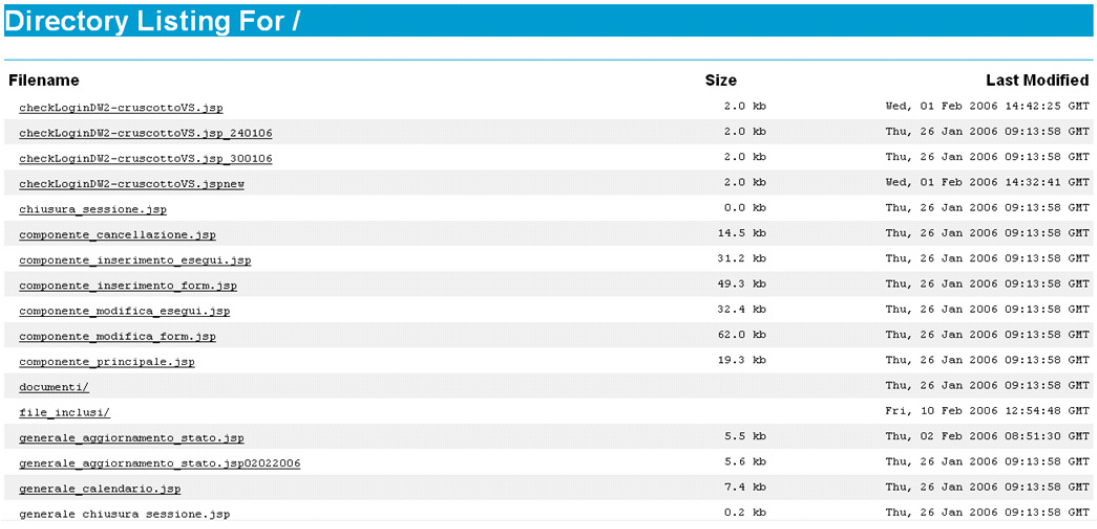
L'esempio di cui sopra mostra come l'applicazione (a seguito di condizioni mal gestite) fornisce messaggi informativi o di errore contenenti dati o informazioni (server type –nginx-, versione ed il S.O. -Ubuntu-) che possono agevolare l'aggressore.

Contromisure

Per evitare di divulgare importanti informazioni, utilizzabili da eventuali attaccanti, è necessario configurare l'application server in modo tale che, nelle intestazioni http di risposta non vengano fornite informazioni quali ad esempio: server type (in questo caso *ngix*), nome e/o release del sistema operativo.
Per tale finalità, prima di sviluppare l'applicazione è fondamentale analizzare le possibili minacce (threat modeling). L'analisi consente di individuare in maniera più puntuale gli elementi a rischio, che potrebbero portare alla divulgazione d'informazioni utili ad un eventuale attaccante.

6.4.3 Directory Listing

Le problematiche di directory listing sono molto comuni nelle applicazioni Web, anche se non unicamente circoscrivibili a quest'ambito. Si manifestano quando un aggressore riesce con apposite richieste a visualizzare il contenuto di una directory, prelevando file dal suo interno o visualizzando dati che dovrebbero di norma essere preclusi agli utenti non autenticati o che non dispongono di specifici privilegi. Comunemente un aggressore riesce a sfruttare questo tipo di problematiche facendo leva su configurazioni applicative errate.
Esempio di una sessione Directory Listing:



Contromisure

I web sever prevedono l'opzione di abilitare/disabilitare il directory listing. Occorre fare attenzione che il default non sia l'abilitazione, nel qual caso impostare la disabilitazione.

6.4.4 Denial of Service (DoS)

Traduzione di "negazione del servizio", un denial of service è una condizione che causa, a seconda di specifiche circostanze, il blocco, la sospensione o il rallentamento dell'applicazione, di un suo singolo processo, di un'unica componente o dell'intero sistema. Ciò è determinato dal tipo di integrazione dell'applicazione stessa con il kernel, le sue strutture e dai privilegi con i quali viene eseguita. Una