Diario di lavoro

Luogo	Canobbio
Data	17.09.2019

Lavori svolti

13h15 – 14h00

Ho terminato i template del sito web, ho completato aggiungendo le pagine di amministrazione.

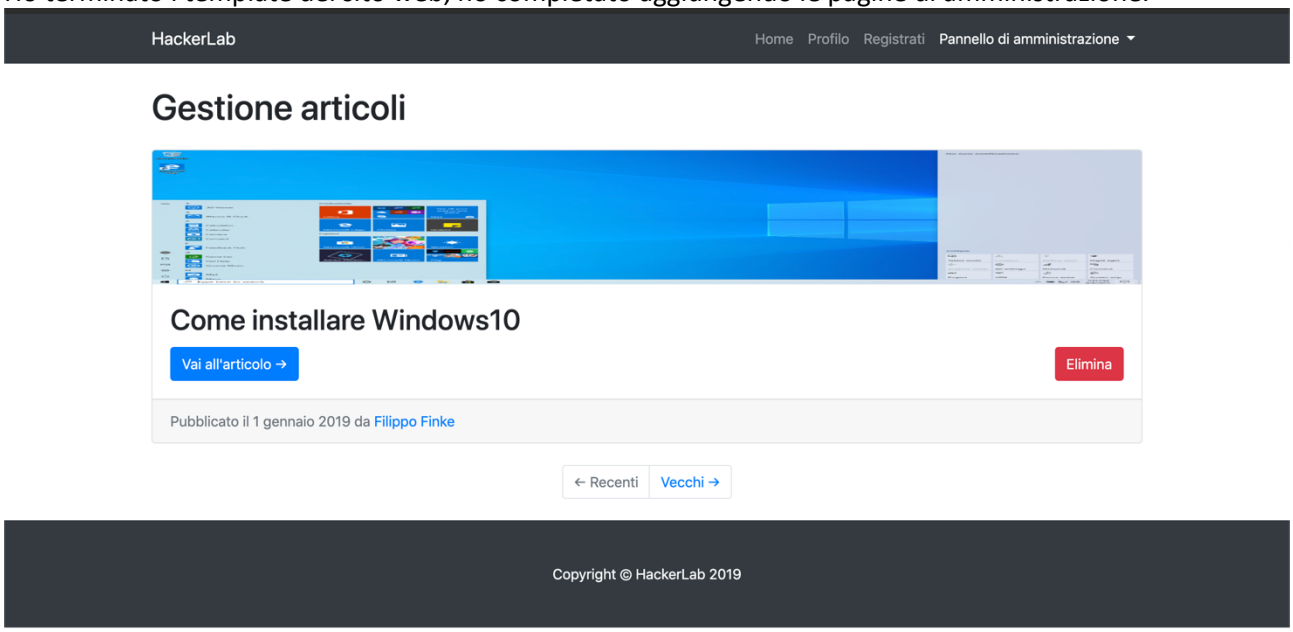

Figura 1 Gestione articoli

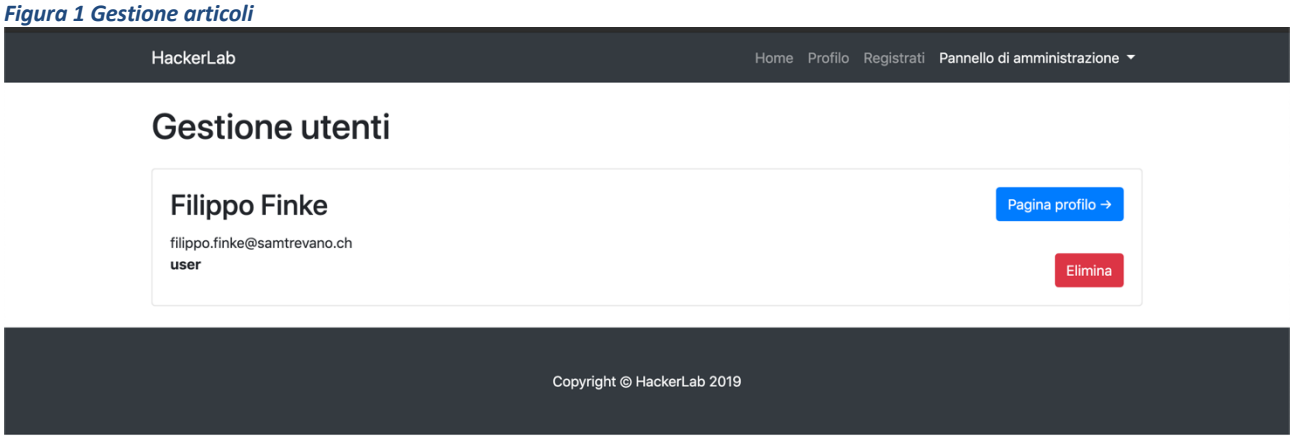

Figura 2 Gestione utenti

14h00 – 16h10
Ho implementato la logica di backend per le seguenti pagine:

- Home
- Profilo
- Post

È quindi ora possibile accedere con le credenziali predefinite all'interno del sito web, eseguire ricerche, accedere alle pagine profilo di altri utenti, visualizzare gli articoli, eseguire ricerche per titolo degli articoli e pubblicare commenti.
Inoltre ho già implementato una vulnerabilità che può essere sfruttata attraverso la modifica di cookie.
La vulnerabilità consiste nel fatto che solamente se si ha un permesso "administrator" si ricevono alcune informazioni in più all'interno delle pagine (indirizzi delle pagine di amministrazione, email nella pagina di profilo). Utilizzando questa vulnerabilità si può quindi risalire alle email degli utenti presenti all'interno del sito web.
Il sistema utilizza questo codice per determinare il permesso all'interno di queste pagina:

```
$permission = isset($_COOKIE["permission"])?base64_decode($_COOKIE["permission"]):null;
```

Per sfruttare la vulnerabilità basterà quindi creare un cookie "permission" con il contenuto "administrator" codificato in base64, ovvero "YWRtaW5pc3RyYXRvcg=="

È inoltre presente anche una vulnerabilità di tipo "Insecure Direct Object References" in quanto sia per i post che per le pagine profilo si può accedere con gli indirizzi "profile/ID" o "post/ID". ID è un valore incrementale, quindi eseguendo un semplice FOR si possono ricavare tutti gli utenti e tutti i profili registrati all'interno del sistema, inoltre in combinazione della vulnerabilità attraverso il cookie è quindi possibile ottenere una copia degli utenti con i dati riguardanti articoli, full_name ed email.
16h10 – 16h30
Stesura diario.

Problemi riscontrati e soluzioni adottate
Non ho riscontrato nessun problema.

Punto della situazione rispetto alla pianificazione
Mi trovo molto avanti rispetto alla pianificazione.

Programma di massima per la prossima giornata di lavoro
Implementare le funzionalità di pubblicazione di un post e la registrazione.