

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 user cards. The first card is for 'Administrator' with email 'admin@hackerlab.ch' and role 'administrator'. It has a blue 'Pagina profilo →' button, a yellow 'Disabilita' button, and a red 'Elimina' button. The second card is for 'Filippo Finke' with email 'filippo.finke@samtrevano.ch' and role 'user'. The name 'Filippo Finke' is highlighted with a red box and followed by '(Disabilitato)'. It has a blue 'Pagina profilo →' button, a yellow 'Abilita' button, and a red 'Elimina' button.

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.