PES University, Bengaluru

(Established under Karnataka Act No. 16 of 2013)

December 2019: End Semester Assessment

B.TECH. VII Semester Elective CSE

UE16CS421: INFORMATION SECURITY

Time: 180 Mins | Answer All Questions | Max Marks: 100

Questions			Marks
Q1	1A	Explain one security challenge for each pillar of the CIA triad. Explain how computer security testing is different from functional testing.	5
Q1	1B	Think about the requirements for a Bank's ATM (Automated teller Machine). Describe the four specializations of the "Manage Account" use case. Derive the resulting Security use case and the linked Misuse case. Who may be the User and Misuser? Explain with help of a diagram.	12
Q1	1C	A process tries to open a file for read. The process's effective user ID is 1000, and real user ID is 2000. The file is readable to user ID 2000, but not to user ID 1000. Can this process successfully open the file? Explain in brief.	3

Q 2	2A	A program abc invokes an external program xyz using system(), which is affected by the PATH environment variable. When we invoke abc from a shell prompt, how does the shell variable PATH in the current shell end up affecting the behaviour of the system() function?	10
Q2	2B	Sam found a very useful web page, which contains links to many interesting papers. He wants to download those papers. Instead of clicking on each of the links, he wrote a program that parses a HTML web page, get the papers' URLs from the web page, and then use a program called wget to fetch each identified URL. The following is the code snippet:	

```
char command[100];
char* line, url;
line = getNextLine(file);
// Read in one line from the HTML file.
while (line != NULL) {
  // Parse the line to get a URL string.
  url = parseURL (line);
  if (url != NULL){
    // construct a command, and execute it
    sprintf(command, "%s %s", "wget", url);
    system(command);
}
  line = GetNextLine(file);
}
```

Please note that the functions getNextLine() and parseURL() are also implemented by Sam (their code is not displayed here). The program wget is a command-line program in Unix that can be used to download web files from a given URL.

The owner of the web page knows what Sam is doing with his page; he wants to attack Sam's program. He knows the code above, but he does not know how Sam implements GetNextLine() or ParseURL(), but he suspects that Sam may make some mistakes there.

(1) If you are the attacker, please describe how you plan to attack. 5

(2) How do you fix the problem? 5

Q3A 3A

In the function epilogue, the previous frame pointer, which is stored in the area below the return address, will be retrieved and assigned to the ebp register. However, when we overflow the return address, the previous frame pointer region is already modified, so after the function epilogue, ebp contains some arbitrary value. Does this matter? Explain. 5

Q3B 3B

Consider the following program: 8

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
extern char **environ;
int main()
{
  char *args[] =
  {
    "/bin/sh", "-c",
    "/bin/ls", NULL
  };
  pid_t pid = fork();
  if(pid == 0) {
     /* child */
     printf("child\n");
execve(args[0], &args[0], NULL); ¿ }
  else if(pid > 0) {
     /* parent */
     printf("parent\n");
  }
return 0;
}
```

		The program forks a child process, and executes the /bin/ls program using /bin/sh, which is a symbolic link to /bin/bash. The program is executed as the following.
		Explain what the output of the below program will be and why.
		`$ gcc prog.c -o prog`
		`$ export foo=’() { echo hello; }; echo world;’`
		`$ ./prog`	

Q3	3C	In which memory segments are the variables in the following code located?
		`int i = 0;`
		`void func(char *str)`
		`{`
		`    char *ptr = malloc(sizeof(int));`
		`    char buf[1024];`
		`    int j;`
		`    static int y;`
		`}`
			7

Q4A	4A	Both buffer-overflow and format-string vulnerabilities can lead to the modification of the return address field, but the ways how the field is modified are different in these two attacks. Please describe their differences, and comment on which one is less restricted.	6
Q4B	4B	i. Do browsers know whether an HTTP request is cross-site or not? ii. Do servers know whether an HTTP request is cross-site or not? iii. Why cannot a web server use the referer header to tell whether a request is cross-site or not? iv. Why is it important for a server to know whether a request is cross-site or not?	8
Q4C	4C	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. Explain.	6

Q5A	Q5A	Assume that you have a file that you would allow other users to read, only if a user’s ID is smaller than 1000. Please describe how you can actually achieve this. Assume your user ID is SEED.	6
Q5B	Q5B	The STRIDE model is commonly used for Threat Modelling. What does “STRIDE” stand for? In one line, write the definition for each?	6

Explain which Security principle/property is violated in each case? As a developer, give one appropriate example of how you would mitigate each Threat?

8

Please give your answer in the below format.

Threat	Definition	Security principle/property violated	Example of Mitigation by Developer