

Verschlüsselung

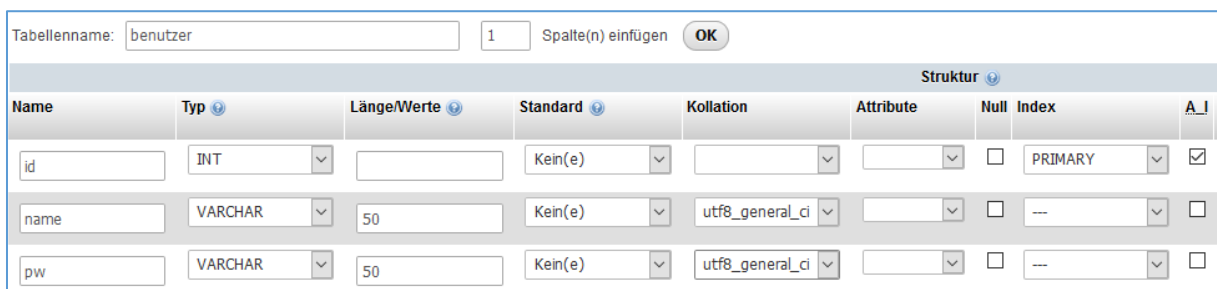
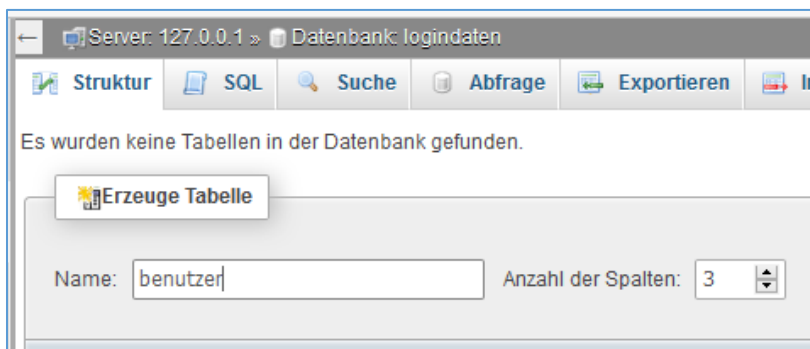
Eine häufig genutzte sichere Methode zur Verschlüsselung von Texten ist „MD5“ – der „Message-Digest-Algorithmus 5“.

Innerhalb von PHP wird dieser Algorithmus mithilfe der Funktion „md5()“ bereitgestellt.

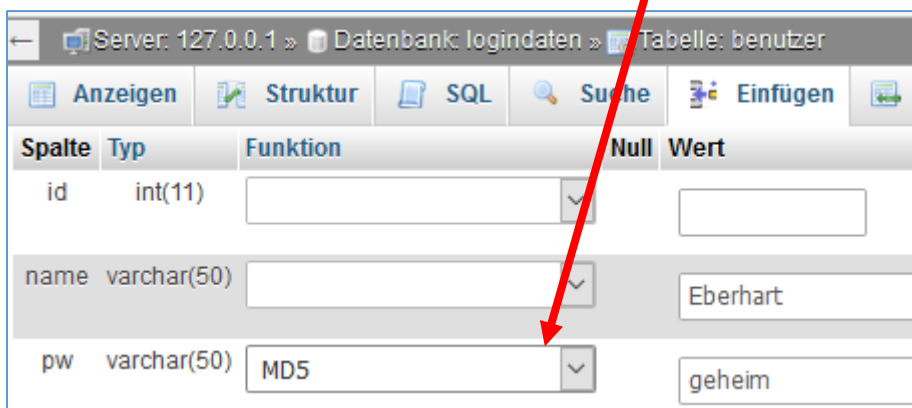
Übung: Passwort verschlüsseln

1) Erstelle eine MySQL-Datenbank mit dem Namen „logindaten“ mit der Tabelle „benutzer“.

- Feld „id“ wird mit dem Primärschlüssel versehen und dem Attribut „auto_increment“
- Feld „name“ ist „varchar(50)“, „utf8_general_ci“
- Für das Passwort erstelle das Feld „pw“ mit „varchar(50)“, „utf8_general_ci“.



- Bei der Eingabe eines Datensatzes verwende die Funktion „MD5“.



Und einen zweiten User. Dieses Mal aber mit einem Umlaut:

Spalte	Typ	Funktion	Null	Wert
id	int(11)			
name	varchar(50)			kölbl
pw	varchar(50)	MD5		streber

Die Speicherung des Passwortes erfolgt bereits verschlüsselt:

	id	name	pw
<input type="checkbox"/> Bearbeiten <input type="checkbox"/> Kopieren <input type="checkbox"/> Löschen	1	Eberhart	e8636ea013e682faf61f56ce1cb1ab5c
<input type="checkbox"/> Bearbeiten <input type="checkbox"/> Kopieren <input type="checkbox"/> Löschen	2	kölbl	88ff0198cf4e825b0f458a41931cf095

2)HTML-Formular erstellen

Das Passwort wird in folgendes Formular eingegeben: speichern als „md5.html“.

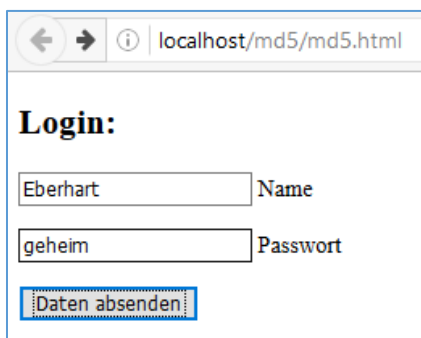
Beim Passwort verwende den „type=“password“ damit die Punkte angezeigt werden und nicht der Klartext.

```
md5.html* x
Code Teilen Entwurf Live-Ansicht Titel: Passwort
1 <!doctype html>
2 <html>
3 <head>
4 <meta charset="utf-8">
5 <title>Passwort verschluesseln</title>
6 </head>
7
8 <body>
9 <h2>Login:</h2>
10 <form action="md5.php" method="post">
11 <p><input name="na"> Name</p>
12 <p><input type="password" name="pw"> Passwort</p>
13 <p><input type="submit"></p>
14 </form>
15
16 </body>
17 </html>
```

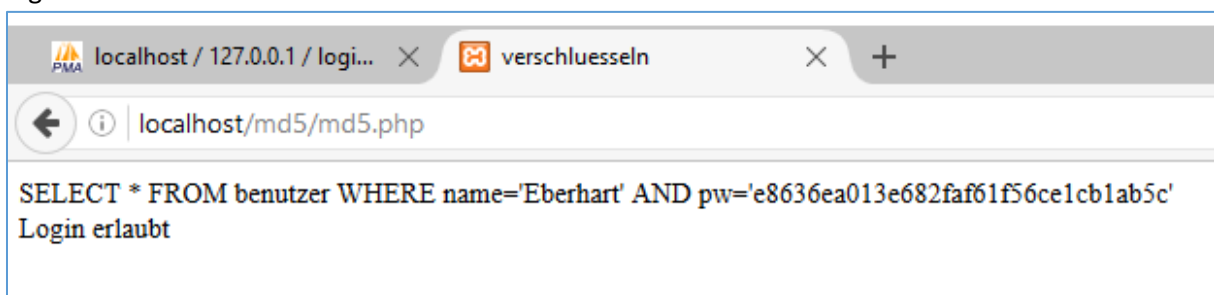
Dazu die passende „md5.php“ Seite:

```
1 <!doctype html>
2 <html>
3 <head>
4 <meta charset="utf-8">
5 <title>verschluesseln</title>
6 </head>
7
8 <body>
9 <?php
10     $con = mysqli_connect("localhost", "root", "", "logindaten");
11     $sql = "SELECT * FROM benutzer WHERE name='" . $_POST["na"]
12     |. "' AND pw='" . md5($_POST["pw"]) . "'";
13     echo "$sql<br>";
14     $res = mysqli_query($con, $sql);
15     if(mysqli_num_rows($res) > 0) echo "Login erlaubt";
16     else
17         echo "Login nicht erlaubt";
18         mysqli_close($con);
19 ?>
20 </body>
21 </html>
```

Das gesendete Passwort wird ebenfalls mit der Funktion „md5()“ verschlüsselt und mit dem gespeicherten, verschlüsselten Passwort verglichen.

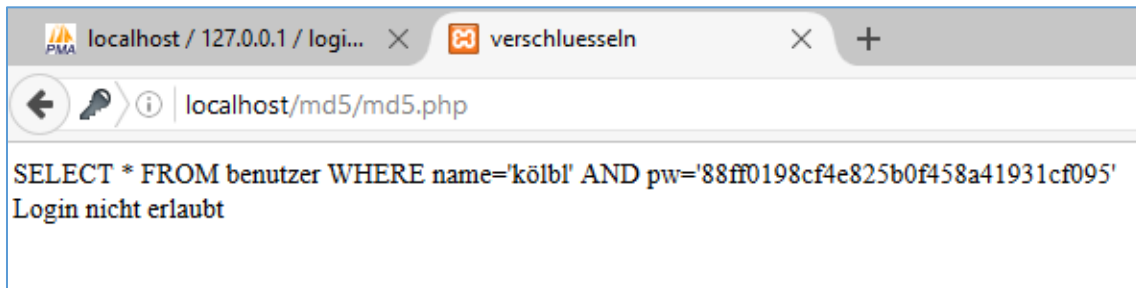


Ergebnis:



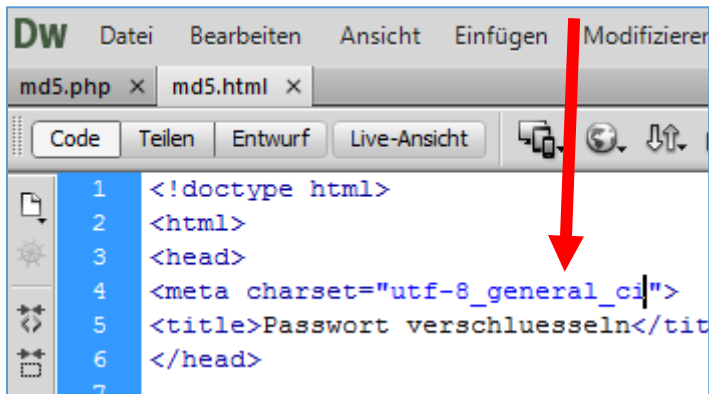
Zur Verdeutlichung wird hier der SQL-Befehl einschließlich des verschlüsselten Passworts ausgegeben.

Probleme bei Umlauten:



Lösung:

In der HTML-Datei eine Verlängerung bei „utf-8“ einfügen:



Ergebnis: Login ist ok, die Ausgabe „kölbl“ ist aber nicht ok.

