Name:

Enrolment No:

UPES
UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2019

Course: IT System Security **Semester: VI**
Program: B. Tech CSE+CSF **Time 03 hrs.**
Course Code: CSIB367 **Max. Marks: 100**

Instructions: (i) Start answering a question on new page, (ii) All parts of a section should be answered together, (iii) Scattered part answers will not be evaluated, (iv) Exchange of mobile phone, calculator or any item is not allowed.
All questions are compulsory. There is an internal choice in Q-9 and Q-11.

SECTION A

S. No.		**Marks**	**CO**
Q 1	Answer the following questions: a) _____________ is the assurance that data has not been changed unintentionally due to an accident or malicious activity. b) What happens in Time-of-Check-to-Time-of-Use (TOCTTOU) attack? c) Name two methods for the prevention of buffer overflow attack. d) In Microsoft Windows, ___________ is designed to use a tamper-proof hardware chip (Trusted Platform Module) which stores encryption key material.	**4**	**CO1, CO2**
Q 2	Explain Cross-Site Scripting. Give Examples of XSS Attack. How Cross-Site Scripting is useful for attacks in performing malicious actions?	**4**	**CO4**
Q 3	Is SSL protocol and TLS protocol same? If not, explain the difference between them.	**4**	**CO4**
Q 4	Discuss different goals of IT System security.	**4**	**CO1**
Q 5	John is the security administrator for company X. He has been asked to oversee the installation of a fire suppression sprinkler system, as recent unusually dry weather has increased the likelihood of fire. Fire could potentially cause a great amount of damage to the organization's assets. The sprinkler system is designed to reduce the impact of fire on the company. In this scenario, what are the threats, vulnerabilities, risks? Suggest countermeasures also.	**4**	**CO5**

SECTION B

Q 6	a) How SSL session is negotiated with the help of handshake protocol? Explain with	**5+2+3**	**CO4**

	the help of proper diagram. b) Explain the difference between extended validation SSL certificate and standard SSL certificate. c) Differentiate between SSL session and SSL connection.		
Q 7	a) What are the possible threats to IT Systems. Explain at least 10 threats with proper example. b) Explain risk identification process briefly. How would you identify, categorize and classify assets involved in risk identification process.	**5+5**	**CO5**
Q 8	a) Discuss key points of database security. Explain database security lifecycle also with proper diagram. b) Why OS is hard to secure? List and discuss various workstation operating system security guidelines.	**5+5**	**CO2, CO5**
Q 9	a) What do you understand by operating system security? Explain three major tasks that are essential to build any successful operating system. b) Name at least 4 programming bugs that can be exploited. **OR** a) Explain 'trust model' and 'threat model' of securing an operating system. b) Discuss various threats in mobile operating systems.	**6+4**	**CO2**
SECTION-C			
Q 10	a) Illustrate the importance of Gartner's magic quadrant. b) Explain all the four sections of Gartner's magic quadrant. Name at least 3-3 companies of each section.	**6+14**	**CO3**
Q 11	a) Is SQL Injection a database application security weakness? If yes, how an attack exploit SQLi vulnerabilities. How does a defender uses discover, avoid and repair, remediate and mitigate strategies in defending against SQLi attacks? b) Briefly discuss various threats posed to different assets of IT Department: Payroll fraud, payroll errors, interruption of operations, disclosure of brokerage of information, network-related threats. **OR** a) When the average person thinks of network security within a school they often think of the student trying to hack into the system to change their grade, to see if they can take over their friend's computer, or to put a prank up on the school	**10+10**	**CO1**

	website. In light of the current network dangers these may be some of least of the school system worries. How can the school ensure this system is used correctly? What are the ethical issues of this situation? How should students be dealt with if they were the people initiating the attack? b) What is endpoint security? Discuss four pillars of endpoint security in bring your own device (BYOD) program: endpoint hardening, endpoint reliability, network prioritization, network resiliency.		

Name: **Enrolment No:**	UPES UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2019

Course: IT System Security **Semester: VI**
Program: B. Tech CSE+CSF **Time 03 hrs.**
Course Code: CSIB367 **Max. Marks: 100**

Instructions: (i) Start answering a question on new page, (ii) All parts of a section should be answered together, (iii) Scattered part answers will not be evaluated, (iv) Exchange of mobile phone, calculator or any item is not allowed.
All questions are compulsory. There is an internal choice in Q-9 and Q-11.

SECTION A

S. No.		Marks	CO
Q 1	Explain the concept of digital signature with proper diagram.	**4**	**CO1**
Q 2	Briefly explain the features of various security testing tools: Qasat, HashQ, Android Emulator, WebScarab and WebSlayer.	**4**	**CO4**
Q 3	Differentiate between Dynamic analysis, black box security testing and static analysis & code review in mobile application security testing.	**4**	**CO4**
Q 4	Explain risk identification process briefly. How would you identify, categorize and classify assets involved in risk identification process.	**4**	**CO5**
Q 5	Does disabling caching protect sensitive data? How does the following code useful in similar process. <FilesMatch ".(pdf|png)> FileETag None Header unset ETag Header set Cache-Control "max-age=0, no-cache, no-store, must-revalidate" Header set Pragma "no-cache" Header set Expires "Wed, 11 Jan 1984 05:00:00 GMT" </FilesMatch>	**4**	**CO1**

SECTION B

S. No.		Marks	CO
Q 6	What is OWASP? List the OWASP top 10 highlighting threats to mobile applications. Compare and contrast these 10 highlighting threats and their impacts.	**10**	**CO4**
Q 7	Discuss different architectures of Database System. What are the steps required to secure a database? How Insider threat is different from login attacks in database security. List various database security practices and planning for database server.	**10**	**CO5**
Q 8	Explain the concept of Gartner's magic quadrant. Briefly explain all the four sections of Gartner's magic quadrant.	**10**	**CO3**

Q 9	Compare and contrast Technical controls in IT system security: identification and authentication, passwords, cryptographic keys, memory tokens, smart tokens. **OR** Why OS is hard to secure? List and discuss various workstation operating system security guidelines. Is there any formal security mechanisms in operating system? If yes, discuss its importance.	**10**	**CO1, CO2**
	SECTION-C		

Q 10	a) Is SQL Injection is an database application security weakness? If yes, how an attack exploit SQLi vulnerabilities. How does a defender uses discover, avoid and repair, remediate and mitigate strategies in defending against SQLi attacks?
	b) Why shellshock is dangerous to application security? List known testing tools for shellshock. How these testing tools helps to protect against shellshock.
	c) What is endpoint security? Discuss four pillars of endpoint security in bring your own device (BYOD) program: endpoint hardening, endpoint reliability, network prioritization, network resiliency.
	d) Explain the importance of following code in OWASP application security risks
	`function isValidEmail (input)`
	`{`
	` var result=false;`
	` var email_regex = /^[a-zA-Z0-9._-]+@([a-zA-Z0-9.-]+.)+[a-zA-Z0-9.-]{2,4}$/;`
	` if ( email_regex.test(input) ) {`
	`  result = true;`
	` }`
	` return result;`
	`}`
		5*4 =20	**CO4, CO5, CO3**

Q 11	Write short note on following Oracle Application Server Portal Security: a) Best Practices for Cookie Security b) Best Practices for Certificates Use c) Review Code and Content Against Already Known Attack d) Common Sense Firewall Practices e) Leverage Declarative Security **OR** a) Think of an organisation you know and the sort of information it may hold for business purposes. What are the particular responsibilities involved in keeping that information confidential? b) What fundamental security measures have been traditionally used in organisations such as banks or government departments, apart from those involving computer networks, and are they relevant to network security?	**2*5 =20**	**CO1, CO2**

	c) When the average person thinks of network security within a school they often think of the student trying to hack into the system to change their grade, to see if they can take over their friend’s computer, or to put a prank up on the school website. In light of the current network dangers these may be some of least of the school system worries. How can the school ensure this system is used correctly? What are the ethical issues of this situation? How should students be dealt with if they were the people initiating the attack? d) Briefly discuss various threats posed to different assets of IT Department: Payroll fraud, payroll errors, interruption of operations, disclosure of brokerage of information, network-related threats.	**5*4 =20**	**CO1, CO2**