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 2024	**PAPER:** THEORY
DURATION: 120 minutes	**MARKS: 100**

1st OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**Mrs. V. Shakela** **Mr. Pius Shambabi** **Mr. Adriaan Grobler**
MODERATOR:	**Mr. E. Nepolo**

THIS QUESTION PAPER CONSISTS OF 7 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 these statements best describes how the website is loaded?

A. Charmell's browser sent an HTTP request to the root web server that stores all the websites in the world. The web server sent back an HTTP response with the HTML for the webpage.
B. Charmell's browser sent an HTTP request to the web server that hosts "charitywater.org". The web server sent back an HTTP response with the HTML for the webpage.
C. Charmell's browser sent an HTTP request to the root web server that stores all the websites in the world. The web server sent back an HTTP response with the HTML for the webpage.
D. Charmell's server sent an HTTP request to the browser that hosts "charitywater.org". The browser sent back an HTTP response with the HTML for the webpage.

2. The programming technique that 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. Viewing a website involves browsers and servers communicating together, often over wide distances. Which of the following statements best describes the role of the web browser?

A. The browser is responsible for sending HTTP requests to the server that hosts the website.
B. The browser is responsible for browsing through its files to find the code for each website.
C. The browser is responsible for figuring out the optimal path of routers for a webpage request to reach the server.
D. The browser is responsible for sending HTTP responses that contain the code of websites.

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 stateful 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. Which of the following statements is correct about Cross-site Request Forgery (CSRF) vulnerabilities?

A. CSRF vulnerabilities only affect pages with forms that do not include usernames in the data sent back to the server.
B. Websites that rely heavily on JavaScript are more prone to CSRF vulnerabilities.
C. CSRF vulnerabilities can be prevented by using modern web frameworks.
D. CSRF vulnerabilities are partially corrected by adding and validating on submission a hidden field with a secure random number as its value.

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. Your web server supports secure (HTTPS) connections. By design, which of the following is the best way to make sure a client will not accidentally request a page over non-secure HTTP connection?

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

9. What attack technique is used to exploit websites by altering backend database queries through manipulated input?

A. Cross Site Scripting
B. SQL injection
C. Server-Side Request Forgery
D. OS commanding

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 can access data of other customers hosted in the same cloud environment.
B. An attacker has access to the administrators' interface URL.
C. A user can 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 the above

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

15. Hackers often gather a multitude of seemingly small, harmless pieces of configuration about a site that, when combined, can help them attack a site. Which of the following error messages is typically considered **NOT** safe to display to the user?

A. A message that states that the system is down for maintenance and tells what time it is expected to be back up. E.g.: Our site is down. We're sorry for the inconvenience. We are doing maintenance on our servers. The site should be up by 12h00.

B. An error message that says there was an internal error message and displays the call stack to assist in debugging and reporting of the error. E.g.: There was an internal error, please copy and paste this page to the sysadmin.

C. A message that says that there was an error logging in mentioning the username. E.g.: User "JoeUser" could not be logged in with the information you provided.

D. An error message that says there was an internal error but does not provide any details to assist in debugging or reporting of the error. E.g.: There was an internal error. Please report this to the sysadmin.

True/False (5 marks)

1. Web application security is not required for finance applications.
2. Client-side scripts may be allowed to execute in the browsers for needed operations.
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 [30 Marks]

1.1. Mention and explain any five (5) HTTP response codes used with web applications **(10)**

1.2. Given the URL: https: www.gbif.com:444, 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 discuss three (3) key components of web applications at the server side **(6)**

1.4. 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? **(5)**

```
<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>
```

1.5. Explain why is it a bad practice to include detailed error information (e.g. including a stack trace) in the HTTP response when the server throws an exception? **(3)**

Question 2 [20 Marks]

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

2.2. Differentiate between the two methods mentioned in question 2.1. **(4)**

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

2.4. Explain the domain attributes that can be configured on session cookies and its implications using an example. **(4)**

2.5. 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 many 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 Fuzz Testing? **(1)**

Question 4 [20 Marks]

4.1. Name and explain three Cross Site Scripting (XSS) Injection attack types. **(6)**

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

4.3. Describe typical security activities performed at each of the Secure Software Development Lifecycle phases below. **(6)**

- **Planning -**

- **Development -**

- **Maintenance -**

4.4. Mention any three (3) defenses to access control vulnerabilities. **(3)**