

# Passwort verschlüsseln

Dienstag, 19. September 2006

<http://www.webmaster-resource.de/tricks/php/passwort-verschluesseln.php>

Sobald Sie Zugangspasswörter in einer Textdatei oder einer Datenbank speichern, sollten sie diese verschlüsseln. Wie dies mit Hilfe der Funktion md5(...) geht, erfahren Sie in diesem Artikel.

Immer dann, wenn Sie Passwörter für einen zugriffsgeschützten Bereich Ihrer Webseite hinterlegen müssen, sollten Sie diese grundsätzlich verschlüsseln. Werden die Passwörter im Klartext nur in einer Textdatei (z.B. "passwort.txt" oder auch "config.inc") gespeichert, reicht es den Link zu dieser Seite herauszufinden und dem Angreifer sind alle Passwörter bekannt. Aus diesem Grund ist es mit Hilfe der PHP-Funktion md5(...) möglich, einen String - das Passwort - zu verschlüsseln, d.h. in eine längere, willkürlich erscheinende Zeichenkette zu verwandeln.

Quellcode

1.

Das vorherige Passwort "1234" ergibt verschlüsselt den String "81dc9bdb52d04dc20036dbd8313ed055". Wird diese Zeichenkette abgelegt, kann ein potentieller Angreifer das originale Passwort nicht mehr herausfinden.

Bei der Benutzung der Funktion md5(...) ist allerdings zu beachten, dass die verschlüsselte Zeichenkette nicht wieder entschlüsselt werden kann, d.h. es existiert keine Funktion, die "81dc9bdb52d04dc20036dbd8313ed055" wieder in "1234" umwandelt. Um später, z.B. bei einem Login, das Passwort überprüfen zu können, kann das eingegebene Passwort wieder mit der Funktion md5(...) umgewandelt werden und das gespeicherte Passwort mit dem umgewandelten verglichen werden.

Beim Abspeichern eines Passwortes in einer MySQL-Tabelle kann auch auf eine MySQL-Funktion zurückgegriffen werden: `INSERT INTO Logins (Name, Passwort) VALUES ('Test', MD5('1234'));`

Wenn Sie vorhandene PHP-Scripte ändern oder neue mit dieser Verschlüsselungsmöglichkeit ausstatten möchten, sollten Sie - gerade bei der Speicherung des Passwortes in einer MySQL-Tabelle - berücksichtigen, dass die verschlüsselte Zeichenkette meist länger als das Original-Passwort ist.