Übungsblatt 1
Gruppe 2
Stand: 11. April 2018 Version: 1.0

1 Footprinting über das Internet

Ausgewählte Hochschule: FH-Bielefeld - University of Applied Sciences
Webserver: Apache/2.4.10 (Linux/SUSE)
Bekannte Schwachstelle: `https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3523`

Listing 1: Ermittlen des Webservers

```
#!/bin/bash
curl -I -s https://www.fh-bielefeld.de | grep Server
```

2 Netzwerkdaten analysieren

1. Username: gurpartap@patriots.in
2. Passwort: punjab@123
3. Betreff: SMTP
4. Sender: gurpartap@patriots.in
5. Empfänger: raj_deol2002in@yahoo.co.in
6. Body*:

   ```
   Hello

   I send u smtp pcap file

   Find the attachment

   GPS
   ```

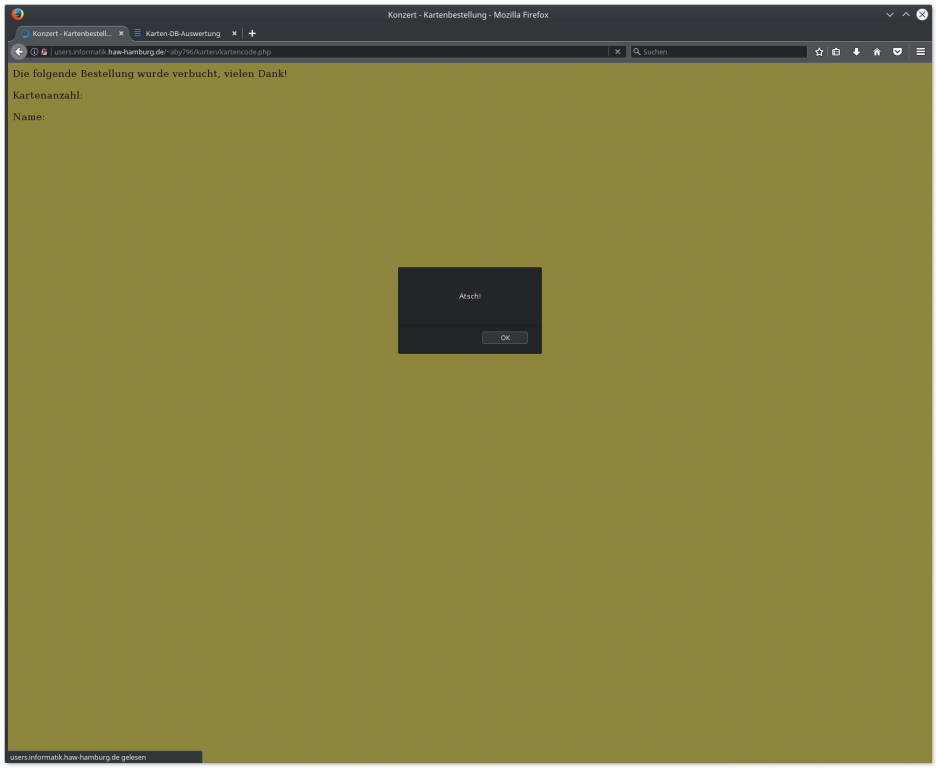
   *Unnötige Leerzeilen entfernt

3 XSS / SQL-Injection

3.1 XSS - Ausführung

Folgendes Code-Snippet in einer der Input-Boxen einfügen:

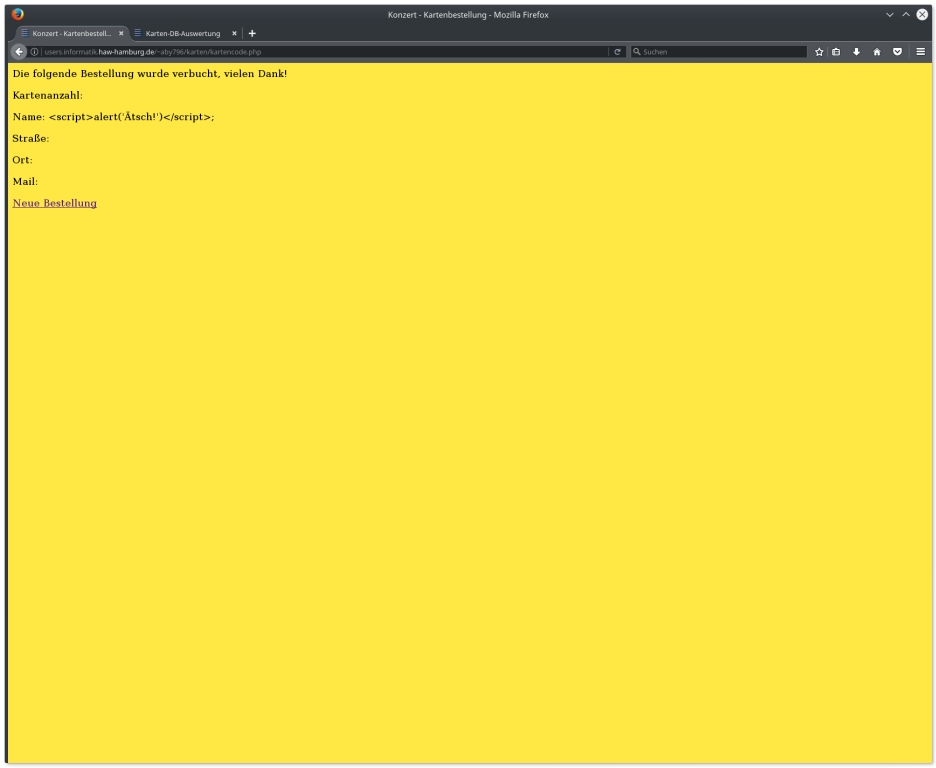
```
<script>alert('Ätsch!')</script>
```



3.2 XSS - Fix

XSS-Fix durch Umwandeln von besonderen Zeichen der Eingabe:

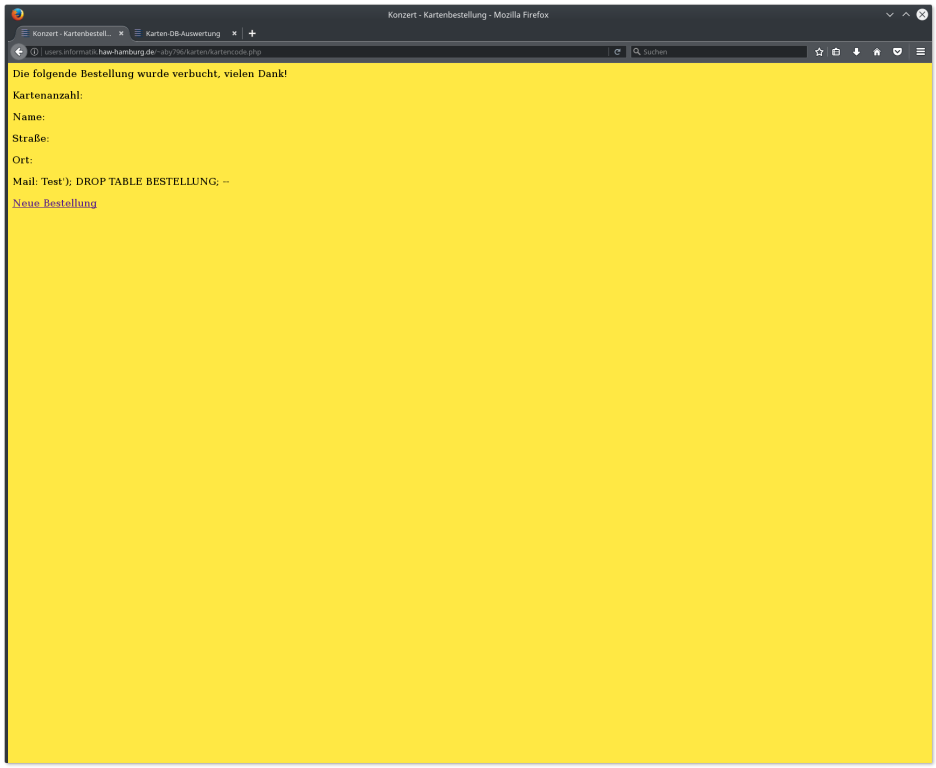
```
$Kartenanzahl = htmlspecialchars($_POST['Kartenanzahl'], ENT_QUOTES, 'UTF-8');
$Name = htmlspecialchars($_POST['Name'], ENT_QUOTES, 'UTF-8');
$Strasse = htmlspecialchars($_POST['Strasse'], ENT_QUOTES, 'UTF-8');
$Ort = htmlspecialchars($_POST['Ort'], ENT_QUOTES, 'UTF-8');
$Mail = htmlspecialchars($_POST['Mail'], ENT_QUOTES, 'UTF-8');
```

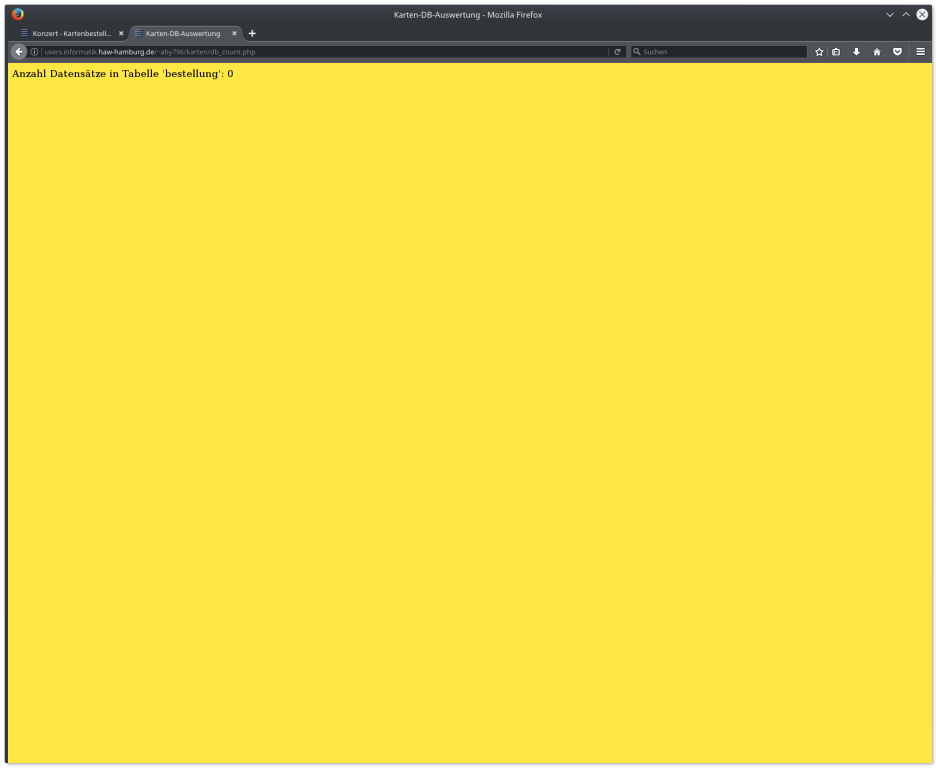


3.3 SQL-Injection - Ausführung

In der Input-Box der Mail-Adresse folgendes Code-Snippet eingeben:

```
Test'); DROP TABLE bestellung; --
```


Konzert - Kartenbestellung - Mozilla Firefox
Konzert - Kartenbestell...
Karten-DB-Auswertung
users.informatik.haw-hamburg.de/~aby796/karten/kartencode.php
Suchen
Die folgende Bestellung wurde verbucht, vielen Dank!
Kartenanzahl:
Name:
Straße:
Ort:
Mail: Test'); DROP TABLE BESTELLUNG; --
Neue Bestellung


Karten-DB-Auswertung - Mozilla Firefox
Konzert - Kartenbestell...
Karten-DB-Auswertung
users.informatik.haw-hamburg.de/~aby796/karten/db_count.php
Suchen
Anzahl Datensätze in Tabelle 'bestellung': 0

3.4 SQL-Injection - Fix

SQL-Injection-Fix durch Anwenden eines Prepared-Statements:

```
$sql = $db->prepare("INSERT INTO bestellung (anzahl, name, strasse, ort, mail)
$sql->bindParam(1,$Kartenanzahl);
$sql->bindParam(2,$Name);
$sql->bindParam(3,$Strasse);
$sql->bindParam(4,$Ort);
$sql->bindParam(5,$Mail);

$sql->execute();
```