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 2025	**PAPER:** Theory
DURATION: 180 minutes	**MARKS:** 100

2nd OPPORTUNITY/SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**Ms. Viktoria Shakela** **Mr. Petrus Katambo** **Mr. Adriaan Grobler** **Mr. Andreas Amukwa**
MODERATOR:	**Mr. E. Nepolo**

THIS QUESTION PAPER CONSISTS OF 7 PAGES
(Excluding 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 **[20 Marks]**

Multiple Choice (15 marks)

1. You are tasked with finding the public IP range and hosting provider of a company's web application before active probing. Which combination of tools or resources would be most effective for this task?
   A. WHOIS lookup and DNS enumeration tools
   B. SQLmap and Nessus vulnerability scans
   C. Hydra brute-force password attacks
   A. Wireshark packet sniffing

2. Your Nmap scan results discovered the following open ports: 21 (FTP), 80 (HTTP), 3306 (MySQL). Based on this results, which of the following security threats should be prioritised for mitigation?
   A. Potential SQL injection in the application login page
   B. Anonymous access to the FTP server
   C. Potential Cross-site scripting on port 3306
   D. SSL certificate misconfiguration on HTTP

3. A script loaded from https://attacker.com tries to read data from an iframe loaded from https://otherdomain.com. According to the Same-Origin Policy (SOP), what will happen?
   A. Access will be denied unless the iframe explicitly allows it via CORS or postMessage
   B. Since both sites are using the same protocol scheme, the script will access the iframe content.
   C. Access will be granted because both sites are using the same web server version
   D. The browser will block the entire web page from loading

4. Which of the following mechanisms enforces trusted sources for content loading?
   A. Same-Origin Policy (SOP)
   B. Secure Socket Layer (SSL)
   C. Cross-Origin Resource Sharing (CORS)
   D. Content Security Policy (CSP)

5. Which of the following techniques is an effective way to mitigate against SQL Injection attacks on a web application?
   A. Using Username and password authentication method
   B. Reducing the amount of data in HTTP responses
   C. Implementing strict password policies
   D. Using Parameterised queries

6. During an ethical hacking project, your reconnaissance tools collected the following information about the web application.
   - WHOIS reveals domain registration with a public email
   - Shodan search shows outdated Apache server version
   - Nmap indicates port 443 is open with weak SSL ciphers

   As an information security specialist, which of the following actions are you going to perform next?
   A. Build payloads and exploit the outdated Apache server
   B. Notify the organisation of the collected information and close the project.
   C. Perform a comprehensive vulnerability scan focusing on Apache and SSL configurations
   D. Send a phishing attack to the public email and perform a brute-force on the admin login page

7. Which method allows immediate server-side user logout by invalidating session data?
   A. Session-based authentication
   B. Token-based authentication
   C. Both token and session-based authentication
   D. Multi-factor authentication (MFA)

8. What is the primary purpose of the Strict-Transport-Security (HSTS) header in HTTP communication?
   A. To allow cross-origin resource sharing (CORS)
   B. To specify allowed content sources for scripts and images
   C. To enable Cross Site Scripting (XSS) filtering in browsers
   D. To enforce that browsers only connect to the server over HTTPS

9. During a security test on a web application, you observe multiple accounts being accessed simultaneously using the same session token. What is the most likely cause for this scenario?
   A. Proper configuration of secure flag on session cookies.
   B. Ineffective session authentication allowing session fixation
   C. The server is using HTTPS with HSTS header enabled.
   D. The users are accessing the system from the same IP address.

10. 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.

11. Which of the following best describes the process of how the session is created and maintained in web applications?
    A. The session is created on client-side by the browser generating a unique token, which it stores in local storage and sends to the server with each request.
    B. Sessions are maintained by the server storing the user's password and re-authenticating the user on every request.
    C. The session is created by the server after a successful login; the identifier is stored as a cookie and sent to the client. The cookie is used to maintain the session state and is sent with every subsequent request.
    D. The session ID is generated by the browsers after the user's successful login. The session is maintained by the server for authentication and is deleted only when the user closes the browser window.

12. How does the Content-Security-Policy (CSP) header enhance web application security?
    A. By blocking all scripts and images loading from different origins
    B. By restricting which domains are allowed to load content such as scripts
    C. By forcing all content to be loaded over HTTP connections
    D. By disabling browser caching to ensure client-side security

13. Which of the following input sources can be directly controlled by a malicious user?
    A. POST/GET Parameters
    B. CSRF headers
    C. HTTP request method
    D. Authorisation header

14. The banking web application websites requires its users to log-in again after 30 minutes. Which of the following cyber security principle describes this scenario?
    A. Compromise recording
    B. Psychological acceptability
    C. Complete mediation
    D. None of the above

15. Which of the following usually considered as the default port number of Apache and several other web servers?
    A. 80
    B. 23

C. 443

A. 21

True/False **(5 marks)**

1. If an iframe is embedded from a different domain, the parent page's scripts can directly read the iframe's DOM without any cross-origin permissions configured.
2. The session token stored in the cookie is essential for the server to identify and maintain the user's session state across multiple requests.
3. SQL Injection vulnerabilities allow attackers to execute arbitrary SQL commands by inserting malicious input into an application's database queries.
4. Vertical access control restricts access between users at the same privilege level.
5. Cross Site Scripting happens when an application takes in user-input data and sends it to a web browser without proper validation.

Section B **[80 Marks]**

Question 1 **[22 Marks]**

1.1. Explain how web browsers implement the same origin policy to achieve web application security. Provide a relevant example to illustrate your explanation. **(6)**

1.2. Discuss the differences between passive and active reconnaissance techniques in web application security assessment and provide one suitable reconnaissance tool that can be used for each technique **(6)**

1.3. You created a web application hosted on https://app.example.com which makes AJAX requests to a backend API at https://api.example.com to fetch user data. During testing phase, you realised that the browser blocks these cross-origin requests due to the Same-Origin Policy. You need to allow the application to access the API securely.

Which configuration(s) will you implement at the backend API server to allow secure cross-origin requests while still preventing unauthorised access from other origins? **(6)**

1.4. Mention four (4) effective Cross Site Scripting (XSS) mitigation techniques used in web applications. **(4)**

Question 2 **[21 Marks]**

The Information security officer is performing a web application security test. The screenshot below shows an intercepted HTTP response headers from the web application. Analyse the screenshot and answer the questions below.

```
HTTP/1.1 200 OK
Date: Mon, 22 Sep 2025 08:55:00 GMT
Server: Apache/2.4.18 (Ubuntu)
X-Powered-By: PHP/7.0.33
Content-Type: text/html; charset=UTF-8
Set-Cookie: PHPSESSID=abc123; path=/; HttpOnly
Cache-Control: no-cache
```

Figure 1

2.1. Identify and discuss three (3) potential security risks from the HTTP headers shown in the response screenshot above? **(9)**

2.2. List and justify three suitable security measures to be implemented as part of the HTTP headers to enhance the security posture of this web application. **(6)**

2.3. What does the HTTP status code "200 OK" indicate about the server's handling of a client's request? **(2)**

2.4. In figure 1, the cookie is set with an attribute "path=/". What does the cookie attribute "path=/" mean for this session cookie? **(4)**

Question 3 **[21 Marks]**

Study the mini case below carefully and answer the following questions.

NUST's students' web portal is used by students to access sensitive academic and financial information. Recently, there have been reports of unauthorised access to students' accounts without password disclosure. Investigations revealed the following weaknesses:

- The session ID assigned at login remains the same throughout the session lifetime and is not regenerated after authentication.
- Session cookies are accessible via client-side JavaScript and were transferred over HTTP communications
- Users are not logged out after long inactivity periods.
- The application is accepting session IDs provided before login.

3.1. According to the case study, identify and discuss at least three (3) web attacks the students' web portal is vulnerable to. Give examples in your explanations. **(9)**

3.2. Recommend effective mitigation techniques NUST should implement to improve session security and prevent attacks identified in 3.1. **(6)**

3.3. Explain why it is important to invalidate a user session on logout in web applications. **(3)**

3.4. Explain major security risks associated with transferring sensitive information such as session cookies over HTTP? **(3)**

Question 4 **[16 Marks]**

4.1. Outline and discuss three essential security practices web developers should follow during coding to mitigate common vulnerabilities like injection and broken authentication in web applications. **(6)**

4.2. Differentiate between a reflected and stored Cross Site Scripting (XSS). **(4)**

4.3. Discuss how the Secure Software Development Life Cycle (SSDLC) enhances web application security? **(6)**

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 2025	**PAPER:** Theory
DURATION: 180 minutes	**MARKS:** 100

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**Ms. Viktoria Shakela** **Mr. Petrus Katambo** **Mr. Adriaan Grobler** **Mr. Andreas Amukwa**
MODERATOR:	**Mr. E. Nepolo**

THIS QUESTION PAPER CONSISTS OF 7 PAGES
(Excluding 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

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 2025	**PAPER:** THEORY
DURATION: 180 minutes	**MARKS: 100**

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION MEMORANDUM	
EXAMINER(S)	**Ms. Viktoria Shakela** **Mr. Petrus Katambo** **Mr. Adriaan Grobler** **Mr. Andreas Amukwa**
MODERATOR:	**Mr. E. Nepolo**

THIS MEMORANDUM CONSISTS OF 10 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