EterNet Team

Vulnerability Assessment

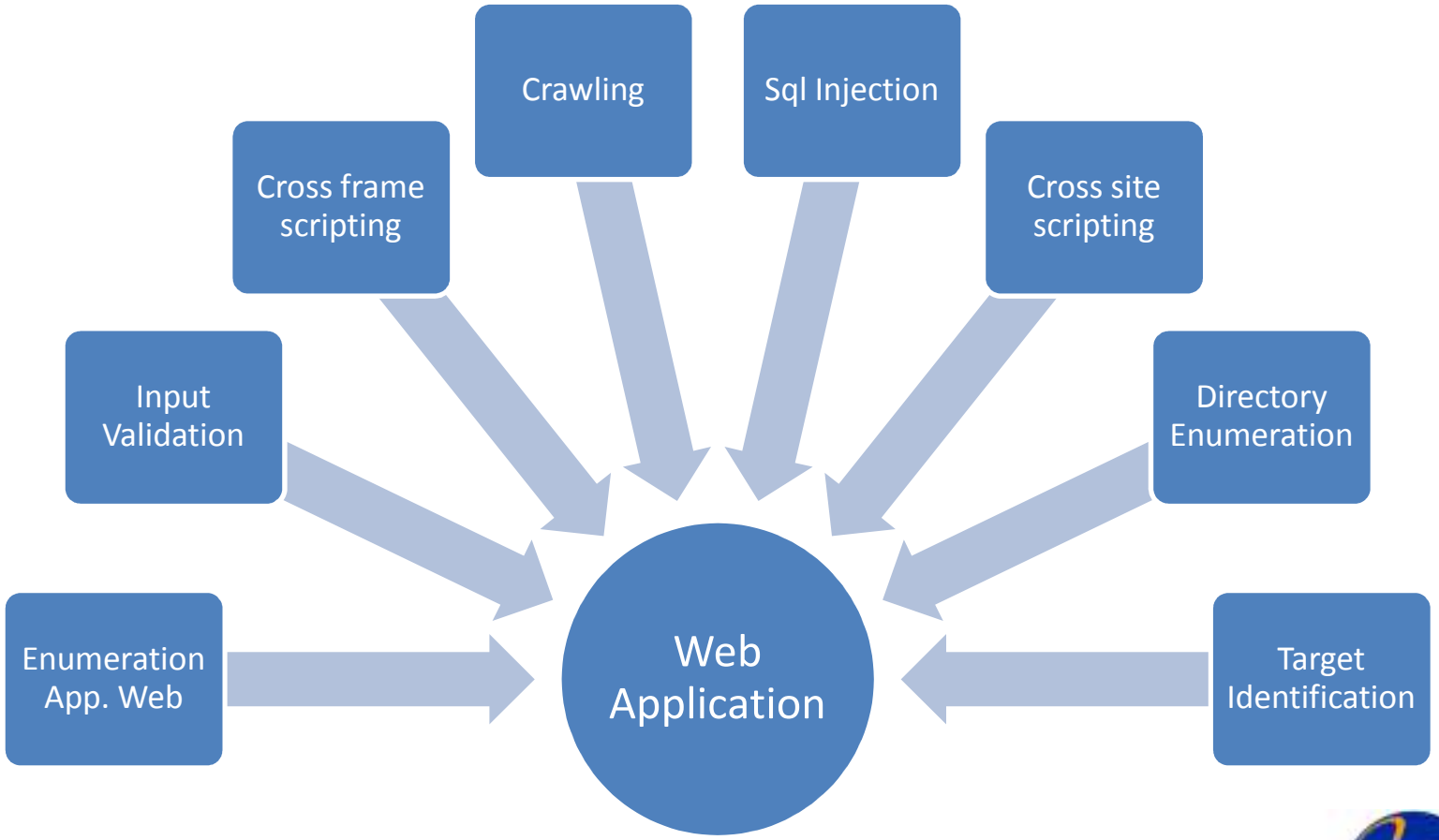
Il vunerability assessment ricerca i punti deboli di un sito internet e del server che lo ospita .

Utilizzando tecniche di hacking manuali si ricercano vulnerabilità sul codice sviluppato .

Tramite software specifici si vanno a ricercare (tramite la cattura dei banner) le informazioni relative al web server.

Con il consenso preventivo , si genera un attacco verso il web server e la web application (utilizzando tool specifici), nel tentativo di ricercare le eventuali vulnerabilità .

Vulnerability Assessment



Enumeration Web Application

La fase di enumeration dell'applicazione web, è mirata a :

Tentativo di accesso a file o directory che non dovrebbero essere rilasciati con l'applicazione web sviluppata.
Ricerca pagine web relative a manuali, esempi sul codice, riferimenti , changelog .

Sql Injection

Sql Injection è una tecnica utilizzata per :

Ricercare informazioni all'interno del database, sfruttando i dati inseriti dai client in query SQL senza prima filtrare i caratteri illegali.

Cross Site Scripting

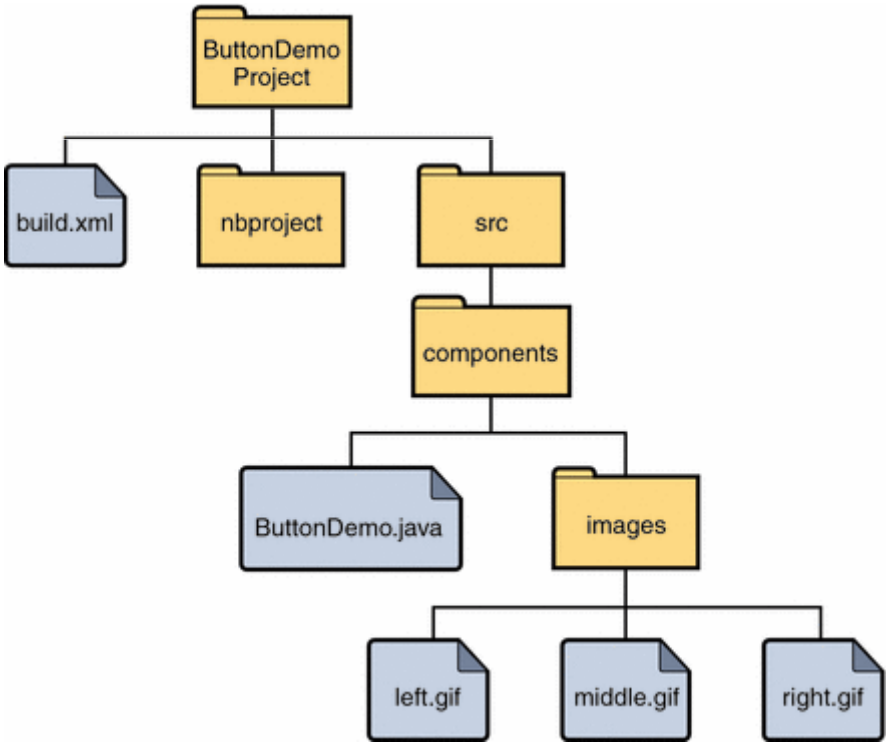
Cross site scripting è una tecnica utilizzata per :

Installare codice dannoso sul server, il cui fine è quello di lanciare attacchi verso terzi, carpire informazioni riservate, bloccare l'applicazione ed il server dove è ospitata.

Directory Enumeration

Directory enumeration è una tecnica utilizzata per :

Ricercare url raggiungibili ed utilizzabili da internet e non controllati dall'applicazione, tentando di eseguire dei comandi all'interno dell'url.



Input Validation

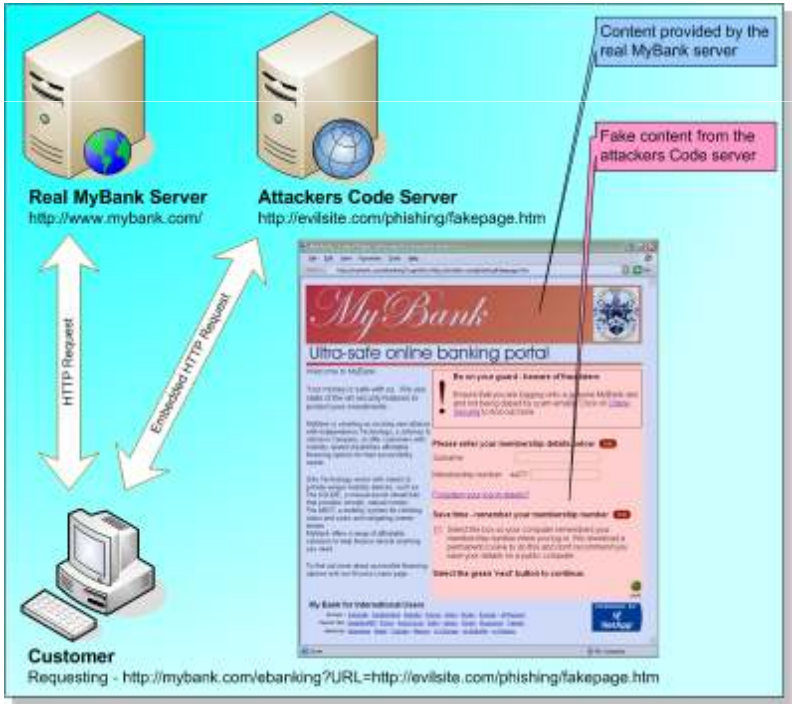
Input Validation è una tecnica utilizzata per :

Tentare l'inserimento di dati non validi all'interno di una form, come per esempio scrivere una stringa di da superiore alla lunghezza massima prevista, oppure introducendo dei caratteri speciali.

Cross Frame Scripting

Cross frame scripting è una tecnica utilizzata per :

Eseguire attacchi di tipo phishing, forzando un utente a credere di navigare in un sito legittimo, passando invece attraverso un sito sotto il controllo dell'hacker.



Crawling

Il crawling consiste nell'effettuare, mediate appositi strumenti, una copia locale dell'intera struttura del sito e la sua analisi off-line, questo ci permette di :

Ricercare commenti in cui gli sviluppatori oppure i sistemi automatici di publishing lasciano evidenti informazioni sulla macchina o sui meccanismi utilizzati.

Errori o inconsistenze, come per esempio link errati che indicano uno sviluppo errato o manutenzione inadeguata

Target Identification

L'attività di Target identification è volta alla ricerca di informazioni relative al tipo di web server utilizzato (attraverso i banner) al fine di sviluppare un attacco piu' mirato.