National University of Computer and Emerging Sciences

FAST School of Computing **Fall-2023** **Islamabad Campus**

CS-2005: 3002: Information Security (BS-CS)

All Sections

Monday, 18th December, 2023

Course Instructor

Urooj Ghani, Muhammad Luqman Sumar, Hina Binte Haq

Serial No:

Final Exam

Part B

Total Time: 1.5 hour

Total Marks:

_____

Signature of Invigilator

Student Name	Roll No.	Course Section	Student Signature

DO NOT OPEN THE QUESTION BOOK OR START UNTIL INSTRUCTED.

Instructions:

1. This is Part B of the final exam; you must have already returned Part A. You MUST write your name and roll number on this page. Please do it now!
2. No additional sheet will be provided for rough work. Use the back of the last page for rough work.
3. If you need more space write on the back side of the paper and clearly mark question and part number etc.
4. After asked to commence the exam, please verify that you have **10** different printed pages including this title page. There are a total of **3** questions.
5. Use permanent ink pens only. Any part done using soft pencil will not be marked and cannot be claimed for rechecking.
6. Calculator sharing is strictly prohibited.
7. You need to be as specific as possible and provide the answers in the space provided. Cutting, overwriting and ambiguous answers would be considered as incorrect.

	Q-1	Q-2	Q-3	Total
Marks Obtained				
Total Marks	**20**	**30**	**10**	**60**

Question 1 [20 Marks]

You are the IT security administrator for a small coffee shop chain with several locations across the city. Each location has its own Wi-Fi network for customers and employees, and they all connect back to a central server for point-of-sale transactions and inventory management.

1. Identify and describe four different types of network security attacks that could be targeted at the coffee shop's network. For each attack, explain its potential impact and how it could be exploited. **[8 marks]**

Attack Type	Potential Impact	Exploitation

2. Discuss three specific wireless security vulnerabilities that are unique to Wi-Fi networks and how they can be exploited by attackers to gain unauthorized access or intercept data. **[3 marks]**

1.
2.
3.

3. Analyze and propose three security measures that the coffee shop can implement to mitigate the identified network and wireless security threats. Consider both technical solutions and best practices for employee awareness and training. **[3 marks]**

1.
2.
3.

4. Imagine a scenario where a hacker successfully breaches the coffee shop's network through a vulnerability in one of their Wi-Fi access points. Describe the steps you would take as the IT security administrator to respond to the incident, including initial containment, investigation, remediation, and recovery. **[6 marks]**

Question 2 [30 Marks]

Read the following case study and attempt the questions that follow.

FAST NUCES employs an online platform named FLEX FACULTY, allowing instructors to efficiently manage student attendance, assessments, and grades digitally. This platform streamlines the process of uploading all the assessments marks, and maintaining attendance records. Students can easily access and review their attendance, marks, and grades. Moreover, the platform has implemented various measures to protect sensitive information and ensure a secure experience, although they have not achieved full website security yet. Additionally, students have the capability to provide valuable feedback on the course and instructors through FLEX STUDENT.

Miss Urooj, an Information Security instructor at FAST NUCES utilizing FLEX FACULTY, routinely accesses the platform to upload marks, record attendance, and generate grades at the end of the semester for students. She frequently uses her laptop, which has up-to-date security software and a modern web browser, to access the platform. She takes comfort in the fact that FLEX FACULTY employs HTTPS (HTTP Secure) to establish a secure connection between her browser and the FLEX servers, ensuring data encryption during transmission. While FLEX FACULTY also offers an HTTP version of the website for older browser compatibility and supports older SSL versions for HTTPS, it has limited functionality.

Part 1:
One day, Urooj receives an email that appears to be from FLEX FACULTY, claiming a security breach and urging her to click on a link immediately to verify her last login attempt. Concerned about her account's security, Urooj clicks the link, unknowingly directing herself to a malicious website controlled by attackers—(her students studying Information Security :D)

Part 2:
The malicious website, designed to closely resemble the legitimate FLEX FACULTY interface, has been specifically crafted such that it contains hidden forms that submit fraudulent data, such as attendance records, marks and grades on behalf of the instructor Urooj without her knowledge. These alterations could manipulate students' data or make unauthorized changes to the platform's settings.

Part 3:
Additionally, it contains Javascript that is meant to send Urooj's cookies set by the FLEX FACULTY website to the attackers. If Urooj is simultaneously logged in to the real FLEX FACULTY website in another window, these scripts attempt to access the real website's DOM and steal the cookies from there.

Part 4:
In case the attack in Part 3 does not work, the website also contains some other malicious links that carry attacks that can only work if Urooj is logged into the original website at the same time. Clicking these links sends particular scripts to the "search this website" function to the FLEX server. The end result is that Urooj's

browser runs these malicious scripts assuming they are from the FLEX server, resulting in the attacker receiving Urooj's cookies.

Part 5:

Since Urooj's educational institution, with thousands of students and faculty members, extensively uses FLEX, an attacker strategically infiltrates the institution. They aim to deceive a substantial part of FLEX user base into revealing their sensitive information. They do this by setting up a fake WiFi network that looks like the institution's legitimate network and ensuring that students and faculty members connect to the fake network by jamming the original one for a while. They then capture all traffic of everyone connected to the fake network so that they can isolate the traffic to and from FLEX and capture sensitive data from it.

1. Suppose FLEX FACULTY becomes aware of the attacks and immediately considers several security measures, given in the first column of the following table. Write down the name of any one attack that each security measure prevents (the attacks may be outside of this scenario).
   [10 marks]

Policy	Attack Prevented
Same-site cookies set to strict	CSRF
Secure cookie attribute set	Cookie stealing over HTTP
HTTP-only cookies set	Session hijacking/cookie stealing
Use of a double-submit cookie	CSRF
Use of input sanitization through blacklisting in "search this website" requests.	Reflected XSS
Use of synchronizer token pattern	CSRF
Removing any mixed HTTP/HTTPS content from the website and strictly using HTTPS only.	Eavesdropping/MITM/Data stealing
Using stronger encryption for data stored in the database	SQLi or data stealing
Updating their backend to use prepared statements when connecting to the database	SQLi
Whitelisting strictly in all input fields	XSS, SQLi
Content security policy for whitelisting Javascript origins.	XSS

2. Name the attacks being attempted in Part 1, Part 2, Part 3, Part 4 and Part 5 respectively. Also name one security measure that can mitigate the attack. **[10 marks]**

Part	Attack	Mitigation
Part 1	Phishing	User awareness
Part 2	CSRF	Anti CSRF token
Part 3	Session hijacking/ cookie stealing	Same origin policy
Part 4	Reflected XSS	Input sanitization/ no echo response
Part 5	Man in the middle / Rouge AP / Honey pot AP	User awareness/fake wifi detection

3. Name one vulnerability in the website that is allowing downgrading attacks, and one specific downgrading attack that is possible. **[2 marks]**

Vulnerability: allowing older SSL version / serving mixed HTTP and HTTPS content.
Attack: SSL strip

4. Which cookie policy can only partially prevent the type of attacks in Part 2? **[1 mark]**

Same site cookies = lax

5. Will the attack in Part 3 work? Which policy prevents this attack? **[2 marks]**

Will it work: No
Policy preventing it if you answered No: Same origin policy

6. Which cookie policy can completely prevent the attack in Part 4? **[1 marks]**

While no single cookie policy can completely prevent this attack, a combination of measures can significantly reduce its risk. HTTP-only cookies , SameSite Attribute etc

7. Select what is being exploited in the attack in Part 4: **[1 mark]**

The client browser's trust in the web server: Yes / No **YES**
The web server's trust in the requests received from the client browser: Yes / No **BOTH**

8. Which known vulnerability of the website is the attack in Part 5 targeting? **[1 mark]**

Older SSL version and mixed content, MITM, Lack of user awareness etc

9. For preventing the attack in Part 5, name two effective security measures that users like Urooj can take? **[2 marks]**

1. Use ForceHTTPS type browser extensions
2. Make sure no sensitive data on HTTP. Or check carefully before connecting to WiFi. / RF scanning, Rogue AP scanning,

Question 3 [10 Marks]

A database at a military installation keeps fingerprint templates for all 1000 employees to be verified at entrance. The probability of false acceptance is 1-in-100,000 (0.001%) per match. In each of the following scenarios:

i. What will be the percentage of a false match/acceptance?
ii. What will be the implication of false match/acceptance?
iii. What will be the implication of false rejection?

1. Identification **[2 Marks]**

1. 1000x0.001=1%
2. security breach

3. inconvenience to genuine employee

4. Verification **[2 Marks]**

1. 1x0.001=0.001%
2. security breach
3. inconvenience to genuine employee

5. A watch list that is a blacklist of 10 criminals that are known to attempt infiltration **[3 Marks]**

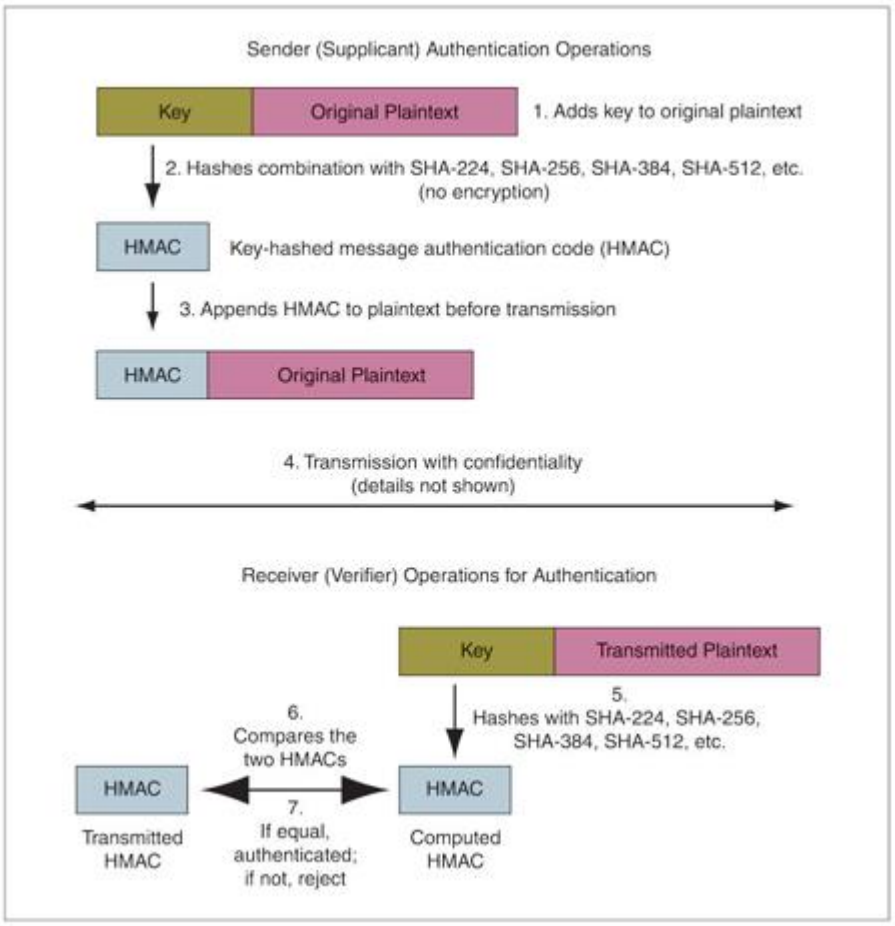
1. 10x0.001=0.01%
2. inconvenience to genuine employee
3. Criminal gets in undetected

4. A watch list that is a whitelist of 50 people from senior command that are to be given preferential treatment **[3 Marks]**

1. 50x0.001=0.05%
2. person not from senior command given preference
3. person from senior command not given preference

Bonus Question:

Draw a diagram to show message confidentiality and authentication process using hash functions, symmetric and asymmetric cryptography.



Best of Luck ☺

Rough Work: