Group A [3 + 2 + 3 + 2 marks]

Q1. Suppose a website's login session expires every two minutes. While obviously inconvenient for users, how does this impact the feasibility of CSRF and XSS attacks? Discuss with reasons.

Q2. State with reasons, if this statement is correct: DOM-based XSS is preventable in server side code.

Q3. What forms of authentication are considered repudiable, and why?

Q4. For the following scenario, list any four attributes that could be used to characterize the subject (healthcare professional)?

[3 + 3 + 2 + 2 marks] **Group B**

Q1. Show how can an attacker use stored XSS to launch a phishing attack. Give a series of events that will take place in a successful attack.

Q2. Discuss how mask attacks help in cracking passwords.

Q3. State with reasons, if the statement is correct: An access matrix is only relevant in discretionary access control.

Q4. For the following scenario, list any four attributes that could be used to characterize the object (patient record)?

A healthcare organization wants to implement Attribute-Based Access Control (ABAC) to manage access to sensitive patient records. They want to ensure that only authorized healthcare professionals can access specific patient information based on their attributes, and the sensitivity of the data.

Group A

Q1

CSRF attack pre-requisite is that victim user must have an active login session with the server. So having a very short login expiry will highly reduce (but not eliminate) the chances of successful CSRF attack.

If XSS attack objective is session hijacking (by cookie stealing), then yes, the attacker will not gain much by stealing the cookies. But attacker might have other goals such as keylogging, website defacing, phishing etc. Those will still work, and session expiry is irrelevant.

Q2

Incorrect. DOM-based XSS attack happens completely on the client side, and so prevention will also be performed in client side.

Q3

Authentication involving knowledge factors (password, pin codes) or possession factors (OTP, smartcard etc.) are repudiable, because in the event of a security incident, a user can easily deny their involvement in the authentication. They can claim that their password was leaked, or their mobile phone (receiving otp) was stolen.

Q4

Possible answers

- Person's id
- Date of birth
- Department (emergency, cardiology, oncology)
- Role (doctor, nurse, surgeon)
- Specialization (Orthopedic, Cardiologist)
- Experience (senior, junior)
- Education (MBBS, higher degree)
- etc.

Group B

Q1

- Identify a vulnerability in target site.
- Exploit that to inject malicious <script> to site database.
- A user visits the vulnerable site. Attacker's <script> is bundled in the response sent to user.
- In victim's browser, the script runs and **redirects** the user to a phishing page (or dynamically pops up a phishing **form** on the same page).

Q2

Mask attacks greatly reduce the time required for brute force cracking, because instead of trying all possible character combinations, the attacker only searches over the space of passwords of particular patterns. *A mask example is needed.*

Q3

No, Role based access control (RBAC) also uses an access matrix, with an important difference that instead of individual subjects, we define privileges of each role.

Q4

Possible answers

- Type of record (prescription, test report)
- Date created/modified
- Patient id
- Department (radiology, pathology, pediatrics)
- Status (archived, current, completed)
- Location (hospital X, clinic Y)
- Category (inpatient, emergency)
- etc.