HTTP-Authentifizierung

Stellt der Webserver fest, dass für eine angeforderte Datei Benutzername oder Passwort nötig sind, meldet er das dem Browser mit dem Statuscode *401 Unauthorized* und dem Header *WWW-Authenticate*. Größere Webauftritte verwenden dieses standardisierte Verfahren jedoch nur selten, da sich die Eingabefelder für Benutzername und Passwort nur mit Javascript in die Webseite einbetten lassen. Dieser Javascript-Anmeldung sollte keine Barriere darstellen, wenn ohne Javascript die gewohnte Passwort-Abfrage des Browsers erscheint. Auf kleinen Homepages ist HTTP-Authentifizierung aber oft zu finden, da viele Webspaceanbieter eine simple Möglichkeit zur Konfiguration bieten.

Es gibt mehrere Möglichkeiten, Benutzer (Clients) zu authentifizieren. Verbreitet sind:

Basic Authentication

Die Basic Authentication nach RFC 2617 ist die häufigste Art der HTTP-Authentifizierung. Der Webserver fordert mit

```
WWW-Authenticate: Basic realm="RealmName"
```

eine Authentifizierung an, wobei RealmName eine Beschreibung des geschützten Bereiches darstellt. Der Browser sucht daraufhin nach Benutzername/Passwort für diese Datei und fragt gegebenenfalls den Benutzer. Anschließend sendet er die Authentifizierung mit dem Authorization-Header in der Form Benutzername:Passwort Base64-codiert an den Server. Beispiel:

Eingabe von Benutzername und Passwort

```
Authorization: Basic d2lraTpwZWRpYQ==
```

d2lraTpwZWRpYQ== ist die Base64-Codierung von *wiki:pedia* und steht damit für Benutzername *wiki*, Passwort *pedia*. Ein Nachteil dieses Verfahrens ist, dass Benutzername und Passwort nur aus technischen Gründen codiert, jedoch nicht verschlüsselt werden. Bei einer Verschlüsselung mit SSL/TLS bei HTTPS wird bereits vor der Ubermittlung des Passwortes eine verschlüsselte Verbindung aufgebaut, so dass auch bei Basic Authentication das Passwort nicht abhörbar ist.