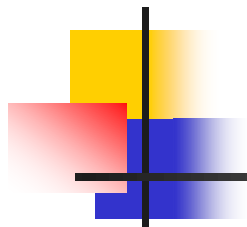


Laboratorio

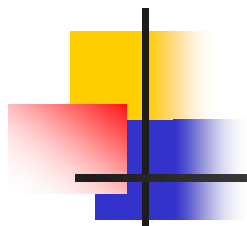
7



Laboratorio 7

Overview:

- **Esercitazioni:**
 - Login e password
- **Tecnologie:**
 - PHP
- **Strumenti:**
 - Specifiche di riferimento PHP (<http://php.net>)
 - Browsers: Chrome e Firefox
 - XAMPP
 - MySQLWorkbench



Hash

Una funzione hash è una funzione che prende in ingresso una stringa di dimensione variabile e produce come risultato una stringa di dimensione fissa.

Le funzioni hash hanno ampio utilizzo nel campo della sicurezza informatica.



Gestione delle password (1)

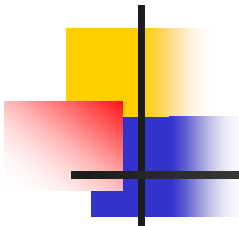
Nel caso il server venisse compromesso le informazioni degli utenti potrebbero essere trafugate.

Per questo motivo conservare in chiaro le password degli utenti è un'operazione rischiosa. Un approccio più prudente prevede l'utilizzo di funzioni hash.



Gestione delle password (2)

- **Registrazione:** in questa fase di server genera l'hash a partire dalla password inserita dall'utente. All'interno del sistema viene salvato solo l'hash della password.
- **Login:** in questa fase il server genera l'hash della password inserita dell'utente e lo confronta con l'hash salvata all'interno del suo database.



Creazione dell'hash

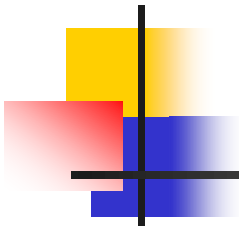
Per creare un hash a partire da una password utilizzare la funzione password_hash().

```
password_hash(string $password, string|int|null  
    $algo, array $options = []): string
```

\$password: la password di cui generare l'hash.

\$algo: l'algoritmo di hashing da utilizzare (utilizzare *PASSWORD_BCRYPT*).

Restituisce l'hash della password.



Verifica dell'hash

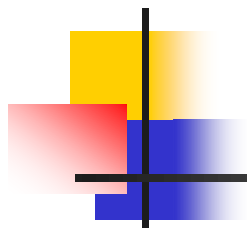
Per verificare la correttezza della password inserita dall'utente utilizzare la funzione password_verify().

`password_verify(string $password, string $hash): bool`

`$password`: la password inserita dall'utente

`$hash` : un hash generato attraverso la funzione *password_hash*.

Ritorna **true** se si verifica un match, **false** altrimenti.



Login & Password

Username:

Password:

Implementare un semplice form che permetta agli utenti di registrarsi presso il sistema. Le informazioni di login devono essere salvate all'interno di un database.

Il sistema deve altresì permettere agli utenti di accedere con le loro credenziali.

Non salvare le password in chiaro all'interno del DB. Utilizzare le funzioni password_hash() e password_verify().