University of Applied Sciences and Arts Northwestern Switzerland
School of Engineering

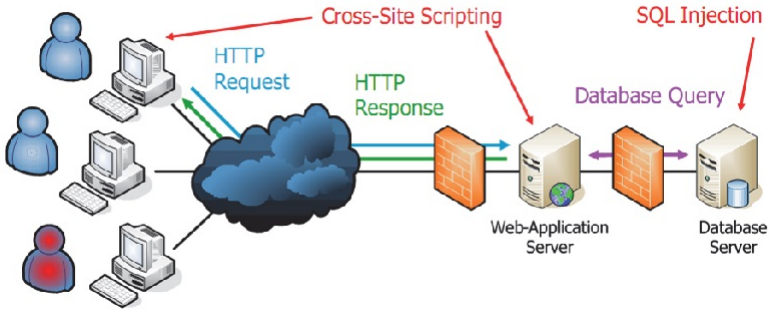
Application Security
Lab 2

Stefan Eggenschwiler & Daniel Gürber

17. Dezember 2013

Inhaltsverzeichnis

1 Aufgabenstellung



2 Softwareaufbau

3 Datenbank

Listing 1: Database Script

```
CREATE TABLE IF NOT EXISTS `company` (
  `username` varchar(64) COLLATE utf8_bin NOT NULL,
  `password` varchar(64) COLLATE utf8_bin NOT NULL,
  `name` varchar(20) COLLATE utf8_bin NOT NULL,
  `address` varchar(255) COLLATE utf8_bin NOT NULL,
  `zip` int(4) NOT NULL,
  `town` varchar(255) COLLATE utf8_bin NOT NULL,
  `mail` varchar(255) COLLATE utf8_bin NOT NULL,
  PRIMARY KEY (`username`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
```

4 Validierung

Im folgenden gehen wir auf die Validierung der Inputdaten ein.

4.1 Firmenname

Nur Gross- und Klein-Buchstaben und Leerzeichen (max. 20).

4.2 Strasse & Strassennummer

Gross- und Klein-Buchstaben, Zahlen, Punkt, Bindestrich, Leerzeichen.

4.3 Postleitzahl

Nur Zahlen, richtige PLZ für die Schweiz, nachkontrolliert mit einem Web-Dienst wie z. B.: http://www.postleitzahlen.ch.

4.4 Stadt

Erlaubte Zeichen: Gross- und Klein-Buchstaben, Punkt, Bindestrich, Leerzeichen.

4.5 E-Mail Adresse

Sie senden aber erst, wenn Sie sicher sind, dass die Email-Adresse auch existiert (no bouncing).

4.6 Benutzername

min. 4 Zeichen, max. 64 Zeichen; Erlaubte Zeichen: Zahlen, Gross- und Klein-Buchstaben mit Umlauten, Punkte, Bindestriche, Unterstriche.

4.7 Passwort

min. 8 Zeichen, max. 64 Zeichen; Erlaubte Zeichen: Zahlen, Gross- und Klein-Buchstaben mit Umlauten, Punkten, Bindestrichen, Unterstrichen.

5 Sicherheit

5.1 SQL-Injection & Cross-site Scripting

5.2 Error Handling

5.3 Passwortspeicherung

6 SSL