

# 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.