Drupal 10 - HTML & XSS Security Interview Preparation

Q1: What is XSS in Drupal 10?

Answer: XSS (Cross-Site Scripting) ek security vulnerability hai jisme attacker malicious JavaScript code inject karta hai website me. Drupal 10 me agar user input properly sanitize na ho to XSS attack ho sakta hai.

Q2: Drupal 10 me XSS se bachne ke liye kya use karte hain?

Answer: Drupal 10 me Twig auto-escaping feature use hota hai. Iske alawa Html::escape(), Xss::filter(), aur render arrays use karte hain taaki output secure rahe.

Q3: Twig auto-escape kya karta hai?

Answer: Twig by default HTML entities escape karta hai. Jaise <script> ko <script> bana deta hai taaki browser usko execute na kare.

Q4: Html::escape() ka use kya hai?

Answer: Html::escape() PHP side par special characters ko safe HTML entities me convert karta hai. Ye tab use hota hai jab custom module me manually output generate karte hain.

Q5: Xss::filter() kya karta hai?

Answer: Xss::filter() allowed HTML tags ko permit karta hai aur baaki dangerous tags remove kar deta hai. Ye limited HTML allow karne ke liye use hota hai.

Q6: Render Array secure kyu mana jata hai?

Answer: Render array automatically safe rendering karta hai. Direct echo karne ke bajay render array return karna best practice hai Drupal me.

Q7: HTML filtering Drupal me kaise hota hai?

Answer: Drupal text formats use karta hai jaise Basic HTML ya Full HTML. Inme allowed tags define hote hain aur CKEditor bhi isi rule ko follow karta hai.

Q8: Interview me agar pooche safe coding practice kya hai Drupal 10 me?

Answer: Kabhi bhi direct $_GET ya $_POST ko print na karein. Hamesha sanitize karein. Twig templates use karein. Render arrays follow karein. Aur Drupal API ka use karein instead of raw PHP output.