Guida della vulnerabilità
Broken Authentication

Introduzione

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

Questo tipo di vulnerabilità permette ad un malintenzionato di poter modificare, intercettare o bypassare i metodi di autenticazione utilizzati da un'applicazione web.

Requisiti

- Browser (Nella guida viene utilizzato Chrome)
  - https://support.google.com/chrome/answer/95346
- Estensione per la modifica di cookie (Nella guida viene utilizzata l'estensione EditThisCookie)
  - https://chrome.google.com/webstore/detail/editthiscookie/fngmhnnpilhplaeedifhccceomclgfbg

Guida

Una volta nella schermata principale, sarà necessario eseguire l'accesso all'interno del sito web. Dopo aver eseguito l'accesso sarà possibile utilizzare l'estensione per la modifica di cookie per leggere i cookie utilizzati da HackerLab.

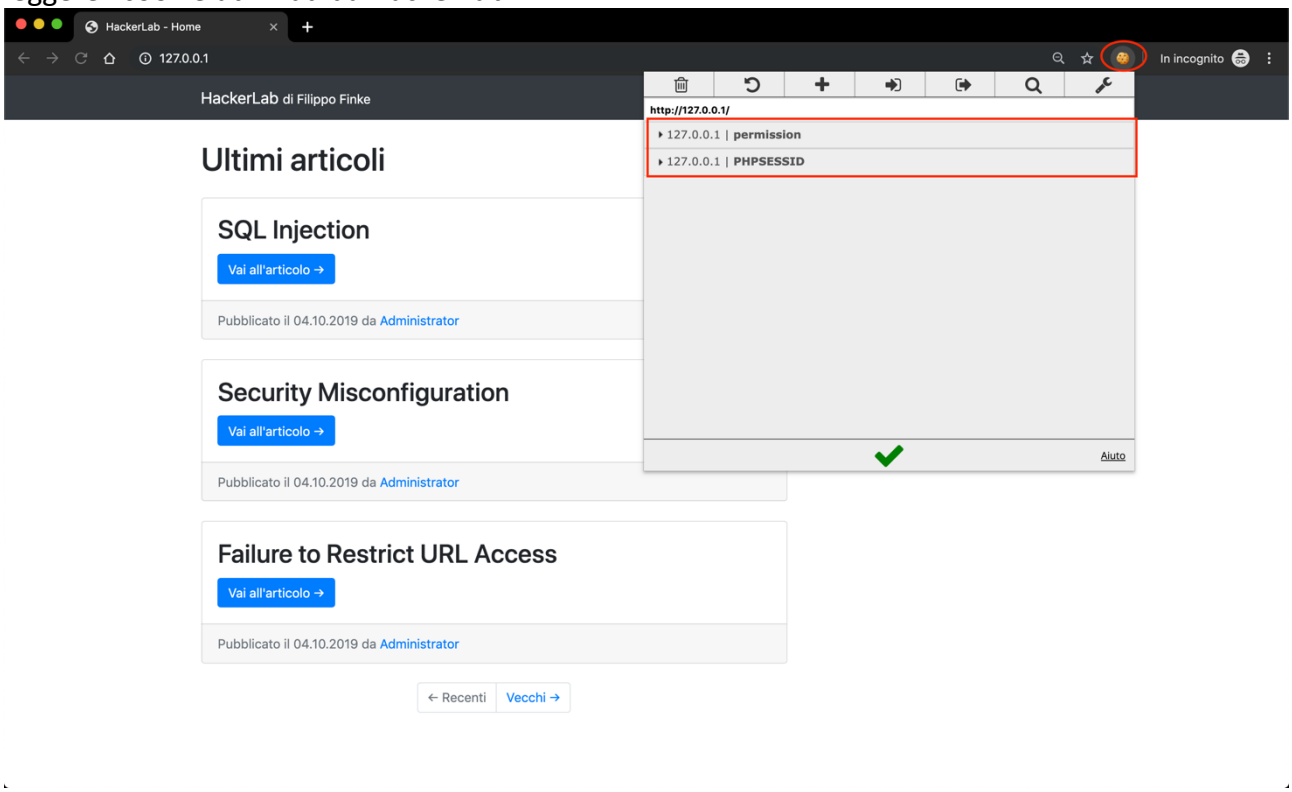

Figura 1 Visualizzazione dei cookie

Aprendo l'estensione possiamo notare la presenta di due cookie, permission e PHPSESSID.
Il cookie PHPSESSID è utilizzato per la gestione delle sessioni attraverso il linguaggio PHP, il contenuto di questo cookie è codificato in modo che non possa essere alterato. Per sfruttare questa vulnerabilità si utilizzerà il cookie chiamato permission.
Quindi proseguiamo leggendone il contenuto, grazie all'utilizzo dell'estensione selezioniamo il cookie desiderato.

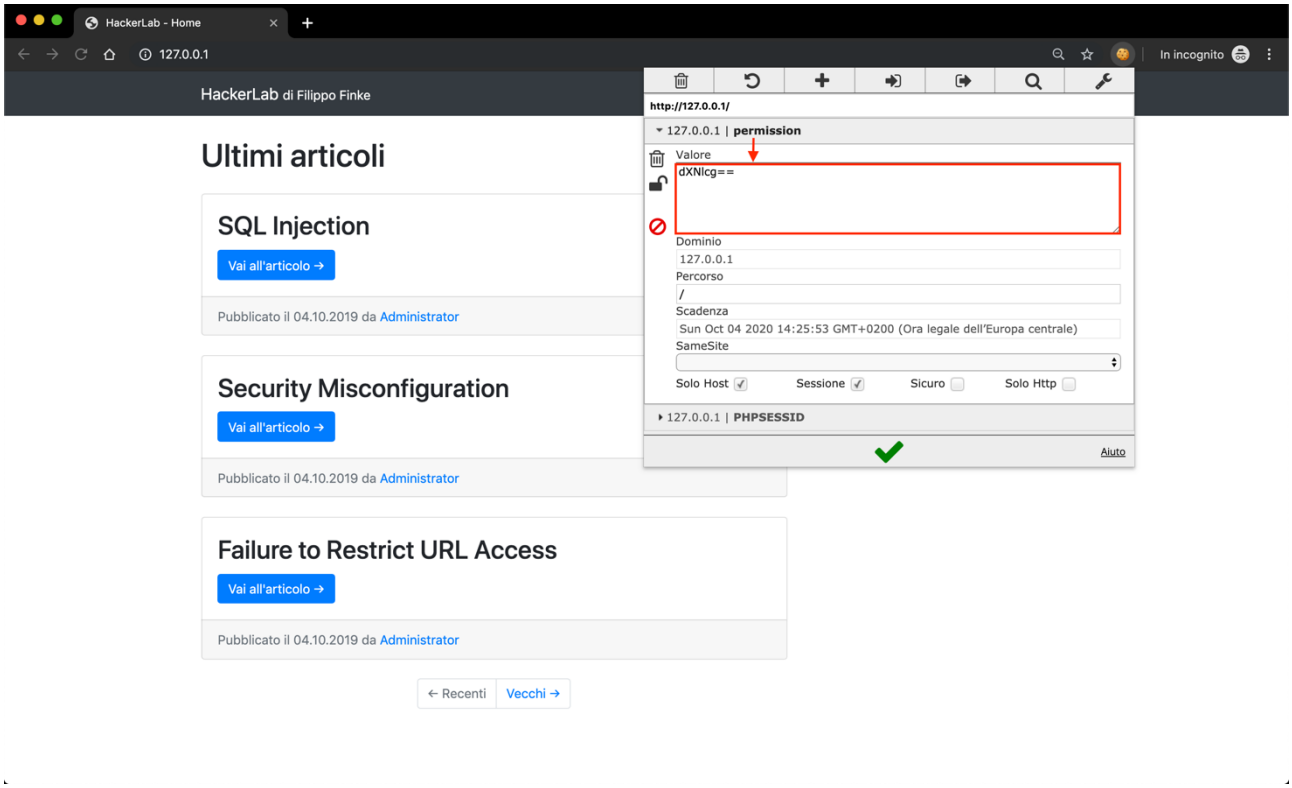

Figura 2 Lettura del cookie permission

Il contenuto del cookie è il seguente: dXNlcg==
Dal contenuto stesso possiamo capire in che modo è stato codificato e cosa rappresenta, il testo presente all'interno del cookie è stato codificato in base64 (intuibile per gli uguali alla fine della stringa), eseguendo quindi una decodifica di questa stringa. Per decodificare la stringa possiamo utilizzare qualsiasi tool in grado di decodificare una stringa in base64, ho quindi utilizzato un sito web (https://base64decode.org) per la decodifica ed il risultato è il seguente:
user
Quindi all'interno del cookie viene salvata una stringa codificata in base64 che determina il permesso visivo dell'utente. Quindi ho supposto che il nome del permesso di un amministratore sia administrator quindi ho utilizzato un tool online (https://base64encode.org) per la codifica di testo in base64. Il risultato di administrator è YWRtaW5pc3RyYXRvcg==
Per sfruttare la vulnerabilità non resta altro che modificare il cookie utilizzando l'estensione.

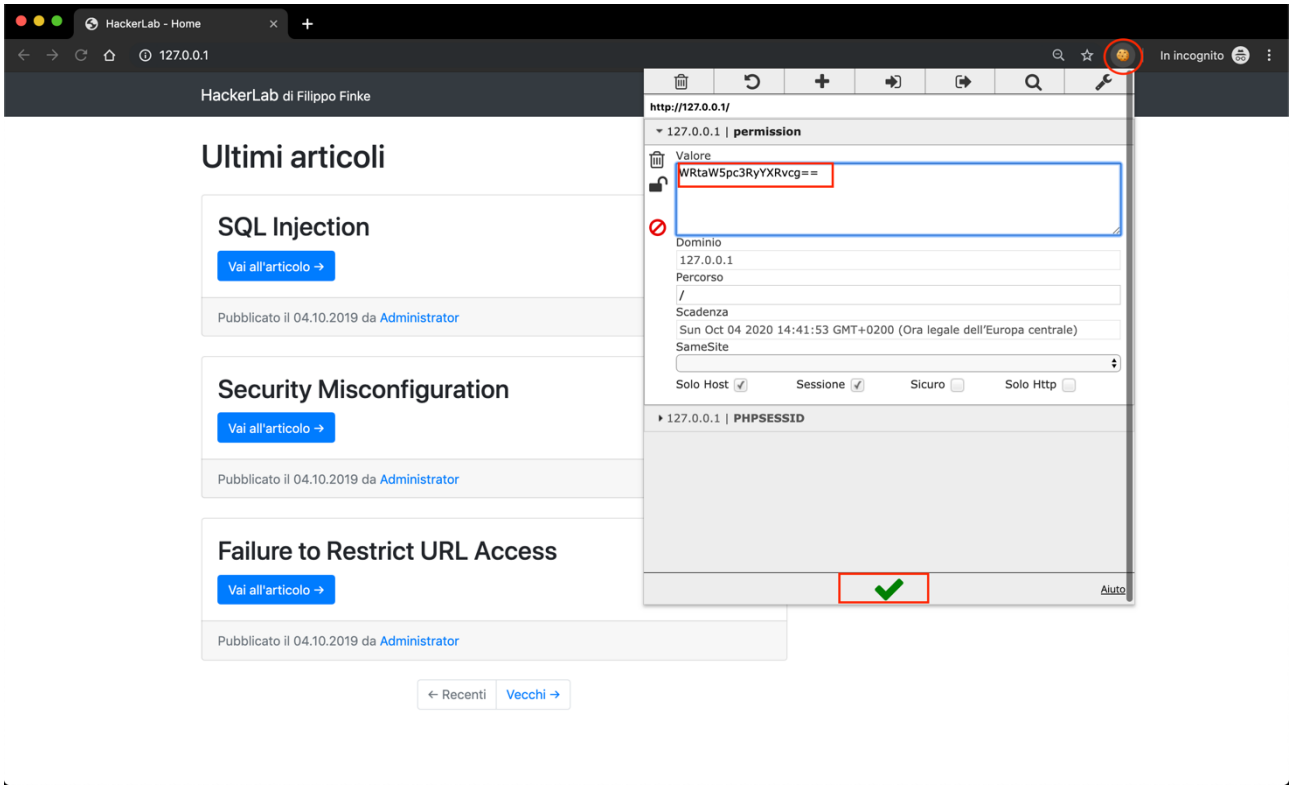

Figura 3 Modifica del cookie permission

Una volta che il cookie è stato modificato basterà aggiornare la pagina per controllare se la modifica del cookie ha apportato delle modifiche visive all'interno del sito web.

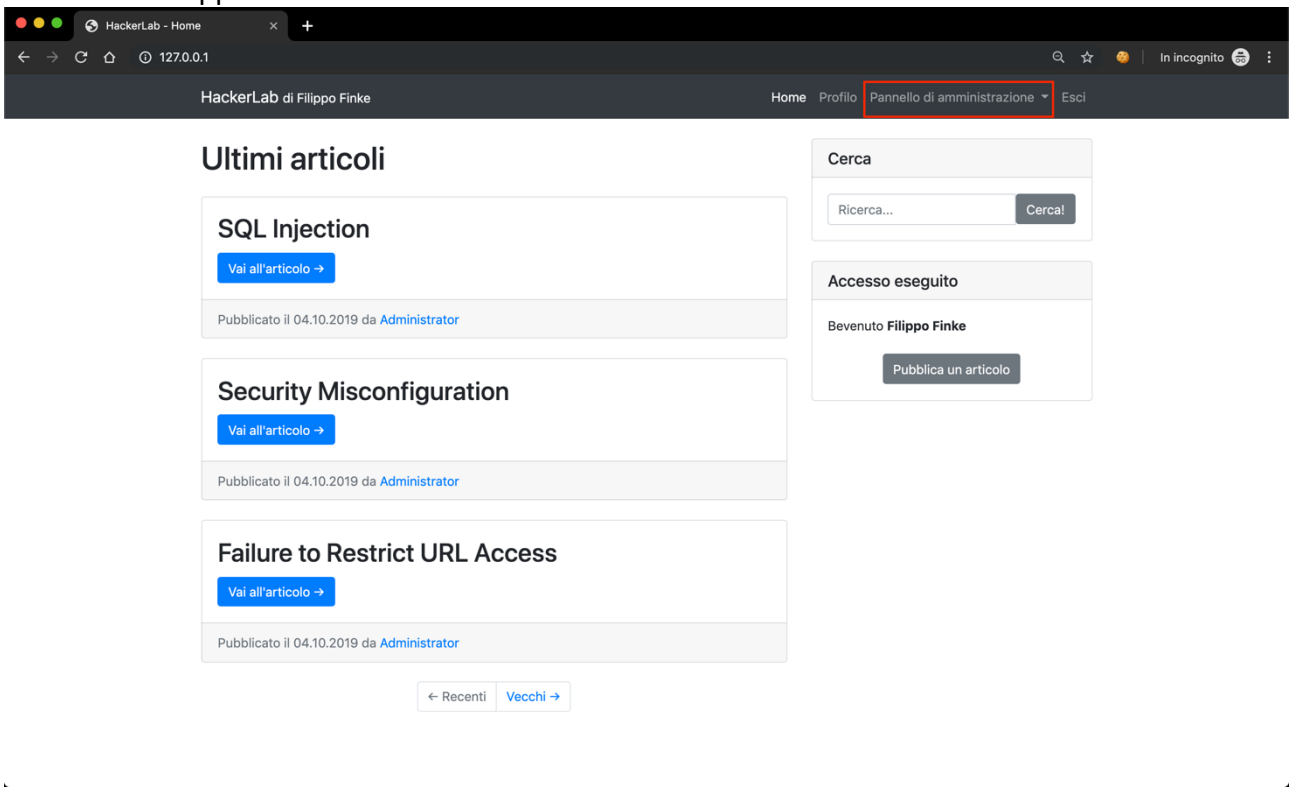

Figura 4 HackerLab dopo aver aggiornato la pagina

Come possiamo vedere, sono apparse delle opzioni in più all'interno della barra di navigazione.