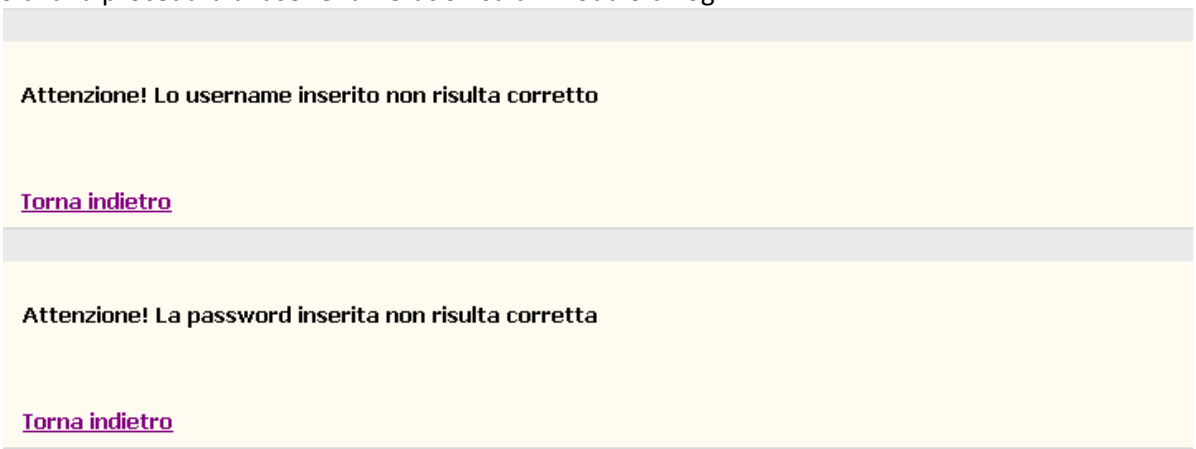
```
java.util.concurrent.ThreadPoolExecutor.runWorker(Unknown Source)at
java.util.concurrent.ThreadPoolExecutor$Worker.run(Unknown Source)
java.lang.Thread.run(Unknown Source)
One or more listeners failed to start. Full details will be found in the
appropriate container log file
```

Di seguito vengono trattate le tecniche più comuni che possono causare l'insorgere delle problematiche descritte nei punti precedenti.

6.4.1 User Enumeration

Consiste nel tentativo, da parte di un attaccante, di indovinare, attraverso un attacco di brute force, l'esistenza di determinate utenze. Questa vulnerabilità è presente su quei servizi o quelle applicazioni che non gestiscono opportunamente le condizioni di errore durante le fasi di login e/o interrogazione, ritornando messaggi specifici e non generici. Gli attacchi di user enumeration colpiscono prevalentemente i portali web, seppur l'ambito di sfruttamento non sia unicamente circoscrivibile a questo genere di ambienti. Le applicazioni o i servizi soggetti a tale problematica vengono stressati da un aggressore con apposite richieste. In base alle risposte ottenute, l'aggressore è in grado di determinare quali siano le utenze valide e quali quelle inesistenti nel sistema/portale. La possibilità di determinare gli utenti regolari, gli permetterà di utilizzare le informazioni acquisiste come base di partenza per attacchi intrusivi più precisi e mirati. Ad esempio, se a seguito di un processo di autenticazione, in risposta alla sua richiesta di login, ottiene il messaggio specifico "Nome Utente Errato", ne conclude che l'utenza utilizzata non esiste; viceversa, se la risposta ritornata è "Password Errata" viene provata invece la sua esistenza. Condizioni simili possono essere riscontrate non solo nei processi di autenticazione, ma anche di registrazione di un nuovo utente, di recupero password o in applicazioni server per lo scambio di posta elettronica.

Esempio:
Risultato di una procedura di user enumeration su un modulo di login:



Contromisure

In nessun caso di errore, l'applicazione deve mostrare pagine di dettaglio dell'errore. L'utente deve essere rinviato su una pagina generica che mostra le informaizoni minime.
I messaggi d'errore devono essere il più generico possibile, per non dare ad un eventuale attaccante informazioni preziose che ne facilitino l'opera. Nel caso mostrato, il messaggio potrebbe essere: "Attenzione! Lo username o la password inseriti non risultano essere corretti". Per gli utenti con profilo Amministratore non deve essere consentito l'utilizzo di user name intuitivi quali "Admin", "Administrator", "Superuser" e simili.

6.4.2 Information disclosure

Le problematiche d'information disclosure sono molto comuni nelle applicazioni Web anche se non unicamente circoscrivibili a questo ambito. Si manifestano quando un aggressore riesce con apposite richieste a sollecitare una condizione non prevista o mal gestita dall'applicazione che ritorna messaggi

informativi o di errore contenenti dati o informazioni che possono agevolarlo nella pianificazione di nuovi attacchi intrusivi. Non tutte le condizioni d'information disclosure sono causate da richieste o eventi non correttamente gestiti dall'applicazione. Alla radice di problematiche simili possono anche esservi script o componenti mal progettati che, interrogati opportunamente con richieste regolari, possono fornire all'aggressore spunti utili per proseguire nella sua attività intrusiva. Sono classificabili come derivanti da problematiche d'information disclosure le seguenti informazioni rilasciate dall'applicazione ad utenze anonime o non autorizzate, a seguito di richieste malevole o regolari:

- I dati che svelano il percorso o i percorsi su disco in cui gli script o le componenti dell'applicazione sono stati installati e risiedono;
- I dati correlabili allo stato attuale dell'applicazione, alla sua versione e agli eventuali moduli o plug-in installati;
- I dati correlabili ai log delle attività manutentive svolte sull'applicazione;
- Tutti gli altri dati eventualmente svelati che per l'organizzazione hanno valenza critica, personale o sensibile;
- etc.

Le applicazioni compilate con l'opzione debugging o verbose possono essere più facilmente soggette a problematiche di information disclosure. Molte di queste condizioni si verificano inoltre a causa di una poco accorta gestione dell'input utente (vedasi ' Validazione dell'input' e relativi sottoparagrafi).

Esempio di default script web soggetto a information disclosure: