7.1.8.14 Chiamate a funzioni

- Ogni chiamata a fprintf() deve avere il suo argomento FILE pointer inizializzato;
- Ogni chiamata a funzione deve contenere i parametri corretti, coerenti con il tipo e il formato del prototipo della funzione.

7.1.8.15 Files

- Ogni nome di file temporaneo deve essere unico e non predicibile;
- Ogni file deve essere chiuso prima di essere riutilizzato (Esempio: fclose()).

7.1.8.16 Gestione degli errori

- I valori di ritorno di tutte le chiamate di sistema devono essere controllati per determinare lo stato di esecuzione del programma. Funzioni come perror(), ferror() ed strerror() e la costante errno devono essere utilizzate per determinare o riportare all'utente il tipo di errore occorso;
- errno non deve essere dichiarato manualmente come un extern se risiede in uno degli include dell'implementazione C/C++ utilizzata;
- Al verificarsi di un errore critico o imprevisto, a seguito di una chiamata di sistema, tutti i puntatori e le aree di memoria utilizzate devono essere dereferenziati/disallocate prima della chiusura del programma.

7.1.8.17 Sicurezza dell'applicazione

- I risultati dei controlli, delle procedure di sicurezza e i relativi dati non devono risiedere in memoria per lunghi periodi. Ad esempio, le chiavi crittografiche devono permanere in memoria solo per il tempo necessario al loro utilizzo e devono essere sovrascritte con dati casuali o "garbage data" al termine del loro impiego;
- I dati critici non devono mai essere serializzati.

7.2 Java

Java è un linguaggio di programmazione orientato agli oggetti, derivato dal C++ e progettato a partire dal 1991 da James Gosling assieme ad un gruppo di dipendenti di Sun Microsystems. Il suo duraturo successo è da attribuire al suo orientamento verso il mondo web, al suo modello object oriented e alla sua peculiarità di poter esserere eseguito su qualsiasi sistema operativo, mediante l'esecuzione di un bytecode, un intermedio di compilazione, su virtual machine.
Java si è rivelato vincente, oltre che nello sviluppo di applicazioni web, anche nella progettazione di applicazioni client-server e nello sviluppo di web services.
Nel 2010 Oracle Corporation ha rilevato Sun Microsystems, continuando a sviluppare il linguaggio Java, apportamdovi migliorie rilevanti, che lo rendono un linguaggio potente, flessibile e al passo coi tempi.

Di seguito le principali vulnerabilità e le relative contromisure da adottare.

7.2.1 Cross-site scripting (XSS)

Come riconoscerla

Reflected XSS. Si tratta di inoculare e far eseguire script dannosi all'interno di una pagina web. Il mezzo attraverso il quale quest'attacco viene perpetrato è la contraffazione dell'input.
Quando l'input viene racchiuso nella risposta senza esser filtrato, siamo in presenza di un reflected XSS.
Stored XSS. In questo caso il codice HTML o lo script incorporato attraverso l'input viene memorizzato permanentemente sulla pagina e diventa parte integrante di essa. Dopo un attacco riuscito, tutti gli utenti che accederanno alla pagina saranno potenzialmente vittime dello script installato abusivamente.
Si pensi, ad esempio, a un blog che consente di inserire dei commenti o delle recensioni. Se non vi è alcun controllo sull'input utente, tag html e script inseriti da un attaccante diverranno parte integrante della pagina, una volta che il commento sarà pubblicato.