Xor-Gerke / webray.com.cn Public template

Code Issues Pull requests Actions Projects Security Insights

main

webray.com.cn / cve / Zoo-Management-System / Zoo-Management-System(XSS).md

Xor-Gerke Rename cve/Zoo-Management-System(XSS).md to cve/Zoo-Managem... … History

1 contributor

33 lines (21 sloc) | 1.65 KB

Zoo Management System - 'admin_name' Stored Cross-Site Scripting(XSS)

Exploit Title: Zoo Management System - 'admin_name' Stored Cross-Site Scripting(XSS)

Exploit Author: webraybtl@webray.com.cn inc

Vendor Homepage: https://www.sourcecodester.com/php/15347/zoo-management-system-source-code-php-mysql-database.html

Software Link: https://www.sourcecodester.com/download-code?nid=15347&title=Zoo+Management+System+source+code+in+PHP+with+MySQL+Database

Version: Zoo Management System 1.0

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

Description

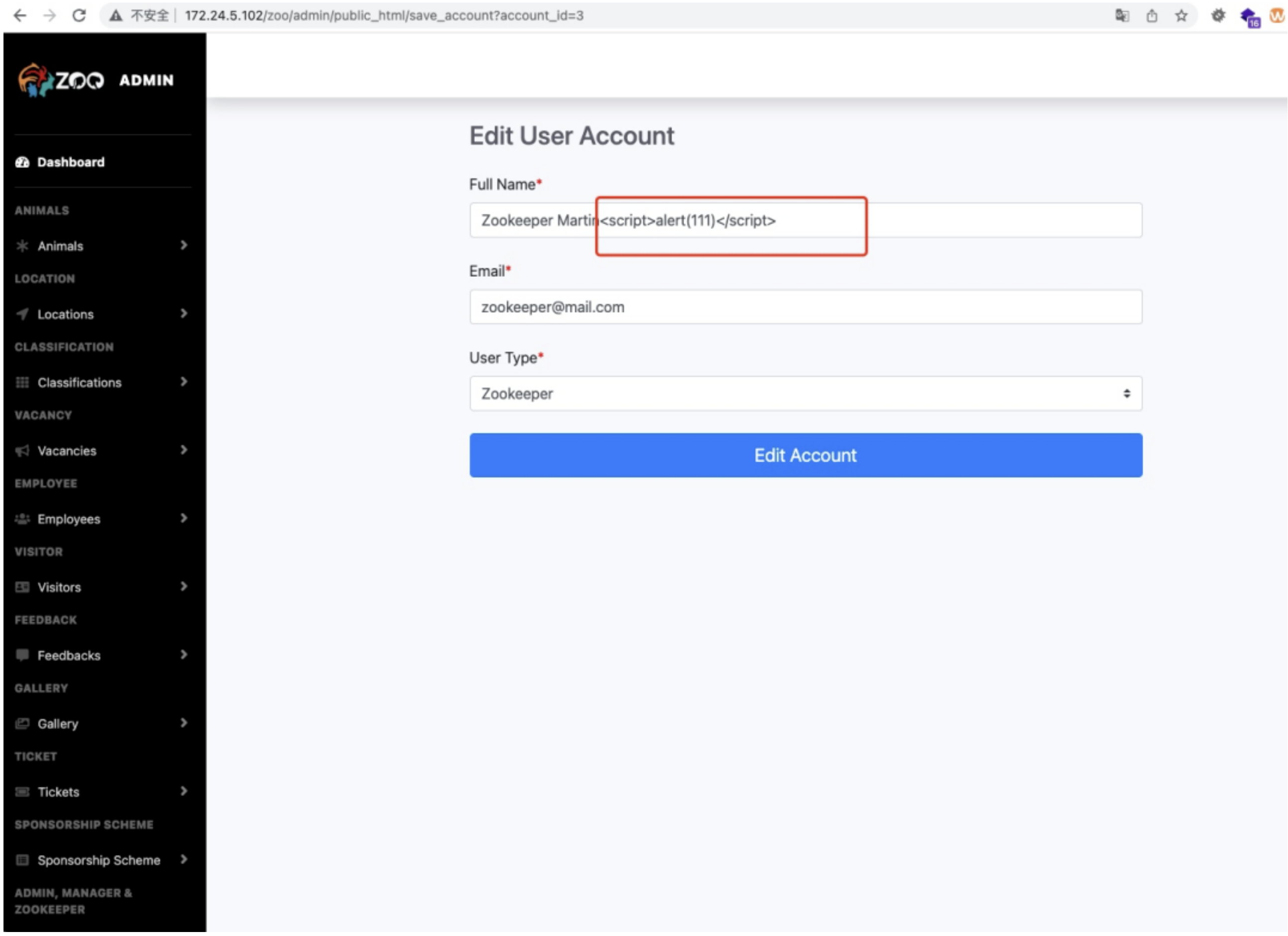
Persistent XSS (or Stored XSS) attack is one of the three major categories of XSS attacks, the others being Non-Persistent (or Reflected) XSS and DOM-based XSS. In general, XSS attacks are based on the victim's trust in a legitimate, but vulnerable, website or web application.Zoo Management System does not filter the content correctly at the "content" 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@mail.com Password: Password@123
2. Open Page http://172.24.5.102/zoo/admin/public_html/view_accounts?type=zookeeper and click Edit button
3. Put XSS payload (`<script>alert(111)</script>`) in the content box and click on Edit Account to publish the page



不安全 | 172.24.5.102/zoo/admin/public_html/save_account?account_id=3

Edit User Account

Full Name*

Zookeeper Martin<script>alert(111)</script>

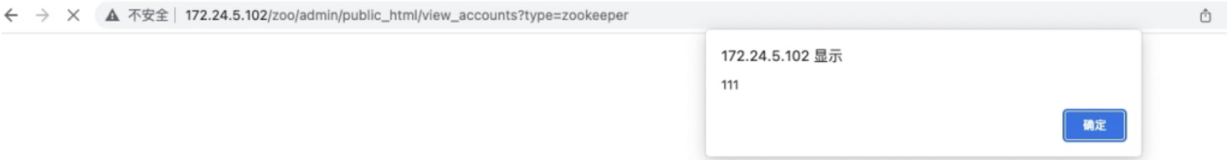
Email*

zookeeper@mail.com

User Type*

Zookeeper

4. Viewing the successfully published page,We can see the alert.



不安全 | 172.24.5.102/zoo/admin/public_html/view_accounts?type=zookeeper

172.24.5.102 显示

111