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: January 2025	**PAPER:** Theory
DURATION: 120 minutes	**MARKS:** 100

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**Mrs. V. Shakela**
MODERATOR:	**Mr. E. Nepolo**

THIS QUESTION PAPER CONSISTS OF 5 PAGES

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 **[20 Marks]**

Multiple Choice (15 marks)

1. Which of the following is a best practice for designing a secure RESTful web service?

   A. Input Validation
   B. Session based authentication.
   C. Use HTTPS
   D. All the above

2. Which of the following domains can be regarded as the same origin according to browser security model.

   A. x.y.z.com; .com; .y.z.com
   B. x.y.z.com; z.com
   C. x.y.z.com; y.z.com; .com
   D. x.y.z.com; .y.z.com; z.com

3. What is the process used in applications to clean or filter input data to remove any characters, symbols, or elements that could potentially be exploited by attackers to inject malicious code or disrupt the applications behavior.

   A. Error-handling
   B. Input validation
   C. Input sanitation
   D. Logging

4. Which of the following access control types restrict access to functionality and resources based upon the state of the application or the user's interaction with it?

   A. Context-based access control
   B. Location Based access control.
   C. Horizontal access control
   D. Referrer Header access control

5. Viewing a website involves browsers and servers communicating together, often over wide distances. What best describes the role of the server?

   A. The server is responsible for serving users with warnings for visiting insecure websites.
   B. The server is responsible for figuring out the optimal path of routers for a webpage to reach the user.
   C. The server is responsible for sending HTTP responses that contain the code of websites.
   D. The server is responsible for sending HTTP requests to the browser that hosts the website.

6. Which of these protocols is used by the browser in fetching and loading the webpage?

A. IMAP
B. HTML
C. HTTP
D. SMTP

7. Which of the following XSS attack types involves the malicious script coming from the website's database?

A. Reflected XSS
B. DOM-based XSS
C. Stored XSS
D. Database XSS

8. The process of discovering and identifying the interactions and interdependencies between application components and their underlying hardware infrastructure.

A. Web Application reconnaissance
B. Web Application Mapping
C. Security Fuzzing
D. Encryption

9. What threat arises from not flagging HTTP cookies with tokens as secure?

A. Access Control violation
B. Session Hijacking
C. Session replay
D. By using strict password policies

10. What flaw can lead to the exposure of resources or functionality to unintended actors?

A. Session Fixation
B. Insecure Cryptographic storage
C. Improper Authentication
D. Unvalidated Redirects and Forwards

11. What threat is the web application vulnerable to if it does not validate the authorisation of the user for direct references to restricted resources?

A. Insecure Direct Object References.
B. SQL injection.
C. Server-Side Request Forgery.
D. Cross Site Scripting.

12. In which way does machine learning make modern web application firewalls more effective?

   A. It allows them to return search results quicker than using traditional filtering methods.
   B. It allows them to adapt to ever changing threat landscape
   C. It allows applications to access online content faster
   D. It allows them to choose the most suitable web application for a specified task

13. Which type of attack exploits the trust that a site has in a user's browser?

   A. Session hijacking
   B. Cross Site Request Forgery
   C. SQL Injection
   D. Cross Site Scripting

14. What information is the attacker hoping to steal in an XSS attack?

   A. Session ID through cookies
   B. HTTP Socket layer information
   C. CSRF Token information
   D. Session ID through tokens

15. 1. Which of the following HSTS headers will disable the HSTS rule on the browser?

   A. Strict-Transport-Security: max-age=none.
   B. Strict-Transport-Security: max-age=disable
   C. Strict-Transport-Security: max-age=0.
   D. Strict-Transport-Security: max-age= “”; includeSubDomains; preload.

True/False (5 marks)

1. The logout process in a web app should mark the session as expired on the server.
2. The Same Origin Policy used for the DOM is the same as the Same Origin Policy applied to cookies.
3. Cross-Origin Resource Sharing (CORS) is an HTTP-header-based mechanism that instructs a server to deny loading resources from any origins other than its own.
4. Two-factor authentication (a password together with a Time-based One-time Password (TOTP) code) is an example of defense-in-depth.
5. If site-a.com loads a website from another domain, site-b.com, inside of an iframe, the same origin policy prevents JavaScript from site-a.com from accessing any of site-b.com's website content in the iframe.

Section B [80 Marks]

Question 1 [25 Marks]

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

1.2. Given the URL: https: www.gbif.com, Name the three parts of a URL that are used to determine the URL's origin and their associated values. **(6)**

1.3. List and explain two (2) key web application components at the client side. **(4)**

1.4. Would the following code running on https://attacker.com be allowed to print out the contents of the students' homepage, which include the currently logged-in user's grades? Why or why not? **(6)**

```
<script>
const res = await fetch('https://students.nust.na')
const data = await res.body.text()
console.log(data) // Haha, got your grades!
</script>
```

NOTE: https://students.nust.na does not send any special HTTP headers such as Access-Control-Allow-Origin, which are also known as "CORS" headers.

1.5. What is the meaning of the following HTTP response status code? **(1)**

200 -

Question 2 [27 Marks]

2.1. What is the purpose of the HTTP Strict-Transport-Security header (HSTS)? What attack does it protect against? **(5)**

2.2 Why is session management important in HTTP communications? **(4)**

2.3. You are a penetration tester evaluating a client's website for security vulnerabilities. You notice that their authentication system chooses sequential session IDs for users.

Specifically, the first user to log in to the site gets a session ID of 1, the second user gets 2, the third user gets 3, and so on. Describe an attack against this authentication system. **(4)**

2.3. What cookie attribute (e.g., Secure, HttpOnly, Domain, SameSite) could be specified when setting the cookie that would prevent attackers from stealing the sessionId cookie? Justify your answer. **(4)**

2.4. Differentiate between stateful and stateless authentication methods of session management in web applications. **(4)**

2.5. List and explain any three functions of a web proxy server. **(6)**

Question 3 **[18 Marks]**

3.1. Explain the goals of Security testing in web applications. **(6)**

3.2. Explain the role of a Web Application Firewall (WAF). **(4)**

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

3.4. Mention and explain the threat a web application is exposed to if it does not verify authorization of user for direct references to restricted resources? **(4)**

3.5. Mention three key conditions that enable Cross-site request Forgery attack **(3)**

Question 4 [10 Marks]

5.1. Define Access Control? **(2)**

5.2. Differentiate between vertical and horizontal access control? **(4)**

5.3. What measures can be implemented to address Broken Access Control vulnerability? **(4)**