

Name:	
Enrolment No:	

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2018

Course: B.Tech CSE+CSF	Semester: V
Programme: IT Application Security	CSIB356
Time: 03 hrs.	Max. Marks: 100
Instructions: All questions in Section A are compulsory. There is an internal choice in Section B and Section C.	

SECTION A (20 Marks)

S. No.	Question	Marks	CO
Q 1	Mention 4 precautions for canonicalization.	4	CO2
Q 2	Distinguish between session and cookies with example.	4	CO3
Q 3	List 4 tools to perform secure code analysis in C, C++, Java and PHP.	4	CO5
Q 4	Mention 4 W's of Logging with examples.	4	CO4
Q 5	Users are unable to connect to a web server at IP address 10.80.1.5. You look at the rules in a firewall's ACL between the user's system and the web server and see the following two rules: permit tcp any host 10.80.1.15 eq 80 permit tcp any host 10.80.1.15 eq 443 What do these rules imply? Explain in brief.	4	CO4

SECTION B (40 Marks)

Q 6	Explain what should be logged and what should not be logged for security?	5+5	CO4
Q 7	“A security professional might have to perform secure code review or write automation scripts.” With respect to this statement list what is the aim and importance of secure code analysis (SAST+DAST)?	5+5	CO5
Q 8	John has a Web App (HTML5/Javascript/AngularJS) which logs user activity into a Backend DB via Web API. This function runs quite frequently on events such as Menu and button clicks throughout the app. making an API call for each such event seems expensive, and John was wondering what are best practices for these kind of updates, and how to handle User Audit Logs (or other frequent client-side actions) in a Web App?	5+5	CO4
Q 9	There are a number of exploitable vulnerabilities in DNS. An attacker sends a forged DNS response, the corrupt data provided by the attacker gets stored for future use by the DNS. As a result, future users that attempt to visit the corrupted domain are routed to the new IP address selected by the attacker. Users continue to receive unauthentic IP addresses from the DNS. Answer the following questions with respect to the above scenario: 1. Which attack is discussed in above scenario? Write about it in 100-200 words. [3]	10	CO2

	<p>2. What is the outcome of the attack and why? [4]</p> <p>3. How can you prevent this attack? Mention any 3 ways. [3]</p>		
OR			
	<p>If there is a social networking site with a valid user logged-in, and the server has issued a session cookie “SESSION-ID” to the user. If the SESSION-ID is the cookie that identifies the session of the user, the attacker can use the SESSION-ID cookie value to login as the valid user. The attacker can perform a cross-site scripting or other technique to steal the cookie from the victim’s browser. Let’s assume the attacker steals the cookie SESSION-ID=User-abc-logged-in-2341785645. Now, he can use the cookie with the following request to post a status (I am hacked!!!!!!) in the victim’s home page:</p> <pre>POST /home/post_status.php HTTP/1.1 Host: www.social-site.com Cookie: SESSION-ID=User-abc-logged-in-2341785645 Content-Length:38 Content-Type:application/x-www-form-urlencoded Status=I am hacked!!!!!!&Submit=submit</pre> <p>1. Which attack is discussed in above scenario? Write about it in 100-200 words. [3]</p> <p>2. What is the outcome of the attack and why? [4]</p> <p>3. How can you mitigate this attack? Mention any 3 ways. [3]</p>	10	CO2
SECTION-C (40 Marks)			
Q 10	<p>Compute the CVSS 2.0 Base Vector and then Base Score for the following vulnerability:</p> <p>Vulnerability A vulnerability in the MySQL Server database could allow a remote, authenticated user to inject SQL code that MySQL replication functionality would run with high privileges. A successful attack could allow any data in a remote MySQL database to be read or modified.</p> <p>Attack An attacker requires an account on the target MySQL database with the privilege to modify user-supplied identifiers, such as table names. The account must be on a database which is being replicated to one or more other MySQL databases. An attack consists of logging in using the account and modifying an identifier to a new value that contains a quote character and a fragment of malicious SQL. This SQL will later be executed as a highly privileged user on the remote system(s). The malicious SQL is injected into SQL statements that are part of the replication functionality, preventing the attacker from executing arbitrary SQL statements. Use the values given below:</p>	20	CO1

	<u>Access Vector</u>		<u>Authentication</u>		
	Local (L)	0.395	Multiple (M)	0.45	
	Adjacent Network (A)	0.646	Single (S)	0.56	
	Network (N)	1.0	None (N)	0.704	
	<u>Access Complexity</u>		<u>CI, II, AI</u>		
	High (H)	0.35	None (N)	0.0	
	Medium (M)	0.61	Partial (P)	0.275	
	Low (L)	0.71	Complete (C)	0.660	

Q 11	<p>Suppose Alice wants her friends to encrypt email messages before sending them to her. The RSA Encryption Scheme is used to encrypt and then decrypt electronic communications.</p> <p>Alice's Setup: • $p = 11$ and $q = 3$. • $n = pq = 11 \times 3 = 33$. • $m = (p - 1)(q - 1) = 10 \times 2 = 20$. • If $e = 3$ and $d = 7$, then $ed = 21$ has a remainder of 1 when divided by $m = 20$. • Publish public key $(n, e) = (33, 3)$.</p> <p>Bob encrypts message $M = 14$: • Public key $(n, e) = (33, 3)$. • When $14^3 = 2744$ is divided by 33, the remainder is $C = 5$. • Sends ciphertext $C = 5$ to Alice</p> <p>Alice decrypts ciphertext $C = 5$: • private key $(n, d) = (33, 7)$. • When $5^7 = 78125$ is divided by 33, the remainder is $R = 14$. • $R = 14 = M$, the original message from Bob!</p> <p>Now, answer the following questions:-</p> <ol style="list-style-type: none"> Callie wants to send the message $M = 13$ to Alice. Using Alice's public and private keys, calculate the ciphertext C, and the value for R when Alice recovers the message. Dexter wants to set up his own public and private keys. He chooses $p = 23$ and $q = 19$ with $e = 283$. Find d so that ed has a remainder of 1 when divided by $(p - 1)(q - 1)$. 	10+10	CO3
------	--	-------	-----

OR

	<ol style="list-style-type: none"> Alice and Bob wish to exchange a secret key using the Diffie-Hellman algorithm. They agree to use the prime number 71 and its primitive root 7. Alice chooses the private key 6 while Bob chooses 12. To their misfortune, Eve, intercepts the public keys sent by Alice and Bob and executes a Man In The Middle (or rather Woman In the Middle) attack to trick them into believing they have exchanged a key with each other, while in reality they would have exchanged two keys with Eve. Execute Eves Page 6 attack and obtain the secret keys shared with Alice and Bob. You may assume Eve chooses the private keys 8 and 14. [4+4+3+3] Convert "MEET ME" into cipher text using Hill cipher with the key matrix. 	14+6	CO3
--	--	------	-----

17	17	5
21	18	21
2	2	19

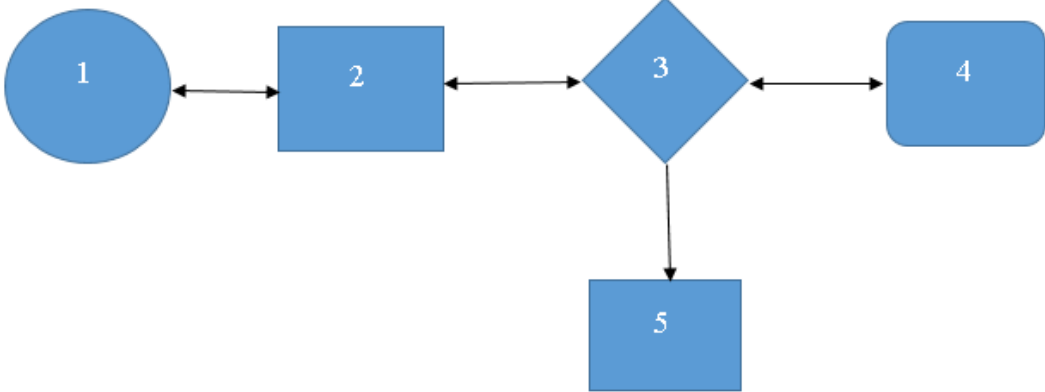
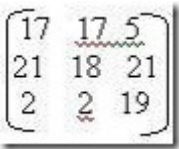
Name:	
Enrolment No:	

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2018

Course: B.Tech CSE+CSF	Semester: V
Programme: IT Application Security	CSIB356
Time: 03 hrs.	Max. Marks: 100


Instructions: All questions in Section A are compulsory. You have internal choice in Section B and Section C.

SECTION A (20 Marks)

S. No.		Marks	CO
Q 1	Mention any 4 challenges involved in logging.	4	CO4
Q 2	Label and mention the core components of AAA:- 	4	CO2
Q 3	What is the importance of log disposal and why?	4	CO4
Q 4	Encrypt the message "PAY" using hill cipher with the following key matrix:- 	4	CO3
Q 5	What web application vulnerabilities are most likely to be found in a source code review? List out any four with example of each.	4	CO5

SECTION B (40 Marks)

Q 6	1. Users are unable to connect to a web server at IP address 10.80.1.5. You look at the rules in a firewall's ACL between the user's system and the web server and see the following two rules: permit tcp any host 10.80.1.15 eq 80 permit tcp any host 10.80.1.15 eq 443 What do these rules imply? Explain in brief.	5+5	CO4
-----	--	-----	-----

	2. “Logging is one way to identify and report an incident”. Comment on this statement with example.		
Q 7	“A security professional might have to perform secure code review or write automation scripts.” With respect to this statement list what is the aim and importance of secure code analysis (SAST+DAST)?	5+5	CO5
Q 8	<p>You are engaged in a penetration-test where you are attempting to gain access to a protected location. You are presented with this login screen:</p>  <p>What are some examples of how you would attempt to gain access?</p>	10	CO2
Q 9	<p>Consider a social networking website (www.socialnetworking-site.com) uses an algorithm to generate cookies for the users. If the user name is “John”, then the cookie generated for the user could be “LOGINID=1322015-iknpgimo”. In this case, the algorithm used to generate the cookie can be as follows: first part of the cookie is the date i.e. 13/2/2015, and second part is the combination of the previous and following alphabet letter for each letter of the username “John” (i.e., the previous letter for J is “I” and the following letter is “k”). If the attacker is able to crack the algorithm, he could guess the cookie of users and hack their session. If the hacker plans to hack the session of Albert, he can create a cookie as LOGINID =1322015-zbkmacdfqssu, login to Albert’s session and post a status on his account.</p> <pre>POST /Status/post.asp HTTP/1.1 Host: www.another-social-site.com Cookie:LOGINID =1322015-zbkmacdfqssu Content-Length:45 Content-Type:application/x-www-form-urlencoded Todays_status=I am hacked!!!!!!&Submit=submit</pre> <p>i. Which attack is discussed in above scenario? Write about it in 200-500 words. [3] ii. What is the outcome/effect of the attack? [4] iii. How can you mitigate this attack? Mention any 5 ways. [3]</p>	10	CO2
OR			
	Imagine that a criminal insider wants to MITM logins to an internal server, or just try and catch the credentials of a particular user. So the criminal poisons the record for ActiveDirectoryServer.myCompany.Internal and has it point back to his own machine (also inside the company). All attempts to interact with the company’s Active Directory (AD) Server are now going through the criminal’s system. He proxies everything on to the AD server until he gets to the credentials he wants (which could be machine or user credentials). Windows has ways to prevent	10	CO2

	<p>MITM, but most people don't use it.</p> <ol style="list-style-type: none"> i. Name and explain the attack being discussed in this scenario.[3] ii. What the attacker might do with the credentials? List any three examples.[3] iii. Mention any four ways to prevent this attack. [4] 																																		
SECTION-C (40 Marks)																																			
Q 10	<p>Compute the CVSS 2.0 Base Vector and then Base Score for the following vulnerability:</p> <p>Vulnerability</p> <p>Adobe Acrobat and Reader are vulnerable to a buffer overflow, caused by improper bounds checking when parsing a malformed JBIG2 image stream embedded within a PDF document. By persuading a victim to open a malicious PDF file, a remote attacker could overflow a buffer and execute arbitrary code on the system with the privileges of the victim or cause the application to crash.</p> <p>Attack</p> <p>The vulnerability is exploited by convincing a victim to open a malicious document on a system that uses a vulnerable version of Adobe Acrobat or Reader. An attacker must deliver a malicious document to the victim and relies upon the user to open it. If the user is privileged, then the code execution achieved by the attacker could result in High impacts to Confidentiality, Integrity, and Availability.</p> <p>Use the values given below:</p> <table style="width: 100%; border: none;"> <tr> <td colspan="2">Access Vector</td> <td colspan="2">Authentication</td> </tr> <tr> <td>Local (L)</td> <td>0.395</td> <td>Multiple (M)</td> <td>0.45</td> </tr> <tr> <td>Adjacent Network (A)</td> <td>0.646</td> <td>Single (S)</td> <td>0.56</td> </tr> <tr> <td>Network (N)</td> <td>1.0</td> <td>None (N)</td> <td>0.704</td> </tr> <tr> <td colspan="2">Access Complexity</td> <td colspan="2">CI, II, AI</td> </tr> <tr> <td>High (H)</td> <td>0.35</td> <td>None (N)</td> <td>0.0</td> </tr> <tr> <td>Medium (M)</td> <td>0.61</td> <td>Partial (P)</td> <td>0.275</td> </tr> <tr> <td>Low (L)</td> <td>0.71</td> <td>Complete (C)</td> <td>0.660</td> </tr> </table>	Access Vector		Authentication		Local (L)	0.395	Multiple (M)	0.45	Adjacent Network (A)	0.646	Single (S)	0.56	Network (N)	1.0	None (N)	0.704	Access Complexity		CI, II, AI		High (H)	0.35	None (N)	0.0	Medium (M)	0.61	Partial (P)	0.275	Low (L)	0.71	Complete (C)	0.660	20	CO1
Access Vector		Authentication																																	
Local (L)	0.395	Multiple (M)	0.45																																
Adjacent Network (A)	0.646	Single (S)	0.56																																
Network (N)	1.0	None (N)	0.704																																
Access Complexity		CI, II, AI																																	
High (H)	0.35	None (N)	0.0																																
Medium (M)	0.61	Partial (P)	0.275																																
Low (L)	0.71	Complete (C)	0.660																																
Q 11	<ol style="list-style-type: none"> 1. User A and B use Diffie-Hellman key exchange a common prime $q=71$ and a primitive root $a=7$. Calculate the following: <ol style="list-style-type: none"> i. If user A has private key $X_A=5$, what is A's public key Y_A. 	10+10	CO3																																

	ii. If user A has private key $X_B=12$, what is B's public key Y_B ? iii. What is shared secret key? 2. Evaluate encryption using RSA algorithm for the following: $p=7$, $q=11$; $e=17$; $m=8$.		
OR			
	Explain encryption, decryption and key generation in DES algorithm with appropriate block diagrams.	20	CO3