Guida della vulnerabilità
Insecure Direct Object References

Introduzione

Questa è la guida della vulnerabilità di tipo **Insecure Direct Object References**, seguendo questa guida riuscirai a sfruttare la vulnerabilità all'interno di HackerLab.

Questo tipo di vulnerabilità permette ad un malintenzionato di poter accedere direttamente alle risorse del sistema, come per esempio accedere a tutti i dati di un database attraverso all'identificativo di ogni riga salvata in esso.

Requisiti

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

Guida

Per eseguire questa vulnerabilità è richiesto solamente un browser in quanto molto semplice e basilare. In questo caso basterà recarsi nella home di HackerLab e procedere selezionando un articolo (è indifferente quale verrà selezionato), per proseguire si dovrà però aver eseguito l'accesso all'interno dell'applicativo.

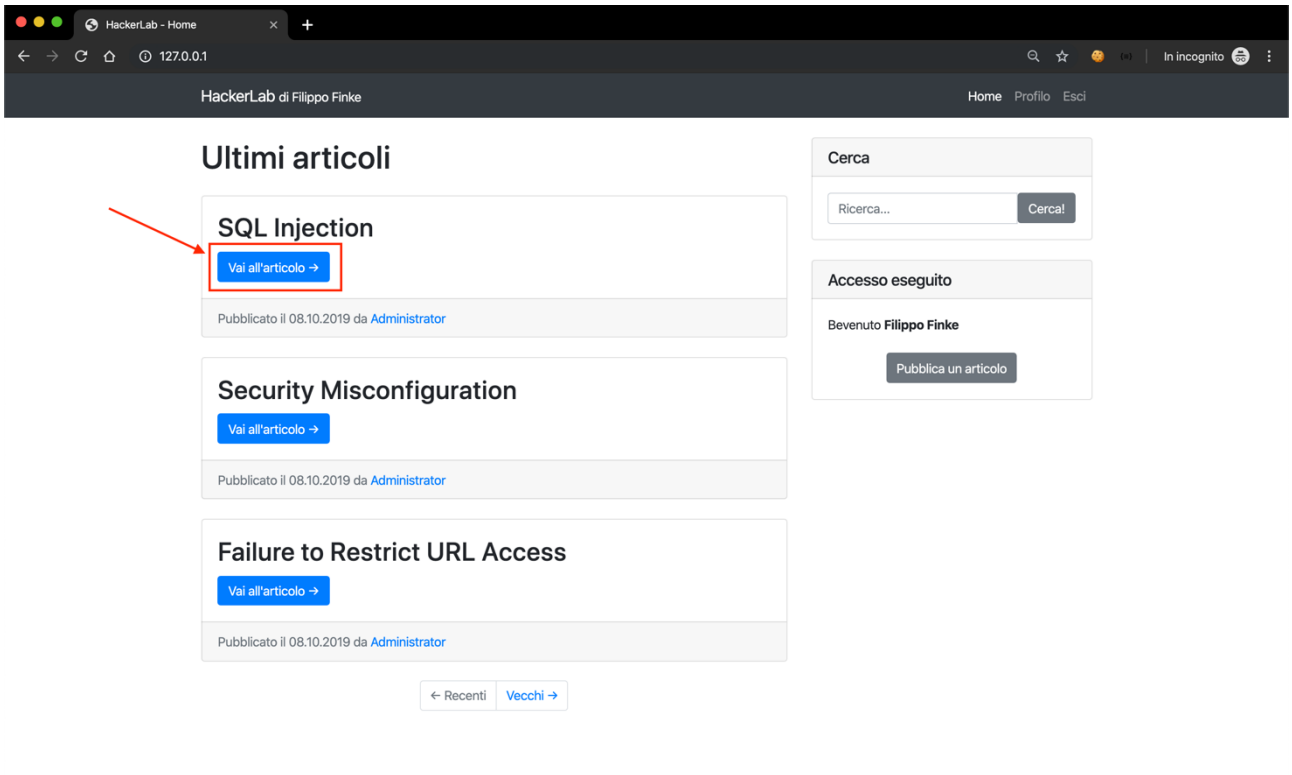

Figura 1 Apertura di un articolo.

Una volta aperto l'articolo ci troveremo nella modalità di lettura di esso. Potremo notare che l'indirizzo al quale si accede per la visione è composto nel seguente modo: /post/numero
In questo caso possiamo assumere che il numero che si passa come percorso sia l'identificativo effettivo presente all'interno del database utilizzato per distinguere i vari articoli.

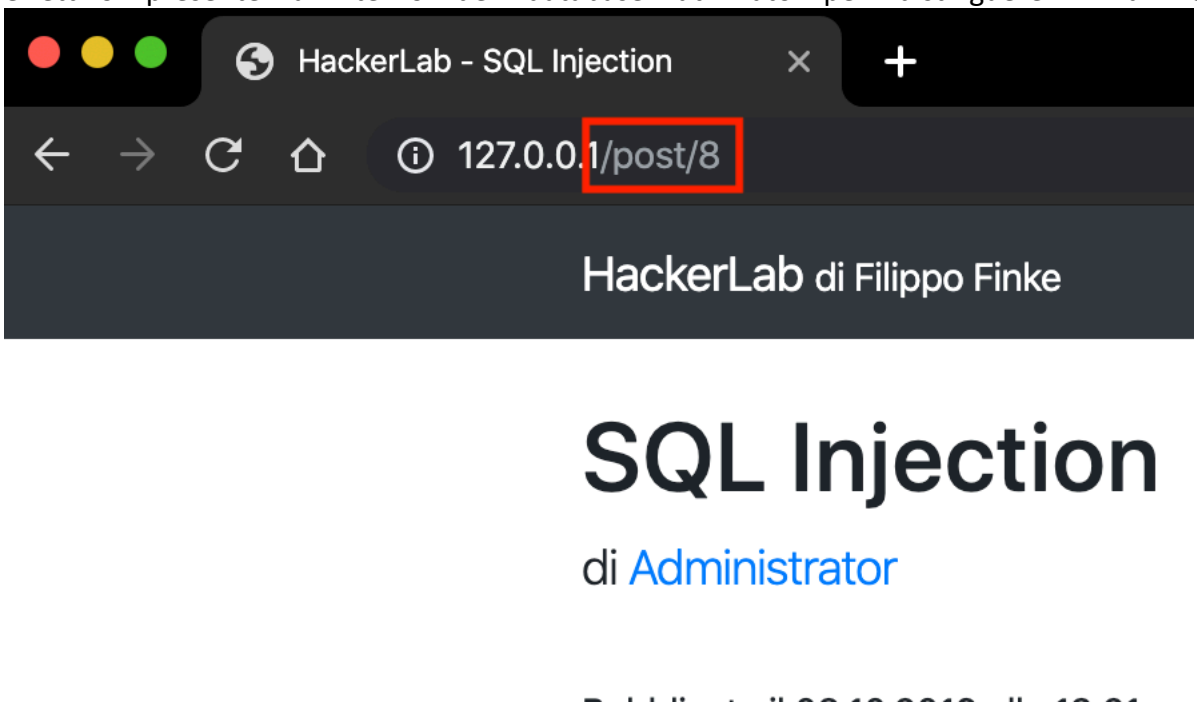

Figura 2 Indirizzo dell'articolo.

Quindi per eseguire questa vulnerabilità non ci resterà altro che provare ad inserire dei numeri interi. In questo caso essendo al numero di articolo 8 ci possiamo aspettare che ci sia un articolo al numero 7,6,5 e così via.
Quindi provando ad accedere all'indirizzo /post/7 possiamo notare come ci viene mostrato un altro articolo presente all'interno del sito web.

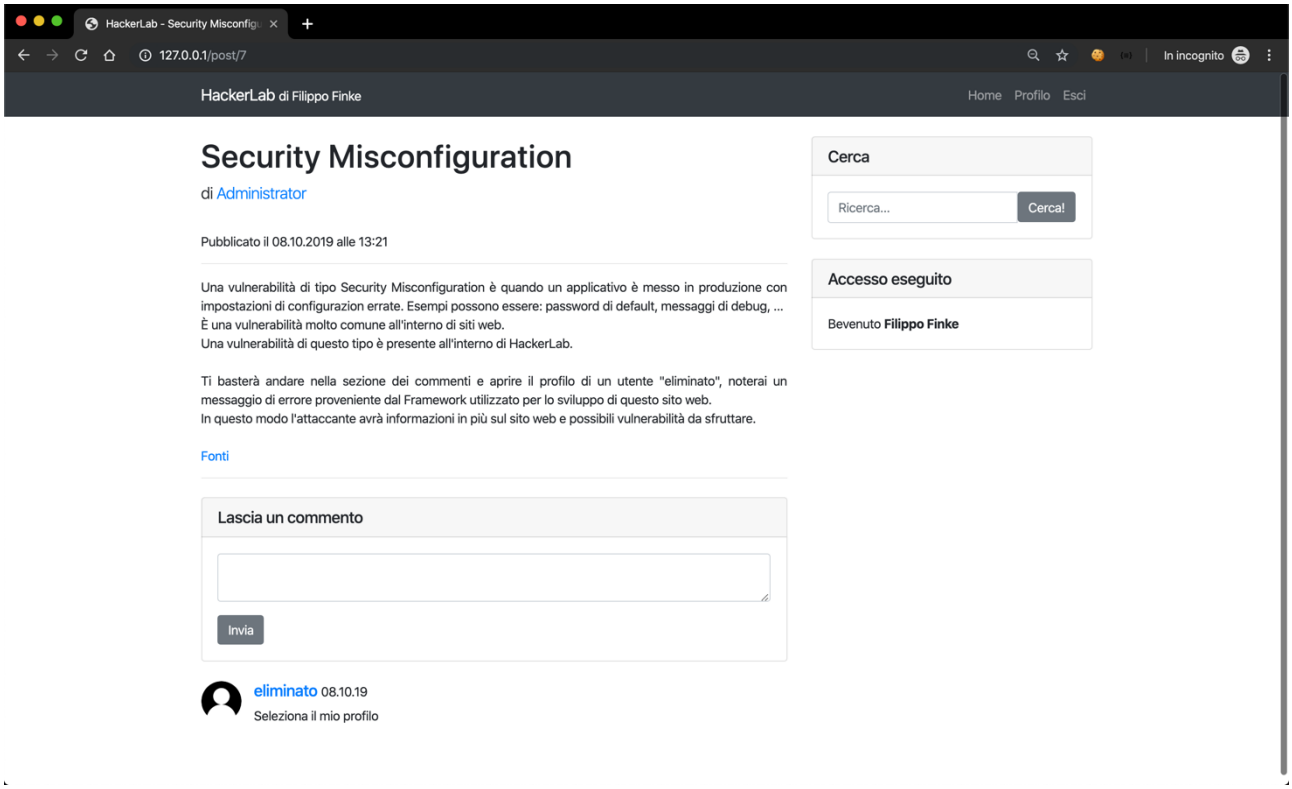

Figura 3 Articolo al percorso /post/7

Questa vulnerabilità è inoltre presente anche nella gestione dei profili. Per accedere alla pagina di profilo di un altro utente ci basterà selezionarlo dalla sezione dei commenti oppure dall'autore.

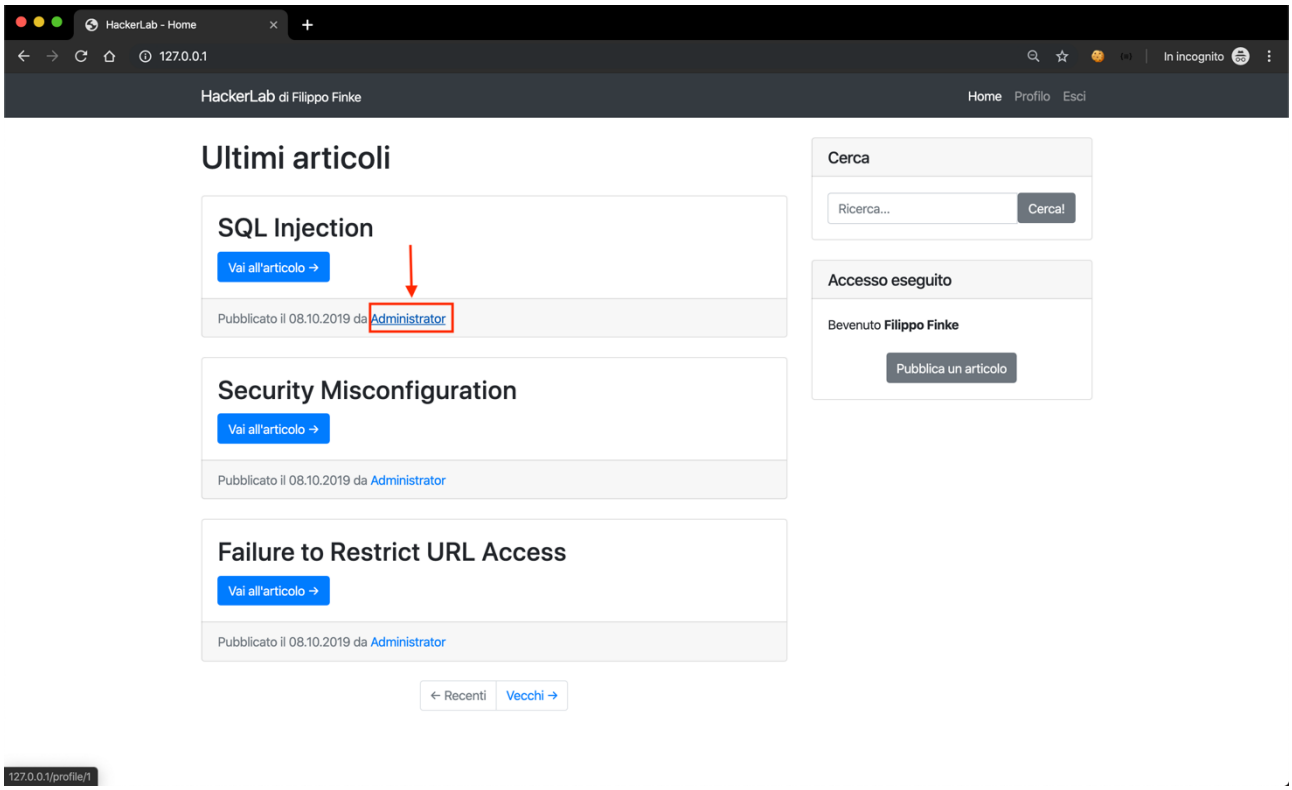

Figura 4 Apertura del profilo di Administrator

In questo caso ho selezionato il profilo di "Administrator" sono quindi stato portato ad una pagina con percorso /profile/1.

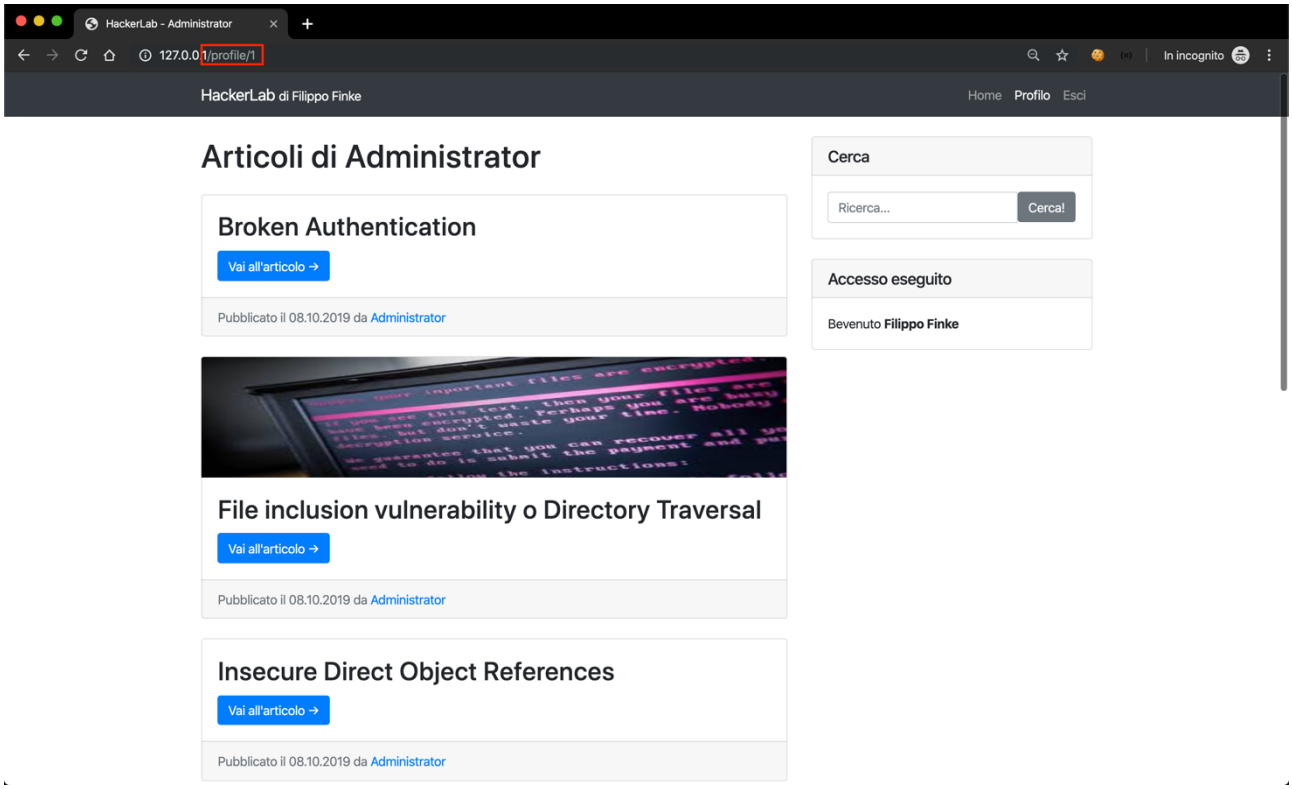

Figura 5 Pagina profilo di Administrator

Possiamo quindi presumere, come per gli articoli, che il numero finale sia l'identificativo dell'utente. Quindi provando a mettere per esempio un profilo con identificativo /profile/2 possiamo notare come ci troviamo nella pagina profilo di un altro utente.

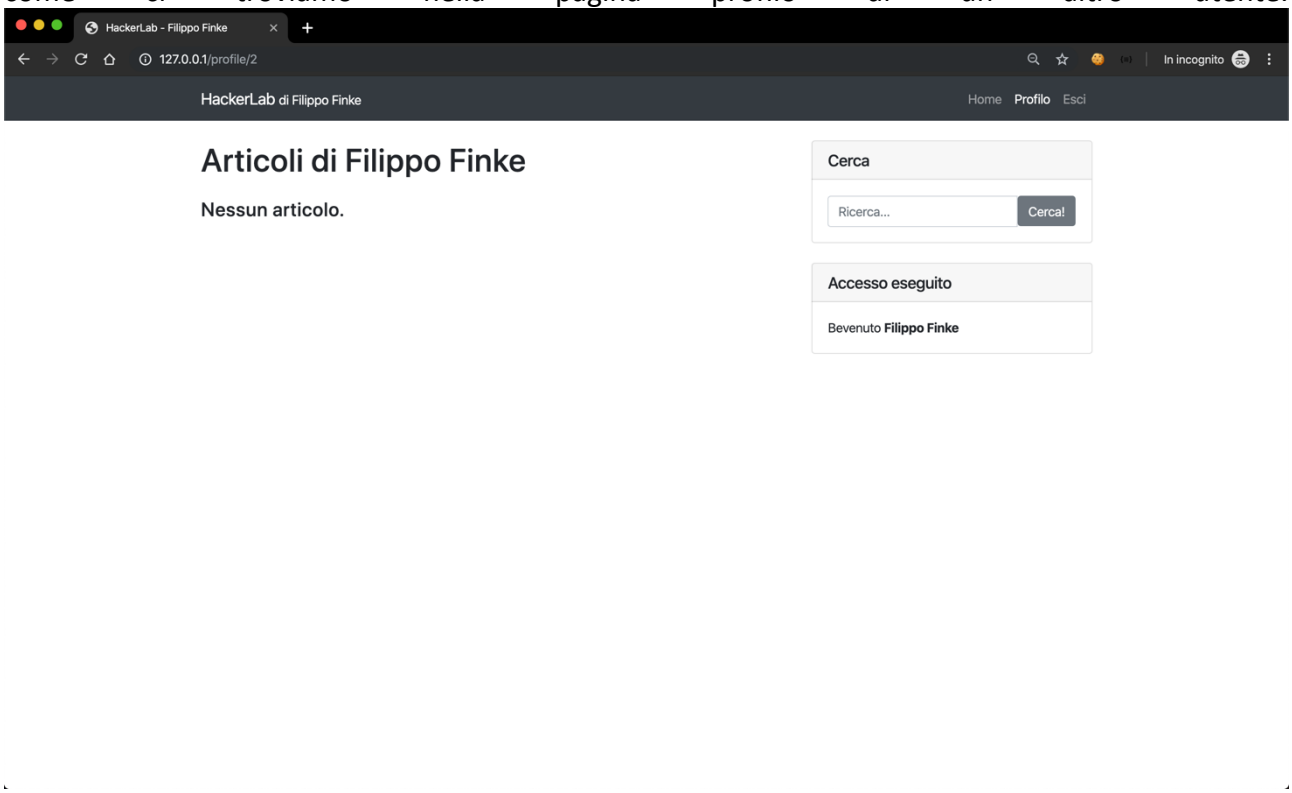

Figura 6 Pagina profilo al percorso /profile/2

Possiamo notare come il profilo sia di un altro utente (in questo caso il mio stesso).

Le conseguenze di questa vulnerabilità mischiate con altre vulnerabilità possono essere pericolose. Per esempio utilizzando questa vulnerabilità è possibile salvare tutti i nomi e cognomi degli utenti registrati all'interno del sito web. Utilizzando questa vulnerabilità assieme ad una falla di tipo Broken Authentication è possibile scaricare anche gli indirizzi email in aggiunta al nome e cognome degli utenti registrati all'interno del sito web. Questo è quindi molto pericoloso per dati sensibili.