javax.servlet.http.HttpServletRequest) e rigettare le informazioni provenienti da host o link incorretti e/o inaspettati.
Trattamento dei files e degli oggetti embedded. Una servlet non deve mai accettare in input contenuti sottomessi da un utente che contengano tag HTML, tipici dell'iclusione di file od oggetti come: <EMBED>, <OBJECT> e <SCRIPT>.

Come già evidenziato altrove, tutte le eccezioni che si verificano durante l'esecuzione delle servlet che costituiscono l'applicazione web devono essere catturate e gestite opportunamente. I relativi mesaggi di errore sollevati (es. dump di databse o codici di errore - out of memory, null pointer exceptions, system call failure, database unavailable, network timeout), devono essere visualizzati verso l'utenza in accordo ad uno schema ben dettagliato: agli utenti generici devono essere inviate le informazioni minime in grado di aiutarli nella comprensione degli errori stessi (senza rivelare dettagli superflui), mentre le informazioni sulla diagnostica devono essere inviate per la visualizzazione esclusivamente agli amministratori dell'applicazione. Il meccanismo di gestione errori deve essere in grado di gestire ogni tipo di dati in ingresso e di garantire la sicurezza. Devono essere previsti dei messaggi di errore semplici, in grado di indicare la causa. I tentativi d'intrusione devono essere registrati nei file di log, qualunque ne sia l'esito, in modo tale da poterli verificare in un secondo tempo. La gestione degli errori non deve essere concentrata soltanto sui dati forniti in ingresso dall'utente, ma deve includere anche tutti gli errori che possono essere generati da componenti interni come system call, query sul db o altre funzioni interne.
Anche il risparmio delle risorse macchina una buona prassi. Ove possibile,implementare meccanismi che consentono di limitare al massimo il numero di risorse allocate per ogni singolo utente. Per gli utenti auntenticati, è possibile fissare una quota in modo da poter limitare il carico massimo che un utente può applicare al sistema. Per gli utenti non autenticati, si dovrebbero evitare tutti gli accessi che comportino query e la possibilità di utilizzare altre applicazioni avide di risorse ritenute superflue, mantenendo ad esempio in una cache il contenuto dei dati ricevuti da questi utenti invece di eseguire delle nuove query sul DataBase.

7.3 PL/SQL

PL/SQL (Programming Language / Structured Query Language) è un linguaggio di programmazione che viene implementato su un Oracle RDBMS. PL/SQL è in grado di utilizzare gli oggetti messi a disposzione dal RDBMS Oracle, poiché è stato realizzato "su misura" per tali oggetti.
I maggiori database relazionali di altri produttori includono linguaggi di programmazione simili a PL/SQL di Oracle, anch'essi in grado di utilizzare le specificità degli oggetti a loro disposizione per incrementare la produttività e creare processi elaborativi automatizzati efficienti. Sybase e Microsoft SQL Server utilizzano Transact-SQL, IBM DB2 utilizza SQL procedural Language, PostgreSQL supporta PL/pgSQL, ecc.

7.3.1 Cross-site scripting (XSS)

Come riconoscerla

Il Cross Site Scripting consiste nella possibilità di inoculare uno script e di mandarlo in esecuzione sul front-end dell'applicazione. Tramite tecniche sviluppate da malintenzionati per ottenere informazioni personali, possono, ad esempio, essere simulate pagine quasi identiche ad altri siti molto frequentati per ottenere informazioni riservate. La prassi del "social engineering" consente di ingannare gli utenti per indurli a visitare pagine fraudolente. Gli attacchi XSS di tipo reflected si verificano ogni qualvolta uno script viene inoculato ed eseguito nel periodo in cui dura la sessione. Gli XSS stored, viceversa, sono script malevoli che sono stati memorizzati su una base dati e vengono pertanto incorporati nella pagina (e quindi eseguiti) ogni volta che qualcuno ne fa richiesta.
Siamo di fronte ad DOM based XSS se i dati malevoli, contenenti tag HTML e script, vengono incorporati direttamente nell'HTML della pagina, in modo che il browser visualizzerà queste informazioni come parte della pagina web eseguendo in maniera silente gli script. Chi visualizza la pagina modificata in modo fraudolento non sarà in grado di riconoscere l'inganno.