# 2.1 md5-Checksum

Da das md5-Verschlüsselungsverfahren schon sehr alt ist, gibt es im Internet unendlich lange „Rainbow-Tables“, in denen die Original-Passwörter neben den md5()-Verschlüsselten stehen, sodass eine einfache Textsuche meist ausreicht, um an das lesbare Passwort zu kommen.

Umgangen werden kann dies, in dem man zusätzlich zu md5() noch ein paar Operationen mit dem generierten Passwort macht. Die Funktionen müssen aber alle eindeutig umkehrbar sein. Wir haben uns mit einem zufällig generierten Salt abgesichert, der neben dem Usernamen in der Datenbank steht. Mit der seit PHP 5.5 crypt()-Methode kommen wir so schnell und sicher an unser Ziel.

# 2.2 Session Handling

Beim Session-Handling können die Sessiondaten über Cookies oder direkt über die URL

übertragen werden. Diskutieren Sie die Vor- und Nachteile dieser beiden Verfahren.

|  |  |
| --- | --- |
| **Session-Management** | |
| **Über Cookies** | Über URL |
| Vorteile | Nachteile |
| * Session-Fixation und –Highjacking sind machbar | |
| * Session-ID nicht dauerhaft einsehbar | * Session-ID dauerhaft sichtbar * Sogar unerfahrene Benutzer können so ihre ID ganz leicht ändern |
| Nachteile | Vorteile |
| * Einrichtung dauert länger | * Debugging fällt einfacher |