Dokumentation

M183

Cassandra Corrodi, Dennis Schäppi

# Inhalt

[Inhalt 2](#_Toc502752677)

[Die Applikation 3](#_Toc502752678)

[Aufgabenanalyse 4](#_Toc502752679)

[Sicherheitsanalyse 4](#_Toc502752680)

[Problembehebung 5](#_Toc502752681)

[Passwort in DB 5](#_Toc502752682)

[Login 6](#_Toc502752683)

[Suche 7](#_Toc502752684)

[Edit 8](#_Toc502752685)

[Testing 10](#_Toc502752686)

[Normalfälle 10](#_Toc502752687)

[Extremfälle 11](#_Toc502752688)

[Angriffsfälle 12](#_Toc502752689)

[Fazit 14](#_Toc502752690)

[Erkenntnisse 14](#_Toc502752691)

[Empfehlungen 14](#_Toc502752692)

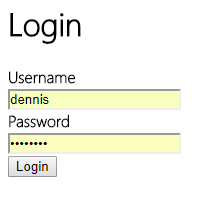
# Die Applikation

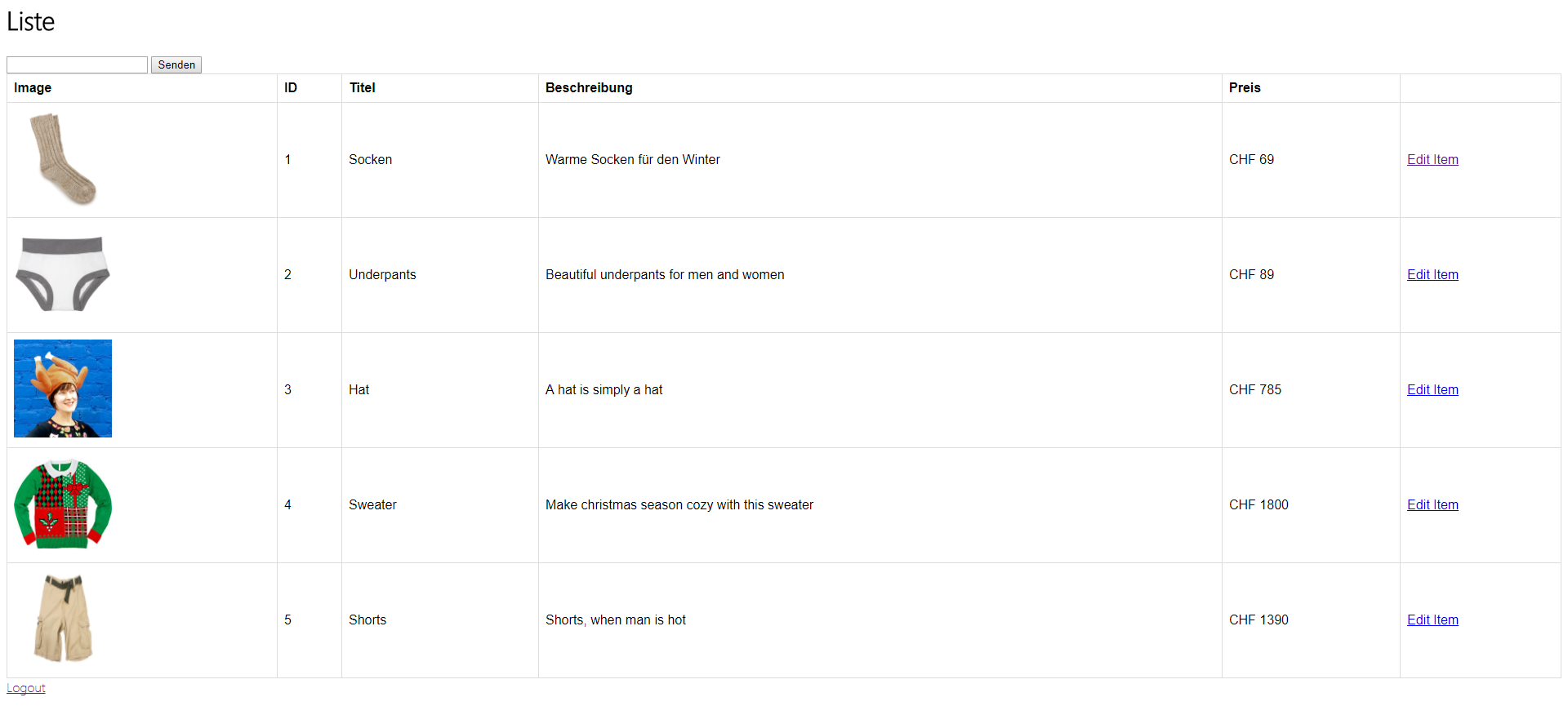
Unsere Applikation ist eine einfache Produktverwaltung. Nur Benutzer mit Adminrechten können die Daten der Produkte ändern.

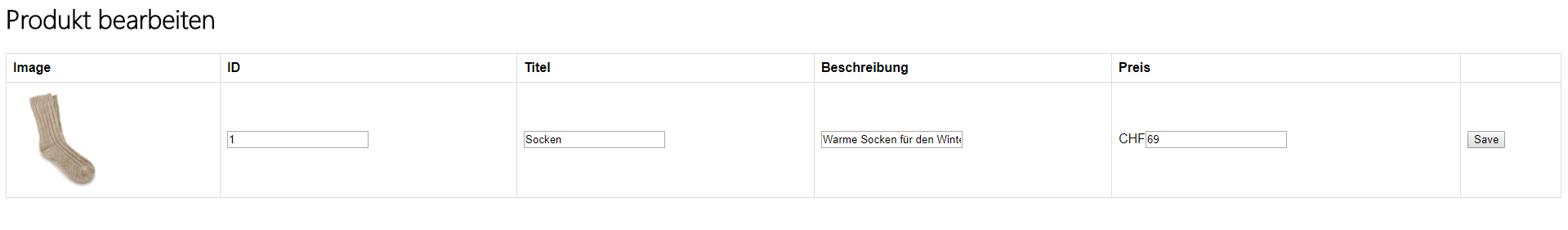
Der Benutzer kann sich mit einem Login anmelden und alle Produkte betrachten. Jedes Produkt hat eine ID, einen Titel, eine Beschreibung und einen Preis.

Der Benutzer kann in der Liste nach dem Produkttitel suchen.

Der Benutzer kann sich auch ausloggen.







# Aufgabenanalyse

Wir haben uns zuerst Gedanken gemacht, wie wir das Projekt absolvieren wollen. Wir sind dann auf folgende Einzelschritte gekommen:

* Analyse der Sicherheitslücken und Klassifizierung der Lücke
* Beseitigung der Lücken
* Testen ob Lücke geschlossen ist
* Persönliches Fazit

# Sicherheitsanalyse

|  |  |  |  |
| --- | --- | --- | --- |
| **Schwachstelle** | **Gefahr** | **Klassifizierung** | **Gegenmassnahme** |
| Passwort in DB | Passwort wurde nicht gehasht:  Leichte Beute für Hacker, welche in die DB eindringen | Kann gravierende Folgen haben | Passworthash mit Salt erzeugen. |
| Login | SQL-Injection möglich:  Benutzer kann über Passwortfeld sich selbst zum Admin machen, Passwörter von anderen Benutzern ändern und Benutzer löschen. | Kann teilweise gravierende Folgen haben | Prepared Statements  Serverseitige Feldüberprüfung vor dem Ausführen des SQL-Syntax |
| Suche | SQL-Injection möglich:  Benutzer kann über Suchfeld sich selbst zum Admin machen, Passwörter von anderen Benutzern ändern und Benutzer löschen. | Kann teilweise gravierende Folgen haben | Prepared Statements  Serverseitige Feldüberprüfung vor dem Ausführen des SQL-Syntax |
| Edit | SQL-Injection und XSS möglich:  Kann über die URL, sowie über die Eingabefelder schadhaften SQL-Code einschleusen.  Kann in den Eingabefeldern schadhaften JavaScript-Code einschleusen, welcher dann auch in der DB gespeichert wird. | Kann gravierende Folgen haben | Prepared Statements  Serverseitige Feldüberprüfung vor dem Ausführen des SQL-Syntax |
| Keine Serverseitige Feldüberprüfung | Somit kann auch schadhafter Code in die Datenbank kommen:  XSS im Edit speichert den schadhaften Code in die Datenbank und führt diesem immer beim Neuladen der Seite aus. | Kann gravierende Folgen haben | Strikte Feldüberprüfung und somit diverse Zeichen verbieten. |
| Sensible Eingabefelder nicht genug gesichert. | Passwortfeld wird im Klartext angezeigt. | Kann teilweise gravierende Folgen haben | Zu einem Passwortfeld machen. |

# Problembehebung

## Passwort in DB

Das Passwort in der DB wurde nicht verschlüsselt, es steht im Klartext in der Datenbanktabelle drinnen. Sollte ein Hacker aus der Datenbank Daten entnehmen können, so ist dies danach ohne verschlüsseltes Passwort noch einfacher, die Accounts zu stehlen.



Um es nun den Hackern noch schwerer zu machen, die Accounts zu stehlen, werden wir die Passwörter verschlüsseln und zwar mit der Hash-Funktion. Leider ist ein einfacher Hash des Passworts auch nicht mehr sicher, da man diese Zeichenfolgen auf Webseiten leicht entziffern kann. Vor allem einfache Passwörter wie «abcdefg» oder «1234678» können somit sehr einfach entschlüsselt werden. Damit dies nicht mehr so leicht passieren kann, fügen wir noch einen «Salt» dazu, dies ist ein zusätzlicher Schlüssel, welcher zusammen mit dem Passwort gehasht und in die Datenbank geschrieben wird. Wir nehmen die ID des Benutzers dafür. Wenn nun beim nächsten Mal der Benutzer sich anmelden will, so ist nur das Passwort nicht mehr genügend, weil es nun den Schlüssel nun auch benötigt.

Die Funktion für die endgültige Verschlüsselung sieht dann so aus:

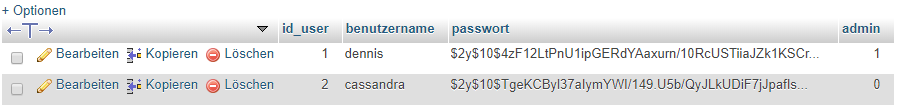
$pw = "panda";

$id = 2;

password\_hash($pw.$id, PASSWORD\_DEFAULT);

‘panda2’ => $2y$10$TgeKCByl37aIymYWI/149.U5b/QyJLkUDiF7jJpafIsvC94.HBpOq

Die Tabelle sieht nun so aus:



## Login

Der darauffolgende SQL-Syntax lässt SQL-Injections zu. Folgende Eingriffe sind dann möglich:

* Benutzer kann sich selbst zum Admin machen
* Passwörter von anderen Benutzern ändern
* Benutzer löschen

Der aktuelle SQL-Query sieht so aus:

$username = ‘cassandra’;

$password = ‘panda’;

$sql = "SELECT id\_user, benutzername, passwort, admin FROM user WHERE benutzername = '$username' AND passwort = '$password'";

Besonders die Variable «password» kann mit einem zusätzlichen SQL-Code ergänzt werden. Die oben genannten Punkte für mögliche Eingriffe werden wir nun alle durchgehen:

Sich selbst zum Admin machen:

$sql = "SELECT id\_user, benutzername, passwort, admin FROM user WHERE benutzername = 'cassandra' AND passwort = 'a'; UPDATE user SET admin = 1 WHERE benutzername = 'cassandra'";

Passwörter von anderen Benutzern ändern:

$sql = "SELECT id\_user, benutzername, passwort, admin FROM user WHERE benutzername = 'cassandra' AND passwort = 'a'; UPDATE user SET passwort = 'hacked' WHERE benutzername = 'dennis'";

Benutzer löschen:

$sql = "SELECT id\_user, benutzername, passwort, admin FROM user WHERE benutzername = 'cassandra' AND passwort = 'a'; DELETE FROM user WHERE benutzername = 'dennis'";

Damit solche Angriffe verteidigt werden können, haben wir mit den Prepared Statements gearbeitet:

$sql = "SELECT id\_user, benutzername, passwort, admin FROM user WHERE benutzername = :username";

$stmt = $db->prepare($sql);

$stmt->execute(array(

'username' => $username

));

Da der Benutzername in der Datenbank ein Unique-Key ist, reicht der Filter für den Benutzernamen. In einer darauffolgenden Überprüfung wird dann auch das Passwort zusammen mit der ID geprüft.

Um dies aber auch noch doppelt abzusichern, haben wir auch noch eine Serverseitige Feldüberprüfung implementiert. Diese wird zusammen mit den Feldeinschränkungen in der Datenbank überprüft:

|  |  |  |
| --- | --- | --- |
| **Name des Feldes** | **Max. zulässige Zeichen** | **Erlaubte Zeichen** |
| Username | 50 | [a-zA-Z][0-9] |
| Password | 128 | [a-zA-Z][0-9][$!?] |

if(!preg\_match("#^[0-9a-zA-Z]+$#", $username)){

header('Location: login.php');

exit;

}

if(!preg\_match("#^[0-9a-zA-Z$!?]+$#", $password)){

header('Location: login.php');

exit;

}

## Suche

Der SQL-Befehl bei der Suche lässt folgendes zu:

* Benutzer kann sich selbst zum Admin machen
* Passwörter von anderen Benutzern ändern
* Benutzer löschen

Der aktuelle SQL-Query sieht so aus:

$sql = "SELECT \* FROM produkte WHERE name LIKE '%$search%'"

Sich selbst zum Admin machen:

$sql = "SELECT \* FROM produkte WHERE name LIKE '%%'; UPDATE user SET admin = 1 WHERE benutzername LIKE '%cassandra%'";

Passwörter von anderen Benutzern ändern:

$sql = "SELECT \* FROM produkte WHERE name LIKE '%%'; UPDATE user SET passwort = 'hacked' WHERE benutzername LIKE '%dennis%'";

Benutzer löschen:

$sql = "SELECT \* FROM produkte WHERE name LIKE '%%'; DELETE FROM user WHERE benutzername LIKE '%dennis%'";

## Edit

Folgende Gefahren sind beim Ändern der Daten möglich:

* Jede Art von SQL-Injection
* Cross Site Scripting

Beim Editieren haben wir die grösste Schwachstelle gefunden. Hier sind nämlich aufgrund des Aufbaus vom SQL-Query alle Art von SQL-Injections möglich und zu gleich kann in den Feldern Schadhafter JavaScript-Code eingeschleust werden und diesen auch noch in der Datenbank speichert.

Die schädlichste Art, einen SQL-Query im PHP zu schreiben und den wir in der Applikation verwenden wäre folgender:

$sql = "SELECT \* FROM produkte WHERE id\_produkt = $id";

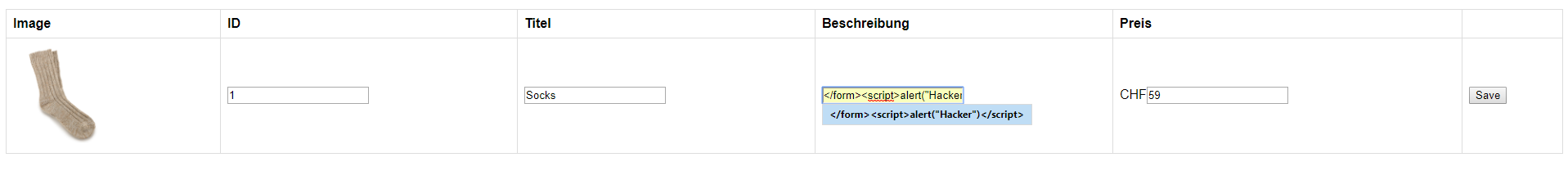
Der SQL-Query ist nämlich so schädlich, weil die Variabel am Ende steht und dazu auch noch ein Zahlenwert verlangt wird. Dadurch muss der Hacker nicht auf die Hochkommas achten und kann nach einem Semikolon einfach einen SQL-Query nach Wahl anhängen. Als Beispiel kann der Hacker einen neuen Benutzer erstellen:

$sql = "SELECT \* FROM produkte WHERE id\_produkt = 1; INSERT INTO user (benutzername, passwort, admin) VALUES ('hacker', 'hacked', 1)";

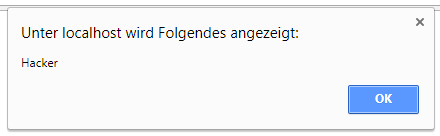
Und Worst-Case:

$sql = "SELECT \* FROM produkte WHERE id\_produkt = 1; DROP DATABASE 'm181\_produktverwaltung'";

Bei der zweiten Gefahr ist es möglich schadhaften JavaScript-Code in die Datenbank zu speichern.



Wie oben im Bild abgebildet, kann man hier einen HTML- und JavaScript-Code per Eingabefeld injiziert werden. Der Grund, warum das Cross Site Scripting hier funktioniert, ist wegen der Datenausgabe im Value. Dadurch wird dies als HTML-Code interpretiert. Der Endtag des Formulars ist zwingend, denn es soll danach der Script-Tag eingeschleust werden. Das HTML erkennt somit dass das Formular zu Ende ist. Im Script drinnen kann man jede Art von Angriff implementieren, wir haben jetzt das einfache Beispiel mit dem Alert gemacht.



Diese Box erscheint nun und jedes Mal, wenn der Benutzer die Seite neu lädt, wird das Script ausgeführt, weil es in der Datenbank gespeichert wurde.

Damit auch dies nicht mehr möglich ist, haben wir bestimmte Zeichen ausgeschlossen:

|  |  |  |
| --- | --- | --- |
| **Name des Feldes** | **Max. zulässige Zeichen** | **Verbotene Zeichen** |
| Name | 50 | <> |
| Beschreibung | - | <> |
| Preis | - | <> |

if(preg\_match("/[<>]/", $titel)){

header('Location: edit.php?id='.$id);

exit;

}

if(preg\_match("/[<>]/", $beschreibung)){

header('Location: edit.php?id='.$id);

exit;

}

# Testing

## Normalfälle

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Name des Tests** | **Eingabe** | **Erwartetes Ergebnis** | **Status** |
| N1 | Login | Benutzername: dennis  Passwort: 12345678 | Benutzer kann sich einloggen und wird zur Liste weitergeleitet. | OK |
| N2 | Suche | Eingabe: Socks | Die Produkte mit dem Titel «Socks» werden aufgelistet. | OK |
| N3 | Edit Button mit Adminrechte | «Edit Item» anklicken | Der Benutzer wird auf die Bearbeitungsseite des jeweiligen Produkts weitergeleitet. | OK |
| N4 | Edit Button ohne Adminrechte | «Edit Item» anklicken | Der Benutzer bekommt die Meldung, dass der Zugriff für ihn verweigert wurde. | OK |
| N5 | Update | Titel: Socken  Beschreibung: Warme Socken für den Winter  Preis: 69  «Save» anklicken | Die eingegebenen Daten werden in der Datenbank aktualisiert und der Benutzer wird zurück zur Liste geleitet. | OK |
| N6 | Logout | «Logout» anklicken | Der Benutzer wird ausgeloggt und wird zum Login weitergeleitet. | OK |

## Extremfälle

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Name des Tests** | **Eingabe** | **Erwartetes Ergebnis** | **Status** |
| E1 | Login: Benutzername Ungültige Zeichen | dennis%& | Benutzer wird nicht weitergeleitet, da:   1. Benutzername nicht existiert 2. Das Feld ungültige Zeichen enthält | OK |
| E2 | Login: Passwort Ungültige Zeichen | 12345678%& | Benutzer wird nicht weitergeleitet, da:   1. Passwort falsch ist 2. Das Feld ungültige Zeichen enthält | OK |
| E3 | Login: Benutzername  Leeres Feld | (leer) | Benutzer bekommt Meldung, dass Eingabe erforderlich ist. | OK |
| E4 | Login: Passwort Leeres Feld | (leer) | Benutzer bekommt Meldung, dass Eingabe erforderlich ist. | OK |
| E5 | Suche Ungültige Zeichen | Socks?%& | Es werden alle Ergebnisse angezeigt. | OK |
| E6 | Update: Titel Ungültige Zeichen | Socken<> | Änderungen werden verworfen | OK |
| E7 | Update: Beschreibung Ungültige Zeichen | Warm<> | Änderungen werden verworfen | OK |
| E8 | Update: Preis Ungültige Zeichen | 69fr | Änderungen werden verworfen | (OK) |
| E9 | Update Titel: Leeres Feld | (leer) | Änderungen werden verworfen | OK |
| E10 | Update Beschreibung: Leeres Feld | (leer) | Änderungen werden verworfen | OK |
| E11 | Update Preis: Leeres Feld | (leer) | Änderungen werden verworfen | OK |

## Angriffsfälle

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Name des Tests** | **Eingabe** | **Erwartetes Ergebnis** | **Status** |
| A1 | Login: SQL-Injection 1 Benutzername | a'; UPDATE user SET admin = 1 WHERE benutzername = 'cassandra | Benutzer wird nicht weitergeleitet, da:   1. Benutzername nicht existiert 2. Das Feld ungültige Zeichen enthält | OK |
| A2 | Login: SQL-Injection 2 Benutzername | a'; UPDATE user SET passwort = 'hacked' WHERE benutzername = 'dennis | Benutzer wird nicht weitergeleitet, da:   1. Benutzername nicht existiert 2. Das Feld ungültige Zeichen enthält | OK |
| A3 | Login: SQL-Injection 3 Benutzername | a'; DELETE FROM user WHERE benutzername = 'dennis | Benutzer wird nicht weitergeleitet, da:   1. Benutzername nicht existiert 2. Das Feld ungültige Zeichen enthält | OK |
| A4 | Login: SQL-Injection 1 Passwort | a'; UPDATE user SET admin = 1 WHERE benutzername = 'cassandra | Benutzer wird nicht weitergeleitet, da:   1. Passwort falsch ist 2. Das Feld ungültige Zeichen enthält | OK |
| A5 | Login: SQL-Injection 2 Passwort | a'; UPDATE user SET passwort = 'hacked' WHERE benutzername = 'dennis | Benutzer wird nicht weitergeleitet, da:   1. Passwort falsch ist 2. Das Feld ungültige Zeichen enthält | OK |
| A6 | Login: SQL-Injection 3 Passwort | a'; DELETE FROM user WHERE benutzername = 'dennis | Benutzer wird nicht weitergeleitet, da:   1. Passwort falsch ist 2. Das Feld ungültige Zeichen enthält | OK |
| A7 | Suche: SQL-Injection 1 | %'; UPDATE user SET admin = 1 WHERE benutzername LIKE '%cassandra | Es werden alle Ergebnisse angezeigt, weil String leer ausfällt | OK |
| A8 | Suche: SQL-Injection 2 | %'; UPDATE user SET passwort = 'hacked' WHERE benutzername LIKE '%dennis | Es werden alle Ergebnisse angezeigt, weil String leer ausfällt | OK |
| A9 | Suche: SQL-Injection 3 | %'; DELETE FROM user WHERE benutzername LIKE '%dennis | Es werden alle Ergebnisse angezeigt, weil String leer ausfällt | OK |
| A10 | Edit: SQL-Injection URL | 1; INSERT INTO user (benutzername, passwort, admin) VALUES ('hacker', 'hacked', 1) | Applikation läuft gewöhnlich weiter und fügt keinen neuen Nutzer ein | OK |
| A11 | Edit: Cross Site Scripting Titel | </form><script>alert("Hacker")</script> | Änderungen werden verworfen | OK |
| A12 | Edit: Cross Site Scripting Beschreibung | </form><script>alert("Hacker")</script> | Änderungen werden verworfen | OK |

# Fazit

## Erkenntnisse

Wir haben erkannt, dass auch scheinbar harmlose Eingabefelder einen grossen Schaden anrichten. Es war uns zuvor schon bewusst, dass solche Sicherheitslücken «erweiterte Datenausgaben» machen können. Auch war uns bewusst, dass man per Eingabefelder auch Daten verändern konnte. Was uns aber zuvor noch nie bewusst war, ist der Schaden, der dabei angerichtet werden kann. Vor allem die Lösch-Syntax im SQL kann die ganze Datenbank zerstören. Dass man auch über ein Eingabefeld Schadhaften JavaScript-Code einschleusen konnte, um damit Phishing-Attacken durchzuführen, haben wir zuvor auch noch nie gesehen. Es war uns bewusst, dass HTML-Code in der Datenbank als diesen erkannt wird, jedoch haben dabei nur an einfache Tags wie <b></b> (Fetter Text) gedacht, aber nie daran, JavaScript-Code einzuschleusen.

Zum Schluss können wir beide sagen, dass wir bei dieser Projektarbeit zu sehr viele Erkenntnissen gekommen sind, an die wir zuvor nie gedacht hätten. In Zukunft werden wir, wenn jemand uns wieder mal eine solche Webapplikation schreiben muss, mehr auf die Sicherheit achten.

## Empfehlungen

Anhand unserer vielen Erkenntnisse haben wir auch einige Empfehlungen an Personen, die sich noch nie mit diesem Thema auseinandergesetzt haben.

1. Mache bei einer Webapplikation mit Eingabefeldern IMMER eine zweiseitige Überprüfung. Mit dem Client und mit dem Server!
2. Kontrolliere die Eingaben IMMER serverseitig auf ihre Gültigkeit:  
   *Bsp.: Ein Nummernfeld kann per F12 auch zu einem Textfeld formatiert werden*
3. Mache dir für jedes Feld eine schwarze Liste von Zeichen, die niemals verarbeitet werden dürfen!
4. Füge für jede Datenbankabfrage ein Prepared Statement hinzu oder Lagere die Syntax in einen Stored Procedure aus!
5. Füge jedem Passworthash einen Salt hinzu!  
   *Bsp.: ID des Benutzers zum Passwort anfügen*
6. (Hier nicht aufgeführt) Verschlüssle die Verbindung zur Website stets mit einem HTTPS um Angriffe auf die Ordner zu vermeiden!