University of Applied Sciences and Arts Northwestern Switzerland
School of Engineering

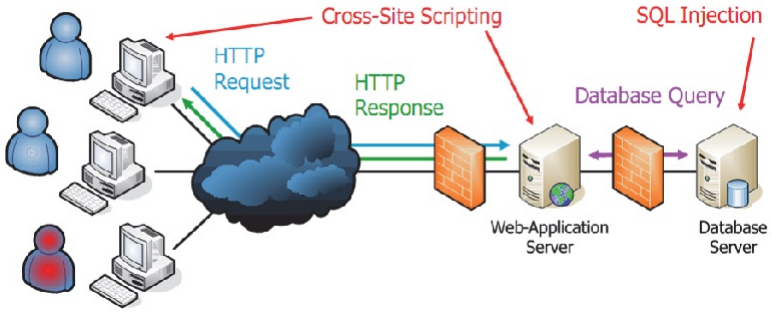
Application Security
Lab 2

Stefan Eggenschwiler & Daniel Gürber

17. Dezember 2013

Inhaltsverzeichnis

1 Aufgabenstellung



2 Softwareaufbau

3 Datenbank

3.1 Aufbau

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;
```

3.2 Sicherheit

4 Validierung

Im folgenden gehen wir auf die Validierung der Inputdaten ein. Angegeben werden jeweils die Voraussetzungen aus der Aufgabenstellung und wie wir diese implementiert haben.

4.1 Firmenname

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

Listing 2: Validierung Firmenname

```
if (name != null) {
  if (name.trim().isEmpty()) {
    errors.add("Firmenname eingeben.");
  } else if (name.trim().length() > 20) {
    errors.add("Firmenname zu lang (max. 20 Zeichen).");
  } else if (!name.matches("([èéÈÉäöüÄÖÜßa-zA-Z\\s]+)")) {
    errors.add("Ung&uuml;ltige Zeichen im Firmennamen");
  }
}
```

4.2 Strasse & Strassennummer

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

Listing 3: Validierung Adresse

```
if (address != null) {
  if (address.trim().isEmpty()) {
    errors.add("Keine Adresse.");
  } else if (!address.matches("[èéÈÉäöüÄÖÜß\\w\\s\\.\\-]+")) {
    errors.add("Ung&uuml;ltige Adresse.");
  }
}
```

4.3 Postleitzahl

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

Listing 4: Validierung PLZ

```
if (zip >= 1000 && zip <= 9999) {
  if(!validatePlz(zip))
    errors.add("Ung&uuml;ltige Postleitzahl.");
} else {
  errors.add("Ung&uuml;ltige Postleitzahl.");
  }
```

4.4 Stadt

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

Listing 5: Validierung Stadt

```
        if (town != null) {
          if (town.trim().isEmpty()) {
            errors.add("Keine Stadt.");
          } else if (!town.matches("[èéÈÉäöüÄÖÜßa-zA-Z\\-\\.\\s]+")) {
            errors.add("Ung&uuml;ltige Stadt.");
          }
        }
```

4.5 E-Mail Adresse

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

Listing 6: Validierung E-Mail

```
        if (mail != null && !mail.trim().isEmpty()) {
            if (!mail.matches("//RFC-822")) {
                errors.add("Ung&uuml;ltige Email-Adresse.");
            } else if(!mxLookup(mail)) {
              errors.add("Ung&uuml;ltige Email-Adresse.");
            }
        } else {
              errors.add("Keine Email-Adresse");
        }
```

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.

Listing 7: Validierung Passwort

```
    /**
```

```
     * Validates the given password.
     * @param pw password
     * @return true if password is valid
     */
6    @CheckReturnValue
    public static final String validatePassword(@CheckForNull String
       pw) {
      String error = null;
      if (pw != null) {
        if (pw.trim().length() < 8) {
11        error = "Passwort zu kurz (min. 8 Zeichen).";
        } else if (pw.trim().length() > 64) {
          error ="Passwort zu lang (max. 64 Zeichen).";
        } else if (!pw.matches("[èéÈÉäöüÄÖÜß\\-\\_\\.\\w]+")) {
            error = "Ungültige Zeichen im Passwort.";
16        }
      } else {
        error = "Passwort zu kurz (min. 8 Zeichen).";
      }
      return error;
21   }
```

5 Sicherheit

5.1 SQL-Injection & Cross-site Scripting

5.2 Error Handling

5.3 Passwortspeicherung

6 SSL