Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2023/2024

COURSE NAME	:	WEB SECURITY
COURSE CODE	:	BIS 20303
PROGRAMME CODE	:	BIW/BIS
EXAMINATION DATE	:	JULY 2024
DURATION	:	3 HOURS
INSTRUCTIONS	:	1. ANSWER ALL QUESTIONS 2. THIS FINAL EXAMINATION IS CONDUCTED VIA ☐ Open book ☒ Closed book 3. STUDENTS ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED VIA CLOSED BOOK

THIS QUESTION PAPER CONSISTS OF **EIGHT (8)** PAGES

PART A

Instructions: Choose the **BEST** answer.

Q1 Which factor contributes significantly to the complexity of securing web applications?

(a) The increasing number of internet users.

(b) Many web applications rely on third-party components.

(c) The diversification of device types and operating systems.

(d) Increasing number of web traffic.

(1 mark)

Q2 What does a "Fail-Open" login mechanism mean in web application security?

(a) It encrypts user credentials during transmission but not at rest.

(b) It allows users in event when the login system breaks down or makes a mistake.

(c) Additional user information is required after a failed login attempt to enhance security.

(d) It involves an automatic logout after a predefined period of inactivity.

(1 mark)

Q3 Identify a flaw associated with multistage login mechanisms in web applications:

(a) They may accidentally log user activities, compromising privacy.

(b) Attackers can bypass subsequent stages if initial stages do not verify completion properly.

(c) They significantly reduce the website's load time, affecting user experience.

(d) They prevent the effective use of cookies and session tokens, reducing usability.

(1 mark)

Q4 Which practice indicates insecure storage of credentials?

(a) Utilizing Transport Layer Security (TLS) for data transmission between the client and server.

(b) Applying weak hashing for passwords before storage.

(c) Storing passwords in plain text within the database.

(d) Generating unique session identifiers for each user login.

(1 mark)

Q5 What mechanism does HTTPS use to secure communications between a web server and a client?

(a) Secure Sockets Layer (SSL).

(b) Transport Layer Security/Secure Sockets Layer (TSL/SSL).

(c) Secure Shell (SSH).

(d) Transmission Control Protocol/Internet Protocol (TCP/IP).

(1 mark)

Q6 Which feature of cookies enhances web application security?

(a) Persistent storage of user preferences.

(b) Encrypted storage on the client side.

(c) Session management and authentication.

(d) Compression of web content for faster loading.

(1 mark)

Q7 Which of the following is a benefit of using HTTP Authentication in web applications?

(a) Enables encrypted communication channels independently.

(b) Facilitates the direct validation of user credentials by the server.

(c) Provides a built-in mechanism for encrypting user credentials.

(d) Offers an integrated method for session management and user tracking.

(1 mark)

Q8 Which of the following is primarily used by web applications to maintain the state between the client and the server?

(a) SSL Certificates.

(b) Cookies and Session Tokens.

(c) HTML5 and CSS3.

(d) GET and POST requests.

(1 mark)

Q9 In the context of future web security measures, which approach involves treating every access attempt as a potential threat and necessitates continuous authentication?

(a) Leveraging Machine Learning for anomaly detection.

(b) Implementing Behavioral Analysis to identify bots.

(c) Adopting a Zero Trust Architecture.

(d) Embracing Automation for task efficiency.

(1 mark)

Q10 In web development, how does the server-side component typically manage user sessions and maintain state?

(a) By storing session data encrypted within the user's browser cache.

(b) Through the use of cookies that keep user information across multiple sessions.

(c) By using a combination of server-side storage and temporary tokens.

(d) Relying solely on dynamically generated links to track user interactions.

(1 mark)

PART B

Instructions: Answer **ALL** of the questions

Q11 State either **True** or **False** for each of the following statements.

(a) The evolution of web applications has solely focused on enhancing user interface designs, with minimal impact on security protocols and measures.

(1 mark)

(b) Future web security applications are expected to incorporate artificial intelligence and machine learning technologies to predict and prevent new types of cyberattacks.

(1 mark)

(c) A digital signature employs asymmetric cryptography to verify the sender's identity and ensure the message has not been altered during transmission.

(1 mark)

(d) While digital signatures verify the authenticity of digital messages, encryption is necessary to protect the message's confidentiality against eavesdropping.

(1 mark)

(e) Anomaly-based detection in Internet and network security monitoring systems can identify threats without prior knowledge of specific attack patterns, making it highly effective against zero-day exploits.

(1 mark)

(f) In the context of secure digital communications, digital signatures alone can encrypt a message's contents to shield it from unauthorized access.

(1 mark)

(g) Utilizing a digital signature in a document's transmission also inherently compresses the document's size, facilitating quicker network transfer speeds.

(1 mark)

(h) Cross-site scripting (XSS) attacks can be prevented by ensuring that all dynamic content on a web page is encrypted.

(1 mark)

(i) One common way XSS attackers exploit web applications is by injecting malicious scripts into forms that are submitted by unsuspecting users.

(1 mark)

(j) Content Security Policy (CSP) headers are a browser security feature that can help prevent Cross-Site Scripting (XSS) attacks by restricting the sources from which content can be loaded.

(1 mark)

Q12 During a routine security review, CyberSafe Solutions observes suspicious activities in their network logs indicating potential unauthorized access attempts on their main server serving the SecureDoc web application. The logs show repeated access attempts to the admin login page from a single IP address over a 4-hour period as shown in **Table Q12.1**:

Table Q12.1

Timestamp	Logs
5/10/2022 2:45:00 AM	Access Denied: SecureDoc\Admin Unknown username or password.
5/10/2022 2:45:02 AM	Access Denied: SecureDoc\Admin Unknown username or password.
5/10/2022 2:45:04 AM	Access Denied: SecureDoc\Admin Unknown username or password.
.....	.....
5/10/2022 6:45:00 AM	Access Denied: SecureDoc\Admin Unknown username or password.

(a) Name the type of attack suggested by these repeated login attempts.

(2 marks)

(b) List **THREE (3)** security measures that are missing or ineffective at CyberSafe Solutions that could allow for such an attack to occur.

(3 marks)

(c) Provide explanations for each identified security measures in **Q12(b).**

(6 marks)

(d) Identify **THREE (3)** conditions under which this type of attack is likely to be successful. Explain the rationale behind each condition.

(6 marks)

(e) Suggest **TWO (2)** specific actions on how CyberSafe Solutions could use the information from these failed login attempts to improve their security posture against future attacks.

(4 marks)

Q13 A web application uses a MySQL database for user management and product inventory with the following setup:

```
CREATE TABLE users(username varchar(32), user_password varchar(32));
CREATE TABLE inventory(item_name varchar(32), stock_quantity int);
INSERT INTO users VALUES ('bob', 'Pa$$w0rd');
INSERT INTO inventory VALUES ('laptop', 20);
```

The application allows users to check the stock quantity of products through a user-provided HTML form. The form data is received in a variable `$item` in a PHP script, which then forms an SQL query to retrieve the stock quantity:

```
$sql = "SELECT stock_quantity FROM inventory WHERE item_name =
'$item'; ";
```

The result is displayed to the user, showing the available stock for the requested item.

(a) What input could an attacker provide in `$item` to:

(i) Reveal the password of user `Bob`?

(3 marks)

(ii) Change the password of user `Bob` to `abcd1234`.

(3 marks)

(b) Briefly describe **THREE (3)** measures that the designer of the web application can implement to mitigate the risks associated with the vulnerability described in **Q13(a)(i).**

(6 marks)

Q14 Consider each scenario described below.

(a) Identify the most appropriate type of firewall configuration or technology that should be implemented to achieve the desired security outcome.

(i) Block all incoming connections to a web server except those necessary for serving HTTPS traffic to users from any geographic location.

(1 mark)

(ii) Prevent users within a corporate network from accessing websites with known malicious content, based on URL filtering and content analysis.

(1 mark)

(iii) Restrict outbound SMTP traffic from the corporate network to only allow emails sent through the company's official email server, blocking potential email-based malware spread.

(1 mark)

(b) Explain for each answer you give in **Q14(a)(i)** to **Q14(a)(iii).**

(6 marks)

Q15 Analyse the described incidents to determine the type of cyber-attack.

(a) During a significant online sale event, "DealDay," the website suddenly becomes unreachable to customers. The server logs indicate a massive influx of requests in a short period, far exceeding the website's capacity to handle traffic, leading to service disruption.

(1 mark)

(b) Employees receive an email from what appears to be the company's IT department, urging them to click on a link to update their email settings. The link redirects to a fraudulent website designed to steal login credentials.

(1 mark)

(c) A new piece of malware is identified on the network that disguises itself as a legitimate antivirus update. Once executed, it scans for and extracts documents, sending them to an external command and control server.

(1 mark)

(d) An application crashes when trying to load a file that contains an unusually long string of characters. This exploit allows the attacker to execute arbitrary code on the system running the application.

(1 mark)

(e) An autonomous program exploits a security flaw in a widely used email server software, replicating itself and sending copies to email addresses in the host's contact list without user intervention.

(1 mark)

(f) The IT department notices an unusual pattern of outbound network traffic. Further investigation reveals that several devices on the network are communicating with known malicious external IPs at regular intervals. The data being transmitted is encrypted, but analysis suggests it might be following a specific communication protocol used by compromised systems. These compromised systems may be receiving instructions or coordinating activities with a central server.

(1 mark)

Q16 Consider the following scenario.

Your company is developing a new web application to handle online customer transactions. Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (STRIDE) is a threat modelling methodology used to identify potential vulnerabilities in web applications. As part of the security process, you need to conduct a risk analysis using STRIDE.

(a) Choose and explain any **THREE (3)** STRIDE threats that could pose vulnerabilities in the web application in the above scenario.

(6 marks)

(b) Once vulnerabilities are identified, identify **THREE (3)** parameters to prioritize the risks they pose to the web application.

(6 marks)

- END OF QUESTIONS -