Offensive Approach to Hunt Bugs

XXE

Background Concept XXE

XML Injection is an attack technique used to manipulate or compromise the logic of an XML application or service. The injection of unintended XML content and/or structures into an XML message can alter the intend logic of the application.

Hunting of XXE

- Attempt to inject XML or reserved characters into input parameters and observe if XML parsing errors are generated.
- For web services, check each input parameter specified in the WSDL document for those of type XML.

Hunting for XXE

- Attempt to inject XML or reserved characters into input parameters and observe if XML parsing errors are generated.
- For web services, check each input parameter specified in the WSDL document for those of type XML.
- Use intruder to inject xml payloads to fetch system configuration files