Verschlüsselung

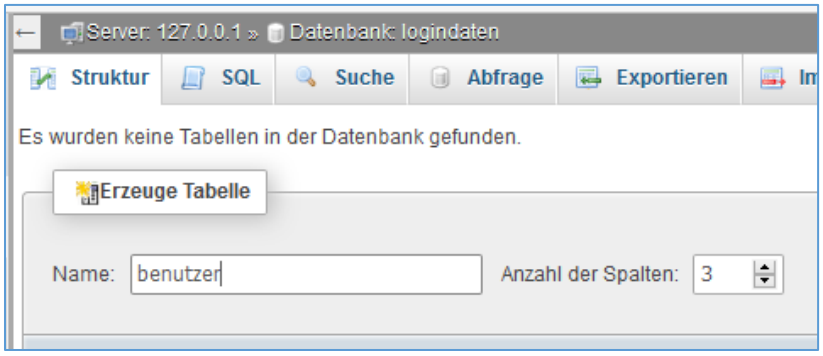
Eine häufig genutzte sichere Methode zur Verschlüsselung von Texten ist „MD5“ – der „Message-Digest-Algorithmus 5“.

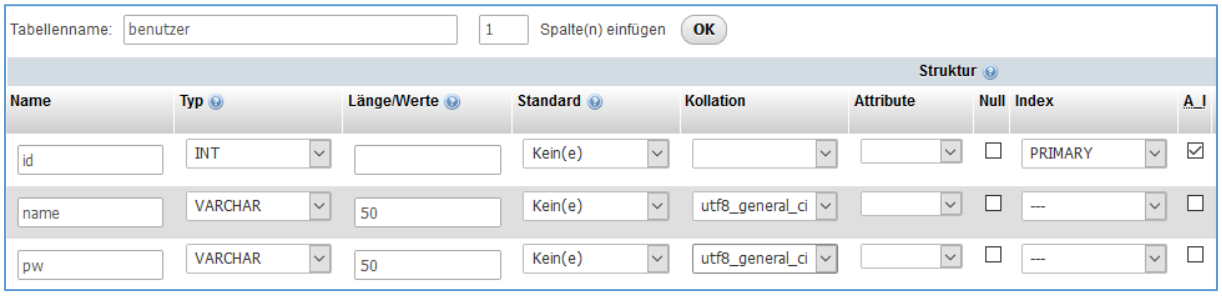
Innerhalb von PHP wird dieser Algorithmus mithilfe der Funktion „md5()“ bereitgestellt.

Übung: Passwort verschlüsseln

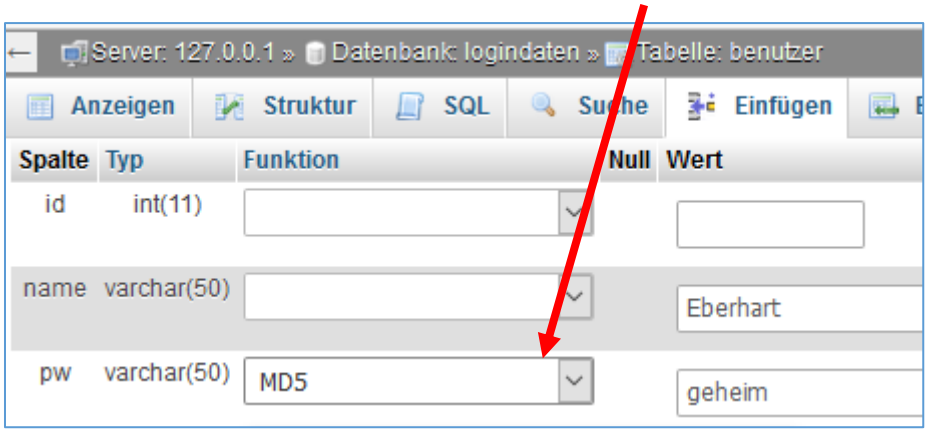
1)Erstelle eine MySQL-Datenbank mit dem Namen „logindaten“ mit der Tabelle „benutzer“.

- 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“.

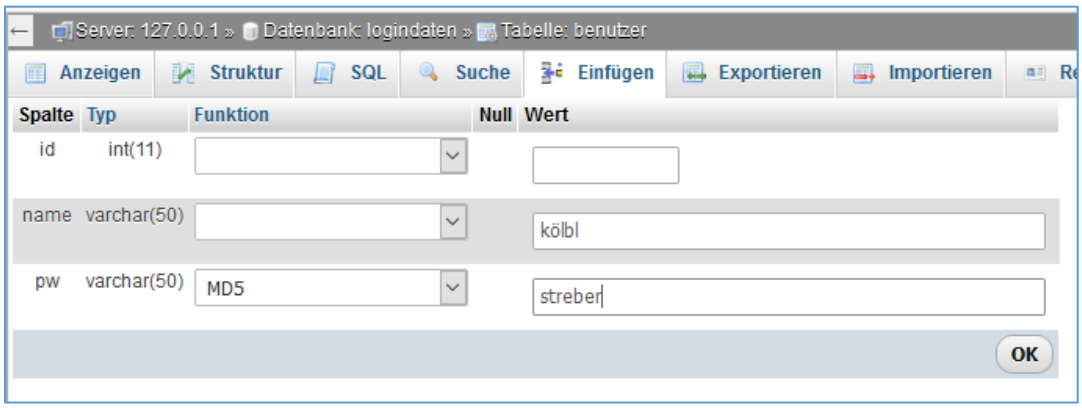




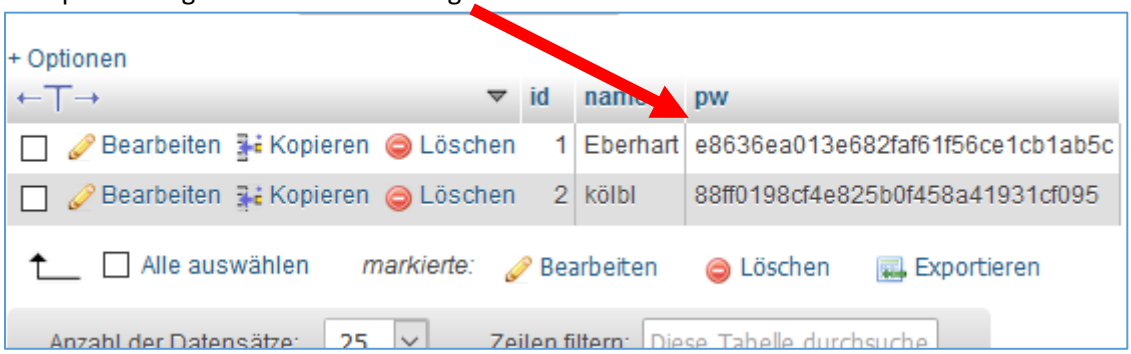
- Bei der Eingabe eines Datensatzes verwende die Funktion „MD5“.



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

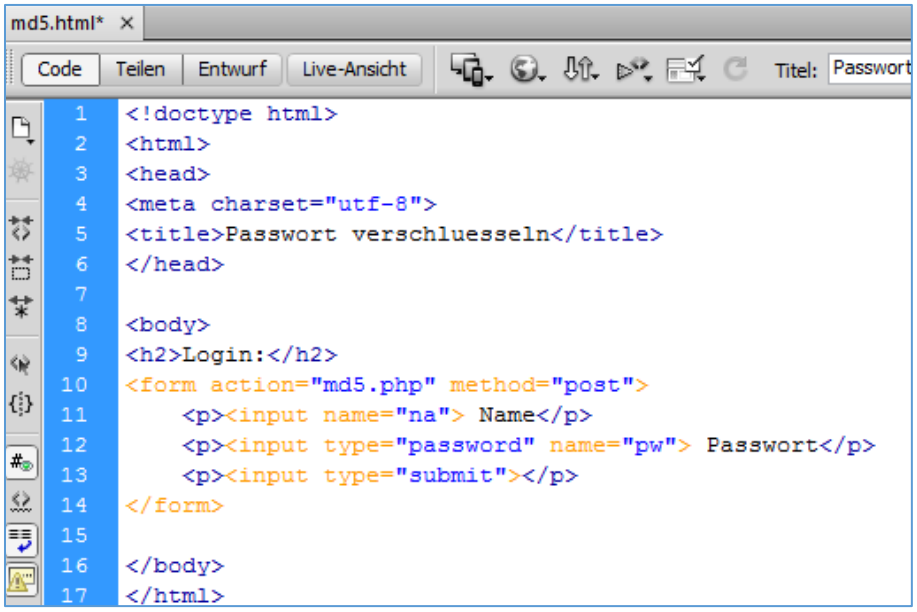


Die Speicherung des Passwortes erfolgt bereits verschlüsselt:



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.

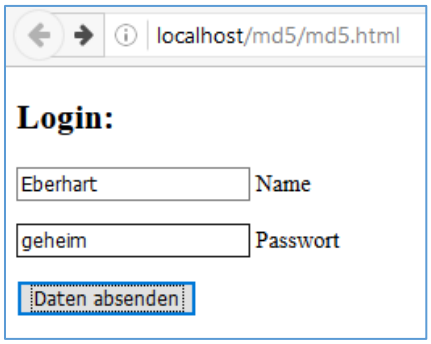


Dazu die passende „md5.php“ Seite:

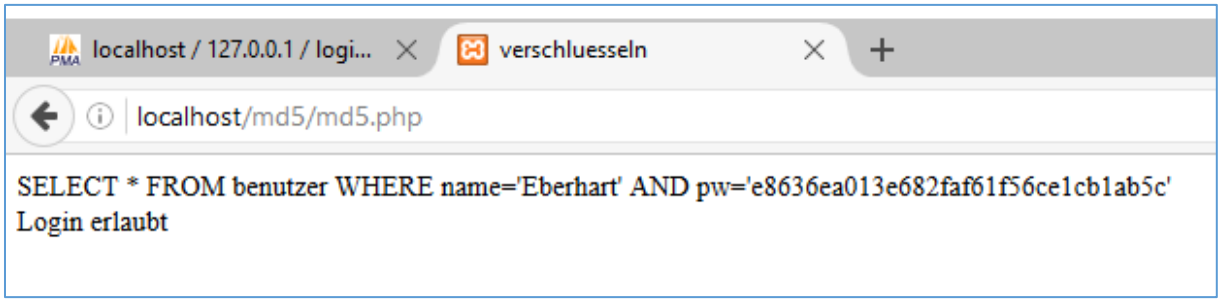
```php
<!doctype html>
<html>
<head>
<meta charset="utf-8">
<title>verschluesseln</title>
</head>

<body>
<?php
    $con = mysqli_connect("localhost", "root", "", "logindaten");
    $sql = "SELECT * FROM benutzer WHERE name='" . $_POST["na"]
    . "' AND pw='" . md5($_POST["pw"]) . "'";
    echo "$sql<br>";
    $res = mysqli_query($con, $sql);
    if(mysqli_num_rows($res) > 0) echo "Login erlaubt";
        else
            echo "Login nicht erlaubt";
            mysqli_close($con);
?>
</body>
</html>
```

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

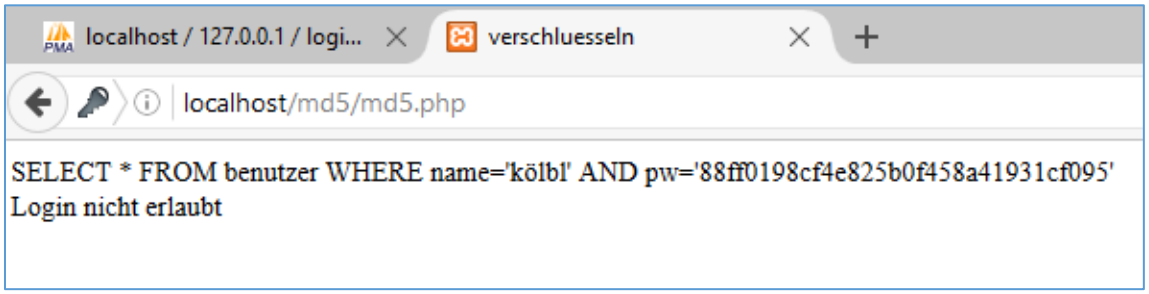


Ergebnis:



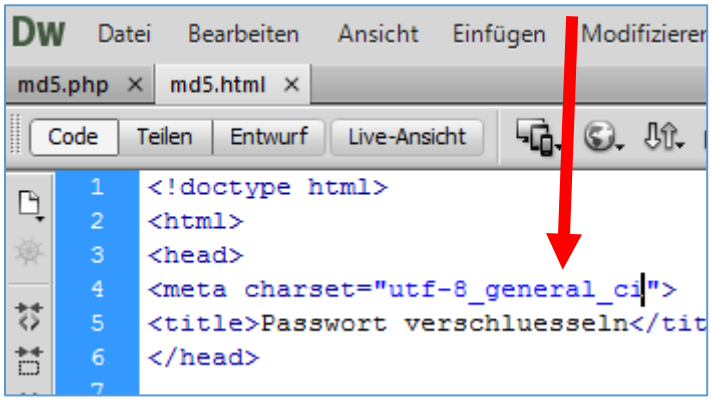
Zur Verdeutlichung wird hier der SQL-Befehl einschließlich des verschlüsselten Passworts ausgegeben.

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.