What is the difference between stored XSS and reflected XSS, and how can both be mitigated?

Answer: Reflected XSS happens when an app takes some input from an HTTP request and embeds that input into the immediate response in an unsafe way. With stored XSS, the app instead stores the input and embeds it into a later response in an unsafe way.

How can an attacker exploit SSRF to access internal resources or perform attacks on behalf of the server?

Answer: SSRF attacks, exploit trust relationships to escalate an attack from the vulnerable application and perform unauthorized actions. These trust relationships might exist in relation to the server, or in relation to other back-end systems within the same organization.

Explain the difference between CSRF and SSRF, focusing on their target and execution.

Answer: A CSRF attack targets the user to execute malicious requests on behalf of the attacker. On the other hand, an SSRF attack primarily targets the backend server to read or update internal resources form an external network.