1. **Give an Write up on the topic authorization & CORS ?**

 a. <u>**Authorization:**</u>

   Authorization is a security mechanism to determine access levels or user privileges related to system resources including files, services, computer programs, data and application features. This is the process of granting or denying access to a network resource which allows the user access to various resources based on the user's identity.

   Most web security systems are based on a two-step process. The first step is authentication, which ensures about the user identity and the second stage is authorization, which allows the user to access the various resources based on the user's identity. Modern operating systems depend on effectively designed authorization processes to facilitate application deployment and management. Key factors contain user type, number and credentials, requiring verification and related actions and roles.

b. <u>**CORS:**</u>

   Cross-origin resource sharing (CORS) is a browser mechanism which enables controlled access to resources located outside of a given domain. However, it also provides potential for cross-domain based attacks, if a website's CORS policy is poorly configured and implemented but CORS is not a protection against cross-origin attacks.

   The CORS standard is needed because it allows servers to specify not only who can access the assets, but also how they can be accessed. Cross-origin requests are made using the standard HTTP request methods. Most servers will allow GET requests, meaning they will allow resources from external origins to read their data.