Q.1 →

To study Session Management for Web Applications

- Session management refers to the process of securely handling multiple requests to a web-based application or service from single user or entity. Websites and browser use HTTP to communicate, and a session is a series of HTTP requests and transactions initiated by the same user. Typically, a session is started when a user authenticates their identity using a password or another authentication protocol. session management involves the sharing of secrets with authenticated, users and as such, secure cryptographic network communication are essential to maintaing session management scaz

Securing Session Management with veracode

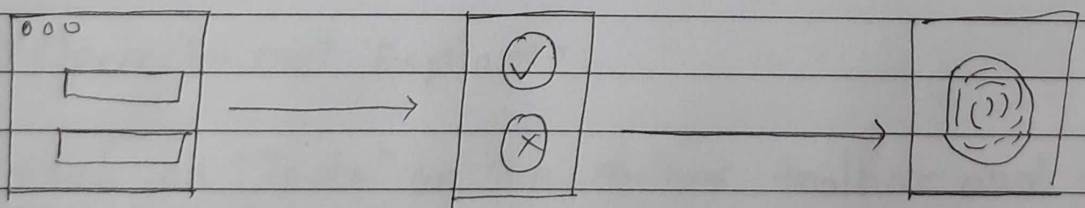
- Vercode provides leading application security testing solutions that help to protect the software driving business today.
- Built on a unified, cloud-based platform, our testing services enables development teams and IT administrators to go beyond the network security firewalls to significantly improve application security without slowing development timelines. With veracode, organization no longer need to choose between speed and security when developing software.

Q.2 Implement identify and authentication controls by applying one of the following security role: ii)

→ ii) Include multi factor authentication

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN MFA is a core component of a strong identify and access management (IAM) policy. Rather than just asking for username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber attack.

Multi factor Authentication



Step1 : Username & password

Step2: Pin from phone app entered

Step 3 Fingerprint verified.

MFA works by requesting additional verification information (factors) One of most common MFA factors that users encounter are one-time passwords (OTP). OTPs are those 4-8 digit codes that

often recieve vial email, SMS or some sort of mobile App with OTPs a new code is generated periodically or each time an authentication request is submitted.

Three Main types of MFA
- Things you know, such as password PIN
- Things you have, such as a badge or smartphone
- Things you are, such as biometric like fingerprint or voice reognition.

Q. 3 Generate Digital Certificate and import it in your browser.

→ Steps to install Digital certificate to web Internet Explorer:

① Open internet Explorer.

② Click on "Tools" on the ~~dollar~~ toolbar and select "Internet Options". If the toolbar is not visible, click the "gear" in the upper-right hand corner and select "Internet Options".

③ Select the "Content tab"

④ Click the "Certificate" button select the "personal" tab and click the "import..." button.

(5) In the "Certificate Import wizard" window, click the "Next" button to start the wizard

(6) Click the "Browse..." button.

(7) Go to the location where you stored your digital certificate and make sure the button next to "File name:" shows "Personal Information Exchange (*.pfx, *.p12)" is selected.

(8) Select the filename you saved the certificate as and click the "Open" button.

(9) Ensure the fileman is correct and click the "next" button in the "Certificate import wizard" window

(10) Enter the PIN or password you used to download the certificate in the "password" text box and secure the second and third check boxes are selected then click the "next" button.

(11) In the window "Completing the certificate Import wizard" verify your information and click the "Finish" button.

(12) You will get a notification window if all steps have been performed properly.