1. OWASP (Open web application security project)

Top 10 vulnerabilities;

1. Injection
2. Broken authentication
3. Sensitive data exposure
4. XML external entities(XXE)
5. Broken access control
6. Security misconfigurations
7. Cross site scripting(XSS)
8. Insecure deserialization
9. Using components with known vulnerabilities
10. Insufficient logging and monitoring

Injection: when attacker uses a query or command to insert untrusted data into interpreter via Sql, NOSQL. The application does something on this data which it is not designed for.

Prevention: using APIs which avoid use of interpreter

Broken authentication: When the authentication module is not implemented properly and attacker can gain access to any users account.

Prevention : MFA, password encryption

Sensitive data exposure: when APIs don’t properly secure sensitive data and the attackers can easily gain access to them like financial data, users personal data, passwords.

Prevention: secure url’s , encrypting sensitive information.

1. SSL- secure socket layer

TLS- Transport Layer security

Used for securing the communication over the computer network. Data is first encrypted and then sent over the network.

TLS is the successor to SSL and provides improved security and efficiency.

TLS used stringer encryption.

SSL is now outdated.

Handshake: When a client connects to a server they exchange information to authenticate each other and establish a secure connection.

Data is encrypted using symmetric encryption which requires a shared secret key.

1. Authentication: To authenticate i.e verify the user trying to access the website.

Used at login/signup.

Authorization: To check whether the user has the permission/authority to access a particular resource.

Example: in an ecommerce website during login step authentication will be used. And authorization will be used when normal users wont be allowed to see the inventory management section but admin will be able to because admin has the permission/authority.

Authentication: userid, password; MFA, Oauth

Authorization: role based, attribute based.

Authorization is responsible.

1. Cookie based authentication: The server generates a session ID corresponding to the user and sends it to the client browser which is stored there in cookies. Session ID is also stored at the server. Whenever the client will send the request the session ID will go with it and will be verified by the server.

So no need to login again and again when the user switches between pages. Just the session ID will be verified by the server and the user will be authenticated.

1. Token based authentication: When the user logs in the server will generate a json web token(JWT) using the user id and will send it to the user which will be stored on the browser. When the user will send request the jwt will go with it and will be decrypted at the server and user id will be extracted. The server will check whether the user id is the same as the user from which the request came.

No need of storing token at the server as in the case of session id. Thus token based is better.

1. Network security group(NSG) provide firewall like functionality to cloud resources. It filters out what type of traffic should be allowed to access the cloud resources. It sits in front of the cloud resources blocking or allowing specific traffic at specific resources.
2. Web application firewall(WAF): A specialized firewall that sits between the application and the internet and filters HTTP/HTTPS requests. Protects applications from threats like SQL injection, XSS, DDoS attacks.

Firewall works at network and transport layer whereas WAF works at application layer. Firewall monitors all the incoming and outgoing traffic from the network whereas WAF works in front of the application protecting it from malicious traffic.

1. Encryption of data is needed to protect the data so that data remains unreadable even if it gets in malicious hands. Proper keys would be needed to decrypt the data.

Symmetric encryption uses a single key to encrypt and decrypt the data. Sender and receiver both would need to have that key.

Asymmetric encryption uses 2 keys- public and private key. Public key for encryption and private for decryption. Sender encrypts the data using the receiver’s public key. It can now be decrypted using only the receiver’s private key.

Data at rest needs to be encrypted so that if the database gets hacked the hacker wont be able to read the data.

Data in transit is encrypted using SSL/TLS so that if the network gets compromised the data should remain unreadable.

1. IAM refers to policies and technologies that manage identities and user access to cloud resources. Authentication, Authorization, Monitoring.

It manages who can access and what he can access.

Principle of least privilege means users should be given minimum access only what is necessary. So that there is no chance of any security breach.

1. OWASP ZAP (Zed attack proxy) automates security testing for websites including testing for common security flaws like cross site scripting(XSS), SQL injections and misconfigurations.