

main

...

webray.com.cn / cve / Product Show Room Site / 'Message' Stored Cross-Site Scripting(XSS).md



Xor-Gerke Create 'Message' Stored Cross-Site Scripting(XSS).md

History

1 contributor



36 lines (22 sloc) | 1.75 KB

...

# Product Show Room Site - 'Message' Stored Cross-Site Scripting(XSS)

Exploit Title: Product Show Room Site - 'Message' Stored Cross-Site Scripting(XSS)

Exploit Author: [webraybtl@webray.com.cn](mailto:webraybtl@webray.com.cn) inc

Vendor Homepage: <https://www.sourcecodester.com/php/15370/product-show-room-site-phpoop-free-source-code.html>

Software Link: <https://www.sourcecodester.com/download-code?nid=15370&title=Product+Show+Room+Site+in+PHP%2FOOP+Free+Source+Code>

Version: Product Show Room Site 1.0

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

Description

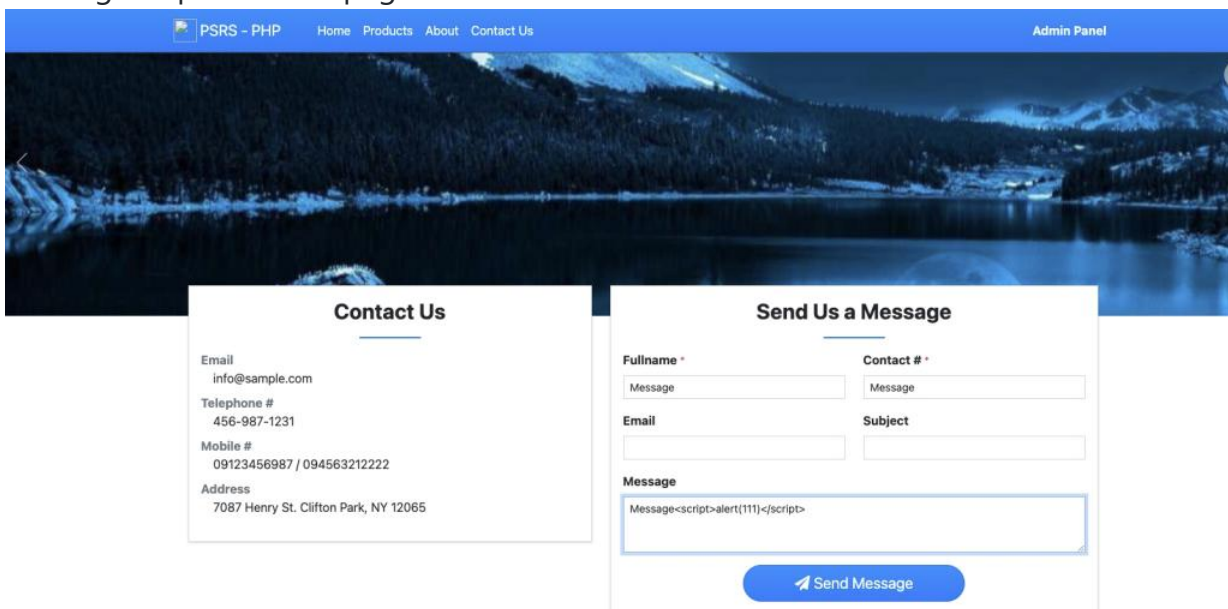
Persistent XSS (or Stored XSS) attack is one of the three major categories of XSS attacks, the others being Non-Persistent (or Reflected) XSS and DOM-based XSS. In general, XSS attacks are based on the victim's trust in a legitimate, but vulnerable, website or web application. Product Show Room Site does not filter the content correctly at the "Contact info-Telephone" module, resulting in the generation of stored XSS.

### Payload used:

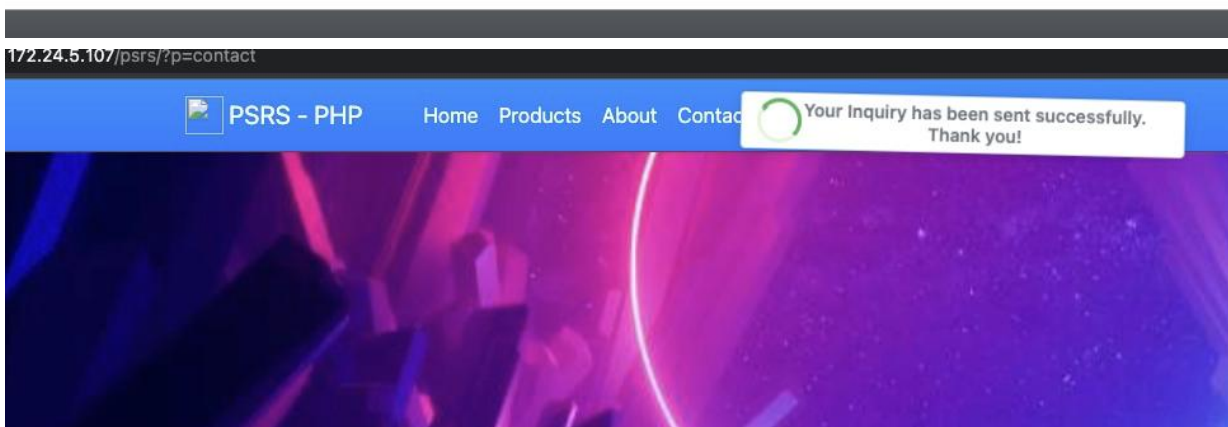
```
<script>alert(111)</script>
```

### Proof of Concept

1. Login the CMS. Default Admin Access Username: admin Password: admin123
2. Open Page <http://172.24.5.107/psrs/?p=contact>
3. Put XSS payload ( `<script>alert(111)</script>` ) in the Message box and click on Send Message to publish the page



The screenshot shows the PSRS - PHP website interface. The top navigation bar includes links for Home, Products, About, and Contact Us, along with an Admin Panel link. The main content area features a large background image of a lake and mountains. Below this, there are two contact forms. The 'Contact Us' form on the left displays contact information: Email (info@sample.com), Telephone # (456-987-1231), Mobile # (09123456987 / 09456321222), and Address (7087 Henry St. Clifton Park, NY 12065). The 'Send Us a Message' form on the right has fields for Fullname, Contact #, Email, Subject, and a large Message box. The Message box contains the XSS payload: `Message<script>alert(111)</script>`. A 'Send Message' button is located at the bottom of the form.



4. Open <http://172.24.5.107/psrs/admin/?page=inquiries>, Viewing the Top 1 of Inquiries page, We can see the alert.

