UNIVERSITY OF GHANA COLLEGE OF BASIC & APPLIED SCIENCE

SCHOOL OF PHYSICAL & APPLIED SCIENCES DEPARTMENT OF COMPUTER SCIENCE

BSC INFORMATION TECHNOLOGY | CSIT 309-DATA NETWORK SECURITY I END OF SEMESTER EXAMS

TIME ALLOWED: 2HRS 30MINS

INSTRUCTIONS: THIS EXAM COMPRISES TWO (2) SECTIONS; SECTIONS A AND B. ANSWER ALL QUESTIONS ANSWER BOOK PROVIDED.

SECTION A (40 MARKS): CHOOSE THE MOST APPROPRIATE LETTERED (a, b, c, d) THAT SUITABLY ANSWERS EACH QUESTION.

1. Which of the following consequences is most likely to occur due to an injection attack?
   a. Spoofing c. Denial of Service
   b. Cross-site request forgery d. Insecure direct object references

2. Your application is created using a language that does not support a clear distinction between code and data. Which vulnerability is most likely to occur in your application?

   a. Injection c. Failure to restrict URL access
   b. Insecure direct object references d. Insufficient transport layer protection
3. Which of the following scenarios is most likely to cause an injection attack?
   a. Unvalidated input is embedded in an instruction stream.
   b. Unvalidated input can be distinguished from valid instructions.
   c. A web application does not validate a client's access to a resource.

   d. A web action performs an operation on behalf of the user without checking a shared secret.

4. A user is able to pass malicious input that invokes control codes in your Web application. Which vulnerability is most likely to occur in your Web application?

   a. Injection c. Failure to restrict URL access
   b. Insecure direct object references d. Insufficient transport layer protection
5. Which of the following is the best way to protect against injection attacks?
   a. SQL queries based on user input
   b. Input validation using an allow list
   c. Memory size checks
   d. Validate integer values before referencing arrays
6. Which of the following is most vulnerable to injection attacks?
   a. Session IDs c. Regular expressions
   b. Registry keys d. Server configuration files
7. Which character is most likely to be used for an SQL injection attack?
   a. Single quote (') c. Less than sign (<)
   b. Null (\0) byte d. Greater than sign (>)
8. Which mitigation technique can help you strictly define valid input?
   a. Allow list c. Table indirection

b. Memory size checks d. Escaping

9. Which of the following functionalities should you include in an authentication and session management system?

a. Logout functionality c. Escaping functionality
b. Regular expressions d. Forwarding system functionality

1. Why should you use CAPTCHA?
   a. To create cryptographically random session IDs
   b. To protect credentials by using encryption or cryptographic salt and hash
   c. To protect authentication systems from automated or brute-force attacks
   d. To ensure that authentication systems implement inactivity timeout functionality
2. Which of the following is the best way to ensure that JavaScript cannot be used to access a cookie?
   a. Set the secure flag in the cookie c. Use the CAPTCHA system
   b. Set HttpOnly flag in the cookie d. Use non-persistent cookies
3. Which of the following is an authentication system mandatory requirement?
   a. Form variables are used for managing session IDs.
   b. Use a GOTCHA to prevent automated attacks.
   c. User logout and session inactivity controls.
   d. Session IDs are only accepted from cookies and parameter variables.

4. A session-based system authenticates a user to a Web site to provide access to restricted resources. To increase security in this scenario an authentication token should meet which of the following requirements?

a. It should identify returning users to the site.
b. It should be public information.
c. It should always use a persistent cookie.
d. It should always use a non-persistent cookie.

5. Which of the following tasks is performed by a session-based system?
   a. Identifying returning users
   b. Using form variables for managing session IDs
   c. Using HTTP protocol
   d. Sending successful logins to a well-known location

6. Which threat is most likely to occur when a Web application fails to validate a client's access to a resource?

a. Injection c. Insecure direct object reference
b. Cross-site scripting d. Cross-site request forgery

7. Which of the following vulnerabilities is most likely to occur due to an insecure direct object reference attack?

a. Executing commands on the server.
b. Impersonating any user on the
c. Modifying SQL data pointed to by the query.

d. Accessing a resource without authorization.

8. Which of the following is the most common result of a cross-site request forgery?
   a. Elevation of privilege c. Enabling of IPsec
   b. Disabled security features d. Misconfigured security features

9. An attacker lures a victim to malicious content on a Web site. A request is automatically sent to the vulnerable site which includes victim's credentials. Which attack is most likely to occur in this scenario?

   a. Injection c. Insecure direct object reference
   b. Cross-site scripting d. Cross-site request forgery

1. HTTP GET parameters limit the types of manipulation a malicious user can perform on the victim to forge a request. (Indicate whether True or False)

   a. True
   b. False

2. If your scan does not look like it covered the application fully, which section of the Application Data view would you look to evaluate the problem?

   a. Filtered URLs section c. Cookies
   b. Parameters Section d. Comments

3. To ensure that multiple-phase scanning is run automatically, which of the following options must you choose:

   a. Start a full automatic scan c. Start with manual explore
   b. Start with automatic explore only

4. Which of the following logs capture details of actions that Security AppScan Standard runs during a scan?

   a. Log c. Test Log
   b. Scan Log d. Explore Log

5. What Lists the pages that Security AppScan Standard did not visit because they were filtered out of the Explore, either by standard filters or by filters that you defined when you configured the scan.

   a. Filtered URLs c. JavaScript
   b. Cookies d. Requests

6. At what stage does the Security AppScan Standard send thousands of custom requests that it created during the explore stage?

a. Test Stage c. Multiple Phase scan stage
b. Test and Explore stages d. all of the above

7. Which type of vulnerability can occur when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter?

a. Cross-site Scripting
b. Insecure Direct Object Reference
c. Injection Flaw
d. Cross Site Request Forgery

1. AppScan sent the following test HTTP request:

GET /web/content/index.php?file=/../../../../../../../../../etc/passwd%00 HTTP/1.0

Cookie:
*JSESSIONID=dqt0LSnfhdVyTJkCwTwfLQQSkTTGYX9D79tLLpT1yLQjVhSpZKP9!914376523; customerLanguage=en Accept: */**
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)

Host*: www.ibm.com*
Although, there is no indication in the response about the existence of a password file, AppScan reported vulnerability with the following reasoning:
Global Validation found an embedded script in the response (<script>alert(25053)</script>), which was probably injected by a previous test.

The presence of this script in the site suggests that the application is vulnerable to which type of attack?

a. Stored Cross-site Scripting
b. Cross-site Scripting
c. Name Path Traversal
d. Directory Listing

2. Which type of vulnerability allows an attacker to execute a malicious script in a user browser?
   a. Cross-site Scripting
   b. Injection Flaw
   c. Insecure Direct Object Reference
   d. Failure to restrict URL access
3. Which statement is true about infrastructure vulnerabilities?

   a. They are caused by insecure coding and are fixed by modifying the application code.

   b. They are detected using application security scanners and exist in the Web application.

   c. They are known vulnerabilities and are fixed by modifying the application code.
   d. They exist in third-party components and are fixed by applying security patches.
4. What does secure session management require?
   a. session tokens that are given long lifetimes

b. session tokens that are invalidated when the user logs out
c. session tokens that are persistent
d. session tokens that are numeric

5. Which Web application operation indicates that the application may be vulnerable to Cross-site Request Forgery?

a. GETtransferfunds.aspx?sacct=3434dacct=56745formtoken= YUR345
b. GETsendemail.aspx?address=jsmith@dfg.com subject=hello content=
c. GET search.aspx text=ersonal banking
d. GET login.aspx

1. Which statement is true about network firewalls preventing Web application attacks?
   a. Network firewalls cannot prevent attacks because ports 80 and 443 must be open.
   b. If configured properly, network firewalls can prevent attacks.
   c. Network firewalls cannot prevent attacks because it is too complex to configure.
   d. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.
2. When would you set up a multi-step operation in AppScan?
   a. when your application requires specific user input
   b. when your application requires JavaScript execution
   c. when your application requires a specific flow
   d. when your application has two-factor authentication
3. What does a Cross-site Scripting vulnerability allow an attacker to do?
   a. execute a malicious script on the Web server
   b. change the Web server configuration
   c. steal a user session tokens
   d. drop database tables
4. When can an injection type attack occur?
   a. when the database is set up on a server outside the demilitarized zone
   b. when an error message is generated by the Web server
   c. when user-supplied data is sent to an interpreter as part of a command, query, or data
   d. when too many users have ADMIN credentials to the Web server console
5. How does an attacker exploit Web application vulnerability?
   a. by hacking the firewall
   b. by installing viruses on a user's machine
   c. by sending malicious HTTP requests
   d. by sniffing the traffic between a user and the Web server
6. Which type of vulnerability allows an attacker to browse files that shouldn't be accessible (e.g. *.bak, "Copy of", *.inc, etc.) or pages restricted for users with higher privileges?
   a. Insecure Cryptographic Storage
   b. Injection Flaw
   c. Failure to Restrict URL Access
   d. Insecure Communication
2. An attacker submits data to the server and the data is stored on the server. Which type of vulnerability is

most likely to occur in your application?

a. DOM-based XSS
c. Persistent XSS
b. Reflected XSS
d. Cross-site request forgery

3. You should set a secure flag in a cookie to ensure that:
    a. The cookie is a persistent cookie.
    b. The cookie is not available to client script.
    c. The cookie is sent over an encrypted channel.
    d. The cookie is deleted when the user closes the browser.

4. Which of the following attacks occurs when a malicious user convinces a victim to send a request to a se rver with malicious input and the server echoes the input back to client?

a.	Reflected XSS	c.	Insecure direct object references
b.	Persistent XSS	d.	Failure to restrict URL access

1. The Explore stage might not have the coverage of the application that you might expect for various reasons. Which of the following reasons apply?

    a. Many of the links might be hidden within the JavaScript code

    b. Some of the application might be on a different domain to the starting web address,

    c. Denial of Service may exist
    d. None of the above.

SECTION B (60 MARKS)

INSTRUCTIONS: ANSWER ALL QUESTIONS FROM THIS SECTION.

Q1

a. What is Cross-Site Scripting? What is the potential impact to servers and clients?

(5 marks)

a. You are designing a new web application service for your company. After an initial design review, it is discovered that a number of attack surfaces have been revealed that go well beyond the initial baseline proposed for the application, including unneeded network services that are enabled. What should you do? **(5 marks)**

b. Your web page includes advertising JavaScript from a third-party service. Is it safe to assume that problems like Cross-Site Scripting, caused by this third-party JavaScript, is not technically possible on your web page? Explain your answer **(5 marks)**

Q2

Explain the following and site typical examples, the following; **(5 marks each)**

a. Cross-Site Scripting

b. Cross-Site Request Forgery

c. Session Fixation.

Q3.

a. Your web application locks out users who provide incorrect input when logging in. What is the best setting to ensure that your application is explored correctly, in configuring your AppScan and why? **(5 marks)**

b. Describe the two (2) distinct phases in AppScan. **(5 marks)**

c. What are the Security Techniques known in web application? State and describe

(5 marks)

Q4

a. AppScan received the following test response:

An Error Has Occurred

Summary:

Syntax error in string in query expression 'userid = ''. Error Message:

System.Data.OleDb.OleDbException: Syntax error in string in query expression 'userid = ''. at System.Data.OleDb.OleDbCommand.ExecuteCommandTextForSingleResult(tagDBPARAMSdbParams, Object executeResult) at?

What type of vulnerability does this error message indicate? Explain your answer.

(5 marks)

a. List five (5) valid suggestions to determine web application coverage in AppScan.

(5 marks)

a. Why does defining your environment improve performance and accuracy when using the AppScan to scan your web application? Explain your answer. **(5 marks)**