PHP och MySQL (Dag 2)

- CRUD-applikation med funktioner
- Inloggning med hash-algoritm för lösenord

SQL Injection

- En säkerhetsrisk
- Används när användaren får skriva in något mot en databas
- Webbapplikationer
- Annan typ av tillämpningsprogram

Exempel på SQL Injection

- Skriva och köra andra SQL-frågor än vad tanken var.
- Försöka förstå databasens uppbyggnad genom ”trial and error”.
- Kan användas för att stjäla data i databasen som t ex användarnamn, lösenord, kreditkortsinformation.
- Kan användas för att lägga till eller uppdatera data i databasen t ex göra beställningar, ändra privilegier för användare.
- Kan användas för att förstöra eller radera data i databasen.

Förhindra SQL Injection

- Användarna har bara nödvändiga rättigheter. T ex inte DROP TABLE eller GRANT om det inte är nödvändigt.
- Ta hand om vanliga *enkelcitat* som en användare skriver in. Gör om ett *enkelcitat* och lägga ett *backslash-tecken* framför det. Använd programmeringsspråkets bibliotek och funktioner.
- Använd förkompilerade SQL-frågor (*prepared statements*). Använd tekniker som t ex ODBC, JDBC eller ESQL.

Rainbow tables

- En hash-algoritm ska vara långsam.
- Vad är Rainbow tables?
- Komma åt lösenord med t ex SQL Injection.
- Spara lösenorden i en databas och jämföra hash-algoritmer med Rainbow tables-listan.

Salt

- För att försvåra lösenorden.
- Man skapar en sträng som krypteras tillsammans med lösenordet innan det sparas i databasen.
- Unik salt för varje lösenord.
- Lösenord med Salt gör Rainbow table-listan näst intill omöjligt lång.

Krav på lösenord för en användare

- Kräv hur långt lösenordet minst ska vara men inte hur långt det får vara. Långa lösenord gör det svårare att lista ut.
- Kräv icke alfanumeriska tecken.
- Låt användaren bekräfta sitt lösenord.
- Spara inte tips för att skapa ett lösenord i databasen.
- Fundera på om det är en bra lösning med ”frågor för att komma ihåg sitt lösenord”.

Hash-algoritmer

SHA-1
SHA-2 (SHA-256, SHA-512)
BCrypt
Whirlpool
Tiger
AES
Blowfish

(MD5 var länge den vanligaste algoritmen)

Hash-algoritmer i PHP

- password_hash()
  För att skapa ett lösenord med en säker hash-algortim (Bcrypt som default) och inbyggd Salt
  http://php.net/manual/en/function.password-hash.php
- Password_verify()
  Kontrollerar att lösenordet matchar med hash-algoritmen i password_hash()
  http://php.net/manual/en/function.password-verify.php

Prepared Statemets

https://www.w3schools.com/php7/php7_mysql_prepared_statements.asp

Övning

- Utveckla Bloggen så att du använder funktioner istället för att strukturera koden.
- Gör en inloggning med sessioner (först utan funktioner). Ev. utveckla genom att ha inloggningen i en funktion.

Exempelkod

Ladda ner:

- customer-mysqli-functions.zip
- sessions-login-mysqli.zip

Övning

- Utveckla Bloggen så att du använder funktioner istället för att strukturera koden.
- Gör en inloggning med sessioner (först utan funktioner). Ev. utveckla genom att ha inloggningen i en funktion.

W3schools

- Titta genom exemplen eller använd som referens (MySQL) https://www.w3schools.com/php7/php7_mysql_intro.asp