

## Beispieldateien für die Webseite (Langfassung)

Dieses Dokument zeigt den Inhalt der Beispieldateien für die Webseite in der Lehrveranstaltung *IT-Security Lab* zu Dokumentationszwecken.

### index.html

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta charset="UTF-8"/>
5     <title>Andreas Unterwegers Spielwiese</title>
6   </head>
7   <body>
8     <h1>Willkommen auf der Spielwiese!</h1>
9     <p>
10      Hier steht viel Text.
11    </p>
12    <ul style="list-style: none;">
13      <li>
14        <a href="top.html">Meistverkauftes Produkt</a>
15      </li>
16      <li>
17        <a href="search.html">Produktsuche</a>
18      </li>
19    </ul>
20  </body>
21 </html>
```

### top.html

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta charset="UTF-8"/>
5     <title>Meistverkauftes Produkt</title>
6   </head>
7   <body>
8     <h1>Produktinformation</h1>
9     <p>
10      Hier steht noch mehr Text.
11    </p>
12    <p>
```

```
13     Geben Sie Ihren Namen ein, um das Produkt zu
14         personalisieren.
15     </p>
16     <form action="customize_v1.php" method="post">
17         Name:
18         <input type="text" name="name"/>
19         <input type="submit" value="Personalisieren"/>
20     </form>
21 </body>
22 </html>
```

### customize\_v1.php

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta charset="UTF-8"/>
5     <title>Personalisiertes Produkt</title>
6   </head>
7   <body>
8     <h1>Ihr Produkt, <?php echo $_POST['name']; ?></h1>
9     <p>
10        Hier steht noch viel mehr Text.
11    </p>
12    <div style="position: relative;">
13      
14      <h2 style="position: absolute; left: 100px; top:
15        300px; color: white;"><?php echo $_POST['
16        name']; ?></h2>
17    </div>
18  </body>
19 </html>
```

### search.html

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta charset="UTF-8"/>
5     <title>Produktsuche</title>
6   </head>
7   <body>
```

```
8     <h1>Produktsuche</h1>
9     <p>
10    Hier steht noch viel, viel mehr Text.
11    </p>
12    <p>
13    Geben Sie einen Begriff ein, um nach einem
14    Produkt zu suchen.
15    </p>
16    <form action="search_v1.php" method="post">
17    Suchbegriff:
18    <input type="text" name="query"/>
19    <input type="submit" value="Suchen"/>
20    </form>
21 </body>
22 </html>
```

### search\_v1.php

```
1 <!DOCTYPE html>
2
3 <?php
4 $connection = mysql_connect("localhost", "root", "
5     wartung") or die("Fehler beim Verbinden zur
6     Datenbank");
7 mysql_select_db("Spielwiese");
8
9 $query = $_POST['query'];
10 $result = mysql_query("SELECT name, description FROM
11     products WHERE name LIKE \"%$query%\";") or die("
12     Fehler beim Abfragen der Datenbank");
13
14 mysql_close($connection);
15 ?>
16
17 <html>
18 <head>
19 <meta charset="UTF-8"/>
20 <title>Suchergebnis</title>
21 <style>
22     table {
23         border-collapse: collapse;
24     }
25     table, th, td {
26         border: 1px solid black;
27     }
```

```
24     </style>
25 </head>
26 <body>
27   <h1>Ihr Suchergebnis zum Begriff &quot;<?php echo
      $query; ?>&quot;;</h1>
28   <p>
29     Hier steht noch viel, viel mehr Text.
30   </p>
31   <table>
32     <tr>
33       <th>Name</th>
34       <th>Beschreibung</th>
35     </tr>
36     <?php
37       $n = 0;
38       while ($row = mysql_fetch_array($result))
39       {
40         $n++;
41         echo "<tr><td>".$row[0]."</td><td>".$row
              [1]."</td></tr>"; #echo "<tr><td>".$row{"
              name"}."</td><td>".$row{"description
              }."</td></tr>";
42       }
43       mysql_free_result($result);
44     ?>
45   </table>
46   <p>
47     <b><?php echo $n; ?></b> Treffer insgesamt
48   </p>
49 </body>
50 </html>
```

### malicious.php

```
1 <?php
2 header("Access-Control-Allow-Origin: *");
3 header("Access-Control-Allow-Methods: PUT, GET, POST")
  ;
4 header("Access-Control-Allow-Headers: Origin, X-
  Requested-With, Content-Type, Accept");
5 header("Content-Type", "text/plain");
6
7 $payload = file_get_contents("malicious.html");
8 print $payload;
9 ?>
```

**top.jpg**

Größe: 385 · 478 Pixel



Bildquelle: [http://ecx.images-amazon.com/images/I/61VT1jx2mfL.\\_UX385\\_.jpg](http://ecx.images-amazon.com/images/I/61VT1jx2mfL._UX385_.jpg)