Authentifizierung
Projekt BierIdee

Danilo Bargen, Christian Fässler, Jonas Furrer

14. April 2012

Inhaltsverzeichnis

Änderungshistorie

Version	Datum	Änderung	Person
v1.0	14.04.2012	Dokument erstellt	cfa
v1.1	00.00.2012	–	kürzel
v1.2	00.00.2012	–	kürzel

1 Einleitung

Der Zweck dieses Dokumentes ist das aufzeigen der verwendeten Authentifizierungsmechanismen für die REST API im Projekt Bieridee. Eine wichtige Voraussetzung ist, dass auch dieser Aspekt Restful implementiert ist, sprich SZustandslos".

2 Verfahren

Zur Authentifizierung kommt das Hash-MAC Verfahren zum Einsatz. Alle Requests (Messages) werden mittels Passwort signiert.

2.0.1 Registrierung

Der Benutzer registriert einen neuen Benutzeraccount. Der Benutzeraccount besitzt ein Passwort, welches dem Server gehasht (SHA-1) übermittelt wird. Der Hashwert wird nachfolgend SSecret"genannt.

2.0.2 Schritt 1

Der Client bereitet seinen REST Request vor.

2.0.3 Schritt 2

Über ein definiertes Set von Attributen wird ein Hashwert (Signatur) gebildet. Für die Bildung dieses Hashwertes wird gemäss RFC2104 das Secret verwendet.

2.0.4 Schritt 3

Der Request wird mit einem zusätzlichen Header Versehen der den Benutzernamen sowie die generierte Signatur beinhaltet. Authorization: ¡username¿:¡signatur¿ Anschliessend wird der Request abgesendet.

Schritt 4

Der Server empfängt den Request und extrahiert den Authorization Header. Anhand der des Benutzernamens kann er in der Datenbank das gemeinsame Secret ausfindig machen und über das selbe Set von Attributen auch die Signatur berechnen.

Schritt 5

Die beiden Signaturen werden verglichen, stimmen Sie überein ist der User erfolgreich authentifiziert.

3 Technische Details

Hashing Algorithmus

Als Hash Algorithmus wird SHA-1 verwendet.

Speicherung der Passwörter

Die Passwörter werden ebenfalls gehast abgespeichert. Somit haben alle Passwörter ein einheitliches Format. Keine Sonderzeichen, gleiche Länge. Für die HMAC Bildung werden die Hashwerte dieser Passwörter verwendet. Das Eigentliche Passwort ist also nicht das ursprünglich eingegebene, sondern der Hashwert davon.

Sicherheit

Der Einzige Schwachpunkt der angedachten Methode ist der initiale Austausch vom gemeinsamen Secret.