PES UNIVERSITY

PES University, Bengaluru

(Established under Karnataka Act No. 16 of 2013)

July 2021: End Semester Assessment

B.TECH. VI Semester Elective CSE

UE18CS347: INFORMATION SECURITY

Time: 180 Mins	Answer All Questions	Max Marks: 100

Questions			Marks
Q1	A	State if these statements are True or False. I. A stack canary is placed above the local variables but below the rip of a given stack frame in order to defend against buffer overflow vulnerabilities. Clarification: “below the rip” means “somewhere below the rip,” not necessarily directly below the rip. II. Modern systems enable stack canaries, W^X, ASLR, and pointer authentication to defend against buffer over-ow attacks. This is an example of defense-in-depth. III. Of the security principles covered in class, two factor authentication is best described as an example of defense in depth. IV. Clickjacking refers to a class of attacks where the attacker manipulates the user interface of a website to convince the user to click something that they did not intend to click on. Clickjacking can help an attacker execute reflected XSS attacks. V. CSRF tokens are an effective defense against CSRF attacks only if clients’ browsers respect the same-origin policy (SOP). VI. If a website only allows HTTPS connections, it is secure from SQL injection attacks.	6
	B	State if these statements are True or False. Justify your answer in NOT MORE than TWO sentences ONLY. I. Input sanitation helps defend against some (but not all) SQL injection and XSS attacks II. A cookie with the Secure flag set cannot be exploited in an XSS attack. III. ASLR prevents all buffer overflow attacks. IV. Randomizing the source IP is a common defense against DNS spoofing.	8

	C	STRIDE is a common framework used in Threat Modelling. Explain what STRIDE stands for?	6
Q2	A	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 the difference?	6
	B	Do browsers know whether an HTTP request is cross-site or not? Do servers know whether an HTTP request is cross-site or not?	3 4
	C	What are the main differences of CSRF and XSS attacks? If you can modify browser's behaviour, how would you modify the browser, so you can help reduce the risks of XSS attacks?	3 4

Q3	A	Consider the below code snippet:
		`char *double(char *str) {`
		`    size_t len = strlen(str);`
		`    char *p = malloc(2*len+1);`
		`    strcpy(p, str);`
		`    strcpy(p+len, str);`
		`    return p;`
		`}`
		As security-conscious programmer, please list your concerns. For each concern, kindly suggest an appropriate fix.
			8

	B	Consider the below code snippet on a 32 bit machine:
		`void function(int a, int b, int c) { char buffer1[5];`
		`char buffer2[10];`
		`}`
		`void main() { function(1,2,3);`
		`}`
		We compile it with gcc using the S switch to generate assembly code output:
		a) Please write the assembly code that would be generated.
		b) When the Function call is initiated, it triggers the procedure Prolog. Please write the assembly code of Procedure Prolog. You should explain how it calculates space for the local variables.
			9

	C	Consider the example below:
		`char buf[80];`
		`void vulnerable() {`
		`gets(buf);`
		`}`
		As a security engineer, explain in brief, what you believe is the problem with above example?
			3

Q4	A	Consider the below code presented to you in a code review:
		`char digit_to_char(int i) {`
		`        char convert[] = "0123456789";`
		`        return convert[i];`
		`}`
		What is the issue you see as a security engineer and what modifications would you suggest to make the code secure?
			5

	B	Abhaya is using a third-party analytics service called ABtesters. Abhaya website includes a tag to load the ABtesters JavaScript library.
		Abhaya's website is located at https://abhaya.com and contains the following HTML:
		`< scriptsrc = "https:// cdn.abtesters.com/lib.js"></script>`
		`<form name= "login" action= "/login" method= "POST”>`
		` <input type= "text" name= "username" / >`
		` <input type= "password" name= "password" / >`
		`</form>`
		Use the above to answer Q4-B, Q4-C and Q4-D
		In the same-origin policy, which parameters are used in determining the origin of an HTTP webpage?
			5

	C	Abhaya is concerned that the ABtesters JavaScript library could steal customer passwords from the login form if the JavaScript library were compromised. Is this a valid concern – Yes, or No? Justify your response.	5
	D	Abhaya realizes that there are no CSRF protections on the transfer form, which means attackers can steal money from users' accounts. Based on your learning from class, what would you propose to prevent CSRF attacks?	5
Q5	A	The `chown` command automatically disables the Set-UID bit, when it changes the owner of a Set-UID program. Please explain why it does that.	4

	B	The following are two different ways to printout environment variables. Please describe their differences:
		`$ /usr/bin/env`
		`$ /usr/bin/strings /proc/$$/environ`
			4

	C	Instead of putting an extra shell command after a function definition, we put it at the beginning (see below).
		`$ export foo=’echo world; () { echo hello;}’`
		`$ bash`
		We then run Bash, which is vulnerable to the Shellshock attack.
		Will the shell command `echo world` be executed?
			3

	D	In a Linux system, a privileged Set-UID program needs to find out which directory it is currently in. As a Security Engineer, which approach would you use? Explain. One is to use the PWD environment variable, which contains the full path of the current directory. Another approach is to use the `getcwd()` which is a system call in Linux.	4
	E	Students were working on the Buffer Overflow attacks. One student obtained the below output. Can you explain why the student got shell access in some cases and not in others? buffer address : 0xbffff180 case 1 : long retAddr = 0xbffff250 -> Able to get shell access case 2 : long retAddr = 0xbffff280 -> Able to get shell access case 3 : long retAddr = 0xbffff300 -> Cannot get shell access case 4 : long retAddr = 0xbffff310 -> Able to get shell access case 5 : long retAddr = 0xbffff400 -> Cannot get shell access	5