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: January 2023	**PAPER:** THEORY
DURATION: 2 hours	**MARKS:** 80

SUPPLEMENTARY/SECOND 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. What's the difference between persistent and non-persistent XSS attacks?
   i. Persistent attack only affects one user.
   ii. Non-persistent attacks, the script is stored on the application's database.
   iii. Persistent attacks, the script is stored on the application's database.
   iv. The difference between persistent and non-persistent XSS attack is that in persistent attack both the user and the server are targets, while in persistent attacks only the user is a target.

2. What information is the attacker hoping to steal in a XSS attack?
   i. HTTP Socket layer information
   ii. CSRF Token information
   iii. Session ID through cookies
   iv. Session ID through tokens

3. Which attack is a user vulnerable to when HTTP Strict-Transport Security is not enabled?
   i. Session Hijacking
   ii. Page-In-The-Middle Attack
   iii. SSL Stripping
   iv. Session Fixation

4. During an XSS attack, which platform is relied upon to execute a script on the client side?
   i. DOM Environment
   ii. XML
   iii. AJAX
   iv. JavaScript

5. Which platform is suitable for making partial server requests?
   i. XMLHttpRequest
   ii. AJAX
   iii. XML
   iv. JavaScript

6. If XSS attacks rely on client-side code execution, why don't we simply switch to server-side code execution?

   i. Client-side code execution offers better round-trip time performance
   ii. No, XSS does not rely on client-side code execution.
   iii. Server-side code execution cannot execute client-side requests.

iv. Server-side execution does not access the cookies that are targeted by XSS attack.

7. If persistent XSS attacks rely on user input points stored on the client side, why don't we use data input on server side?

i. The server does not allow data input from server side.
ii. The server does not allow user input on client side.
iii. No, persistent XSS attacks do not rely on user input points stored on the client side.
iv. Data input on server side will increase communication delay.

8. What are some common types of attacks that can be launched against a web application? Choose two.

i. IoT Botnets
ii. SQL Injection Attacks
iii. DNS Attacks
iv. Cross-Site Scripting Attacks
v. Encryption Attacks

9. Jason Web Tokens are standards for sharing security information. What information is provided in the payload? Choose two.

i. Subject
ii. Algorithm
iii. Application
iv. Claim

10. Select an authentication process that allows users to access multiple applications using one set of login credentials.

i. Multifactor Authentication
ii. Two Factor Authentication
iii. Single Sign-On
iv. Two Factor Verification

Section B

Question 1 [42 Marks]

1.1 How does Cross-Site Scripting attack work? [4 Marks]

1.2 Explain the difference between Cross-Site Scripting and Cross-Site Request Forgery. [4 Marks]

1.3 SSL Stripping is one of the attacks targeted at web applications. Explain how an SSL Stripping attack works. [4 Marks]

1.4 Mention and explain one technology used to mitigate SSL Stripping attacks. [4 Marks]

1.5 What's the biggest risk when using cookies to store session information? [4 Marks]

1.6 Mention and explain two measures that can be used to counter buffer overflow attacks?
[4 Marks]

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

1.8 Name and explain 3 security measures 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]

2.0 How does one defend against Cross-Site Request Forgery? [2 Marks]

Question 2 [16 Marks]

2.1 What is password proliferation, and what technologies are available to address password proliferation? [4 Marks]

2.2 The 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 Mention and explain two types of cookies used in session management? [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 -