

Name:  
Enrolment No:



**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

**End Semester Examination, December 2019**

**Course: IT Application Security**

**Semester : V**

**Program: B.Tech CSE-CSF V Sem**

**Time : 03 hrs.**

**Course Code: CSSF 3002**

**Max. Marks: 100**

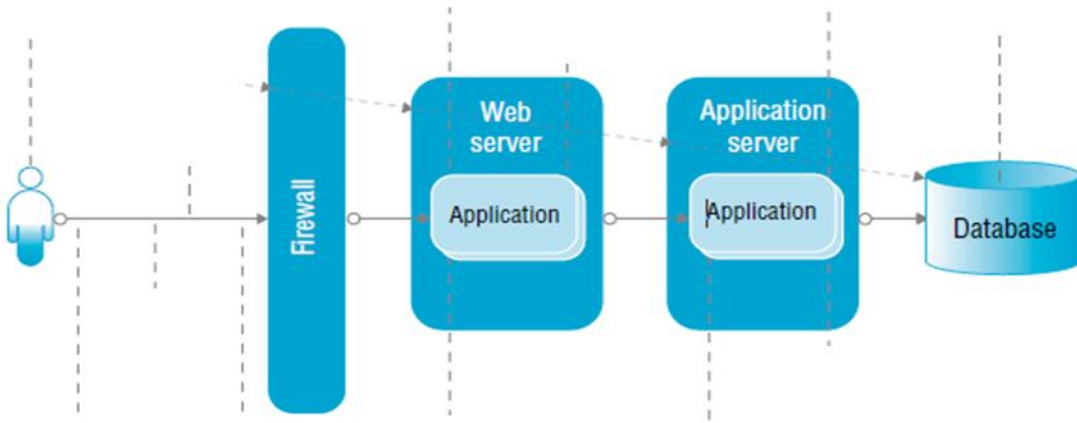
**Instructions: All questions are compulsory in Section A. There is an internal choice in Section B and Section C.**

**SECTION A (20 Marks)**

S. No.		Marks	CO
Q 1	Write the full forms of the following acronyms:- i. S-SDLC ii. ARP iii. OWASP iv. CLASP	4	CO1
Q 2	Define Insecure Deserialization with example	4	CO2
Q 3	Distinguish between session and cookies with example.	4	CO3
Q 4	State the importance of log disposal.	4	CO4
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	Explain Buffer Overflow Technique and the damage caused with it. Also mention 3 ways to prevent Buffer overflow.	10	CO2
Q 7	A site doesn't use or enforce TLS for all pages or supports weak encryption. An attacker monitors network traffic (e.g. at an insecure wireless network), downgrades connections from HTTPS to HTTP, intercepts requests, and steals the user's session cookie. The attacker then replays this cookie and hijacks the user's (authenticated)	10	CO3

	<p>session, accessing or modifying the user’s private data. Instead of the above they could alter all transported data, e.g. the recipient of a money transfer.</p> <ol style="list-style-type: none"> <li>i. Which type of OWASP vulnerability is discussed in the above scenario? Explain in brief. [3]</li> <li>ii. “Session data is stored on the server, whereas cookies store data in the visitor's browser.” Justify this statement in not more than 100 words with respect to given scenario. [4]</li> <li>iii. How can you mitigate such attack? [3]</li> </ol>		
Q 8	<p>In a web application, you can see in BurpSuite that the request is carrying a CSRF token, which is not getting changed for each request, even the token is same for different sessions. Is the application vulnerable to CSRF attack? Justify your opinion. If the application is vulnerable, what should be the mitigation steps?</p>	10	CO2
<b>OR</b>			
	<p>A database query fetches username and password from the database:-  <b>Query:</b> SELECT * FROM USERTABLE WHERE USER ='&amp;password=';</p> <ol style="list-style-type: none"> <li>i. Write a payload to inject to perform SQL Injection, and justify why your payload should work.</li> <li>ii. Transform the query using secure coding practices so that SQL injection cannot be performed.</li> </ol>		
Q 9	<p><b>Apply Authentication and Authorization to the architecture shown below and explain the entire process briefly:-</b></p> 	10	CO3
<b>SECTION-C (40 marks)</b>			

<p>Q 10</p>	<p>Compute the CVSS 2.0 Base Vector and then Base Score and Temporal Score for the following vulnerability:</p> <p><b>Vulnerability</b></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><b>Attack</b></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 border="0" style="width: 100%;"> <tr> <td colspan="2"><b>Access Vector</b></td> <td colspan="2"><b>Authentication</b></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"><b>Access Complexity</b></td> <td colspan="2"><b>CI, II, AI</b></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>	<b>Access Vector</b>		<b>Authentication</b>		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	<b>Access Complexity</b>		<b>CI, II, AI</b>		High (H)	0.35	None (N)	0.0	Medium (M)	0.61	Partial (P)	0.275	Low (L)	0.71	Complete (C)	0.660	<p><b>20</b></p>	<p><b>CO1</b></p>
<b>Access Vector</b>		<b>Authentication</b>																																	
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																																
<b>Access Complexity</b>		<b>CI, II, AI</b>																																	
High (H)	0.35	None (N)	0.0																																
Medium (M)	0.61	Partial (P)	0.275																																
Low (L)	0.71	Complete (C)	0.660																																
<p>Q 11</p>	<p><b>A.</b> How would you perform a security/penetration test on a Web application covering the following scenarios:- [10]</p> <ol style="list-style-type: none"> <li>i. Unauthenticated tests on login page.</li> <li>ii. Authenticated tests with one user account</li> <li>iii. Authenticated tests with multiple user accounts</li> </ol> <p>Explain each with appropriate example.</p> <p><b>B.</b> What is logging? What are 4 W's of logging? What are the challenges faced during logging? [10]</p>	<p><b>20</b></p>	<p><b>CO4</b> <b>CO5</b></p>																																

**OR**

- A.** 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:



What are some examples of you how you would attempt to gain access?

- B.** What do you understand by auditing? List the steps that would take place during closing meeting of an audit.

**20**

**CO4  
CO5**