Guida della vulnerabilità
Security Misconfiguration

Introduzione

Questa è la guida della vulnerabilità di tipo **Security Misconfiguration**, seguendo questa guida riuscirai a sfruttare la vulnerabilità all'interno di HackerLab.

Questo tipo di vulnerabilità permette ad un malintenzionato di poter accedere a messaggi di errore destinati solamente nell'ambito di sviluppo di un applicativo, in generale sfruttare falle presenti nei file di configurazione di default dei software (credenziali di default, messaggi di errore, …).

Requisiti

- Browser (Nella guida viene utilizzato Chrome)
  - https://support.google.com/chrome/answer/95346

Guida

Questa vulnerabilità è molto basilare e comune nell'ambito dello sviluppo web. In questo caso HackerLab è stato messo in produzione con file di configurazione destinati alla versione di sviluppo. Sono dunque abilitati messaggi di errore in modalità verbosa che permettono ad un utente qualsiasi ti poter generare un errore e leggere alcune informazioni riservate solamente agli sviluppatori dell'applicativo stesso. Per causare un errore all'interno di HackerLab basterà visitare l'account di un utente inesistente. Il percorso per visitare i profili degli utenti è il seguente: /profile/ID, per generare un errore sarà quindi sufficiente inserire un ID inesistente. Per esempio accedendo al percorso con l'ID -1 genererà un errore.

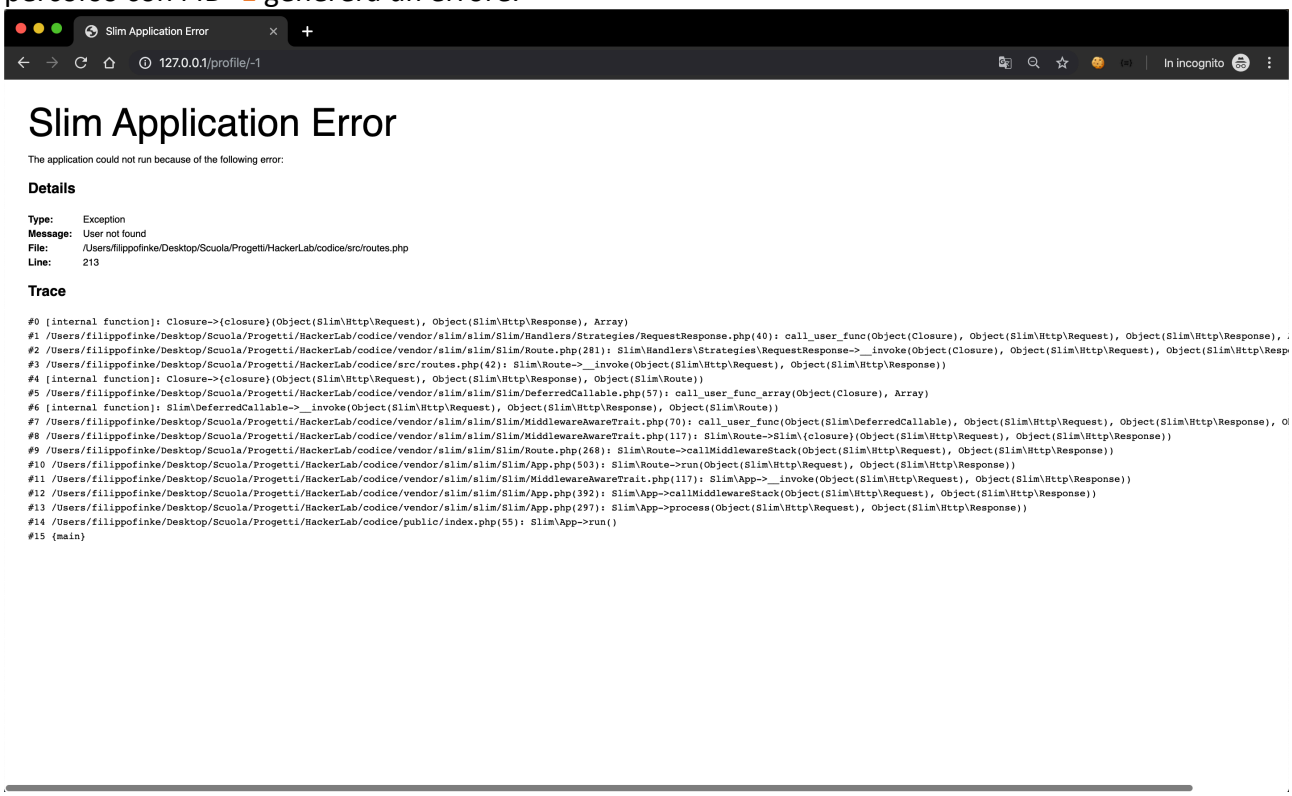

Figura 1 Generazione errore.

Come possiamo notare è stato generato un errore che non viene gestito dall'applicativo. Da questo errore possiamo ricavare molte informazioni utili da poter utilizzare per la ricerca di vulnerabilità mirate sull'applicativo. Per esempio grazie a questo errore possiamo notare che per lo sviluppo del sito web è stato utilizzato un framework chiamato Slim inoltre possiamo anche determinare il percorso del sito web e altre informazioni utili.
Solitamente per arrivare a trovare vulnerabilità di questo tipo bisogna cercare qualsiasi pagina dinamica che accetti parametri da parte dell'utente e passare valori che lo sviluppatore non ha pensato di controllare.