a shell via a buffer overflow attack. The attack surface is the `strcpy()` function that copies the user input into a buffer.

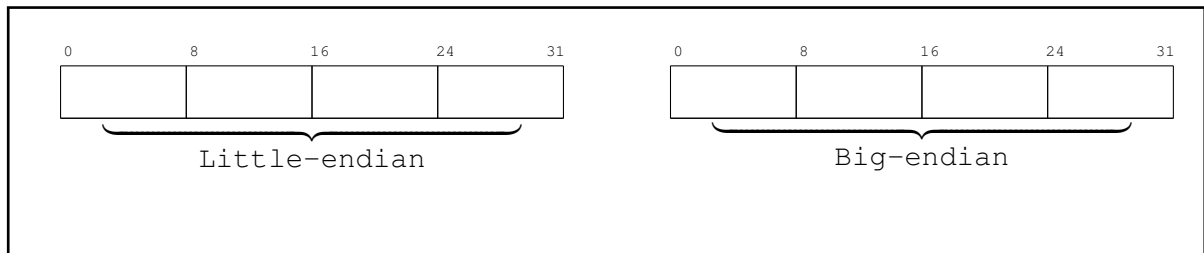
After checking the memory layout for the compiled code using the debugging mode (gdb), she prepared a badfile and injected the new return address based on `ebp+75` (hex), where `ebp` is `0xbffffc8b`. She has turned off address randomisation, made the stack executable and disabled all stack countermeasures. Her attack should be successful; however, a `Segmentation fault` error message has been received instead of a shell when the vulnerable program is executed on the input. **(5 marks)**

- (a) Explain the role of the NOP (0x90) in the attack and how it increases the chance of a successful attack. **(1 mark)**

- (b) Explain what is the main cause of the attack failing. **(4 marks)**

SECTION C Format String**[10 marks]**

15. What is the “Little-endian” and “Big-endian” representations of the 32-bit integer 0xA934D7B2? **(2 marks)**



16. The “width” modifier allows you to control the number of characters to be printed out. Using the `%x` and `%n` specifiers along with the width modifier, provide a format string to write 400 (decimal) into a variable on the stack if you know its address is 16 bytes above the `va_list` pointer. **(3 marks)**

17. An attacker targeted a format string vulnerability on a system, where the aim was to print out a secret value stored on the system. Based on some investigations, the attacker was able to find the distance between the address of the secret value and the `va_list` pointer. Accordingly, she provided 20 `%s` specifiers that is enough to advance the pointer to the right position and print out the value. **(5 marks)**

- (a) Explain why her attack was not successful. **(4 marks)**

- (b) How can you fix the problem? **(1 mark)**

SECTION D Web Security**[15 marks]**

18. 3. A website (cybr271.com) utilises the 'Content Security Policy' (CSP) mechanism to prevent XSS attacks and allows script code to be executed based on the following CSP role Which of the following java script codes will, or will not, be allowed to run? **(5 marks)**

```
Content-Security-Policy: default-src 'self;' script-src 'self'
'nonce-3fX254s' google.com
```

1. <script>... JavaScript code ...</script>
2. <script src="stduents.js">... JavaScript code ...</script>
3. <script src="http://abc.com/sss.js">... JavaScript code ...</script>
4. <script nonce="3fX25DD">... JavaScript code ...</script>
5. <script nonce="3fX254s">... JavaScript code ...</script>

- 1.
- 2.
- 3.
- 4.
- 5.

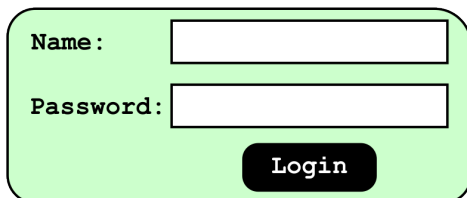
19. To defeat XSS attacks, a developer decides to implement filtering on the browser side. Basically, the developer plans to add JavaScript code on each page, so before data are sent to the server, it filters out any JavaScript code contained inside the data. Let's assume that the filtering logic can be made perfect. Can this approach prevent XSS attacks? **(2 marks)**

20. Adopting the Secret Token approach represents an effective mechanism to prevent CSRF attacks, where the server injects a secret into its own page after the user has been authenticated. This secret token must be attached with each subsequent request sent from the user's browser to the server; otherwise, the request might be discarded. Discuss whether this approach (CSRF tokens) can also be used to prevent stored XSS attacks or not.? **(3 marks)**

21. Data sanitisation (including both filtering and encoding approaches) can mitigate SQL-injection attacks, but does not address the fundamental cause of the problem. Discuss why “Prepared Statements”, on the other hand, is a perfect solution for this type of attacks. **(3 marks)**

22. A web application uses the login form presented in the figure below to allow access only to those who have a record in the application’s database. The system does not sanitize the input before forming and submitting the query to the database.

As an attacker, suggest an input that will let you access the system even if you are not registered. **(2 marks)**



```
<?php
    $sql = "SELECT *
            FROM users
            WHERE uid='$input_name' AND password='$input_password'";
    $result = $conn->query($sql);
?>
```

* * * * *