**A4 XML External Entity (XXE)**

* **Leicht Verwundbar, wenn**
  + ein XML-Parser die Spezifizierung von externen Entitäten (d.h. eine URI, die während der XML-Verarbeitung dereferenziert und evaluiert wird) erlaubt
  + eine Applikation XML direkt oder XML-Uploads akzeptiert, insbesondere von nicht vertrauenswürdigen Quellen, und diese XML-Dokumente anschließend von einem XML-Parser parsen lässt
  + eine der XML-Prozessoren in der Applikation oder in den SOAP-basierten Webservices DTDs aktiviert hat
* **Beispiel Attacken**
  + Upload einer schädlichen XML-Datei, mit der der Angreifer
    - versucht, Daten vom Server zu extrahieren
    - etwas über das private Netzwerk des Servers in Erfahrung bringt
    - versucht, einen Denial-of-Service-Angriff zu starten, indem er eine potenziell endlose Datei inkludiert
* **Wie verhindert man Attacke auf verwundbare Stellen der/des Software/Betriebssystems**
  + Bei sämtlichen XML-Parsern in der Applikation die Verarbeitung von externen XML-Entitäten und DTDs deaktivieren
  + Implementierung von Eingabevalidierungen oder Filterung, um gefährliche Daten innerhalb XML-Dokumenten oder Headern zu verhindern
  + Verifizieren, dass XML- oder XSL-Datei-Upload-Funktionalität eingehende XML-Dateien mithilfe von XSD-Validierung validiert
  + Patchen oder Upgraden aller XML-Prozessoren und Bibliotheken, die von der Applikation genutzt werden, oder auf dem zugrundeliegenden Betriebssystem. Die Nutzung von Dependency-Checkern ist entscheidend, um das Risiko von notwendigen Bibliotheken und Komponenten in einer Applikation managen zu können
  + Upgraden von SOAP auf die neueste Version
* **Ziele eines Angreifers (Umgebung und Nutzen)**
  + Offenlegung vertraulicher Daten
  + Denial of Service
  + Remote-Code-Ausführung
* **Gefährdete Personengruppen**
  + Nutzer, die keine Software-Updates ausführen
  + Personen oder Unternehmen, die XML-basierte Webservices besitzen