UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2017

Program Name	**: B.Tech CSE + CSF**	**Semester**	**: V**
Course Name	**: IT Application Security**	**Max. Marks**	**: 100**
Course Code	**: CSIB 356**	**Duration**	**: 3 Hrs**
No. of page/s	**: 03**		

Note:

1. Answers to question 1 to 5 of Section A carries 4 marks each.
2. Answers to question 6 to 9 of Section B carries 10 marks each.
3. Answers to question 10 and 11 of Section C carries 20 marks each.

SECTION A

1. What does Log Analysis includes?

2. What are the 4Ws in logging? Write at least two example for each.

3. Give some examples what should not be logged.

4. State true or false for following statements:

   a. Luring attack is a type of elevation-of-privilege attack in which an attacker lures a highly privileged component to do something on his behalf.

   b. A cookie is a small text file, for example cookie.txt, rendered by a web application browser; available on your web server.

   c. Dictionary attack is a type of brute force attack that seeks to find the desired values by trying all words present in a dictionary.

   d. In order to countermeasure from network eavesdropping, the quality of authentication and encryption mechanism doesn't matters at all.

5. Use the affine cipher to decrypt the message "ZEBBW" with the key pair (7, 2) in modulus 26.

SECTION B

6. (a) The main difference between cookies and sessions is that cookies are stored in the user's browser, and sessions are not. Justify the statement in maximum 75 words.

(b) Name Session ID Properties and with a short one line description for each.

7. Brad has a bank client who wants a web application to be developed which will be used by their VIP Account Holders for maintaining their bank accounts. Now Design a High Level Architectural Diagram and a Low Level Architectural Diagram, which should show at what point's security controls will be implemented.

Hint: Security Controls could be like Authentication, Input Validation, Logging etc.

8. Alice and Bob agree on using Diffie-Hellman Algorithm with p = 23, g = 5, x =6 and y = 16. Now demonstrate working of MITM Attack mathematically in Diffie-Hellman by introducing a MITM. (choose any value of your choice for MITM)

9. For RSA algorithm consider p = 17, q=11 and message m = 88. So calculate Public Key, Private key, cipher text and plain text again from cipher text.

SECTION C

10. Brad is a new security administrator within a retail company. He is discovering several issues that his security team needs to address to better secure their organization overall. When reviewing different web server logs he finds several HTTP server requests with the following characters "%20" and "../". The web server ensures that users input the correct information within the forms that are presented to them via their web browsers. Brad identifies that the organization has a two-tier network architecture in place, which allows the web servers to directly interact with the back end database.

(a) Which attack could be taking place against the organization? Name the attack first & justify your answer in maximum 50 words.

(b) Pertaining to the network architecture described, which type of the attack should brad be concerned with? Name the attack first & justify your answer in maximum 50 words.

(c) Which of the following functions is the web server software currently carrying out and what is an associated security concern Brad should address?

i. Client Side Validation
ii. Server Side includes validation
iii. Data source name logical naming access

11. Calculate the CVSS 2.0 Base Score for the following vulnerability:

Vulnerability
The iCloud subsystem in Apple iOS before 7.1 allows physically proximate attackers to bypass an intended password requirement, and turn off the Find My iPhone service or complete a Delete Account action and then associate this service with a different Apple ID account, by entering an arbitrary iCloud Account Password value and a blank iCloud Account Description value.
Attack
Find My iPhone helps you locate and protect your iPhone, iPad, iPod touch, or Mac if it is ever lost or stolen. With Find My iPhone set up on your device, you can do the following:

- Locate your device on a map
- Play a sound on your device to help you find it
- Use Lost Mode to lock and track your device
- Remotely erase all of your personal information from the device.

Find My iPhone includes a feature called Activation Lock that is designed to prevent anyone else from using your iPhone, iPad, or iPod touch if it's ever lost or stolen. Activation Lock is enabled automatically when you turn on Find My iPhone on a device using iOS 7 or later. Find My iPhone Activation Lock,your Apple ID and password will be required before anyone can:

- Turn off Find My iPhone on your device
- Erase your device
- Reactivate and use your device

This vulnerability allows the attacker to bypass the Activation Lock when attempting to turn off Find My iPhone. The attacker can turn off Find My iPhone feature, delete the current iCloud account and associate the device with new iCloud Account with out any Apple ID and password of current user.

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

Roll No: ----------

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2017

Program Name	**: B.Tech CSE + CSF**	**Semester**	**: V**
Course Name	**: IT Application Security**	**Max. Marks**	**: 100**
Course Code	**: CSIB 356**	**Duration**	**: 3 Hrs**
No. of page/s	**: 03**		

Note:

1. Answers to question 1 to 5 of Section A carries 4 marks each.
2. Answers to question 6 to 9 of Section B carries 10 marks each.
3. Answers to question 10 and 11 of Section C carries 20 marks each.

SECTION A

1. What are the major challenges in logging?

2. Why is log disposal important?

3. What are the 4Ws in logging? Write at least two example for each.

4. State true or false for following statements:

   a. Attacker can install network monitoring hardware or software through physical access to the network.

   b. The luring attack attack uses possible combinations of words based upon some likely values and tends to exclude remote possibilities.

   c. The web application server is smart to identify the cookie and grant all privileged data access, but not smart enough to check the malicious user from gaining access to your own personal information.

   d. Luring attack is a type of eavesdropping attack in which an attacker lures a highly privileged component to do something on his behalf.

5. Use Hill Cipher Decrypt “PFO” while encryption key was:

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix}$$

SECTION B

6. (a) Sessions are not reliant on the user allowing a cookie. Justify the statement in maximum 75 words.

(b) What is the major difference in first party and third party cookies? Give some examples for all first party cookies.

7. Brad has a bank client who wants a web application to be developed which will be used by their VIP Account Holders for maintaining their bank accounts. Now Design a High Level Architectural Diagram and a Low Level Architectural Diagram, which should show at what point security controls would be implements.

Hint: Security Controls could be like Authentication, Input Validation, and Logging etc.

8. Alice and Bob agree on using Diffie-Hellman Algorithm with p = 23, g = 5, x = 6 and y = 16. Find R_1, R_2 and the secret key for both Alice and Bob.

9. For RSA algorithm consider p = 5, q=11 and message m = 100. So calculate Public Key, Private Key, cipher text and plain text again from cipher text.

SECTION C

10. Brad is a new security administrator within a retail company. He is discovering several issues that his security team needs to address to better secure their organization overall. When reviewing different web server logs he finds several HTTP server requests with the following characters "%20" and "../". The web server ensures that users input the correct information within the forms that are presented to them via their web browsers. Brad identifies that the organization has a two-tier network architecture in place, which allows the web servers to directly interact with the back end database.

(a) Which attack could be taking place against the organization? Name the attack first & justify your answer in maximum 50 words.

(b) Pertaining to the network architecture described, which type of the attack should brad be concerned with? Name the attack first & justify your answer in maximum 50 words.

(c) Which of the following functions is the web server software currently carrying out and what is an associated security concern Brad should address?

i. Client Side Validation
ii. Server Side includes validation
iii. Data source name logical naming access

11. Calculate the CVSS 2.0 Base Score for the following vulnerability:

Vulnerability

SearchBlox is an enterprise search and data analytics service utilizing Apache Lucene and Elasticsearch.
A cross-site request forgery (CSRF) vulnerability in SearchBlox Server before version 8.2 allows remote
attackers to perform actions with the permissions of a victim user, provided the victim user has an active
session and is induced to trigger the malicious request.

Attack

A specially-crafted URL to the SearchBlox Server containing the appropriate parameter values of an
action the attacker wants to perform may be sent to a victim user. This URL may be sent to the victim as
part of an HTML document, an email, or via some other method. If the user interacts with the URL while
the user has an active session on the SearchBlox Server, the URL will send a request to the server to
perform some action with the victim user's credentials. Since SearchBlox Server prior to version 8.2 has
no request validation mechanism, the request will be completed if the victim user's permissions allow
such an action. Possible actions include creating or deleting a user account, or uploading new SearchBlox
configuration settings.

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

UPES
UNIVERSITY WITH A PURPOSE