1.

a) A
b) F
c) A
d) A
e) F
f) F
g) A
h) F

4.

- Un atacator modifica un parametru dintr-un URL sau dintr-un form pentru a accesa date la care nu ar trebui sa aiba acces. Aceasta problema poate aparea daca dezvoltatorul ofera acces la diverse obiecte strict bazat pe input-ul utilizatorului (*insecure direct object reference*). Impactul este major, intrucat adversarul poate vizualiza informatii private sau sa actioneze sub identitatea unor alti utilizatori, ducand la scurgeri de date sau actiuni neautorizate. Preventia poate fi realizata prin implementarea unor verificari a autorizarii corespunzatoare, bazata pe “session tokens”.
- Un atacator introduce cod malitios in cadrul unui formular sau al unui parametru URL (*cross site scripting*), care mai apoi va fi executat in browserele victimelor atunci cand pagina web este accesata. Aceasta problema apare atunci cand aplicatia web foloseste input-ul userilor fara sa il valideze sau sa il codifice inainte. Atacatorul poate ajunge sa fure informatii sensibile, precum datele de logare ale victimei, sau sa actioneze in numele victimei (spre exemplu, pentru a face cumparaturi). Pentru ca un astfel de atac sa fie prevenit, dezvoltatorul trebuie sa se asigure ca orice user input este validat si sanitizat (orice caracter nedorit este scos) inainte de a fi folosit mai departe.
- Un atacator introduce comenzi malitioase in cadrul unui formular sau al unui parametru URL, comenzi care sunt ulterior executate de catre aplicatie (*injection attacks*). Aceasta problema apare in aceleasi conditii ca cea anterioara, iar metodele de prevenire sunt similare. Impactul este, de asemenea, major, intrucat atacatorul poate accesa informatii sensibile sau poate modifica / sterge in mod neautorizat date.
- Un atacator pacaleste o victima sa apese pe un link care executa o actiune ce necesita autorizare (*cross stie request forgery*). Problema apare cand aplicatia nu verifica corespunzator ca o cerere a fost facuta in mod intentionat de catre utilizator. Astfel, atacatorul poate provoca utilizatorul sa execute actiuni nedorite, ce pot duce la scurgeri de date sau pierderi financiare.
- Un atacator introduce un URL malitios drept destinatie a unui *redirect* sau *forward*, pacalind victima sa acceseze un site malitios (open redirect attack).

Acest atac poate aparea daca aplicatia nu valideaza destinatia unui redirect sau forward sau daca permite altor entitati sa ofere destinatia. Victima poate fi expusa atacurilor tip phishing sau malware, ducand la scurgeri de date sau alte probleme. Pentru preventie, aplicatia trebuie sa se asigure ca destinatia unui redirect este o pagina de incredere si nu ar trebui sa lase utilizatorii sa ofere aceste destinatii.