SRN | | | | | | | | | | | | |

PES UNIVERSITY

PES University, Bengaluru

(Established under Karnataka Act No. 16 of 2013)

UE18CS347

DECEMBER 2021: END SEMESTER ASSESSMENT (ESA) B TECH VI SEMESTER

UE18CS347 – INFORMATION SECURITY

Time: 3 Hrs	Answer All Questions	Max Marks: 100

1	a)	Give the anatomy of the attack briefly to understand the process of an attack	3
	b)	List the three core security principles and illustrate them with an appropriate scenario.	6
	c)	Discuss about Privacy and Security. Are they related or different? Justify with an example.	3
	d)	Elaborate the different phases involved in Secure Software development life cycle.	8
2	a)	Which attack is the result of remote code execution vulnerability in BASH? Explain the process of the attack with an example.	5
	b)	What do you mean by SetUID bit? Enumerate the attack surfaces of SetUID programs and explain each of them.	8
	c)	Bob says that he never uses any environment variable in his code, so he does not need to worry about any security problem caused by environment variables. Is he correct?	2
	d)	Discuss the key steps in the process of launching buffer overflow attack in your lab virtual environment	5
3	a)	What do you mean by Trust boundary? List some three interesting trust boundaries	4
	b)	Enumerate any four Threat Modelling techniques. Explain any one of them in detail	8
	c)	Discuss the four key aspects to be considered by an organization in detail with respect to the privacy of each user of the organization.	8
4	a)	The following SQL statement is sent to the database, where $eid and $passwd contain data provided by the user. An attacker wants to try to get the database to run an arbitrary SQL statement. What should the attacker put inside $eid or $passwd to achieve that goal. Assume that the database does allow multiple statements to be executed. $Sql = "SELECT * FROM employee WHERE eid='$eid' and password='$passwd'"	3
	b)	Explain the SQL Injection Attack and discuss launch of that attack using cURL	6
	c)	List the different types of XSS attacks and differentiate them	6
	d)	Discuss Cross site request forgery attack with a neat diagram	5
5	a)	Discuss and differentiate static and dynamic analysis with their advantages and disadvantages	6
	b)	What is Penetration testing? Enumerate and explain the phases of penetration testing in detail.	8
	c)	What is Nmap? What Does Nmap do? Explain the working of Nmap	6