UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2022/2023

COURSE NAME	:	WEB SECURITY
COURSE CODE	:	BIS 20303
PROGRAMME CODE	:	BIS / BIW
EXAMINATION DATE	:	JULY / AUGUST 2023
DURATION	:	3 HOURS

INSTRUCTION

1. ANSWER ALL QUESTIONS
2. THIS FINAL EXAMINATION IS CONDUCTED VIA **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 **NINE (9)** PAGES

SECTION A

Instruction: Choose the BEST answer for each of the following questions.

Q1 Which of the following statements is true about reflected Cross Site Scripting (XSS) attacks?

A. The malicious code is stored in the server's database.
B. The malicious code is stored on the victim's computer.
C. The malicious code is reflected back to the victim by the server.
D. The malicious code is executed by the victim's browser.

(1 mark)

Q2 What is the difference between reflected and stored XSS?

A. Reflected XSS is executed when a user visits a specific page, while stored XSS is executed when the user submits a form.
B. Reflected XSS is stored on the server, while stored XSS is stored on the victim's computer.
C. Reflected XSS is temporary, while stored XSS is permanent.
D. Reflected XSS is caused by an error in the server's input validation, while stored XSS is caused by a vulnerability in the website's code.

(1 mark)

Q3 Which of the following is a characteristic of a stateless firewall?

A. It inspects packets based on their content.
B. It tracks the state of connections between hosts.
C. It allows or blocks traffic based on predefined rules.
D. It can identify and block attacks such as Structured query language (SQL) injection and cross-site scripting.

(1 mark)

Q4 Which type of firewall is best suited for networks that require high performance and low latency?

A. Stateless firewall.
B. Stateful firewall.
C. Next-generation firewall.
D. Single box firewall.

(1 mark)

Q5 Which of the following is a characteristic of a stateful firewall?

A. It inspects packets based on their content.
B. It tracks the state of connections between hosts.
C. It allows or blocks traffic based on predefined rules.
D. It can identify and block attacks such as SQL injection and cross-site scripting.

(1 mark)

Q6 Which type of firewall is best suited for networks that require deep packet inspection and application awareness?

A. Stateless firewall.
B. Stateful firewall.
C. Next-generation firewall.
D. Single box firewall.

(1 mark)

Q7 What is the main advantage of using a stateful firewall?

A. It provides a higher level of security than a stateless firewall.
B. It can track and filter traffic based on the context and state of the connections.
C. It is more flexible and customizable than a stateless firewall.
D. It can inspect and block traffic based on the application layer.

(1 mark)

Q8 Which of the following is a disadvantage of using Hypertext Transfer Protocol (HTTP) authentication for web applications?

A. It is not secure and can be easily bypassed.
B. It is difficult to implement and manage large user bases.
C. It is not supported by all web browsers and devices.
D. It can slow down website performance and load times.

(1 mark)

Q9 What is the difference between a session cookie and a persistent cookie?

A. A session cookie expires after a user closes their web browser, while a persistent cookie remains on their computer.
B. A session cookie stores sensitive information, while a persistent cookie tracks user behaviour.
C. A session cookie is used for authentication, while a persistent cookie is used for advertising.
D. A session cookie is used by web servers, while a persistent cookie is used by web browsers.

(1 mark)

Q10 How do web cookies pose a security risk?

A. By exposing sensitive user information to hackers.
B. By slowing down website performance and increasing load times.
C. By preventing users from accessing certain parts of a website.
D. By creating backdoors for malware and viruses to infect a user's computer.

(1 mark)

Q11 State either **TRUE** or **FALSE** for the following statements:

(a) HTTP POST requests are less secure than GET requests because they are transmitted in plain text.

(b) Uniform Resource Locator (URLs) can contain sensitive information such as user credentials and session IDs.

(c) XSS attacks occur on the server-side of a website.

(d) Client-side encryption is more secure than server-side encryption.

(e) If two users choose the same password and the same salt is added to both passwords before hashing, their hash values will be the same.

(f) Brute force attacks are always carried out manually by human attackers.

(g) Transmission Control Protocol (TCP) scans, (Synchronization)SYN scans, and port scans in general are considered ethical hacking techniques that can help identify and prevent potential security threats.

(h) A TCP scan is a type of port scan that sends a full TCP handshake to the target machine to determine which ports are open.

(i) Risk analysis can be a time-consuming and resource-intensive process, making it difficult for small organizations to undertake.

(j) Once risks have been identified, the only way to mitigate them is through the implementation of technical controls such as firewalls and intrusion detection systems.

Q12 The following segment of Hypertext pre-Processor (PHP) source code in **Figure Q12** illustrates a common buffer overrun vulnerability. The function `strlen` is used to count the length of a string.

(a) Draw a diagram to illustrate the occurrence of buffer overrun based on the codes in **Figure Q12**. In the diagram, provide **ONE (1)** example of input data to illustrate the buffer overrun scenario.

```
<?php
$input = $_GET['input'];
$buffer = array_fill(0, 10, 0);

for ($i = 0; $i <= strlen($input); $i++) {
    $buffer[$i] = $input[$i];
}

echo "Buffer contents: ";
for ($i = 0; $i < count($buffer); $i++) {
    echo $buffer[$i];
}
?>
```

Figure Q12

(5 marks)

(b) Explain why buffer overrun is considered a threat to a system?

(3 marks)

Q13 Questions **Q13(a)** to **Q13(d)** are based on **Table Q13(a)** and **Table Q13(b)**, which are logs that keep records of authentication activity on a web system.

Table Q13(a)

Timestamp	Username	Password	Success
2022-05-01 14:23:45	admin	password	No
2022-05-01 14:24:15	admin	123456	No
2022-05-01 14:25:22	admin	admin	No
2022-05-01 14:26:01	admin	pass	No
2022-05-01 14:26:58	admin	p@ssword	Yes

Table Q13(b)

Timestamp	Username	Password	Success
2022-05-01 14:23:45	admin	1234	No
2022-05-01 14:24:15	admin	1235	No
2022-05-01 14:25:22	admin	1236	No
2022-05-01 14:26:01	admin	1237	No
2022-05-01 14:26:58	admin	1238	Yes

(a) Identify the type of attack that may have taken place in
  (i) **Table Q13(a).**
  (ii) **Table Q13(b).**

(2 marks)

(b) Provide the reason for the given answer in the question
  (i) **Q13(a)(i).**
  (ii) **Q13(a)(ii).**

(2 marks)

(c) Explain **TWO (2)** methods that can be used to mitigate the attack in both **Table Q13(a)** and **Table Q13(b)**.

(4 marks)

Q14 **Figure Q14** contains two tables which are `Table USER` and `Table COMMODITY`. Questions **Q14(a)** to **Q14(d)** are based on **Figure Q14**.

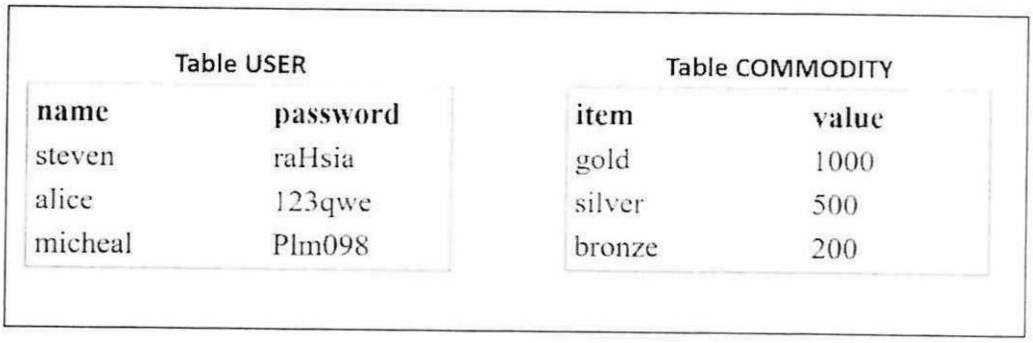

Table USER

name	password
steven	raHsia
alice	123qwe
micheal	Plm098

Table COMMODITY

item	value
gold	1000
silver	500
bronze	200

Figure Q14

(a) In the web system, there is a menu to look up the current price from the `Table COMMODITY`. The application receives a string in variable `$lookPrice` from a user-provided Hyper Text Markup Language (HTML) form, which will be sent to the SQL statement to look up the corresponding price from the table as the following:

```
$sql = "SELECT value FROM commodity WHERE item='$lookPrice';"
```

To launch an SQL injection attack, what should the attacker write in the form for the variable `$lookPrice` to get do the following:

  (i) the value displayed is the password for user *steven*.

(3 marks)

  (ii) the password for user *steven* is changed to *qwerty*.

(3 marks)

(b) Briefly describe **TWO (2)** measures that the designer of the web application can take to reduce the risks of getting the attack described in **Q14(a)**.

(4 marks)

(c) Explain how the keyword "`Order`" is used in SQL statements to help an attacker to know the number of table columns.

(2 marks)

(d) After knowing the number of columns in *Table USER*, the attacker now execute the following queries :

```
First attack: ' UNION SELECT 'a',NULL--
Second attack: ' UNION SELECT NULL,'a'–
```

(i) Explain what is the purpose of running these queries.

(2 marks)

(ii) Explain the information that the attacker wants to get in the `first attempt` and the `second attempt`.

(2 marks)

(e) Choose and explain whether either whitelisting or blacklisting approach is better to be used to sanitize input for the variable `$lookprice` in **Q14(a)**.

(2 marks)

Q15 Consider the following code snippet in **Figure Q15(a)**.

```
if (employee_type == "full-time") {
    salary = base_salary + bonus;
} else {
    salary = hourly_rate *
hours_worked; }
```

Figure Q15(a)

An attacker has gained access to the system and changed the codes to be the following

```
if (employee_type == "full-time") {
    if (month == "April") {
        salary = (base_salary + bonus) / 2;
    } else {
        salary = base_salary + bonus;
    }
} else {
    salary = hourly rate * hours worked; }
```

Figure Q15(b)

(a) The attacker has changed the codes in **Figure Q15(a)** to be a malicious program as shown in **Figure Q15(b).** Identify the type of malicious program in **Figure Q15(b).**

(2 marks)

(b) Explain the difference between what the codes in **Figure Q15(a)** and **Figure Q15(b)** will do.

(2 marks)

(c) Explain **TWO (2)** measures that can be taken to prevent this kind of attack.

(4 marks)

Q16 (a) Identify the type of attack that has occurred based on the following scenario:

(i) The small business owner logs in to their client-server application with their credentials as usual. However, instead of being directed to the normal display of the requested data, they are presented with a mix of nonsensical symbols and numbers. The owner soon realizes that important data is missing, and after receiving a call, they come to know that their system has been hacked by exploiting a vulnerability in the database.

(1 mark)

(ii) The attack started when a user open a Word document, that was sent to their email. The Word document contains the malware that will encrypt every file that the user is opening on the machine being attacked.

(1 mark)

(iii) At 12:00 PM on April 30th, 2023, all machines running ABC software suddenly went down, leaving staff unable to perform their tasks. Upon investigation, it was discovered that all files in the root directory have been deleted recursively. Further analysis revealed that a malicious code had been inserted into the system, with instructions to execute the file deletion at a specific time or in response to certain conditions.

(1 mark)

(iv) You received a WhatsApp message from somebody disguised as your friend and ask you to provide your date of birth and your mother's maiden name.

(1 mark)

(v) You are the system administrator for a large company and you have noticed some strange activity on the server. You investigate and find that there is an additional user account that you did not create. This account has administrative privileges and seems to be used for some unknown purpose. You suspect that there may be some unauthorized access happening through this account.

(1 mark)

(vi) You work for a large company that uses a shared network drive to store important files. One day, you notice that all the files on the network drive have been mysteriously modified and some of them have been deleted. You investigate and find that the files were modified and deleted from multiple computers on the network, even those that weren't being actively used at the time. The IT department discovers that the network has been infected by a malicious program that spread itself to all the connected computers, causing the damage.

(1 mark)

(vii) A software program is installed on a computer system without the user's knowledge or consent. This program is designed to replicate itself and attach its code to other legitimate files on the system, causing them to behave erratically or stop working altogether. The program spreads to other systems through file sharing or network connections, causing widespread disruption to businesses and individuals who rely on these systems.

(1 mark)

(viii) An online store suddenly becomes inaccessible to customers. The website owner notices a significant increase in traffic, which slows down the website's performance and eventually causes it to crash. Upon investigating, the website owner realizes that the influx of traffic was not from legitimate customers, but rather from a large number of requests from different IP addresses. The server becomes overloaded and can no longer respond to legitimate requests, causing the website to be unavailable for an extended time.

(1 mark)

(b) Provide the reason for every answer you provided in **Q16(a)(i)** to **Q16(a)(viii).**

(8 marks)

-END OF QUESTIONS-