Diario di lavoro

|  |  |
| --- | --- |
| Luogo | Scuola d’arti mestieri Trevano |
| Data | 30.10.2020 |

|  |
| --- |
| Lavori svolti |
| Oggi ho iniziato a creare il sistema che permette di cambiare la password provissorie. Prima di tutto ho creato un nuovo models che si chiama Password. Al suo interno posso gestire la codifica delle password.  In effetti ho creato tre metodi che si chiamano criypt, decript e getSalt.  La funzione salt mi permette di generare a random un sal che verrà utilizzata con l’hashing delle password. un salt è una sequenza casuale di bit utilizzata assieme ad una password come input a una funzione unidirezionale, di solito una funzione hash, il cui output è conservato al posto della sola password, e può essere usato per autenticare gli utenti. Usare lo stesso salt per ogni input significa che tutte le password uguali avranno lo stesso valore hash. Questo rende facile attaccare utenti multipli decodificando un solo hash. Per questo motivo ho creato il metodo getSalt che crea csualmente un salt.  Immagine che contiene testo  Descrizione generata automaticamente  La variabile $charset contiene la seguenza di caratteri che andranno a comporre la salt. La variabile $randStringLen corrisponde alla lunghezza del salt e per finire la variabile $randString è il salt che verrà generata casualmente. Nel ciclo utilizzo il metodo mt\_rand che permette di generare un valore casuale tramite il generatore di numeri casuali Mersenne Twister (generazione di numeri pseudocasuali).Utilizzo questo metodo per generarmiun numero casuale che corrisponderà all’indice dell’array $charset (una variabile di stringhe corripsonde anche ad un array).  Il metodo cript invece mi permette di codficare la password.  Immagine che contiene testo  Descrizione generata automaticamente  La funzione hash permette di creare un hash di una password. Questa funzione riceve due parametri che sono tipo di codifica e stringa da codificare. Come tipo di codifica utilizzo sha256 (Secure Hash Algorithm) è una funzione hash crittografica. L’hash crittografico può essere considerato un tipo di firma per un file di testo o di dati e non deve essere confuso con la “crittografia”. Un hash crittografico non può essere decodificato ed è una funzione unidirezionale. Nel codice ho anche aggiunto alla password il salt che ho generato casualmente.  Il metodo decrypt permette di verificare che la password corrisponde al hash.  Immagine che contiene testo  Descrizione generata automaticamente  In effetti la funzione password\_verify verifica che l'hash fornito corrisponda alla password fornita.  Nel metodo checkAggiungiUtente del controller aggiungi\_utente, permette di verificare il form che crea un nuovo utente. La password che fornisco al metodo addUser del model utente\_model viene codificata in sha256.  Immagine che contiene testo  Descrizione generata automaticamente  Nel metodo getUtente del models login\_model verifico che la password che è viene passata dall’utente corrisponde al hash della password dell’account.  Immagine che contiene testo  Descrizione generata automaticamente  Se la password corrisponde al hash, l’utente riesce a fare il login altrimenti se non riesce vuol dire cha ha sbagliato la password.  Per ora questo condizione non funziona perché ho creato un salt e quindi la password che do non corrisponde al hash visto che ho aggiunto anche un salt alla password. Per la password provissoria, invio un email con la passwor provssoria e quando l’utente entra per l aprima volta può direttamente cambiare la password. |

|  |
| --- |
| Problemi riscontrati e soluzioni adottate |
| Non riesco a fare il login perché ho codificato le password. In effetti la funzione verify\_password mi permette di verificare che una password corrisponde all’hashing. Visto che ho utilizzato anche un salt prima di codificare, a password in chiaro non corrisponderà all’hashing. Questo perché verify\_password lavora con il metodo password\_hash. In effetti devo utilizzare quest’ultimo per codificare le password. Non ancora implementato la soluzione, in effetti devo realizzarla per la prossima giornata. |

|  |
| --- |
| Punto della situazione rispetto alla pianificazione |
| Rispetto al GANTT sono ad un buon punto, anche se non ho ancora creato la pagina nell quale posso cambiare la password provissoria, voglio realizzare un pagina che permette di cambiare la password. Quando un utente entra per la prima volta nell’applicativo, ha la possibilità di cambiare la password. |

|  |
| --- |
| Programma di massima per la prossima giornata di lavoro |
| Devo terminare il sistema delle password provissorie e finire anche il problema legato al login. |