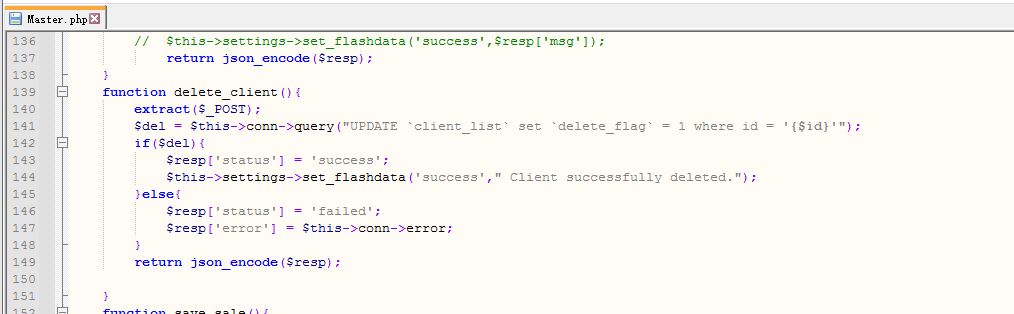
Download sourcecode from <https://www.sourcecodester.com/php/16061/sales-tracker-management-system-using-php-free-source-code.html>

Deploy the system

The sql injection url: [http://192.168.131.135/php-sts/classes/Master.php?f=delete\_client](http://192.168.131.135/php-sts/admin/clients/manage_client.php?id=1)

 Vulnerability trigger parameter: id

sourcecode:



The delete\_client function received the parameter and there is no filtering operation for parameters. Directly compose sql statements for database operation. This causes sql injection.



Sqlmap: sqlmap.py -r c:\tmp\sts-1.txt -p id --risk 2 --dbs



