- Come potrebbe un utente malintenzionato bloccare l'applicazione?
- Come potrebbe un utente malintenzionato ottenere dettagli utili ai propri fini?

Revisione e registrazione (audit):

- Come potrebbe un aggressore coprire le sue tracce?
- Come si può dimostrare che un utente malintenzionato (o un utente legittimo) ha eseguito azioni specifiche?

6.1.4.2 Identificazione delle potenziali minacce annidate nei casi d'uso

Occorre esaminare i casi d'uso chiave, che sono stati individuati nella fasi precedenti, per comprendere il modo in cui un utente potrebbe influenzare premeditatamente o involontariamente l'applicazione ad eseguire un'operazione non autorizzata o a divulgare dati riservati o privati. In questa fase ci si pongono domande immedesimandosi nella figura dell'aggressore. Alcuni esempi di domande da porsi:

- Come può un utente iniettare un input dannoso in un caso d'uso specifico?
- I dati vengono pubblicati in base all'input fornito dall'utente o in base all'input non validato fornito dall'utente?
- In che modo un aggressore potrebbe manipolare i dati della sessione?
- Come potrebbe un utente malintenzionato ottenere dati sensibili quando questi vengono trasmessi attraverso la rete?
- In che modo un aggressore potrebbe eludere i controlli di autorizzazione?

6.1.4.3 Identificazione delle potenziali minacce annidate nei flussi di dati

Occorre rivedere i casi d'uso e gli scenari chiave e analizzare i flussi di dati, in particolare, i flussi di dati tra i singoli componenti dell'architettura. Il flusso di dati che attraversa un confine di fiducia richiede particolare attenzione. Nella stesura del codice, si deve assumere che, tutti i dati esterni al confine di fiducia dell'applicativo siano dannosi. Nel codice si dovrebbe eseguire una validazione dei dati adeguatamente robusta. Per identificare le minacce associate ai flussi di dati, ci si deve porre le seguenti domande:

- Quale è il percorso del flusso di dati dal front-end al back-end dell'applicazione?
- Quali componenti chiamano altri componenti?
- Quale aspetto hanno i dati validi?
- Dove viene eseguita la validazione dei dati?
- Quali sono i vincoli imposti ai dati?
- Come vengono validati i dati in base ai parametri previsti in termini di lunghezza, intervallo di valori, formato e tipo?
- Quali dati sensibili vengono trasmessi tra i componenti dell'applicazione e attraverso le reti, e come vengono protetti durante il transito?

L'uso della documentazione quali ad esempio, i diagrammi DFD e i diagrammi di sequenza UML, aiuta nell'analisi dell'applicazione e nell'identificazione dei flussi di dati.

6.1.4.4 Esplorare ulteriori minacce utilizzando gli alberi delle minacce/attacchi

Vedi Paragrafo 5.5.4.2.

6.1.5 Identificazione delle vulnerabilità

Così come è stato fatto nel processo di identificazione delle minacce, si fornisce di seguito una rassegna delle diverse categorie di vulnerabilità. In questa fase, l'obiettivo è quello di analizzare le