Guida della vulnerabilità
Cross Site Scripting

Introduzione

Questa è la guida della vulnerabilità di tipo **Cross Site Scripting** anche chiamata XSS, seguendo questa guida riuscirai a sfruttare la vulnerabilità all'interno di HackerLab.

Questo tipo di vulnerabilità permette ad un malintenzionato di poter eseguire del codice JavaScript malevolo all'interno di un sito web in modo che tutti gli utenti che lo visitino eseguano quel codice.

Requisiti

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

Guida

Per eseguire questa vulnerabilità basterà recarsi nella home di HackerLab ed eseguire l'accesso. Una volta eseguito l'accesso all'applicativo per sfruttare la falla bisognerà creare un articolo premendo il pulsante "Pubblica un articolo".

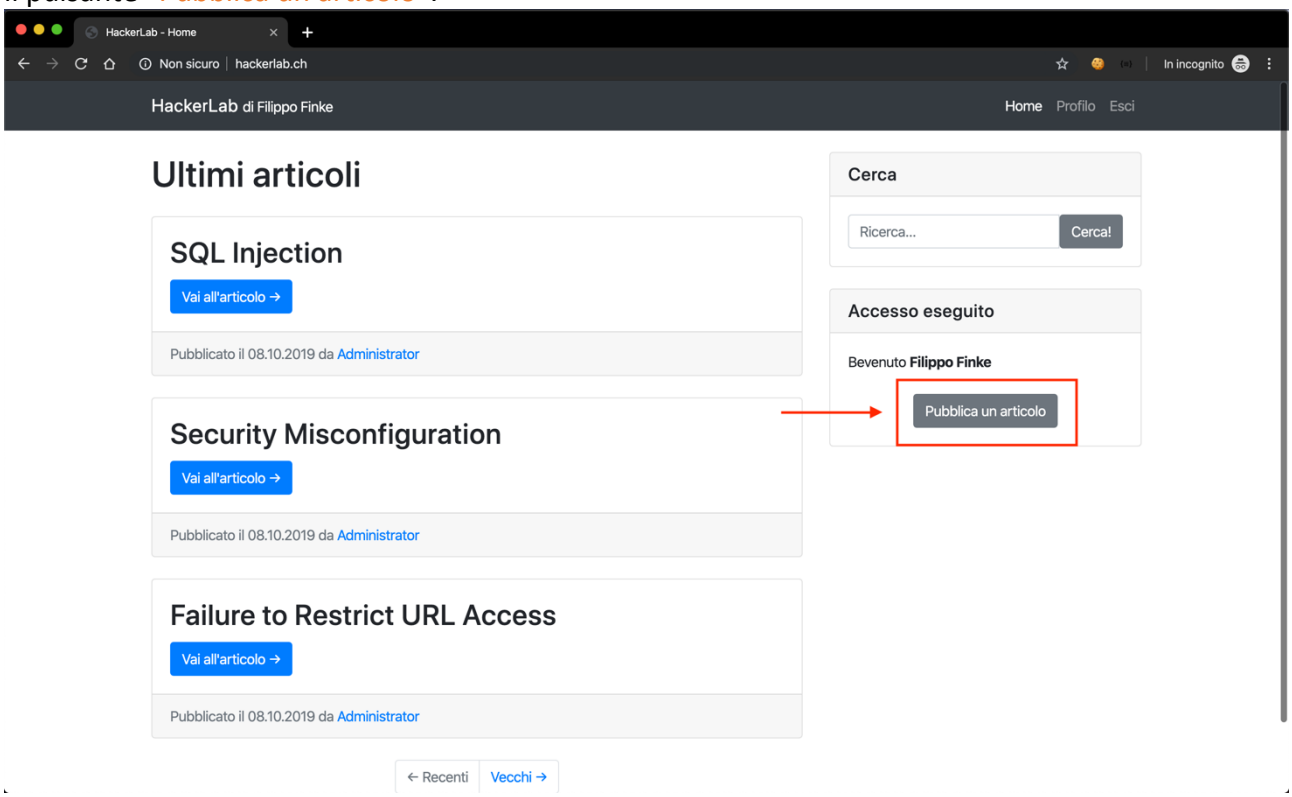

Figura 1 Pubblicazione articolo.

Una volta cliccato pubblicazione sarà necessario scrivere l'articolo contenente il codice malevolo.

Figura 2 Creazione articolo.

Come possiamo notare sono disponibili 2 campi principali. Il titolo e il contenuto. All'interno del titolo non è possibile scrivere del codice HTML o JavaScript in quanto il tutto è validato correttamente. Mentre nel campo contenuto è possibile scrivere del codice html con tag limitati. Non è possibile però scrivere degli script JavaScript in quanto il tag verrà rimosso. Quindi per eseguire del codice malevolo utilizzeremo i tag a nostra disposizione utilizzando determinati eventi. Quindi andremo a creare del contenuto contenente il codice malevolo.

Figura 3 Articolo vulnerabile.

All'interno del contenuto ho inserito un tag html che permette di rappresentare delle immagini. Ho impostato l'immagine da caricare ad un percorso inesistente in modo da generare una chiamata da parte dell'evento onerror, quando quindi verrà sollevata la chiamata verrà eseguito il codice JavaScript alert('Vulnerabilità sfruttata!'); che mostrerà all'utente un popup con la scritta "'Vulnerabilità sfruttata!".
Ora basterà pubblicare l'articolo.

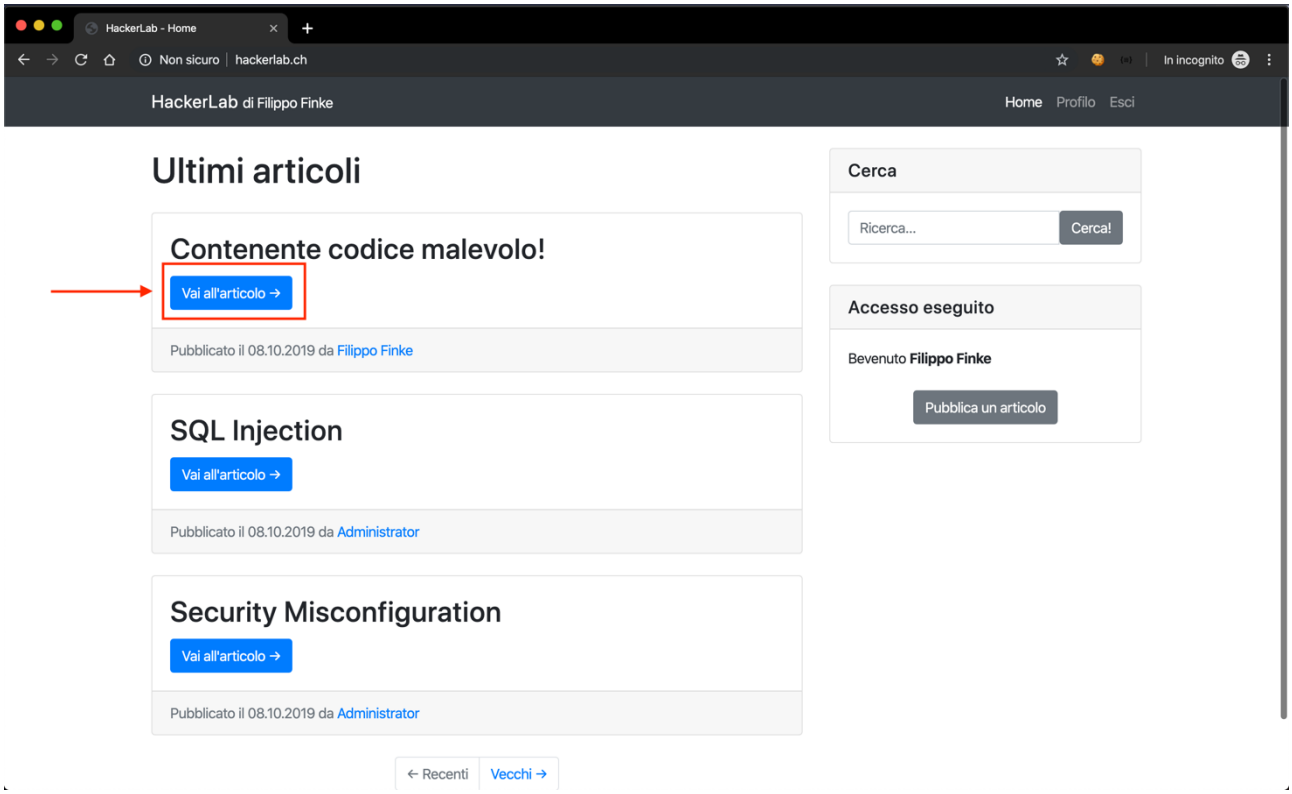

Figura 4 Accedere all'articolo.

Una volta pubblicato basterà andare all'articolo appena creato utilizzando il tasto "Vai all'articolo". Come possiamo notare, appena aperto l'articolo è apparsa una notifica da parte del browser frutto del codice malevolo contenuto nell'articolo stesso.

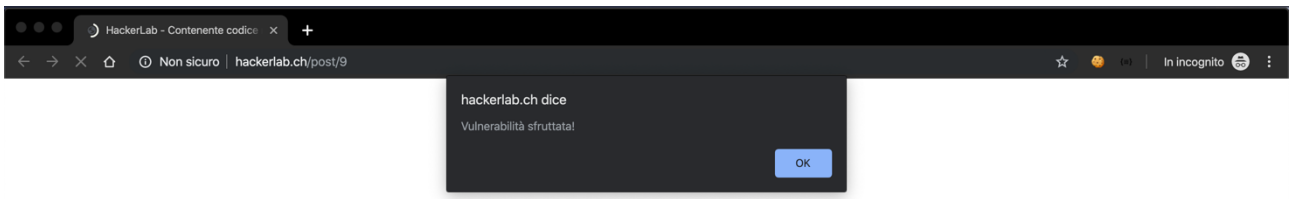

Figura 5 Codice eseguito.

Questa vulnerabilità è molto pericolosa in quanto è possibile accedere ad informazioni sensibili dell'utente, come per esempio cookies ed è possibile modificare la pagina stessa che verrà mostrata all'utente.

Per esempio con il seguente codice:

```
<img src='inesistente.jpg' onerror='document.getElementsByClassName("lead")[0].innerText = "Cross Site Scripting";'>
```

Sarà possibile modificare l'autore dell'articolo in "Cross Site Scripting".

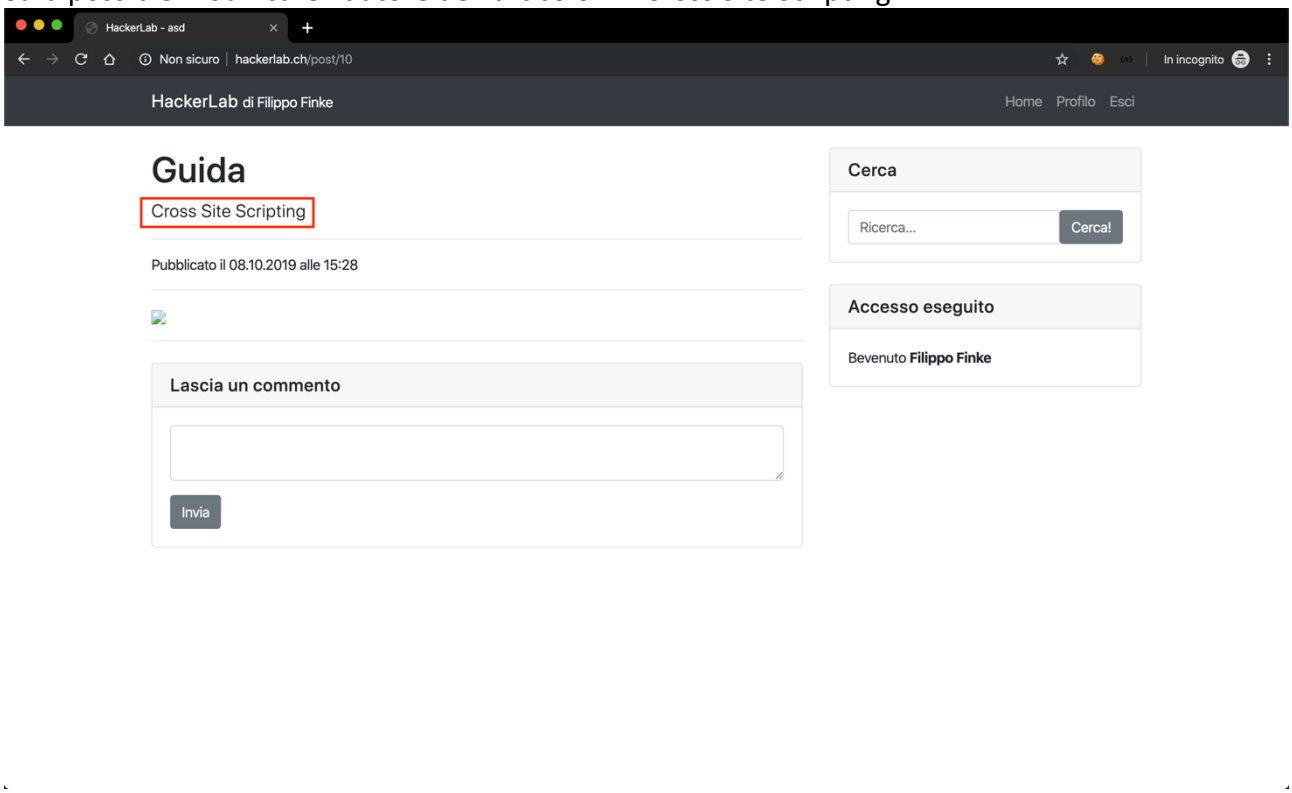

Figura 6 Autore modificato.