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 2024	**PAPER:** THEORY
DURATION: 2H00	**MARKS:** 100

SECOND OPPORTUNITY/SUPPLEMENTARY 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. 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 of the above

2. Which of the following domains can be regarded as the same origin in a same origin policy 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. Which attack is a user vulnerable to when HTTP Strict-Transport Security is not enabled?
   A. Session Hijacking
   B. Page-In-The-Middle Attack
   C. SSL Stripping
   D. Session Fixation

6. An authentication process that allows users to access multiple applications using one set of login credentials.?
   A. Multifactor Authentication
   B. Two Factor Authentication
   C. Single Sign-On
   D. Two Factor Verification

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 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. 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 platform is suitable for making partial server requests??

A. JavaScript

B. XML
C. XMLHttpRequest
D. AJAX

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. Which statement is NOT true for buffer overflows?
    A. The buffer overflow problem is partly caused by the way C language handles memory management.
    B. The buffer overflow is partly caused by C programmers not handling their own memory management properly by checking the boundaries of the buffer.
    C. All buffer overflows are simple programmer errors that can easily be spotted.
    D. Due to complexity of buffer overflows, they can easily be overlooked even by seasoned programmers.

True/False (5 marks)

1. The server can trust cookie values in HTTP requests to be untampered since the cookies are set by the server.
2. The cookie attribute HttpOnly helps to mitigate the effects of XSS attacks by preventing client-side JavaScript from reading the cookie.
3. Cross-site request forgery is a type of injection attack.
4. Two-factor authentication (a password together with a Time-based One-time Password (TOTP) code) is an example of defense-in-depth.
5. You should set the Secure flag in a cookie to ensure that the cookie is only sent over encrypted HTTPS connections.

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. Describe the client-server architecture in the context of web applications **(3)**

d. 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.

Question 2 [27 Marks]

2.1. Why is it a bad idea to include detailed error information (e.g. including a stack trace) in the HTTP response when the server throws an exception? **(5)**

2.2. 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. Your friend has built a personal site hosted at https://nust.edu/clueless. They have built an authentication system so certain pages of the site can only be accessed by authorized individuals. Once a user logs in successfully, the server sends a response with a Set-Cookie HTTP header to set a sessionId cookie in the user's browser.

Set-Cookie: sessionId=1234; Path=/clueless

Your friend is specifying the Path attribute on the cookie so that the cookie is scoped to the path prefix /clueless. This means that the cookie will be sent when the user visits https://nust.edu/clueless or https://nust.edu/clueless/secret but not when they visit https://nust.edu/attacker.

Nonetheless, it turns out that https://nust.edu/attacker can read the sessionId cookie that was scoped to your friend's site with the Path attribute.

Explain what the page at https://nust.edu/attacker could do to read the cookie. **(6)**

2.4. What cookie attribute (e.g., Secure, HttpOnly, Domain, SameSite) could your friend in 2.3 have specified when setting the cookie that would have prevented the attacker from stealing the sessionId cookie? Justify your answer. **(4)**

2.5. What's the biggest risk when using cookies to store session information? **(4)**

2.6. Differentiate between authentication and authorisation. **(4)**

Question 3 [10 Marks]

3.1. Mention and explain any two (2) server-side security best practices. **(4)**

3.2. Web browsers like Firefox and operating systems like macOS and Windows ship with a large built-in list of public keys of Certificate Authorities. What are these used for? **(4)**

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

Question 4 [15 Marks]

1.1 Mention and explain two measures that can be used to counter buffer overflow attacks. **(4)**

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

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

1.4 What is the use of Cross-origin Resource Sharing (CORS)? **(3)**

Question 5 [8 Marks]

5.1. Describe a scenario of Horizontal privilege escalation? **(2)**

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

5.3. Mention any two purposes of secure coding practices in web applications. **(2)**

END