



**NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY
Faculty of Computing and Informatics**

Department of Computer Science

QUALIFICATION : Bachelor of Computer Science in Cyber Security	
QUALIFICATION CODE: 07BCCS	LEVEL: 6
COURSE: Web Application Security	COURSE CODE: WAS621S
DATE: November 2022	PAPER: THEORY
DURATION: 2 hours	MARKS: 80

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	MR EDWARD NEPOLO
MODERATOR:	DR MERCY CHITAURO

THIS QUESTION PAPER CONSISTS OF 7 PAGES
(Including this front page)

INSTRUCTIONS

1. Answer ALL the questions.
2. Write clearly and neatly.
3. Number the answers clearly.
4. When answering questions, you should be guided by the allocation of marks. Do not give too few or too many facts in your answers.

PERMISSIBLE MATERIALS

1. Non-programmable calculator

Section A

[12 Marks]

1. Select a programming interface used to represent a page in a tree structure, so that programs can read, access and modify document structure.

- i. XML
- ii. DOM
- iii. HTML
- iv. JWT

2. _____ allows applications to send and retrieve data from a server without interfering with the current page.

- i. DOM
- ii. JWT
- iii. XML
- iv. AJAX

3. _____ is a networking and cryptography library for encryption, decryption, signatures etc.

- i. NaCL
- ii. Sockets
- iii. HTML
- iv. JWT

4. A session is an instance of a sequence of HTTP requests and responses of a particular user. Authentication is essential in session management. Which technology is used for authentication during stateful authentication?

- i. Tokens
- ii. Cookies
- iii. OAuth
- iv. JWT

5. Single Sign-On relies on three important elements. What are they? Select 3

- i. Users
- ii. Service Providers
- iii. Organization
- iv. Encryption
- v. Hashing
- vi. Identity Providers

6. During Single Sign-On, the user agent first authenticates through the IDP. What does the IDP do after verifying the identity of the user agent?

- i. The user agent provides the SAML Assertion
- ii. The Service Provider sends a verification code to the IDP
- iii. IDP issues an SAML Assertion
- iv. The IDP sends a verification code to the Service Provider

7. How does the Service Provider ensure the integrity of the SAML assertion?

- i. Service Provider signs the SAML Assertion
- ii. IDP digitally signs the SAML Assertion
- iii. Verification is not required
- iv. Service Provider creates a hash of the SAML Assertion

8. Which technology is used to prevent SSL Stripping?

- i. HTTP SSL
- ii. HTTP Strict-Transport-Security
- iii. HTTP TLS
- iv. HTTP

9. What is the best way to mitigate against SQL Injection attacks on a web application?

- i. By authenticating users
- ii. By using prepared statements
- iii. By reducing the amount of data
- iv. By using strict password policies

10. During SQL Injection, which in-band injection technique allows a user to use error responses to manipulate data?

- i. Union Based
- ii. Error Based
- iii. Out of Band
- iv. Inferential

Section B

Question 1

[42 Marks]

1.1 How does Cross-Site Scripting attack work?

[4 Marks]

1.2 Explain the different types of Cross-Site Scripting attacks.

[4 Marks]

1.3 Why is HTTP Strict-Transport Security needed when there is already HTTP Secure?

[4 Marks]

1.4 There are two authentication methods during authentication in web application session management. Explain the two methods.

[4 Marks]

1.5 Name two differences in the two authentication methods mentioned in Question 1.4. [4 Marks]

1.6 Explain what is meant by a buffer overflow attack?

[4 Marks]

1.7 Mention two attributes that are configured on session cookies and what the attributes imply. [4 Marks]

1.8 Name and explain 3 security measures that can be put in place to ensure that cookies are secured during communication. [6 Marks]

1.9 Name and explain three SQL Injection attack modes.

[6 Marks]

1.10 How is SQL Injection different from Cross-Site Scripting?

[2 Marks]

Question 2

[16 Marks]

2.1 Explain the concept of single sign on, and what issues are addressed by single-sign on.

[4 Marks]

2.2 There are three elements that single sign-on depends on, explain the flow of single sign-on.

[6 Marks]

2.3 What is SAML Assertion?

[2 Marks]

2.4 How does the service provider ensure that the SAML Assertion provided is authentic? [4 Marks]

Question 3

[10 Marks]

3.1 Mention five ways in which you would mitigate against SQL Injections.

[5 Marks]

3.2 Name and explain the type of Man-In-The-Middle attack that can take place if HTTP Strict-Transport Security is not enabled? [5 Marks]

- END OF EXAMINATION PAPER -



NAMIBIA
UNIVERSITY
OF SCIENCE AND
TECHNOLOGY

P/Bag 13388
Windhoek
NAMIBIA

2022 -10- 18

FACULTY OF COMPUTING & INFORMATICS
DEPARTMENT: COMPUTER SCIENCE