pratica nel caso di file locali. Nel caso dei remote files non vi è altra soluzione che verificare il contenuto o l'hash del file prima di adoperarlo in qualsiasi modo.

6.1.3 XML external entity (XXE) injection

L' XML external entity injection, o iniezione di entità esterne XML, nota anche come XXE, è una vulnerabilità della sicurezza che consente a un attaccante di manipolare l'elaborazione di dati XML da parte di un'applicazione web. L'attaccante può essere in grado di accedere al file system dell'application server e di interagire con qualsiasi sistema esterno a cui l'applicazione stessa è autorizzata ad accedere. In alcune situazioni, può portare alle estreme conseguenze l'attacco, fino a compromettere il server sottostante o altre infrastrutture di back-end, sfruttando la vulnerabilità XXE e falsificando delle richieste sul lato server (SSRF).
Alcune applicazioni utilizzano il formato XML per trasmettere dati tra il browser e il server. Le applicazioni che lo fanno praticamente utilizzano sempre una libreria standard o un'API della piattaforma per elaborare i dati XML sul server. Le vulnerabilità di XXE sorgono perché la specifica XML contiene varie funzionalità potenzialmente pericolose e i parser standard supportano queste funzionalità, anche se non vengono normalmente utilizzate dall'applicazione.
Le entità esterne XML sono un tipo di entità XML personalizzata i cui valori definiti vengono caricati dall'esterno del DTD in cui sono dichiarati. Le entità esterne sono particolarmente interessanti dal punto di vista della sicurezza perché consentono di definire un'entità in base al contenuto di un percorso di file o URL.
Le entità XML sono un modo per rappresentare un elemento di dati all'interno di un documento XML, anziché utilizzare i dati stessi. Varie entità sono integrate nelle specifiche del linguaggio XML. Per esempio, le entità < e > rappresetano i metacaratteri '<' e '>'. Poiché sono usati per indicare i tag XML, devono generalmente essere rappresentati usando le loro entità quando compaiono all'interno dei dati.
L'XML consente di indicare delle entità personalizzate all'interno del loro DTD di riferimento, come nell'esempio seguente:

```
<!DOCTYPE foo [ <!ENTITY entitaPersonalizzata "entità personalizzazta per usi
interni" > ]>
```

Questa definizione significa che qualsiasi utilizzo dell'entità &entitaPersonalizzata; all'interno del documento XML verrà sostituito con il valore definito: "entità personalizzazta per usi interni".
Se un utente ha la possibilità di intodurre un'entità che si riferisca a una risorse esterna, il parser XML riporterà all'interno dell'applicazione qualsiasi contenuto. Un malintenzionato può così introdurre e far eseguire codice malevolo.
Ad esempio può essere referenziato un percorso URL, che può puntare a un file del sistema operativo (tramite il protocollo file://) o esterno (tramite il protocollo http://).

Esempio:

Entità esterna che espone a vulnerabilità l'applicazione:

```
<!DOCTYPE foo [ <!ENTITY ext SYSTEM "file:///path/to/file" > ]>
```

Se si indica il file /etc/passwd, se ne ottiene l'automatica lettura e inclusione nel documento.

Contromisure

Tutte le vulnerabilità XXE sorgono perché la libreria di parsing dell'XML utilizzata dall'applicazione supporta funzionalità XML potenzialmente pericolose. Il modo più semplice ed efficace per prevenire gli attacchi XXE è disabilitare tali funzionalità.