Beispieldateien für die Webseite & den Angreifer

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

index.html

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8"/>
    <title>Andreas Unterwegers Spielwiese</title>
  </head>
  <body>
    <h1>Willkommen auf der Spielwiese!</h1>
    <p>
      Hier steht viel Text.
    </p>
    <ul style="list-style: none;">
      <li>
        <a href="top.html">Meistverkauftes Produkt</a>
      </li>
      <li>
        <a href="search.html">Produktsuche</a>
      </li>
    </ul>
  </body>
</html>
```

top.html

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8"/>
    <title>Meistverkauftes Produkt</title>
  </head>
  <body>
    <h1>Produktinformation</h1>
    <p>
      Hier steht noch mehr Text.
    </p>
    <p>
      Geben Sie Ihren Namen ein, um das Produkt zu
          personalisieren.
```

```
14      </p>
15      <form action="customize_v1.php" method="post">
16        Name:
17        <input type="text" name="name"/>
18        <input type="submit" value="Personalisieren"/>
19      </form>
20    </body>
21  </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        <img src="top.jpg" alt=""/>
14        <h2 style="position: absolute; left: 100px; top:
              300px; color: white;"><?php echo $_POST['
            name']; ?></h2>
15      </div>
16    </body>
17  </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
              Produkt zu suchen.
14      </p>
15      <form action="search_v1.php" method="post">
16        Suchbegriff:
17        <input type="text" name="query"/>
18        <input type="submit" value="Suchen"/>
19      </form>
20    </body>
21  </html>
```

search_v1.php

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

```
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: $385 \cdot 478$ Pixel

Bildquelle: `http://ecx.images-amazon.com/images/I/61VTljx2mfL._UX385_.jpg`