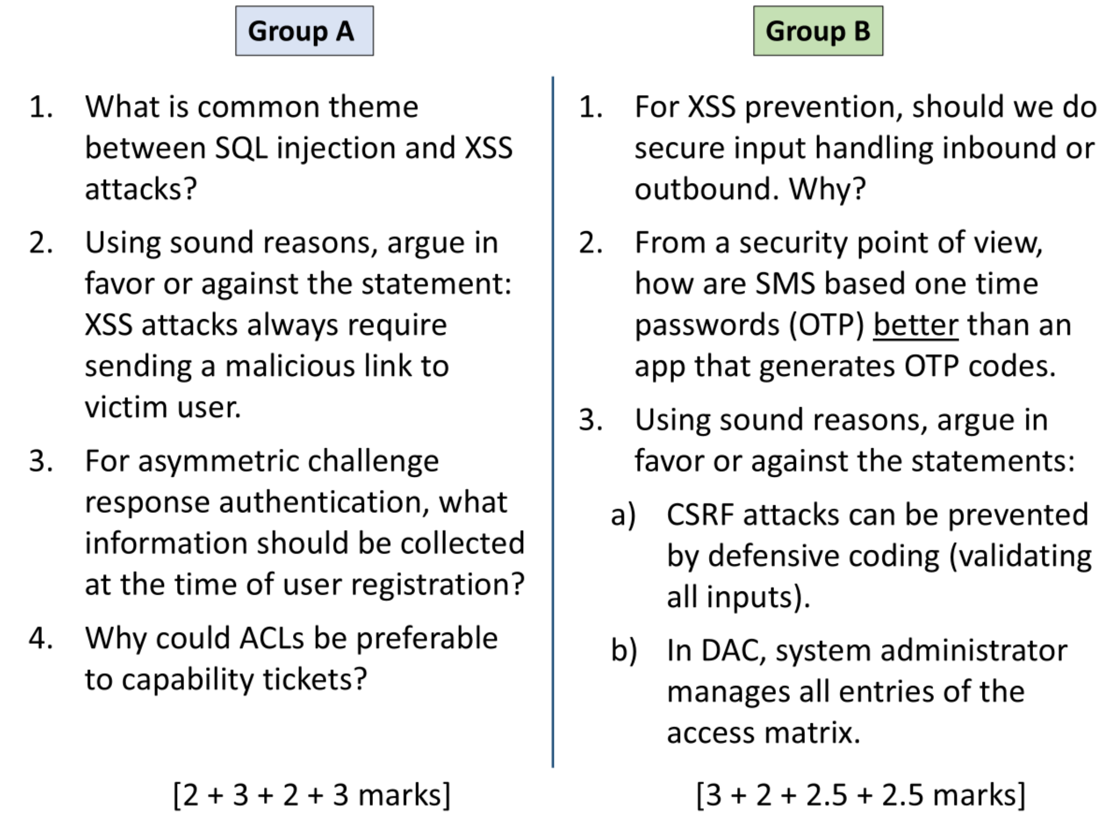

Group A

1. What is common theme between SQL injection and XSS attacks?
2. Using sound reasons, argue in favor or against the statement: XSS attacks always require sending a malicious link to victim user.
3. For asymmetric challenge response authentication, what information should be collected at the time of user registration?
4. Why could ACLs be preferable to capability tickets?

[2 + 3 + 2 + 3 marks]

Group B

1. For XSS prevention, should we do secure input handling inbound or outbound. Why?
2. From a security point of view, how are SMS based one time passwords (OTP) better than an app that generates OTP codes.
3. Using sound reasons, argue in favor or against the statements:
   a) CSRF attacks can be prevented by defensive coding (validating all inputs).
   b) In DAC, system administrator manages all entries of the access matrix.

[3 + 2 + 2.5 + 2.5 marks]

Group A

Q1

Both are ‘injection’ attacks in the sense that attacker inserts a malicious code/script into target system. The injected code gets executed in the victim’s browser in case of XSS, and in db server in case of sqli.

Q2

Sending a malicious link is certainly one of the XSS ways, but it only works for reflected XSS. For stored XSS, no link is sent to user, rather attacker somehow inserts their malicious code in the server database.

Q3

Apart from the obvious username/id, a public key for each user should be collected.

Q4

When capability tickets are handed over to users, extra measures (such as cryptographic MACs) are needed to protect against ticket forgery.

For ACLs, we do not need those measures, since OS itself will maintain and enforce all ACL rules.

Group B

Q1

Secure input handling consists of two parts: input validation and output encoding. The former should be done inbound, as soon as input is received from user. The latter should be done outbound, before the data is included in web page.

Both should be performed for best protection.

Q2

With SMS based OTPs, the server retains the possession of secret seed.

In app-based OTP, the seed has to be transferred to client during app setup so that the app itself may generate the passcode. Hence there is possibility of secret being leaked from the app.

[*Note that despite the above plus point, SMS based OTPs are generally criticized because of SIM swapping attacks and weaknesses in telecom SMS protocols*]

Q3

a)

Unlike other attacks, CSRF is NOT caused due to lack of input validation. Its prevention involves confirming the origin of client's requests (same site or cross site).

b)

No, the whole point of DAC is to give resource owners full control of the permissions. So permissions of each object are at the discretion of owner, not system administrator.