

Diario di lavoro

Luogo	Canobbio
Data	03.09.2019

Lavori svolti

13h15 – 14h45

Durante le prime due ore della mattinata abbiamo avuto l'occasione di guardare tutti i progetti disponibili e scegliere quelli più adatti a noi. Ho ricevuto il progetto "Hacker Lab"

15h00 – 16h30

Mentre nelle seconde due ore seguenti ho iniziato a strutturare la repository di GitHub disponibile all'indirizzo: <https://github.com/filippofinke/HackerLab>

All'interno della repository ho iniziato ad inserire tutto il necessario che riguarda documentazione, presentazione, diari e una struttura basilare.

Ho inoltre iniziato a creare una pianificazione basilare del progetto.

Problemi riscontrati e soluzioni adottate

Punto della situazione rispetto alla pianificazione

Programma di massima per la prossima giornata di lavoro

Verificare la pianificazione del progetto.

Diario di lavoro

Luogo	Canobbio
Data	05.09.2019

Lavori svolti

13h15 – 13h33

Ho discusso con il superiore per quanto riguarda il progetto, ho espresso le mie idee e posso dire di aver capito a pieno il progetto.

13h33 – 13h56

Ho continuato la documentazione e completato i capitoli 1.1, 1.3 e 2.1

13h56 – 14h05

Ho iniziato la ricerca di vulnerabilità da implementare all'interno del prodotto.

Ho trovato le seguenti vulnerabilità:

- SQL Injection
- Cross Site Scripting (XSS)
- Broken Authentication
- Insecure Direct Object References
- Security Misconfiguration
- Failure to restrict URL Access
- File inclusion vulnerability
- Account takeover vulnerability

14h06 – 14h45

Ho creato una base MVC utilizzando Slim framework (<http://www.slimframework.com/>) alla versione 3.

In questo modo quando inizierò lo sviluppo sarà più facile gestire il tutto. Inoltre ho creato un file gitignore per ignorare i file inutili all'interno della repository.

15h00 – 15h50

Ho iniziato la creazione di schizzi delle pagine web, al momento ho completato la Home, il Post e la pagina di registrazione.

15h50 – 16h30

Ho iniziato il capitolo di analisi dei requisiti, per la prossima giornata di lavoro continuerò ad analizzare e documentare i vari requisiti richiesti.

Problemi riscontrati e soluzioni adottate

Il software che utilizzo al momento per la creazione del Gantt non può essere utilizzato.

Per risolvere il problema ho intenzione di creare una macchina virtuale Windows10 per installare Microsoft Project che può essere utilizzato.

Punto della situazione rispetto alla pianificazione

Mi trovo in linea con i tempi della pianificazione.

Programma di massima per la prossima giornata di lavoro

Preparare una macchina virtuale con Windows10 per l'installazione di Microsoft Project, continuare la parte di analisi della documentazione.

Filippo Finke I4AC

Diario di lavoro

Luogo	Canobbio
Data	06.09.2019

Lavori svolti

13h15 – 14h45

Ho installato una macchina virtuale con Windows10 ed installato il software Microsoft Project. Utilizzando MicrosoftProject ho ricreato il Gantt completandolo in modo preventivo.

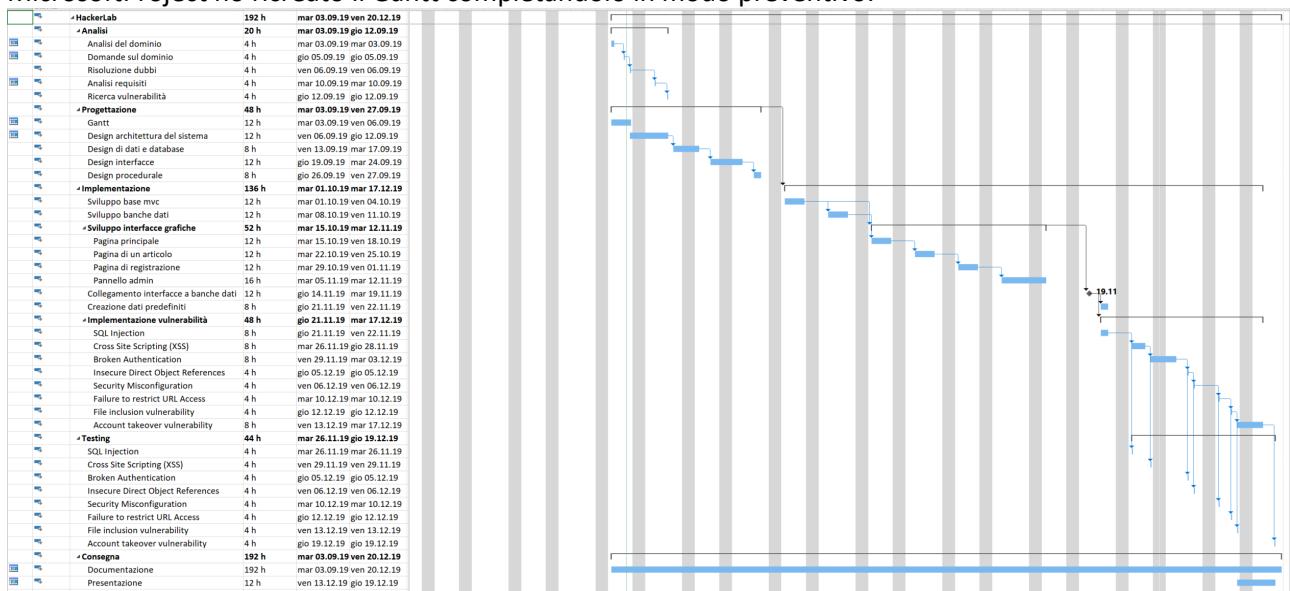


Figura 1 Gantt

15h00 – 15h50

Ho lavorato alla sezione 2.2 della documentazione completando i requisiti richiesti da soddisfare nel progetto.

15h50 – 16h06

Ho creato una bozza dello schema di use case del capitolo 2.3 della documentazione.

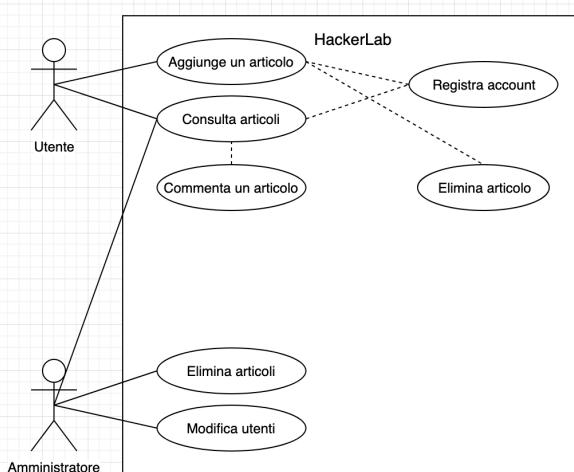


Figura 2 Bozza UseCase

16h06 – 16h30

Stesura del diario, aggiornamento repository GitHub e correzione del capitolo 1 all'interno della

documentazione.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo in linea con la pianificazione.

Programma di massima per la prossima giornata di lavoro

Continuare la creazione degli schemi del design del progetto.

Diario di lavoro

Luogo	Canobbio
Data	10.09.2019

Lavori svolti

13h15 – 14h10

Ho creato lo schema del database che verrà utilizzato dal blog.

Il database è molto semplice, composto da quattro tabelle.

Una tabella che conterrà i permessi degli utenti, una tabella che conterrà gli utenti stessi, una tabella che conterrà gli articoli ed in fine una tabella contenente i commenti.

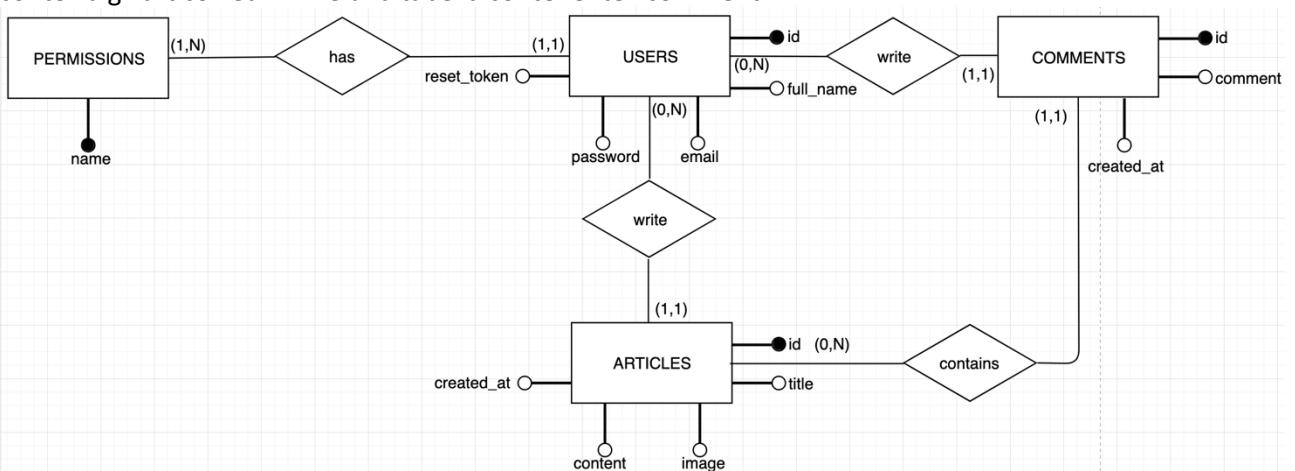


Figura 1 Schema database

14h10 - 14h30

Ho completato lo schema da utilizzare nella sezione use case della documentazione.

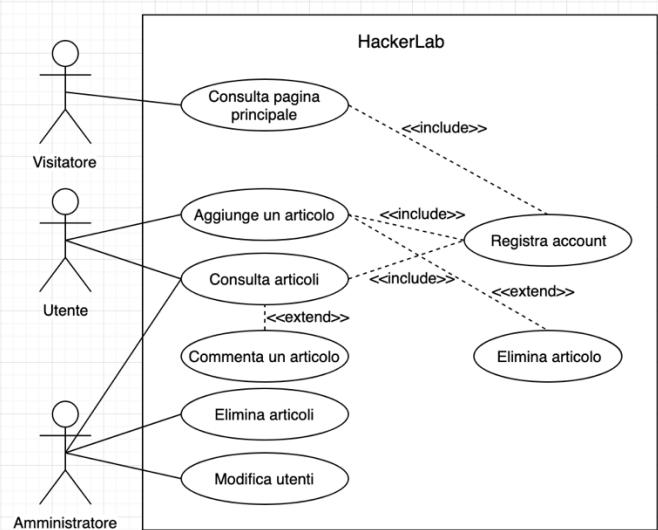


Figura 2 Schema usecase

Chi accede al sito web senza avere un account è considerato “Visitatore”. I visitatori hanno la sola possibilità di visitare la home page con la lista degli articoli per titoli e la possibilità di registrarsi al sito web. Quindi i visitatori non hanno la possibilità di aggiungere articoli oppure commenti al sito web.

Viene considerato “Utente” chi ha un account registrato all’interno dell’applicativo. Gli utenti possono contribuire al sito web pubblicando articoli, visualizzarli nel dettaglio e la possibilità di esprimere le proprie

opinioni nei commenti.

Un utente di livello avanzato viene considerato "Amministratore", gli amministratori possono eseguire tutte le azioni degli utenti e dei visitatori ma possono anche modificare lo stato degli utenti registrati al sito web e la possibilità di eliminare gli articoli.

14h30 – 14h45 15h00 – 15h40

Ho lavorato al capitolo 2.4 della documentazione completando il diagramma di Gantt e descrivendo nel dettaglio ogni fase di esso.

15h40 – 16h00

Ho creato uno schema di rete basilare che rappresenta un client che si vuole collegare al sito web.

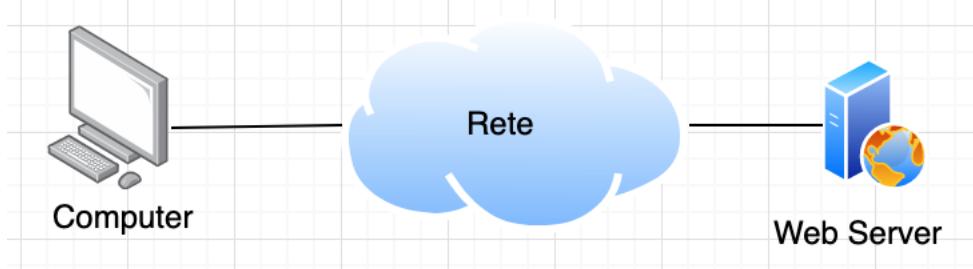


Figura 3 Schema di rete

16h00 – 16h15

Ho creato una sitemap schematica del sito web per dare un'idea delle varie pagine che saranno implementate all'interno dell'applicativo.

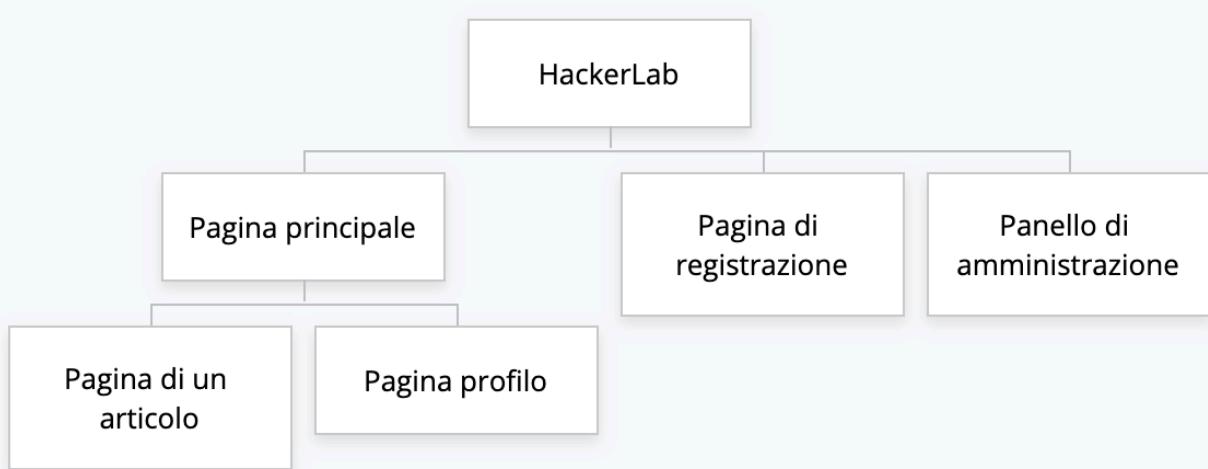


Figura 4 Sitemap

16h15 – 16h25

Ho iniziato a descrivere lo schema ER del database all'interno della documentazione.

16h25 – 16h30

Stesura diario e aggiornamento repository GitHub.

Problemi riscontrati e soluzioni adottate

Non ho riscontrato nessun problema.

Punto della situazione rispetto alla pianificazione

Mi trovo in linea con la pianificazione.

Programma di massima per la prossima giornata di lavoro

Continuare la sezione design architettura del sistema e il design dei dati.

Diario di lavoro

Luogo	Canobbio
Data	12.09.2019

Lavori svolti

13h15 – 13h30

Ho aggiunto un attributo al database nella tabella utente. Ho aggiunto l'attributo enabled che determina se un utente è abilitato oppure no.

13h30 – 14h00

Ho creato lo schema basilare del diagramma di flusso. Lo schema è il seguente:

[Torna alla pagina principale](#)

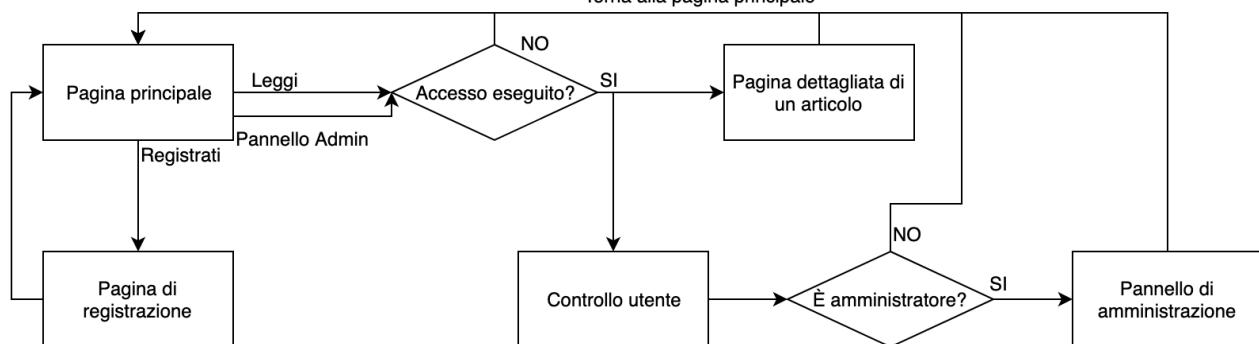


Figura 1 Diagramma di flusso

Quando l'utente accede all'applicativo web si ritroverà alla pagina principale, una pagina nella quale verranno mostrati gli articoli postati recentemente all'interno del sito web. L'utente potrà decidere di registrarsi al sito oppure accedere. Se l'utente desidera leggere un articolo dovrà aver eseguito l'accesso all'interno del sito web, in caso contrario verrà reindirizzato alla pagina principale. Eseguendo l'accesso l'utente potrà visionare l'articolo completo e i commenti. Per accedere al pannello di amministrazione del sistema l'utente dovrà aver eseguito l'accesso all'interno dell'applicativo e dovrà avere i permessi richiesti.

14h00 – 14h25

Ho descritto le varie tabelle del database specificandone i tipi di dati, i limiti e le loro correlazioni sotto forma di una tabella.

PERMISSIONS	
Attributo	Descrizione
name	Rappresenta il nome di un permesso all'interno del sistema. È un attributo di tipo stringa con un limite di 30 caratteri. Non può essere nullo e deve essere univoco. Esempio: utente

USERS	
Attributo	Descrizione
id	Rappresenta un identificatore di un utente. È un attributo di tipo intero e viene impostato in modo automatico dall'applicativo. Non può essere nullo e deve essere univoco. Esempio: 1

email	Rappresenta un indirizzo email dell'utente. È un attributo di tipo stringa con limite di 255 caratteri. Non può essere nullo e deve essere univoco. Esempio: filippo.finke@samtrevano.ch
password	Rappresenta la password di un utente. È un attributo di tipo stringa con limite di 255 caratteri. Non può essere nullo. Il dato salvato in questo campo sarà un hash generata dal sistema. Esempio: \$2y\$10\$NmiaiLmr3dhUg3ePIExyt.l2KvE7SK6le1UH67QVikBlyBjjTHgVG
full_name	Rappresenta il nome completo di un utente. È un attributo di tipo stringa con un limite di 30 caratteri. Può contenere solamente lettere dell'alfabeto e uno spazio. Non può essere nullo. Esempio: Filippo Finke
reset_token	Rappresenta un codice per il recupero della password. È un attributo di tipo stringa con limite di 255 caratteri. Può essere nullo e viene generato dal sistema in modo automatico. Sarà un hash. Esempio: ced70e86c03186acbe5ab76a5ccfd4f64b77ea9ae2d466948d6ec68c52c30984
enabled	Rappresenta lo stato di un utente. È un attributo di tipo intero con massimo una cifra. Viene impostato dal sistema, di default è 1. Esempio: 1

ARTICLES	
Attributo	Descrizione
id	Rappresenta un identificatore di un articolo. È un attributo di tipo intero e viene impostato in modo automatico dall'applicativo. Non può essere nullo e deve essere univoco. Esempio: 1
user_id	Rappresenta il creatore dell'articolo. È un attributo di tipo intero, non può essere nullo e deve esistere all'interno della tabella USERS . Esempio: 1
title	Rappresenta il titolo di un articolo. È un attributo di tipo stringa con un limite di 255 caratteri. Non può essere nullo. Esempio: Come installare Windows 10
image	Rappresenta il percorso dell'immagine di sfondo di un articolo. È un attributo di tipo stringa con un limite di 255 caratteri. Può essere nullo. Esempio: 35d91262b3c3ec8841b54169588c97f7
content	Rappresenta il contenuto di un articolo. È un attributo di tipo stringa con un limite di 1000

	<p>caratteri. Non può essere nullo.</p> <p>Esempio: Per installare Windows 10 si ha bisogno di ...</p>
created_at	<p>Rappresenta la data di creazione di un articolo. È un attributo di tipo interno che contiene un timestamp.</p> <p>Esempio: 1568290770</p>

COMMENTS	
Attributo	Descrizione
id	<p>Rappresenta un identificatore di un commento. È un attributo di tipo intero e viene impostato in modo automatico dall'applicativo. Non può essere nullo e deve essere univoco.</p> <p>Esempio: 1</p>
article_id	<p>Rappresenta l'articolo al quale è assegnato il commento. È un attributo di tipo intero, non può essere nullo e deve esistere all'interno della tabella ARTICLES.</p> <p>Esempio: 1</p>
user_id	<p>Rappresenta il creatore del commento. È un attributo di tipo intero, non può essere nullo e deve esistere all'interno della tabella USERS.</p> <p>Esempio: 1</p>
comment	<p>Rappresenta il contenuto di un commento. È un attributo di tipo stringa e ha un limite di 255 caratteri. Non può essere nullo.</p> <p>Esempio: Articolo utilissimo!</p>
created_at	<p>Rappresenta la data di creazione di un articolo. È un attributo di tipo interno che contiene un timestamp.</p> <p>Esempio: 1568290770</p>

14h25 – 14h45

Ho revisionato alcuni capitoli della documentazione (soprattutto formattazione) e ho iniziato a disegnare i mockup delle interfacce grafiche.

15h00 – 15h45

Ho completato il capitolo design delle interfacce.

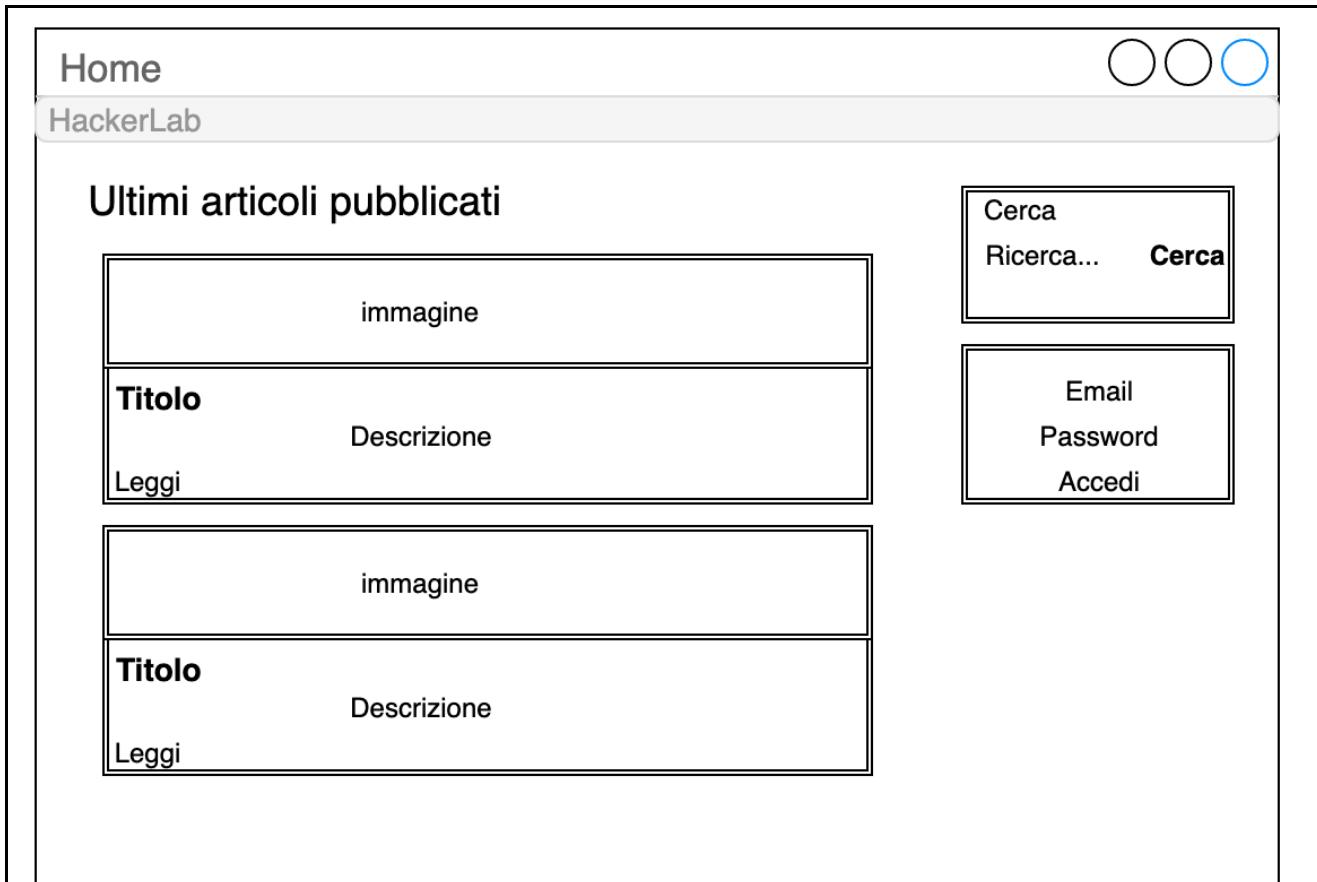


Figura 2 Pagina principale

Questa è la pagina principale che verrà mostrata all'utente appena si collegherà al sito web.



Figura 3 Pagina di registrazione

Questa è la pagina di registrazione, sarà accessibile tramite la pagina principale del sito web.

The wireframe shows a registration form. At the top left, there's a placeholder 'Post' and a user handle 'HackerLab'. On the right, there are three circular icons: two white with black outlines and one blue with a black outline. Below this is a search bar with the placeholder 'Cerca Ricerca...' and a 'Cerca' button. The main form area has sections for 'Titolo' (Title) containing 'immagine' (image), 'Descrizione' (Description), and 'Commenti' (Comments). The 'Commenti' section contains a placeholder for a user icon and the text 'Username' and 'Commento' (Comment).

Figura 4 Pagina di un articolo

Questa è la pagina di quando si aprirà un articolo.

The screenshot shows a user profile page. At the top, there's a header with the word "Profilo" and three circular icons (two white, one blue). Below the header, the user's name "HackerLab" is displayed. The main content area features a large title "Filippo Finke". Underneath the title, there are two identical card-like structures. Each card has a placeholder "immagine" (image) at the top, followed by a bolded "Titolo" (Title), a "Descrizione" (Description) below it, and a "Leggi" (Read) button at the bottom right. The entire page is contained within a light gray border.

Figura 5 Pagina profilo

Questa è la pagina profilo di un utente.

The screenshot shows an administration panel titled "Pannello di amministrazione" at the top, with three circular icons (two white, one blue). Below the title, the word "HackerLab" is visible. The main content area is titled "Articoli". It contains two cards, each representing an article. The first card has a placeholder "immagine" (image) at the top, followed by a bolded "Titolo" (Title), a "Descrizione" (Description) below it, a "Leggi" (Read) button at the bottom left, and an "Elimina" (Delete) button at the bottom right. The second card follows the same structure. The entire panel is enclosed in a light gray border.

Figura 6 Pannello di amministrazione, Articoli

Questa è la pagina di amministrazione degli articoli del sito web.

The screenshot shows a user interface for managing articles. At the top, there is a header bar with three icons: two white circles and one blue circle. Below the header, the title "Pannello di amministrazione" is displayed, followed by the subtitle "HackerLab". The main content area is titled "Utenti". It lists three users, each represented by a card:

- Nome Cognome:** [REDACTED] **Pagina profilo:** [REDACTED] **Elimina:** [REDACTED]
email
permesso
- Nome Cognome:** [REDACTED] **Pagina profilo:** [REDACTED] **Elimina:** [REDACTED]
email
permesso
- Nome Cognome:** [REDACTED] **Pagina profilo:** [REDACTED] **Elimina:** [REDACTED]
email
permesso

Figura 7 Pannello di amministrazione, Utenti

Questa è la pagina di amministrazione degli utenti del sito web.

15h45 – 16h20

Ho terminato lo sviluppo della banca dati basilare che è possibile trovare al seguente percorso:

codice/database.sql

16h20 – 16h30

Aggiornamento repository GitHub e diario.

Problemi riscontrati e soluzioni adottate

Non ho riscontrato nessun problema.

Punto della situazione rispetto alla pianificazione

Attualmente mi trovo più avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

Completare il diagramma procedurale.

Diario di lavoro

Luogo	Canobbio
Data	13.09.2019

Lavori svolti

13h15 – 13h30

Ho descritto l'implementazione del database nel capitolo 4.1 della documentazione.

13h30 – 13h40

Ho chiesto al docente Montalbetti se fosse richiesto creare un diagramma di flusso dettagliato per ogni azione all'interno del sito web nella sezione 3.4 e mi è stato detto che non è necessario. In quella sezione verranno inseriti e descritti i diagrammi UML delle classi che compongono il programma.

13h40 – 14h45

Ho iniziato lo sviluppo delle interfacce web con dei dati statici per testing.

15h00 – 16h10

Ho continuato lo sviluppo delle interfacce web.

The screenshot displays a website layout. At the top, there's a dark header bar with the text "HackerLab" on the left and navigation links "Home", "Profilo", "Registrati", and "Pannello di amministrazione" on the right. Below the header, the main content area features a title "Come installare Windows10" and a subtitle "di Filippo Finke". A timestamp "Pubblicato il 1 gennaio 2019 alle ore 12:22" is shown. The central part of the page contains an image of a Windows 10 desktop screen with various icons and a taskbar. To the right, there's a sidebar with a search bar labeled "Cerca" and a button "Cerca!", followed by a section titled "Accesso eseguito" containing the message "Bevenuto Filippo Finke!". At the bottom of the main content area, there's a section titled "Windows10" with a bullet point "• Test" and a link "Test".

Figura 1 Pagina di un articolo

The screenshot shows the registration form for the HackerLab website. The header includes links for Home, Profilo, Registrati, and Pannello di amministrazione. The main form is titled "HackerLab - Registrati" and contains fields for Nome e cognome (Name and Surname), Indirizzo email (Email address), Password, and Ripeti la password (Repeat password). A "Registrati" button is at the bottom. Below the form, a copyright notice reads "Copyright © HackerLab 2019". A small inset image in the bottom right corner shows a tablet displaying the registration page.

Figura 2 Pagina di registrazione

The screenshot shows the profile page for Filippo Finke. The header links are identical to the registration page. The main content area features a large image of a Windows 10 desktop with pinned icons for File Explorer, Mail, Photos, and others. Below the image is the title "Articoli di Filippo Finke" and the subtitle "SE ADMIN: email@email.com". A specific article titled "Come installare Windows10" is highlighted with a thumbnail showing the Windows desktop and a "Vai all'articolo →" button. To the right, there's a search bar labeled "Cerca" and a sidebar titled "Accesso eseguito" with the message "Bevenuto Filippo Finke!". Navigation buttons at the bottom left include "Recenti" and "Vecchi". A small inset image in the bottom right corner shows a tablet displaying the profile page.

Figura 3 Pagina profilo

The screenshot shows the main page of the HackerLab website. At the top, there's a dark header bar with the text "HackerLab" on the left and "Home Profilo Registrati Pannello di amministrazione" on the right. Below the header, the main content area has a title "Ultimi articoli" and a thumbnail image of a Windows 10 desktop. A post titled "Come installare Windows10" is displayed, with a blue button "Vai all'articolo →" below it. To the right of the article, there's a search bar labeled "Cerca" with a "Ricerca..." input field and a "Cerca!" button. Further down, there's a "Accedi" (Log In) form with fields for "Indirizzo email" (Email) and "Password". Below the form are buttons for "Accedi" and "Oppure Registrati", and a link "Password dimenticata?". On the far right, there's a box titled "Accesso eseguito" (Access performed) containing the message "Bevenuto Filippo Finke!". At the bottom of the main content area, there are navigation links "← Recenti" and "→ Vecchi".

Figura 4 Pagina principale

This screenshot shows the same website as Figure 4, but with a modal window open over the content. The modal is titled "Imposta la tua password" (Set your password) and contains three input fields: "Password" (with value "asd"), "Ripeti password" (with value "Password"), and a "Imposta password" (Set password) button. The background content is partially visible, including the "Ultimi articoli" section and the login form from Figure 4.

Figura 5 Recupero password

16h10 – 16h30

Stesura diario e revisione documentazione.

Problemi riscontrati e soluzioni adottate
Non ho riscontrato problemi.

Punto della situazione rispetto alla pianificazione
Mi trovo avanti rispetto alla pianifica preventiva.

Programma di massima per la prossima giornata di lavoro

Continuare lo sviluppo delle interfacce web.

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.

HackerLab Home Profilo Registrati Pannello di amministrazione ▾

Gestione articoli

Come installare Windows10

Vai all'articolo → Elimina

Pubblicato il 1 gennaio 2019 da Filippo Finke

← Recenti Vecchi →

Copyright © HackerLab 2019

Figura 1 Gestione articoli

HackerLab Home Profilo Registrati Pannello di amministrazione ▾

Gestione utenti

Filippo Finke

filippo.finke@samtrevano.ch user

Pagina profilo → Elimina

Copyright © HackerLab 2019

← Recenti Vecchi →

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 pagine:

```
$permission = isset($_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.

Diario di lavoro

Luogo	Canobbio
Data	19.09.2019

Lavori svolti

13h15 – 13h47

Implementato la possibilità di registrarsi all'interno del sito web.

13h47 – 13h58

Implementato la funzionalità di recupero password parzialmente, manca l'invio tramite email.

13h58 – 14h45

Ho creato un account gmail che andrà a collegare tramite l'utilizzo della libreria "PHPMailer" per l'invio delle email.

Email: hackerlab.notify@gmail.com

Password: Password&1

Utilizzando la libreria <https://github.com/PHPMailer/PHPMailer> ho creato una classe che permette l'invio di posta elettronica.

La classe è la seguente:

```
1. <?php
2. use PHPMailer\PHPMailer\PHPMailer;
3. use PHPMailer\PHPMailer\Exception;
4.
5. class Mailer {
6.
7.     public static function send($to, $full_name, $subject, $message) {
8.         $mail = new PHPMailer(true);
9.         try {
10.             $mail->SMTPDebug = 0;
11.             $mail->isSMTP();
12.             $mail->Host = 'smtp.gmail.com';
13.             $mail->SMTPAuth = true;
14.             $mail->Username = 'hackerlab.notify@gmail.com';
15.             $mail->Password = 'Password&1';
16.             $mail->SMTPSecure = 'tls';
17.             $mail->Port = 587;
18.             $mail->setFrom('hackerlab.notify@gmail.com', 'HackerLab');
19.             $mail->addAddress($to, $full_name);
20.             $mail->Subject = $subject;
21.             $mail->msgHTML($message);
22.
23.             $mail->send();
24.             return true;
25.         } catch (Exception $e) {
```

```
26.         return false;
27.     }
28. }
29.
30. }
```

Attraverso la libreria PHPMailer eseguo l'accesso a gmail tramite il quale ho la possibilità di inviare email.

15h00 – 15h30

Implementata la possibilità di resettare la password attraverso il link ricevuto tramite email. Il reset avviene tramite una schermata a comparsa.

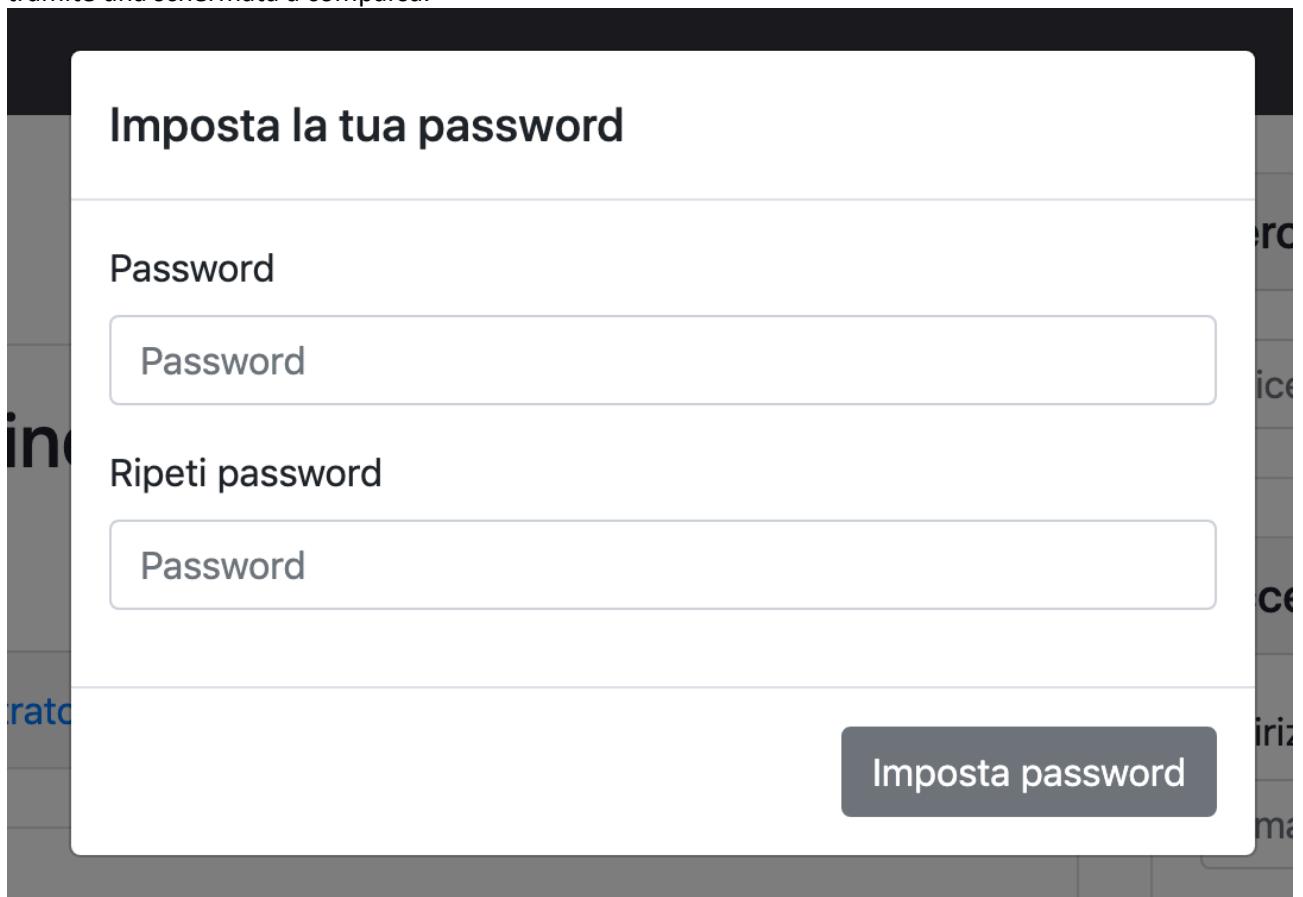


Figura 1 Schermata a comparsa

15h30 – 16h20

Aggiunta la possibilità di eliminare utenti dal pannello di amministrazione.

Ho eseguito della pulizia e delle correzioni nel codice:

Vedi sezione problemi del diario.

Problemi riscontrati e soluzioni adottate

Dalla pagina di registrazione si veniva rimandati alla pagina principale in caso di errore, ora invece si viene rimandati alla pagina di creazione di un account e mostrati gli errori.

Ho risolto con il seguente pezzo di codice:

```
return $response->withRedirect("/register", 302);
```

All'interno della pagina profilo se un utente non aveva articoli non veniva mostrato nulla. Ora viene mostrata la scritta "Nessun articolo."

```
<?php if(count($articles) == 0): ?>
    <h4>Nessun articolo.</h4>
<?php endif; ?>
```

Era possibile inserire dei caratteri non numerici come numero di pagina di articolo, questo dava svariati problemi. Ho risolto con il seguente codice che si accerta che la pagina sia un numero, altrimenti verrà impostata a 0.

```
if(!is_numeric($page)) $page = 0;
```

16h20 – 16h30

Stesura diario.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

Implementare la possibilità di pubblicare articoli e il pannello di amministrazione.

Diario di lavoro

Luogo	Canobbio
Data	20.09.2019

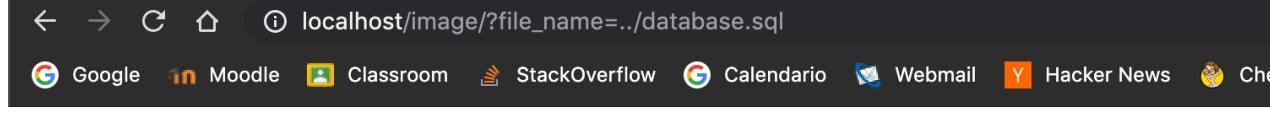
Lavori svolti

13h15 – 14h45

Ho implementato la possibilità di pubblicare degli articoli all'interno del sito web.
Al momento è possibile caricare anche delle immagini. I controlli per contenuto e titolo possono considerarsi sicuri, mentre la chiamata per ricavare le immagini dei post è vulnerabile ad un attacco di tipo Directory Traversal.
La chiamata per la lettura delle immagini è la seguente:

http://localhost/image/?file_name=FILE_NAME

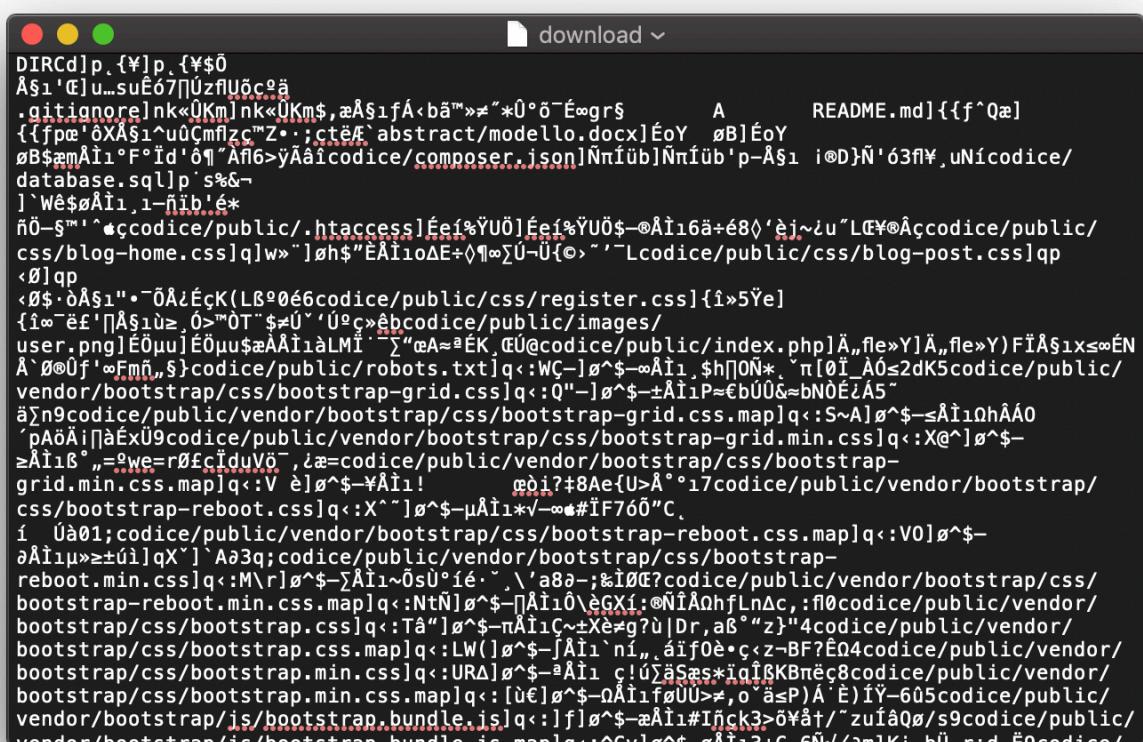
Mettendo al posto di FILE_NAME per esempio il valore “..../database.sql” è possibile sfruttare questa chiamata per leggere il file che si trova nella cartella codice/database.sql e stamparne il contenuto.



```
#  
# HackerLab  
# Filippo finke  
#  
# Creazione database  
#  
DROP DATABASE IF EXISTS hackerlab;  
CREATE DATABASE hackerlab;  
USE hackerlab;  
  
#  
# Creazione tabelle  
#  
  
# Tabella permessi  
CREATE TABLE permissions(  
    name VARCHAR(30) PRIMARY KEY  
);  
  
# Tabella utenti  
CREATE TABLE users(  
    id INT AUTO_INCREMENT PRIMARY KEY,  
    email VARCHAR(255) NOT NULL,  
    password VARCHAR(255) NOT NULL,  
    permission VARCHAR(30),  
    full_name VARCHAR(30) NOT NULL,  
    reset_token VARCHAR(255) DEFAULT NULL,  
    ...  
);
```

Figura 1 Esempio vulnerabilità

Questa vulnerabilità è pericolosa nonostante non si possa eseguire del codice remoto, questo perché è possibile caricare dei file html contenenti javascript vulnerabile per fare eseguire azioni all'utente involontariamente. Inoltre si può navigare completamente il sistema del server.



The screenshot shows a terminal window with a large amount of encoded file content. The content appears to be a mix of binary data and ASCII characters, possibly a compressed archive or a file with non-printable characters. The terminal has a dark background with light-colored text. At the top, there's a browser-like header with links to Google, Moodle, Classroom, StackOverflow, Calendario, Webmail, and Hacker News.

Figura 2 Secondo esempio

In questo secondo esempio si può notare come attraverso questa vulnerabilità si possa ricostruire l'intera struttura del progetto.

15h00 – 15h10

Ho risolto un problema grafico per i dispositivi mobile, ora le immagini hanno una larghezza massima come la larghezza della finestra, questo per prevenire che le foto sforino dallo schermo.
Vedi sezione problemi del diario.

15h10 – 16h20

Ho implementato la parte mancante del pannello di amministrazione, ora è possibile eliminare gli articoli.

HackerLab

Home Profilo Pannello di amministrazione ▾ Esci

Gestione articoli

test

Test

Vai all'articolo → Elimina

Pubblicato il 20.09.2019 da Administrator



Password leaks

Vai all'articolo → Elimina

Pubblicato il 20.09.2019 da Administrator

← Recenti Vecchi →

Copyright © HackerLab 2019

Figura 3 Pannello amministrazione

16h20 – 16h30
Stesura diario.

Problemi riscontrati e soluzioni adottate

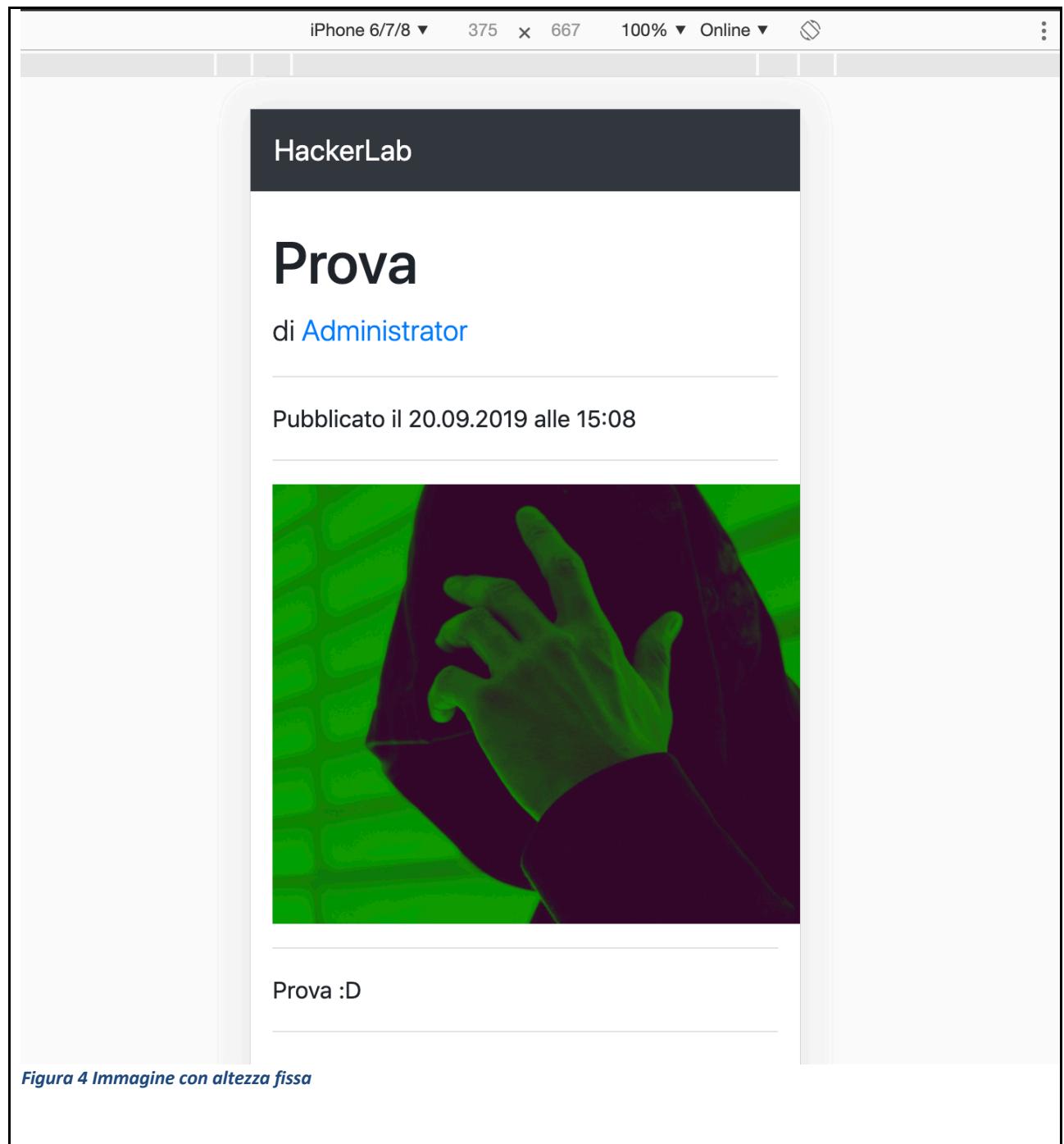
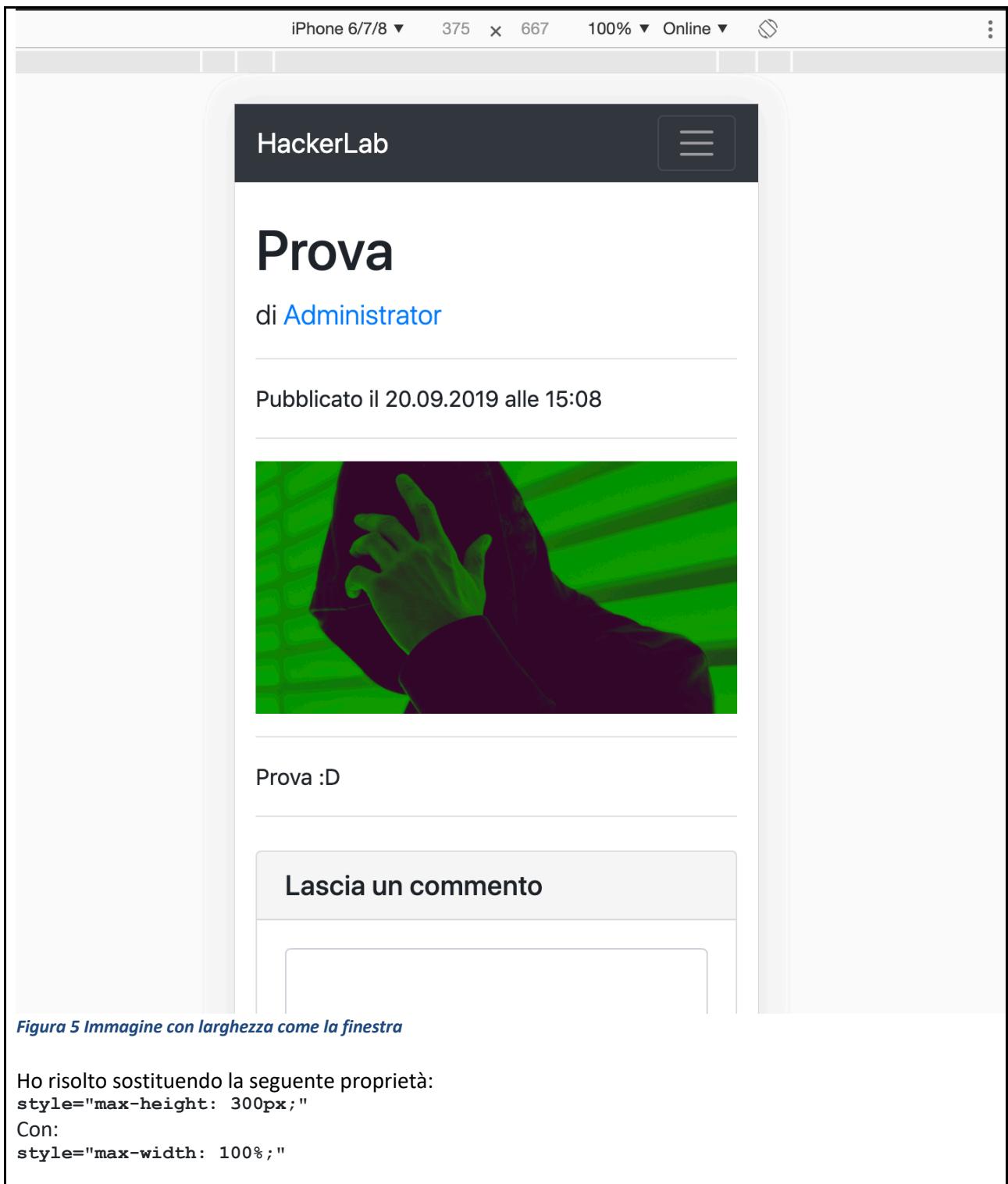


Figura 4 Immagine con altezza fissa



Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianificazione preventiva.

Programma di massima per la prossima giornata di lavoro

Rivedere il codice e valutare le vulnerabilità.

Diario di lavoro

Luogo	Canobbio
Data	24.09.2019

Lavori svolti

13h15 -14h45

Come scritto nel diario precedente, durante queste prime due ore ho commentato tutto il codice da me prodotto. Inoltre ho eseguito alcune modifiche principalmente di stile del codice. Ho separato la classe di connessione al database dalla pagina principale ad una sottoclasse.

15h00 – 16h20

Ho iniziato a creare le documentazioni di come eseguire le vulnerabilità presenti in HackerLab. Al momento le documentazioni si trovano accedendo ad HackerLab sotto forma di articoli web.

Broken Authentication

di [Administrator](#)

Pubblicato il 24.09.2019 alle 16:17

Questi tipi di vulnerabilità possono consentire a un aggressore di catturare o bypassare i metodi di autenticazione utilizzati da un'applicazione web.

All'interno di HackerLab è presente una vulnerabilità di questo tipo.

Per sfruttare questa vulnerabilità basterà utilizzare una comune estensione come per esempio:

[EditThisCookie](#)

Una volta installata l'estensione sarà possibile modificare i cookie all'interno dei siti web.

Noterai che HackerLab ha un cookie chiamato **permission**, il contenuto di questo cookie è familiare, è un testo codificato in base64.

dXNlcg== -> user

Con un po' di fortuna è possibile indovinare quale sarà il permesso di un amministratore, quindi provando per esempio a modificare il cookie in

YWRtaW5pc3RyYXRvcg== -> administrator

e ricaricando la pagina potrai notare delle modifiche nel layout, ora potrai vedere informazioni e pagine aggiuntive come se fossi un amministratore!

Mmm, sono curioso di come potresti sfruttare questa vulnerabilità...

[Fonti](#)

Figura 1 Broken Authentication

File inclusion vulnerability o Directory Traversal

di Administrator

Pubblicato il 24.09.2019 alle 16:17



Una directory traversal (o path traversal) consiste nello sfruttare l'insufficiente validazione della sicurezza / sanificazione dei nomi dei file di input forniti dall'utente, in modo che i caratteri che rappresentano "traverse to parent directory" siano passati attraverso le API dei file.

Grazie a questa descrizione potresti già aver individuato un percorso vulnerabile a questo tipo di attacco, se non lo hai trovato un indizio potrebbe essere l'immagine di questo articolo.

Il percorso tramite il quale vengono ricavate le immagini in HackerLab è il seguente

`/image/?file_name=IMAGE`

Bene, per eseguire questa vulnerabilità basterà sostituire il valore del nome dell'immagine con dei file conosciuti, potremmo per esempio iniziare tentando di capire la struttura del programma provando svariati file:

- .htaccess
- ./composer.json
- e così via

Possiamo notare come nel caso di `/image/?file_name=../composer.json` abbiamo ricevuto una risposta:

```
{  
  "name": "filippofinke/HackerLab",  
  "description": "Sito web per la dimostrazione di vulnerabilità",  
  "authors": [  
    {  
      "name": "Filippo Finke"  
    }  
  ],  
  "require": {  
    "php": ">=5.6",  
    "slim/php-view": "^2.0",  
    "slim/slim": "^3.1",  
    "phpmailer/phpmailer": "^6.0"  
  },  
  "scripts": {  
    "start": "sudo php -S 127.0.0.1:80 -t public"  
  }  
}
```

Attraverso questa risposta possiamo confermare la presenza della vulnerabilità.

Ci saranno altri file accessibili?

[Fonti](#)

Figura 2 File Inclusion o Directory Traversal

Insecure Direct Object References

di [Administrator](#)

Pubblicato il 24.09.2019 alle 16:17

I riferimenti diretti agli oggetti insicuri si verificano quando un'applicazione fornisce l'accesso diretto agli oggetti in base all'input fornito dall'utente. Come risultato di questa vulnerabilità gli aggressori possono aggirare l'autorizzazione e accedere direttamente alle risorse del sistema, ad esempio i record o i file del database.

In base a questa piccola descrizione forse avrai già riconosciuto questa vulnerabilità all'interno di HackerLab.

Se presti attenzione alla pagina di questo post noterai che il percorso per arrivarcì è [/post/3](#)

Quindi possiamo considerare il percorso come [/post/POST_ID](#)

Questo conferma dunque la presenza di questa vulnerabilità.

Chissà cosa può comportare questa vulnerabilità...

Quando navighi presta attenzione :D

[Fonti](#)

Figura 3 Insecure Direct Object References

Account takeover vulnerability

di [Administrator](#)

Pubblicato il 24.09.2019 alle 16:17

Una vulnerabilità di tipo "Account takeover vulnerability" è quando un attaccante riesce a prendere il controllo completo dell'account di un'altra persona registrata ad una determinata piattaforma.

Anche questa vulnerabilità è presente in HackerLab.

Questa vulnerabilità è più difficile da identificare, per accedere ad HackerLab si dispongono di solamente una opzione, ovvero di accedere con email e password.

Se hai prestato attenzione a ciò che ho scritto precedentemente ti sarai soffermato sui parametri [email](#) e [password](#), perfetto. Analizzando bene i due parametri possiamo dire che il parametro [email](#) non è possibile da attaccare in quanto non è possibile eseguirne una modifica, mentre in HackerLab è presente una funzionalità di recupero password che può modificare il parametro [password](#).

Bene, abbiamo trovato cosa testare per rilevare se è presente una vulnerabilità di questo tipo.

Richiedendo una email di recupero password possiamo notare che il contenuto dell'email è simile al seguente:

[Recupera la tua password premendo il seguente link:](#)

http://hackerlab.ch/?reset_token=MTU20Dk40DU20A%3D%3D

Possiamo notare un parametro, [reset_token](#), che andremo ad attaccare.

Se si analizza più attentamente il parametro possiamo notare che è una codifica in base64, andandola a decodificare otteniamo:

[156898856](#)

A primo impatto può sembrare un numero casuale, ma provando ad inviare più email di recupero possiamo notare che continua ad incrementare con una logica, ovvero quella del tempo.

Il token di recupero è quindi la codifica in base64 del tempo di quando è stato richiesto il recupero.

Possiamo fare una bozza del codice:

[\\$token = base64_encode\(time\(\)\);](#)

Questo è tutto, chissà come potrai sfruttarla...

Figura 4 Account takeover

16h20 – 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 pianifica.

Programma di massima per la prossima giornata di lavoro

Diario di lavoro

Luogo	Canobbio
Data	26.09.2019

Lavori svolti

Non ho svolto nessun lavoro in quanto non sono stato presente in sede causa reclutamento militare.

Problemi riscontrati e soluzioni adottate

Nessun problema.

Punto della situazione rispetto alla pianificazione

-

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	27.09.2019

Lavori svolti

13h15 – 13h40

Ho creato la guida per la vulnerabilità Cross-site Scripting (XSS).

Cross Site Scripting (XSS)

di [Administrator](#)

Pubblicato il 27.09.2019 alle 13:33

Gli attacchi Cross-Site Scripting (XSS) sono un tipo di iniezione, in cui gli script dannosi vengono iniettati in siti web altrimenti benigni e affidabili. Gli attacchi XSS si verificano quando un attaccante utilizza un'applicazione web per inviare codice dannoso, generalmente sotto forma di script lato browser, a un altro utente finale. I difetti che permettono il successo di questi attacchi sono abbastanza diffusi e si verificano ovunque un'applicazione web utilizza l'input di un utente all'interno dell'output che genera senza convalidarlo o codificarlo.

Un attaccante può usare XSS per inviare uno script dannoso ad un utente ignaro. Il browser dell'utente finale non ha modo di sapere che lo script non deve essere considerato attendibile e lo eseguirà. Poiché pensa che lo script provenga da una fonte attendibile, lo script dannoso può accedere a qualsiasi cookie, token di sessione o altre informazioni sensibili conservate dal browser e utilizzate con quel sito. Questi script possono anche riscrivere il contenuto della pagina HTML.

All'interno di HackerLab è presente una vulnerabilità di tipo XSS, ed è proprio in questa pagina che può accadere.

Nonostante vi siano dei controlli nella validità del testo contenuto in un articolo è possibile comunque eseguire un attacco di tipo XSS. Di seguito segue un esempio:

`Cliccami`

Prova a cliccare il seguente testo:Cliccami

Potrai notare l'esecuzione dello script javascript.

Questa vulnerabilità è molto pericolosa e potente.

[Fonti](#)

[Figura 1 Articolo XSS](#)

13h40 – 14h05

Ho implementato una vulnerabilità di tipo Failure to Restrict URL Access e creato un articolo all'interno del blog che spiega come sfruttare la vulnerabilità.

Failure to Restrict URL Access

di [Administrator](#)

Pubblicato il 27.09.2019 alle 13:56

Se l'applicazione non riesce a limitare adeguatamente l'accesso agli URL, la sicurezza può essere compromessa da una tecnica chiamata navigazione forzata. La navigazione forzata può essere un problema molto serio se un aggressore cerca di raccogliere dati sensibili attraverso un browser Web richiedendo pagine specifiche o file di dati. Questo significa che l'applicativo è affetto da una vulnerabilità di tipo Failure to restrict URL Access.

HackerLab a sua volta è vulnerabile a questo tipo di attacco. Solitamente nel file robots.txt vengono salvate delle regole riguardanti i percorsi del sito web specificando ai bot che indicizzano siti web cosa fare.

Richiedendo il file robots.txt al percorso `/robots.txt` è possibile vedere il seguente contenuto:

```
# Regola da applicare a tutti i robot
User-agent: *
# Non fare accedere alle pagine di amministrazione
Disallow: info.php
Disallow: /admin/
```

Possiamo notare due regole che ci possono interessare, ovvero il fatto di bloccare l'indicizzazione della cartella `admin` e del file `info.php`.

Non ci resta che provare ad accedere a queste cartelle direttamente dal browser.

Accedendo alla pagina `/info.php` possiamo notare come vengano caricate e mostrate tutte le informazioni riguardanti PHP, questo è molto pericoloso in quanto un attaccante può ricercare vulnerabilità in base alle versioni installate, inoltre è possibile vedere altre informazioni come per esempio il percorso del progetto, ...

Questa vulnerabilità sfruttata con altre vulnerabilità può essere molto pericolosa.

Fonti

[Figura 2 Articolo Failure to Restrict URL Access](#)

14h05 – 14h20

Implementata una vulnerabilità di tipo Security Misconfiguration, inoltre ho creato anche il relativo articolo all'interno del sito web che la documenta.

Security Misconfiguration

di [Administrator](#)

Pubblicato il 27.09.2019 alle 14:12

Una vulnerabilità di tipo Security Misconfiguration è quando un applicativo è messo in produzione con impostazioni di configurazione errate. Esempi possono essere: password di default, messaggi di debug, ...

È una vulnerabilità molto comune all'interno di siti web.

Una vulnerabilità di questo tipo è presente all'interno di HackerLab.

Ti basterà andare nella sezione dei commenti e aprire il profilo di un utente "eliminato", noterai un messaggio di errore proveniente dal Framework utilizzato per lo sviluppo di questo sito web.

In questo modo l'attaccante avrà informazioni in più sul sito web e possibili vulnerabilità da sfruttare.

Fonti

[Figura 3 Articolo Security Misconfiguration](#)

14h20 – 14h45

Ho creato un utente dedicato al sito web per prevenire che attraverso vulnerabilità si possano toccare anche altri database esterni.

15h00 – 16h20

Ho iniziato a pensare a come implementare la vulnerabilità SQL Injection in un modo che non sia distruttiva. Al momento è stata implementata all'interno della funzionalità di ricerca di HackerLab.

I problemi che può causare al momento sono:

- Update, Insert, Delete, Select e Drop del database hackerlab
- Possibilità di eliminare file

Il problema che devo risolvere è la possibilità di eliminare file. Al momento se un utente modifica tramite SQL Injection l'immagine di un articolo può eliminare qualsiasi file a sua scelta, esempio:

`a%'; UPDATE articles SET image = ".../composer.json"; --`

Questo perché la funzione di delete è implementata nel seguente modo:

`unlink(__DIR__.'/../../storage/'.$article['image']);`

Quindi, ho intenzione di rendere sicura la rimozione del file in modo di permettere solamente azioni al database.

16h20 – 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

Rendere sicura eliminazione di file, implementare la funzionalità di reset dei dati e del database.

Diario di lavoro

Luogo	Canobbio
Data	01.10.2019

Lavori svolti

13h15 – 13h50

Ho aiutato un compagno, Giulio Bosco, con un problema riguardante un applicativo in Java.

13h50 – 14h45

Come definito nello scorso diario, ho reso l'eliminazione di file correlati con gli articoli sicura.

Mi sono documentato sulla funzione basename di php

(<https://www.php.net/manual/en/function.basename.php>), attraverso questa funzione posso ricavare in modo sicuro il nome del file di un articolo senza il percorso stesso, in questo modo non sarà possibile eliminare file al di fuori della cartella storage sfruttando la vulnerabilità di SQL Injection.

Il codice per l'eliminazione dei file è diventato il seguente:

```
$file = basename($article["image"]);
$path = __DIR__ . '/../../storage/' . $file;
if (file_exists($path)) {
    unlink($path);
}
```

15h00 – 16h20

Ho iniziato a pensare come implementare una funzionalità di reset all'interno del sito web, inoltre ho iniziato la stesura dell'articolo riguardante SQL Injection.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

Continuare lo sviluppo della funzionalità di reset e la documentazione per la vulnerabilità SQL Injection.

Diario di lavoro

Luogo	Canobbio
Data	03.10.2019

Lavori svolti

13h15 – 13h50

Ho aggiornato il mio responsabile sullo stato del progetto mostrando quanto fatto fino ad ora. E sono sorte alcune aggiunte da eseguire riguardante il lato della documentazione degli exploit, per ogni exploit è richiesto anche una sezione che spiega in modo dettagliato come sfruttare la vulnerabilità in modo che anche utenti meno esperti possano riuscire ad eseguire tutte le vulnerabilità documentate. Inoltre mi sono stati forniti altri spunti da poter utilizzare, come per esempio nell'ambito di SQL Injection.

13h50 – 14h35

Mi sono documentato sul funzionamento del metodo HttpOnly all'interno dei cookies.

<https://www.owasp.org/index.php/HttpOnly>

Ho scoperto che grazie a questo metodo è possibile prevenire l'accesso a dei cookie da parte di javascript. Ho quindi provato ad impostare un cookie HttpOnly per testare l'accesso e il risultato è stato il seguente:

The screenshot shows a browser's developer tools Network tab. A cookie named "HttpOnlycookie" is listed. The "Value" field contains "Set-Cookie: NonHttpOnlyCookie=". The "HttpOnly" checkbox is checked. Other fields include "Dominio": 127.0.0.1, "Percorso": /, "Scadenza": Sat Oct 03 2020 14:03:21 GMT+0200 (Ora legale dell'Europa centrale), "SameSite": No Restriction, and checkboxes for "Solo Host" (checked), "Sessione" (unchecked), "Sicuro" (unchecked), and "Solo Http" (checked). Below this, another cookie named "NonHttpOnlyCookie" is shown.

Provando ad accedere ai cookie da javascript con `document.cookie`:

"NonHttpOnlyCookie=""

Quindi il cookie HttpOnlycookie viene reso inaccessibile.

Ho inoltre provato a scrivere un piccolo script in JavaScript per provare ad eseguire un bypass di questa funzionalità e questo è stato il risultato:

```
var xhr = new XMLHttpRequest();
xhr.onreadystatechange = function() { if (xhr.readyState == 4) {
  console.log(xhr.getResponseHeader('Set-Cookie'));
}
};
xhr.open('GET', '/', true);
xhr.send(null);
```

Console: Refused to get unsafe header "Set-Cookie"

Viene protetto in qualsiasi caso anche all'interno di altre funzioni.

14h35 – 14h45

15h00 – 15h05

Aggiornamento dello stile del sito, rimossi i footer in modo che il contenuto del sito sia più visibile.

15h05 – 16h20

Ho utilizzato questo tempo per documentarmi su delle vulnerabilità.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

Diario di lavoro

Luogo	Canobbio
Data	04.10.2019

Lavori svolti

13h15 – 14h00

Ho creato l'articolo relativo alla vulnerabilità di tipo SQL Injection all'interno del sito web.

SQL Injection

di [Administrator](#)

Pubblicato il 04.10.2019 alle 13:51

Nella sicurezza informatica SQL injection è una tecnica di code injection, usata per attaccare applicazioni di gestione dati, con la quale vengono inserite delle stringhe di codice SQL malevole all'interno di campi di input in modo che queste ultime vengano poi eseguite. Questa tecnica viene utilizzata per ricavare dati non direttamente visibili o accessibili dalle banche dati all'interno di siti web. Questa falla è molto comune e pericolosa.

Una falla di questo tipo è presente all'interno di HackerLab, più precisamente nella barra di ricerca. Per eseguire un attacco di questo tipo si ha bisogno di una conoscenza di SQL Injection e un po' di fortuna.

All'interno della barra di ricerca è quindi possibile inserire del codice SQL malevolo e farlo eseguire.

Un esempio di semplice query all'interno della barra di ricerca che si può utilizzare è la seguente:

`test%' OR 1=1; --`

Questo codice non è malevolo ma dimostra la vulnerabilità, stiamo completando la query utilizzata per eseguire la ricerca che possiamo presumere sia simile a:

`SELECT * FROM articles WHERE title LIKE $ricerca;`

E la stiamo trasformando nella seguente query:

`SELECT * FROM articles WHERE title LIKE '%test%' OR 1=1; --`

Quindi questa query ritornerà tutti gli articoli presenti nel sito web.

Ci sono moltissime altre possibilità, sta a te scoprirle!

Fonti

[Figura 1 Articolo SQL Injection](#)

14h00 – 14h45

15h00 – 16h20

Ho iniziato a creare le guide dettagliate di come eseguire le vulnerabilità, ho iniziato dalla vulnerabilità di tipo Broken Authentication che ho terminato. È disponibile nella cartella documentazione/vulnerabilità.

Ho inoltre completato la guida sulla vulnerabilità File Inclusion o Directory Traversal e mi sono documentato sul formato della cartella .git per la gestione di GitHub.

<https://www.siteground.com/tutorials/git/directory-structure/>

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

Continuare a documentare le vulnerabilità in un file word.

Diario di lavoro

Luogo	Canobbio
Data	08.10.2019

Lavori svolti

13h15 – 14h00

Ho creato la guida sulla vulnerabilità Insecure Direct Object References.

14h00 – 14h45 15h00 – 15h15

Ho creato la guida riguardante la vulnerabilità Account Takeover Vulnerability.

15h15 – 16h00

Ho creato la guida riguardante la vulnerabilità Cross Site Scripting (XSS).

16h00 – 16h20

Formattazione e rilettura delle guide prodotte fino ad ora.

16h20 – 16h30

Stesura del diario.

Tutte le documentazioni create sono presenti nella cartella /documentazione/vulnerabilità/docx del progetto.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

Continuare a creare i manuali per l'esecuzione delle vulnerabilità.

Diario di lavoro

Luogo	Canobbio
Data	10.10.2019

Lavori svolti

13h15 – 14h20

Ho creato la documentazione per la vulnerabilità Failure To Restrict URL Access.

14h20 – 14h45

Ho creato la documentazione per la vulnerabilità Security Misconfiguration.

15h00 – 16h00

Ho creato la documentazione per la vulnerabilità SQL Injection.

16h00 – 16h20

Ho ristrutturato la repository di GitHub rinominando tutti i diari in modo che vengano mostrati in ordine cronologico. Inoltre ho riguardato le documentazioni prodotte riguardandone la formattazione ed il contenuto.

16h20 – 16h30

Stesura diario

Tutte le documentazioni create sono presenti nella cartella /documentazione/vulnerabilità/docx del progetto.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianificazione.

Programma di massima per la prossima giornata di lavoro

Procedere all'implementazione della procedura di ripristino del sito web.

Diario di lavoro

Luogo	Canobbio
Data	11.10.2019

Lavori svolti

13h15 – 14h45
Ho assistito alla presentazione del docente Valsangiacomo per quanto riguarda la valutazione dei progetti d'esame.

15h00 – 16h20
Ho implementato la funzionalità di reset che permette di ricaricare tutti i dati di default all'interno del database di HackerLab. Questa funzionalità sarà accessibile in qualsiasi momento nella barra di navigazione o al percorso /reset.



HackerLab di Filippo Finke [Home](#) [Registrati](#) [Reset database](#)

Ultimi articoli

SQL Injection
[Vai all'articolo →](#)
Pubblicato il 11.10.2019 da [Administrator](#)

Security Misconfiguration
[Vai all'articolo →](#)
Pubblicato il 11.10.2019 da [Administrator](#)

Failure to Restrict URL Access
[Vai all'articolo →](#)
Pubblicato il 11.10.2019 da [Administrator](#)

[← Recenti](#) [Vecchi →](#)

Figura 1 Funzionalità di reset.
Ho implementato la funzionalità di reset nel seguente modo:

```
public static function reset() {
    $query_sql = file_get_contents(__DIR__ . '/../restore.sql');
    $query = self::get()->query($query_sql);
    return $query;
}
```

Viene caricato un file contenente le istruzioni per il reset del database e tutte le query vengono eseguite.

16h20 – 16h30
Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	15.10.2019

Lavori svolti

13h15 – 13h20

Il docente Raimondi ha aperto la porta 587 del firewall in modo che le connessioni SMTP possano essere effettuate, quindi per testare la funzione di recupero password non è più richiesto l'ausilio di una rete esterna.

13h20 – 13h50

Ho modificato la funzionalità di reset del sito web, una volta resettato il database viene mostrato lo stato dell'azione ed inoltre l'utente viene riportato alla pagina di logout.

```
if (Database::reset()) {  
    $_SESSION["success"] = "Database ripristinato con successo!";  
} else {  
    $_SESSION["error"] = "Impossibile ripristinare il database!";  
}  
return $response->withRedirect("/logout", 302);
```

Questo quindi introduce una vulnerabilità aggiuntiva avanzata in quanto un utente può risultare loggato con un utente ormai eliminato se blocca la richiesta di redirect alla pagina logout.

13h50 – 14h25

Ho revisionato ancora una volta tutte le guide delle vulnerabilità e dopo averle revisionate ho generato i vari PDF di esse.

14h25 – 14h45

Ho iniziato a descrivere il progetto e la sua struttura per l'abstract del progetto in una pagina. Il file si trova al percorso /abstract/abstract.docx

15h00 – 15h30

Ho aggiunto al pannello di amministrazione la possibilità di abilitare o disabilitare un utente

Gestione utenti

The screenshot shows a user management interface with two entries:

- Administrator**:
 - Email: admin@hackerlab.ch
 - Username: administrator
 - Action buttons: "Pagina profilo →" (blue), "Disabilita" (yellow, highlighted with a red box), and "Elimina" (red).
- Filippo Finke (Disabilitato)**:
 - Email: filippo.finke@samtrevano.ch
 - Username: user
 - Action buttons: "Pagina profilo →" (blue), "Abilita" (yellow, highlighted with a red box), and "Elimina" (red).

Figura 1 Possibilità di abilitare o disabilitare un utente.

Un utente disabilitato non può eseguire l'accesso all'applicativo.

La funzione per abilitare un utente è stata implementata nel seguente modo:

```
public static function enable($user_id) {
    $query = Database::get()->prepare("UPDATE users SET enabled = 1 WHERE id = :user_id");
    $query->bindParam(":user_id", $user_id);
    $query->execute();
    if (!$query) {
        $_SESSION["error"] = "Impossibile abilitare l'utente!";
        return false;
    }
    $_SESSION["success"] = "Utente abilitato!";
    return true;
}
```

Viene semplicemente impostato un flag (enabled) ad 1.

La funzione per disabilitare l'utente è praticamente identica solo che al posto che impostare il flag a 1 viene impostato a 0.

15h30 – 16h20

Ho continuato con la documentazione revisionando le librerie utilizzate ed iniziato a scrivere il capitolo dell'implementazione.

16h20 – 16h30

Stesura del diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato

Punto della situazione rispetto alla pianificazione

Molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

Continuare con la revisione della documentazione.

Diario di lavoro

Luogo	Canobbio
Data	17.10.2019

Lavori svolti

13h15 – 13h30

Ho distanziato i pulsanti di abilitazione e disabilitazione di un utente, questo in modo che anche su dispositivi mobili si veda in modo corretto.

Gestione utenti

Administrator Pagina profilo →
admin@hackerlab.ch
administrator Disabilita Elimina

Filippo Finke Pagina profilo →
Disabilitato
filippo.finke@samtrevano.ch
user Abilita Elimina

Figura 1 Pannello di amministrazione

13h30 – 13h40

Ho aggiornato il formatore sullo stato del progetto.

13h40 – 14h00

Come consigliato dal formatore, ho implementato una notifica di conferma quando si richiede un reset del database.

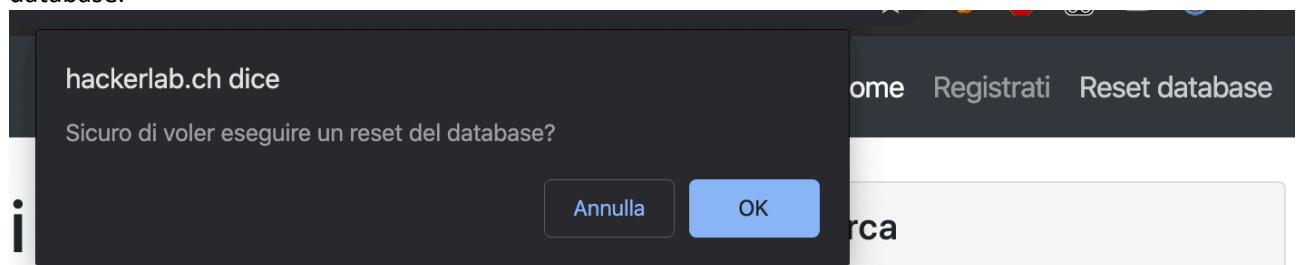


Figura 2 Notifica che chiede la conferma.

14h00 – 14h45

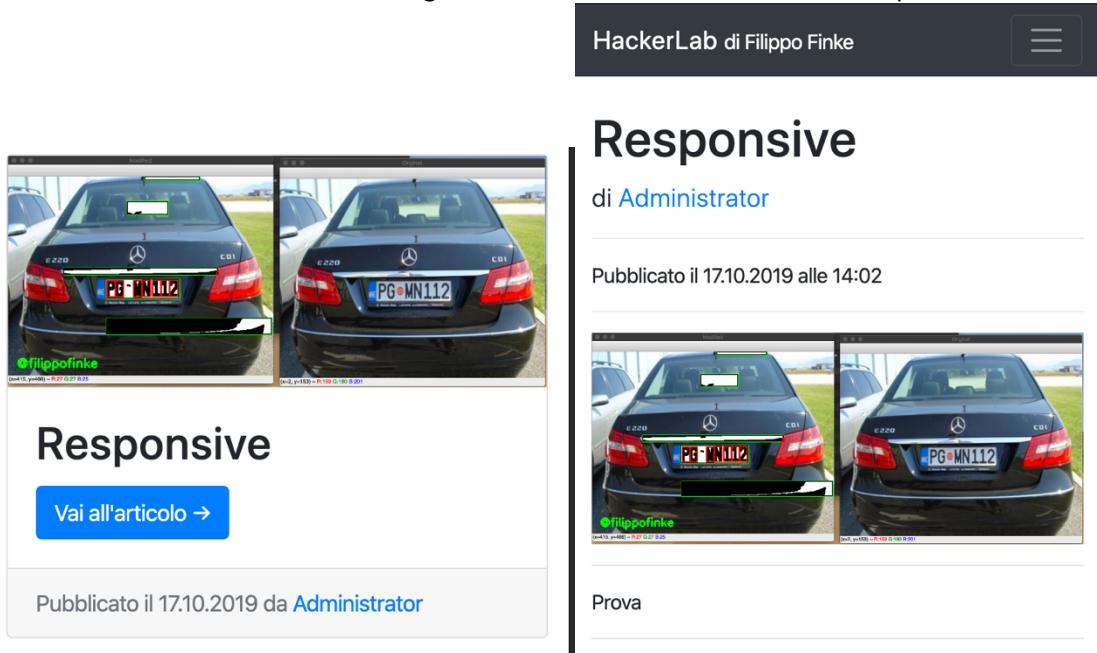
Ho ispezionato tutti il sito web navigandolo attraverso un emulazione di un iphone7, di conseguenza ho corretto alcune cose per dispositivi mobile.

Quando si accede ad una sezione riservata agli utenti registrati ora è presente un pulsante che reindirizza al form di accesso.

Per eseguire questa azione devi aver eseguito l'accesso! [Accedi!](#)

Figura 3 Schermata che richiede l'accesso.

Tutte le schermate contenenti immagini sono mostrate correttamente in dispositivi mobile.



15h00 – 16h20

Revisionato la documentazione scritta fino ad ora, controllato e corretto errori di lingua.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti.

Programma di massima per la prossima giornata di lavoro

Proseguire con il capitolo dell'implementazione e iniziare a documentare le vulnerabilità nascoste.

Diario di lavoro

Luogo	Canobbio
Data	18.10.2019

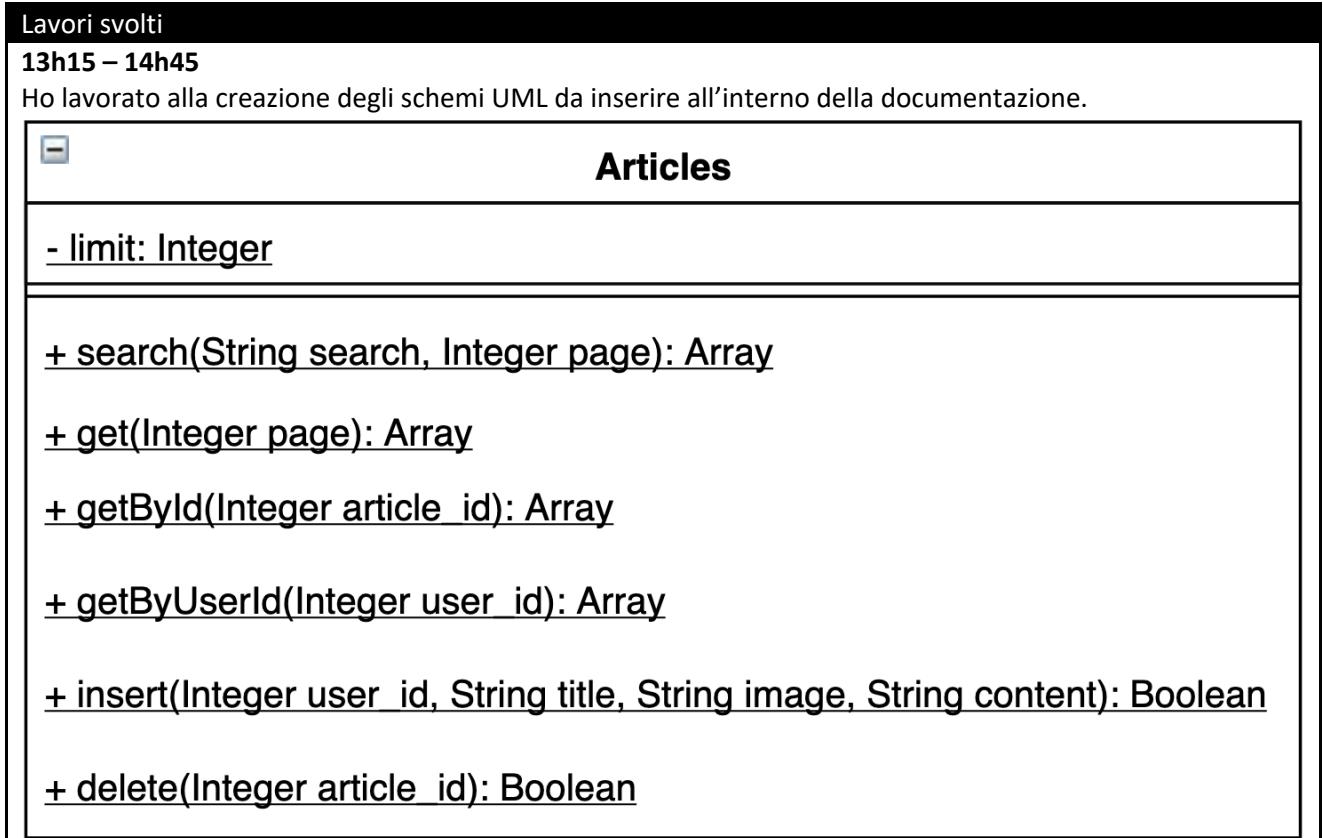


Figura 1 Diagramma UML classe Articles.

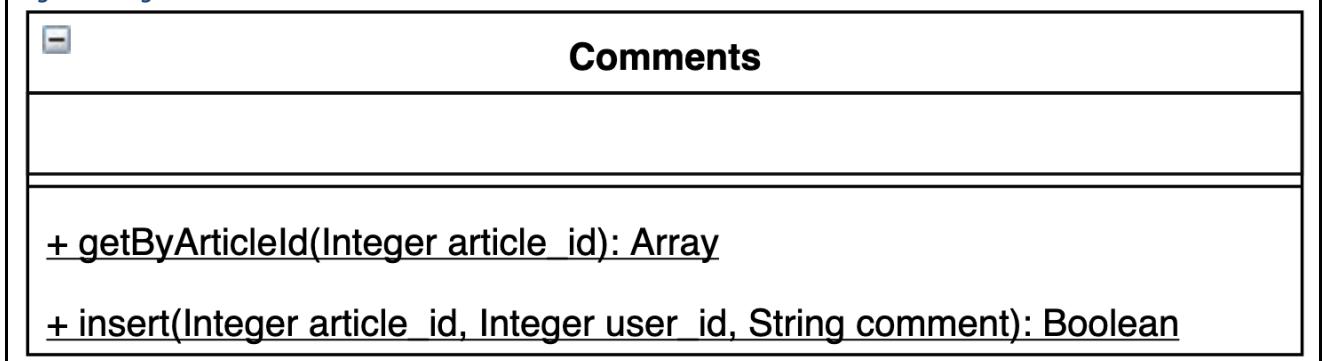


Figura 2 Diagramma UML classe Comments.

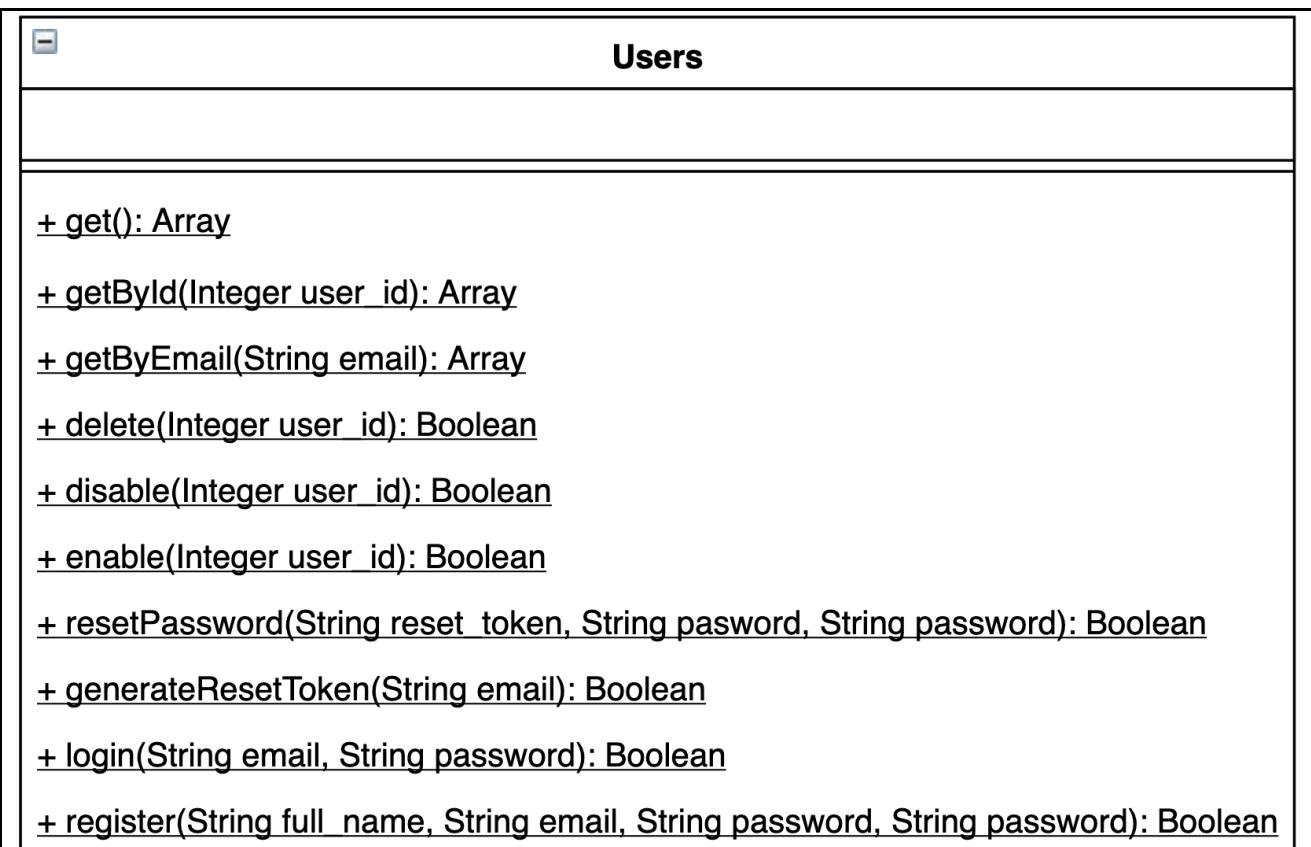


Figura 3 Diagramma UML della classe *Users*.

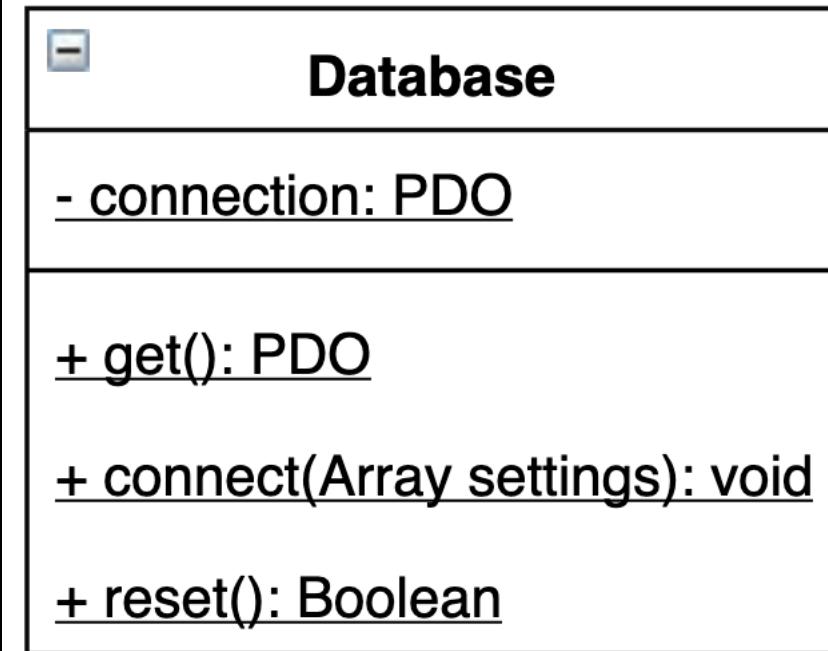


Figura 4 Diagramma UML della classe *Database*.

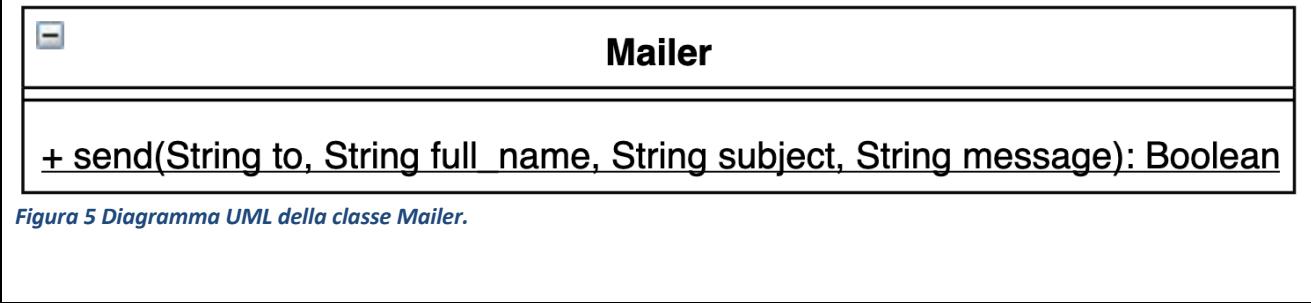


Figura 5 Diagramma UML della classe *Mailer*.

15h00 – 16h20

Ho continuato il capitolo dell'implementazione all'interno della documentazione.

16h20 – 16h30

Stesura del diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

Documentazione vulnerabilità nascoste e implementazione nella documentazione.

Diario di lavoro

Luogo	Canobbio
Data	22.10.2019

Lavori svolti

13h15 -16h20

Ho continuato il capitolo dell'implementazione all'interno della documentazione.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	24.10.2019

Lavori svolti

13h15 -14h10

Ho revisionato il codice scritto documentando in un modo migliore la presenza di vulnerabilità all'interno del codice.

14h10 – 14h45 15h00 - 16h20

Ho iniziato a documentare le vulnerabilità “nascoste” di HackerLab. Ho iniziato con lo sviluppo di script di esempio per degli attacchi di tipo bruteforce.

Questo è un esempio di bruteforce del login di HackerLab. Si inserisce un email ed una lista di password, lo script proverà ad accedere con tutte le password inserite nella lista, se riuscirà ad accedere mostrerà la password utilizzata.

```
[i] Dimostrazione di bruteforce del login di HackerLab
[i] Autore: Filippo Finke
[?] Inserisci una email: filippo.finke@samtrevano.ch
[i] Caricate 501 passwords!
[-] Accesso con    123456      -> FALLITO! (0/501)
[-] Accesso con    password    -> FALLITO! (1/501)
[-] Accesso con    12345678   -> FALLITO! (2/501)
[-] Accesso con    pussy       -> FALLITO! (3/501)
[-] Accesso con    12345       -> FALLITO! (4/501)
[-] Accesso con    dragon     -> FALLITO! (5/501)
[-] Accesso con    qwerty     -> FALLITO! (6/501)
[-] Accesso con    696969     -> FALLITO! (7/501)
[-] Accesso con    mustang    -> FALLITO! (8/501)
[-] Accesso con    letmein    -> FALLITO! (9/501)
[-] Accesso con    1234       -> SUCCESSO!
[!] PASSWORD TROVATA: 1234
[!] CREDENZIALI -> filippo.finke@samtrevano.ch:1234
```

Figura 1 Dimostrazione bruteforce login

Questo invece è un esempio di email checker, ovvero uno script che si occupa di verificare se una email è registrata all'interno di HackerLab. Per la creazione di questo programma è stata sfrutta la chiamata del recupero password. Questa chiamata permette di stabilire se un account esiste oppure no.

```
[i] Dimostrazione di email checker di HackerLab
[i] Autore: Filippo Finke
[i] Caricate 32 emails!
[-] Email      gerry.lillie@hackerlab.ch      -> INESISTENTE! (0/32)
[-] Email      otha.arzate@hackerlab.ch      -> INESISTENTE! (1/32)
[-] Email      jonathon.wentworth@hackerlab.ch  -> INESISTENTE! (2/32)
[-] Email      victor.hartness@hackerlab.ch    -> INESISTENTE! (3/32)
[-] Email      allen.fenimore@hackerlab.ch     -> INESISTENTE! (4/32)
[-] Email      filippo.finke@samtrevano.ch    -> REGISTRATA! (5/32) 
[-] Email      darius.holloway@hackerlab.ch    -> INESISTENTE! (6/32)
[-] Email      glenn.wallis@hackerlab.ch     -> INESISTENTE! (7/32)
[-] Email      isiah.branstetter@hackerlab.ch -> INESISTENTE! (8/32)
[-] Email      adalberto.maheux@hackerlab.ch -> INESISTENTE! (9/32)
[-] Email      tristan.nottage@hackerlab.ch   -> INESISTENTE! (10/32)
[-] Email      derrick.gressett@hackerlab.ch -> INESISTENTE! (11/32)
[-] Email      julio.cullum@hackerlab.ch    -> INESISTENTE! (12/32)
[-] Email      whitney.schleusner@hackerlab.ch -> INESISTENTE! (13/32)
```

Figura 2 Dimostrazione bruteforce email

Questi due script con una grande quantità di dati possono essere molto pericolosi in quanto ci sarebbero alte probabilità di trovare account registrati (Sempre se hackerlab fosse online e famoso).

16h20- 16h30

Stesura del diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianificazione.

Programma di massima per la prossima giornata di lavoro

Creare le documentazioni docx e pdf delle vulnerabilità nascoste.

Diario di lavoro

Luogo	Canobbio
Data	25.10.2019

Lavori svolti

13h15 – 14h45

Ho creato la documentazione per l'attacco bruteforce al login di HackerLab ho inoltre finalizzato il programma di esempio commentandolo.

15h00 – 16h20

Ho creato la documentazione per l'attacco bruteforce alle email di HackerLab ho inoltre finalizzato il programma di esempio commentandolo.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	05.11.2019

Lavori svolti

13h15 – 14h45 15h00 – 16h20

Mi sono occupato di procedere con il capitolo dell'implementazione della documentazione.

Ho quindi documentato nella sezione di Sviluppo dell'implementazione:

- Connessione al database
- Invio di posta elettronica

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	07.11.2019

Lavori svolti

13h15 – 14h45 15h00 -16h20

Ho continuato il capitolo dell'implementazione all'interno della documentazione. Ho continuando documentando i seguenti punti:

- Gestione delle sessioni
- Vulnerabilità
 - o Security Misconfiguration
 - o SQL Injection
 - o Failure To Restrict URL Access
 - o Cross Site Scripting

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

Continuare capitolo implementazione per ogni vulnerabilità

Diario di lavoro

Luogo	Canobbio
Data	08.11.2019

Lavori svolti

13h15 – 13h40

Ho avuto un colloquio con il docente Valsangiacomo per quanto riguarda un progetto futuro.

13h40 – 14h45 15h00 -16h20

Ho continuato con il capitolo implementazione della documentazione, ho documentato i seguenti capitoli:

- Broken Authentication
- Insecure Direct Object References

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	12.11.2019

Lavori svolti

13h15 – 16h20

Ho continuato con il capitolo dell'implementazione documentando le seguenti vulnerabilità:

- File Inclusion o Directory Traversal
- Account Takeover

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianificia.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	14.11.2019

Lavori svolti

13h15 – 13h30

Ho aggiornato il mio formatore sullo stato del progetto

13h30 – 16h20

Ho continuato la documentazione nel capitolo di implementazione. Ho iniziato a documentare le vulnerabilità avanzate

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Non ho riscontrato nessun problema.

Punto della situazione rispetto alla pianificazione

Mi trovo avanti rispetto alla pianificazione.

Programma di massima per la prossima giornata di lavoro

Documentare i vari UML e finire di documentare vulnerabilità avanzate.

Diario di lavoro

Luogo	Canobbio
Data	15.11.2019

Lavori svolti

13h15 – 14h45 15h00 – 16h20

Ho continuato il capitolo dell'implementazione documentando:

- Bruteforce login
- Bruteforce email

Ho inoltre descritto le relazioni tra le classi nella sezione degli UML e aggiornato i seguenti capitoli della documentazione:

- Mancanze/limitazioni conosciuti
- Conclusioni
- Sviluppi futuri
- Considerazioni personali
- Sitografia
- Allegati

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

Terminare sitografia ed iniziare a documentare i test.

Diario di lavoro

Luogo	Canobbio
Data	19.11.2019

Lavori svolti

13h15 – 14h45 15h00 – 16h20

Ho revisionato quanto scritto fino ad ora controllando:

- Documentazione
- Guide
- Abstract

Ho inoltre iniziato a riportare i test eseguiti durante lo sviluppo all'interno della documentazione.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	21.11.2019

Lavori svolti

13h15 – 13h45

Modificato la navigazione tramite pagine all'interno del sito web aggiungendo un controllo per prevenire pagine inesistenti.

13h45 – 14h45 15h00 – 16h20

Ho continuato la documentazione inserendo e completando i seguenti capitoli:

- Protocollo di test
- Risultati test

16h20 – 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 pianifica.

Programma di massima per la prossima giornata di lavoro

Rileggere e controllare la documentazione, iniziare a creare un GANTT consuntivo.

Diario di lavoro

Luogo	Canobbio
Data	22.12.2019

Lavori svolti

13h15 – 14h00

Aggiunto ulteriori controlli negli input lato client sfruttando HTML5.

Nome e cognome:

```
<input type="text" class="form-control" name="full_name" placeholder="Nome e cognome" pattern="^ [a-zA-Z]* \s{0,1} [a-zA-Z]* $" required>
```

Password:

```
<input type="password" class="form-control" name="password" placeholder="Password" minlength="4" required>
```

Ricerca:

```
<input type="text" class="form-control" name="search" placeholder="Ricerca..." required>
```

Titolo:

```
<input type="text" class="form-control" name="title" placeholder="Titolo" maxlength="255" required>
```

Contenuto:

```
<textarea class="form-control" name="content" rows="10" placeholder="Contenuto" maxlength="2000" required></textarea>
```

14h00 - 14h45 15h00 – 16h20

Controllo e revisione documentazione.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica iniziale.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	26.11.2019

Lavori svolti

13h15 – 14h00

Corretto errori di ortografia presenti nella documentazione

14h00 – 14h20

Corretto formattazione della documentazione mettendo il tutto in tipo di testo giustificato.

14h20 – 14h45

Approfondito la documentazione e i commenti del codice.

15h00 – 16h20

Ho eseguito una pulizia del codice risolvendo piccoli bug documentati nella sezione problemi riscontrati.

Eseguito le seguenti modifiche:

- Rinominato i pulsanti delle pagine
- Pulsante per tornare indietro da un articolo

Il pulsante per tornare alla pagina precedente è stato implementato nel seguente modo:

```
<button type="button" class="btn btn-secondary" onclick="history.go(-1);">Torna  
indietro</button>
```

Quando il pulsante viene premuto l'utente verrà rimandato di una pagina indietro rispetto alla sua cronologia.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Risolto problema di impaginazione, il numero di pagine massimo era calcolato in modo errato.

Ho risolto utilizzando la funzione **ceil** al posto della funzione **round** per arrotondare il numero della pagina.

In questo modo se per esempio gli articoli sono **10** e il massimo per pagina è **3**:

$10 / 3 = 3.33 \rightarrow 4$

4 sono le pagine

Mentre prima era:

$10 / 3 = 3.33 \rightarrow 3$

3 sono le pagine

Il problema di paginazione era presente anche quando un utente eseguiva la ricerca all'interno del sito, ho risolto implementando una funzione che si occupa di ricavare tutti i risultati della ricerca dell'utente.

```
/**  
 * Metodo che permette di ricavare la pagina massima di una ricerca.  
 *  
 * @param String $search La ricerca.  
 * @return Integer La pagina massima.  
 */
```

```
public static function getSearchMaxPage($search)
{
    $search = '%' . $search . '%';
    $query = Database::get()->prepare("SELECT COUNT(*) FROM articles WHERE title LIKE
:title");
    $query->bindParam(":title", $search, PDO::PARAM_STR);
    $query->execute();
    $maxPage = ceil($query->fetch(PDO::FETCH_NUM)[0] / self::$limit) - 1;
    if ($maxPage < 0) {
        $maxPage = 0;
    }
    return $maxPage;
}
```

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	28.11.2019

Lavori svolti

13h15 – 16h20

Revisione del codice scritto fino ad ora aggiunto il supporto per la versione di visione tablet.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	29.11.2019

Lavori svolti

13h15 – 16h20

Ho continuato la revisione della documentazione correggendo alcuni piccoli errori e approfondendo alcuni temi. Inoltre ho eseguito nuovamente il test di tutto il sito web nei vari formati disponibili, quindi Desktop, Tablet e Mobile.

HackerLab di Filippo Finke

Home Registrati Reset database

Ultimi articoli

test
Vai all'articolo →
Pubblicato il 28.11.2019 da [Test](#)

SQL Injection
Vai all'articolo →
Pubblicato il 28.11.2019 da [Administrator](#)

Security Misconfiguration
Vai all'articolo →
Pubblicato il 28.11.2019 da [Administrator](#)

Cerca
Ricerca... Cerca!

Accedi
Indirizzo email Email
Password
Accedi oppure [Registrati](#)
[Password dimenticata?](#)

← Pagina precedente [Prossima pagina →](#)

Figura 1 Versione desktop

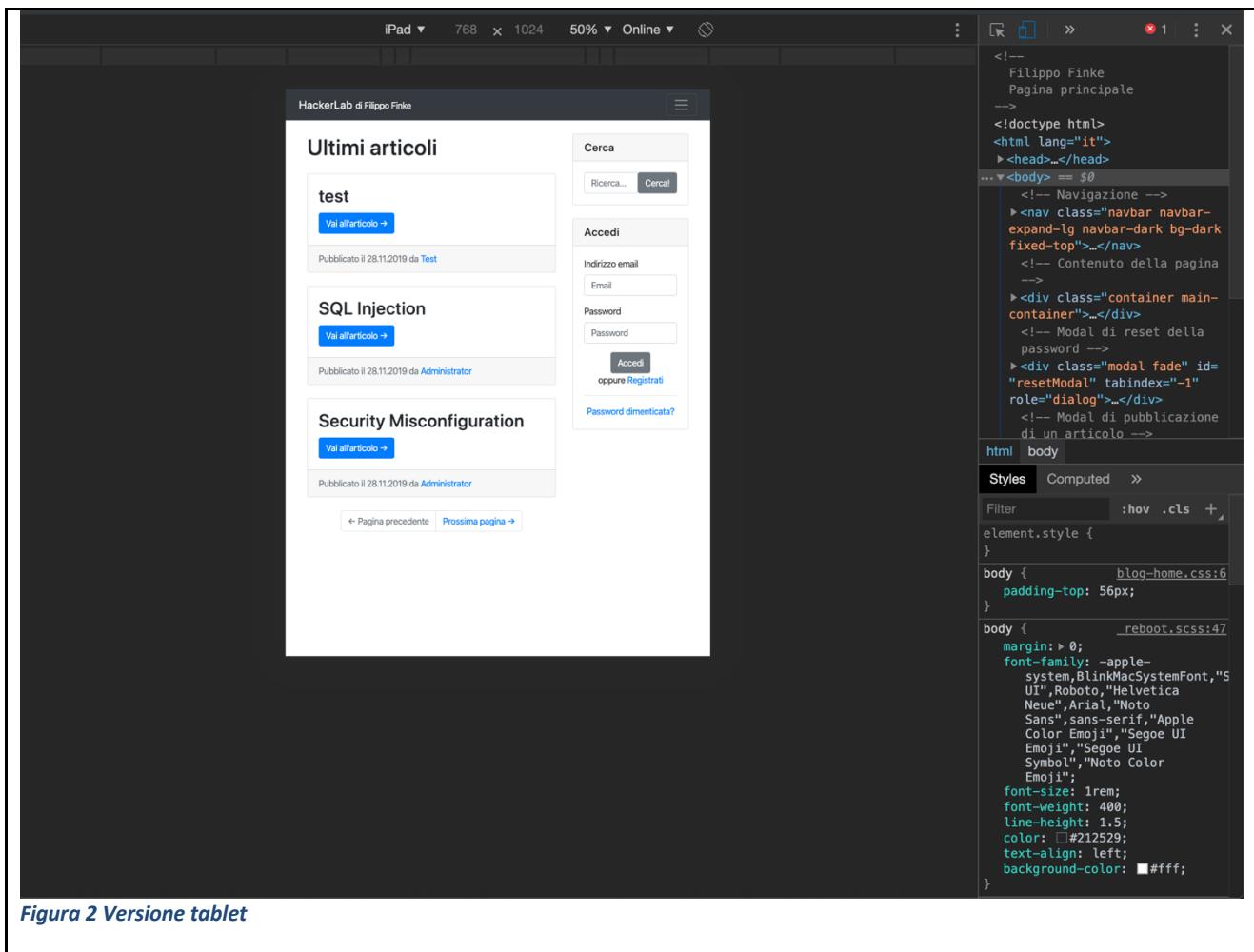


Figura 2 Versione tablet

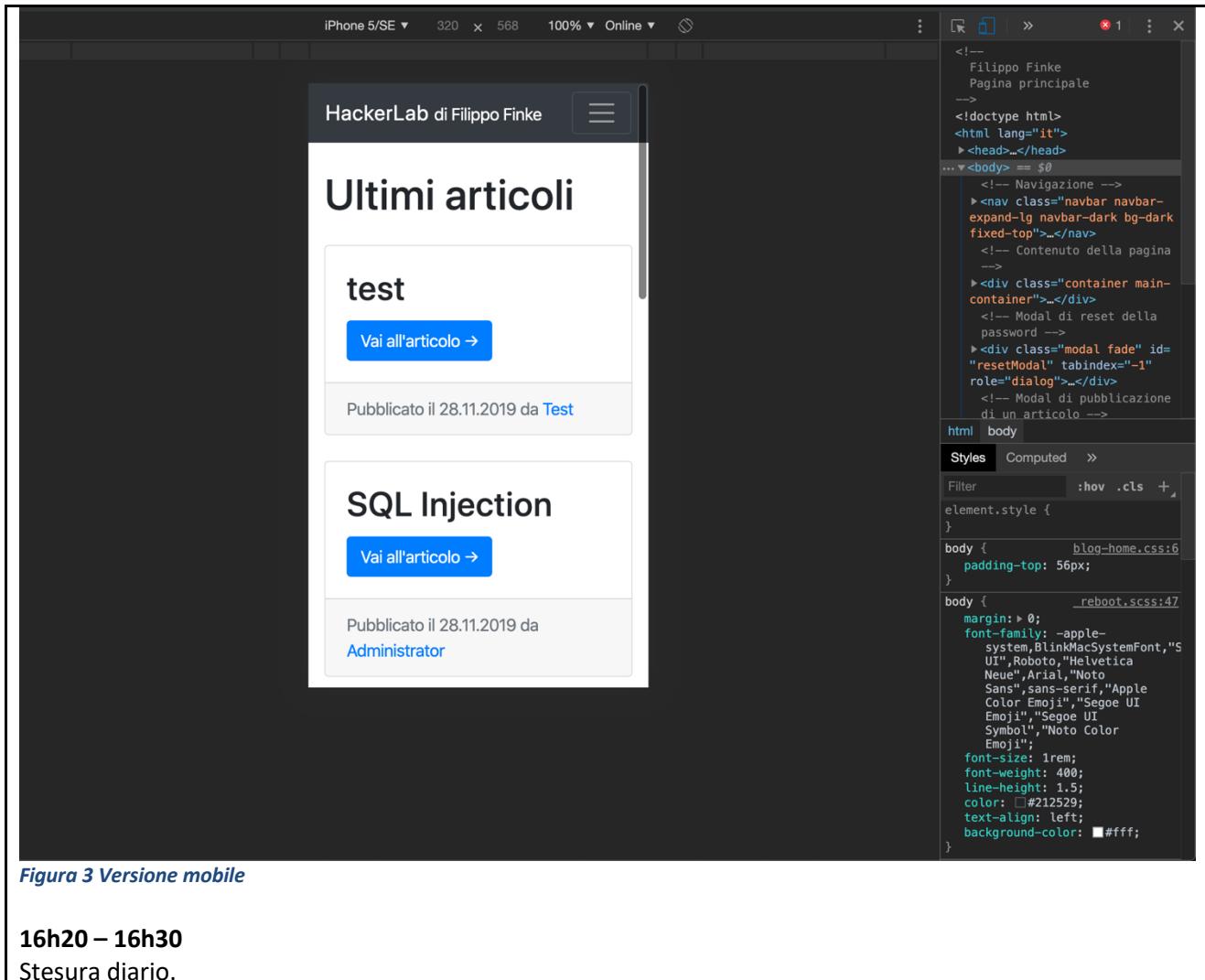


Figura 3 Versione mobile

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	03.12.2019

Lavori svolti

13h15 – 14h45 15h00 - 16h20

Ho riletto tutti i diari e creato una tabella Excel contenente un riassunto delle azioni eseguite in essi in modo tale da poter creare il Gantt consuntivo.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

Creare il GANTT Consuntivo.

Diario di lavoro

Luogo	Canobbio
Data	06.12.2019

Lavori svolti

13h15 – 14h45

Ho completato la creazione del diagramma di Gantt consuntivo il quale è anche stato documentato all'interno della documentazione.

Io e il collega Fadil Smajilbasic abbiamo posto delle domande riguardanti il capitolo dell'implementazione al docente Fabrizio Valsangiacomo il quale ci ha dato dei consigli su cosa documentare e che modo utilizzare. Ho quindi iniziato a documentare anche le interfacce del prodotto al quale sto lavorando. Ho quindi iniziato a documentare il capitolo: Interfacce grafiche.

15h00 – 16h20

Ho continuato la stesura del capitolo Interfacce grafiche aggiungendo tutte le pagine e maschere presenti all'interno di HackerLab. Ho quindi aggiunto e completato i seguenti capitoli nella documentazione:

- Gantt consuntivo
- Interfacce grafiche

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	10.12.2019

Lavori svolti

13h15 – 14h45

Ho iniziato a creare una bozza della presentazione per il progetto stesso.

15h00 – 16h20

Ho approfondito le descrizioni del capitolo Design procedurale.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	12.12.2019

Lavori svolti

13h15 – 14h45

Ho riletto le documentazioni riguardanti le vulnerabilità dando una revisione finale, una volta riletto tutte le guide ho ricreato i PDF aggiornati delle stesse. Successivamente ho creato un file PDF unico contenente tutte le guide delle vulnerabilità in modo da facilitarne la stampa e la lettura.

Revisionato anche l'abstract che andrà messo in prima pagina della documentazione e anche per esso ho creato il PDF.

15h00 – 16h20

Durante questo periodo di lezione ho stampato i seguenti PDF:

- Abstract
- Guide vulnerabilità
- QDC

I quali sono stati rilegati attraverso l'uso della rilegatrice, ha preso tempo perché ho dovuto ricavare il materiale da utilizzare per rilegare dal custode.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

Revisionare documentazione per una possibile stampa.

Diario di lavoro

Luogo	Canobbio
Data	13.12.2019

Lavori svolti

13h15 – 16h20

Durante la giornata di oggi mi sono occupato di revisionare e stampare la documentazione del progetto. Inoltre, assieme a Bryan Beffa, abbiamo posto alcuni quesiti al docente Valsangiacomo riguardanti la documentazione. Ci è stato consigliato di separare tutti gli allegati con dei fogli bianchi, i quali abbiamo stampato per la rilegatura.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	17.12.2019

Lavori svolti

13h15 – 16h20

Durante questa giornata mi sono occupato di rilegare i vari capitoli stampati nei giorni precedenti.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	19.12.2019

Lavori svolti

13h15 – 16h20

Oggi mi sono occupato della masterizzazione su CD del progetto consegnato dal docente Valsangiacomo.

16h20 – 16h30

Stesura diario.

Problemi riscontrati e soluzioni adottate

Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione

Avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro

-

Diario di lavoro

Luogo	Canobbio
Data	20.12.2019

Lavori svolti 13h15 – 14h45 Consegna del progetto.

Problemi riscontrati e soluzioni adottate Nessun problema riscontrato.

Punto della situazione rispetto alla pianificazione Conclusione del progetto.
--

Programma di massima per la prossima giornata di lavoro Il progetto è concluso.
--