IceHrm employee management system allows companies to centralize confidential employee information and define access permissions to authorized personnel to ensure that employee information is both secure and accessible.

CVE-2021-38822

Problem Type: The application is vulnerable to cross site scripting attack. The vulnerability is a Stored XSS Using Unrestricted File Upload.

This vulnerability was found in IceHrm version 30.0.0 OS.

Description: A Stored Cross Site Scripting vulnerability via Malicious File Upload exists in multiple pages of IceHrm 30.0.0.OS that allows for arbitrary execution of JavaScript commands.

Affected Component: File Upload functionality in the Training Sessions page, File Upload functionality in the Travel Requests page.

Proof of Concept - [Link] [Link]

CVE-2021-38823

Problem Type: The application is vulnerable to a Session Management Issue.

This vulnerability was found in IceHrm version 30.0.0 OS.

Description: The IceHrm 30.0.0 OS website was found vulnerable to Session Management Issue. A signout from an admin account does not invalidate an admin session that is opened in a different browser.

Proof of Concept - [Link]

Contact
navidkagalwalla@hotmail.com