Session Handling

Das vorliegende PHP Projekt verwendet Sessions um den Endbenutzer eindeutig zu identifizieren. Um den Zugriff von JavaScript auf die Session zu verhindern wird der PHP Parameter „session.use\_only\_cookies“ auf TRUE gesetzt. Auf das im nachfolgenden Schritt erzeugte Cookie „sec\_session\_id“ kann nur mittels dem http Protokoll zugegriffen werden.[[1]](#footnote-1) Die Erstellung des Cookies ist in der PHP Funktion „sec\_session\_start()“ gekapselt und wird auf jeder PHP Seite zum Erstellen einer Session verwendet.

Login Verfahren

Die Veranstaltungsmanagement Software verwendet einen sha512 Hashing-Algorithmus[[2]](#footnote-2) für die Benutzerpasswörter. Zusätzlich werden die Passwörter in der Datenbank mit einem Salt[[3]](#footnote-3) abgelegt um die Sicherheit weiter zu erhöhen. Im Folgenden wird das eigentliche Login Verfahren anhand des Schaubilds 1 näher erklärt.

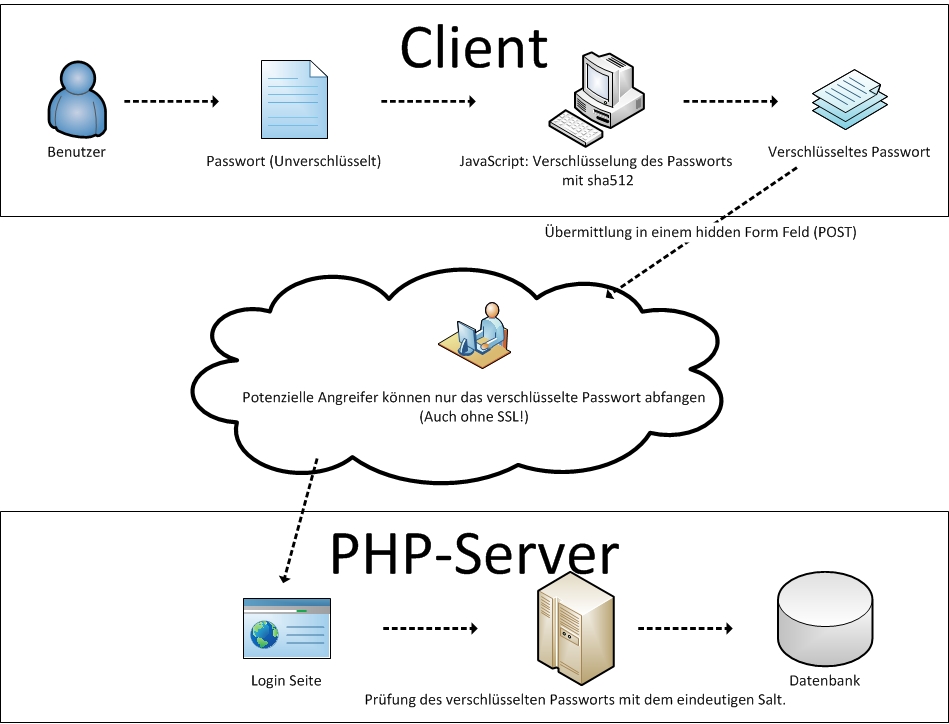


Abbildung 1 Client / Server Login Verfahren

Der Benutzer gibt seine Login Daten in der HTML Form „login\_form“ ein. Nach dem Bestätigen per Tastendruck auf „Login“ wird die JavaScript Methode „formhash()“ ausgeführt.

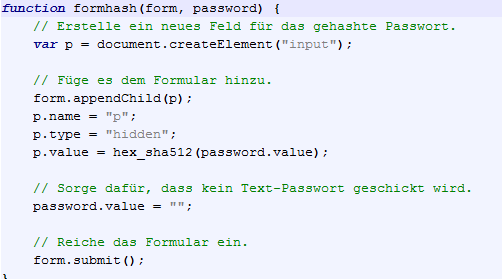


Abbildung 2 JavaScript Methode formhash()

Die Methode erzeugt ein Form Feld in dem das Passwort mit einer sha512 Verschlüsselung abgelegt wird. Das Klartext Passwort Feld wird danach geleert und die Form bestätigt. Durch das leeren des Klartext Feldes wird das Passwort nicht mehr mit übertragen.

Nach erfolgreicher Übertragung des verschlüsselten Passwortes an den Server wird die PHP Funktion „login()“ ausgeführt. Diese Methode ermittelt anhand der eingegebenen E-Mail Adresse das in der Datenbank hinterlegte verschlüsselte Passwort mit zugehörigen Salt. Zusätzlich wird geprüft ob der Benutzer innerhalb der letzten zwei Stunden versucht hat sich mehr als fünf Mal erfolglos Anzumelden. Dies dient dem Schutz gegen Bruteforce angriffe. Falls ein Bruteforce Angriff ausgeschlossen werden kann wird das in der Datenbank hinterlegte Passwort mit dem übertragenen Passwort abgeglichen. Falls der Login Versuch erfolgreich ist wird der Benutzer direkt auf die geschützte Seite weitergeleitet. Um sicherzustellen Zugriff auf die internen Seiten hat wird mittels der PHP Funktion „login\_check()“ geprüft ob der Benutzer angemeldet ist.

1. <http://php.net/manual/de/function.session-get-cookie-params.php> (2017) [↑](#footnote-ref-1)
2. JavaScript Implementierung übernommen von http://pajhome.org.uk/crypt/md5/sha512.html [↑](#footnote-ref-2)
3. Salt bezeichnet in der Kryptographie eine zufällig gewählte Zeichenfolge, die an einen gegebenen Klartext vor der Verwendung als Eingabe einer Hashfunktion angehängt wird. [↑](#footnote-ref-3)