NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS
DEPARTMENT OF CYBER SECURITY

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE IN CYBER SECURITY	
QUALIFICATION CODE: 07BCCS	**LEVEL:** 6
COURSE: WEB APPLICATION SECURITY	**COURSE CODE**: WAS621S
DATE: NOVEMBER 2023	**PAPER:** THEORY
DURATION: 2H00	**MARKS:** 100

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	MRS. VIKTORIA SHAKELA MR. ERICKY IIPUMBU
MODERATOR:	MR. EDWARD NEPOLO

THIS QUESTION PAPER CONSISTS OF 6 PAGES
(Excluding this front page)

INSTRUCTIONS

1. Answer ALL the questions on the answer scripts.
2. Write clearly and neatly.
3. Number the answers clearly.

PERMISSIBLE MATERIALS

1. Calculator.

Section A [20 Marks]

Multiple Choice (15 marks)

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

   A. XML
   B. DOM
   C. HTML
   D. JWT

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

   A. DOM
   B. JWT
   C. XML
   D. AJAX

3. Networking and cryptography library for encryption, decryption, signatures etc.

   A. NaCL
   B. Sockets
   C. HTML
   D. 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 stateless authentication?

   A. Tokens
   B. Cookies
   C. OAuth
   D. JWT

5. In which of the following exploits does an attacker insert malicious code into a link that appears to be from a trustworthy source?

   A. XSS
   B. Command Injection
   C. Path Traversal Attack
   D. Buffer Overflow

6. Web application firewalls (WAFs) help prevent which application layer attack?

   A. XSS
   B. SQL Injection
   C. DDoS
   D. All of the above

7. Which application security testing method is considered most costly?

A. Static application security testing (SAST)
B. Dynamic application security testing (DAST)
C. Mobile application security testing (MAST)
D. Software Composition Analysis (SCA)

8. Which technology is used to prevent SSL Stripping?

A. HTTP SSL
B. HTTP Strict-Transport-Security
C. HTTP TLS
D. HTTP

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

A. By authenticating users
B. By using prepared statements
C. By reducing the amount of data
D. By using strict password policies

10. During SQL Injection, which in-band injection technique cause the application to send data to a remote endpoint?

A. Union Based
B. Error Based
C. Out of Band
D. Inferential

11. Which of the following statements is an example of a horizontal privilege escalation?

A. A cloud customer is able to access data of other customers hosted in the same cloud environment.
B. An attacker has access to the administrators' interface URL.
C. A user is able to perform restricted actions on a web application.
D. A user has access to files and directories they are not authorized to have access to.

12. If a web Application does not validate authorisation of the user for direct references to restricted resources, it is vulnerable to

A. SQL injection
B. Insecure Direct Object References
C. Platform misconfiguration
D. URL- matching discrepancies

13. Which vulnerabilities may be missed by manual code reviews but picked up by automated pen testing tools?

A. Logic Flaws
B. Authorization issues
C. Encryption misconfigurations
D. All of the above

14. Which of the following cannot be accepted as a guideline to writing secure codes?
A. Storing Passwords as ciphertext.
B. B. Using hardcoded credentials in your code.
C. C. Writing a code that handles errors to prevent a program from crashing.
D. Cleaning and filtering input data

15. Which of the following is not among the top 10 OWASP vulnerabilities
A. Insecure Design
B. Security policy non-compliance
C. Broken Access Control
D. Server-side Request Forgery

True/False (5 marks)

1. Client-Side Request Forgery (CSRF) allows an attacker to execute arbitrary JavaScript within the browser of a victim user.
2. REST APIs are implemented to handle requests between applications.
3. A cookie with the SameSite flag can be sent across domains.
4. Web application mapping refers to collecting data points regarding the application code, network structure and feature set of an application.
5. If an attacker modifies the id parameter value to that of another user and gain access, it is referred to as horizontal privilege escalation.

Section B **[80 Marks]**

Question 1 [20 Marks]

a. Mention and explain any four (4) HTTP request methods used with web applications **(8)**

b. Name the three parts of a URL that are used to determine the URL's origin. **(3)**

c. List three advantages REST APIs have over Simple Object Access Protocol (SOAP) **(3)**

d. Would the following code running on https://attacker.com be allowed to listen to the 'submit' event on the bank's login form and grab the username and password? Why or why not? **(6)**

```
<iframe src='https://bank.com'></iframe> <script>   const loginForm =
window.frames[0].forms[0]   loginForm.addEventListener('submit', () => {
console.log(loginForm.username) // Haha, got your username...
console.log(loginForm.password) // ...and password!   }) </script>
```

Question 2 [25 Marks]

2.1. An attacker includes the following HTML in their site hosted at https://attacker.com which makes a GET request to a vulnerable bank server and transfers money into the attacker's account.

<img src='https://bank.com/withdraw?amount=1000&to=attacker' />

The attacker is hoping the user is already authenticated with the bank site before they visit https://attacker.com and send the above GET request to the bank. The attacker entices users to visit their site by including hundreds of cute kittens:

Explain how the bank can modify their server code to protect users from this attack. (5)

2.2. There are two authentication methods in web application session management. Mention and explain the two methods. **(4)**

2.3. Differentiate between the two methods mentioned in question 2.2. **(4)**

2.4. Name and explain 3 security measures can be put in place to ensure that cookies are secured during communication. **(6)**

2.5. Mention two attributes that are configured on session cookies and their implications **(4)**

2.6. Differentiate between authentication and authorisation **(2)**

Question 3 [10]

3.1. Describe a server-side defenses that mitigates the effects of brute force (testing multiple passwords from a dictionary against a single account), credential stuffing (testing username/password pairs obtained from a breach), as well as password spraying (testing a single weak password against a large number of different accounts). **(5)**

3.2. Suppose an attacker steals the private key of a website that uses TLS and remains undetected. What can the attacker do using the private key? **(4)**

3.3. What is security fuzzing? **(1)**

Question 4 [20 Marks]

1.1 Name and explain three SQL Injection attack modes. **(6)**

1.2 Explain buffer overflow attack **(3)**

1.3 Mention five methods that can be used to mitigate SQL injections. **(5)**

1.4 List and explain three types of web applications security scanning **(6)**

Question 5 [5 Marks]

Mention five (5) types of access control implemented for web applications **(5)**

END