

TN Postal Circle Web Application

Security Audit Report Date: 04-12-2024

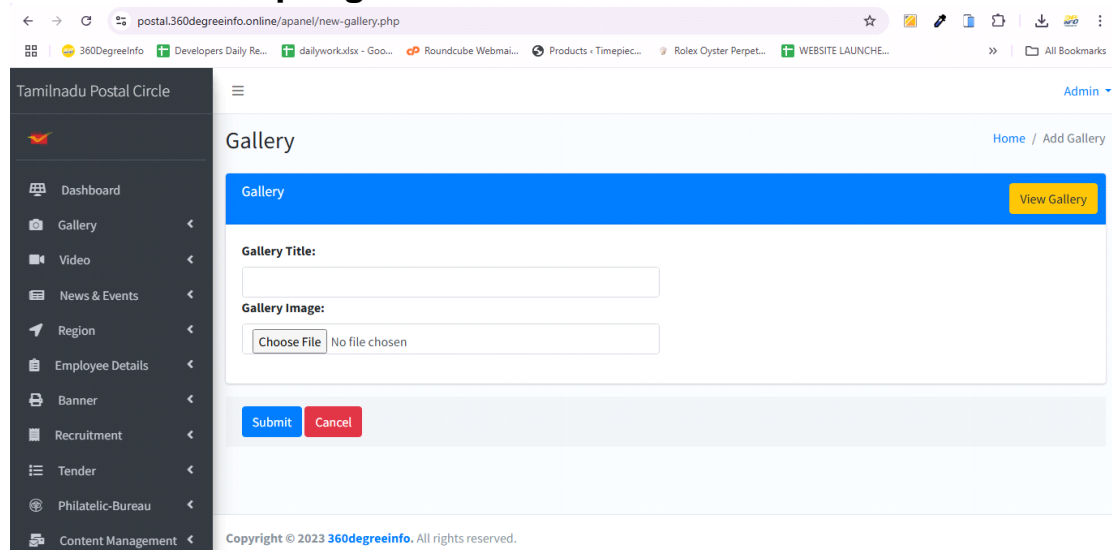
Staging server Link: <https://postal.360degreeinfo.online/>

Summary: The identified issues in the security audit report dated 04-12-2024 have been addressed. Solutions for each issue are provided, and screenshots have been attached corresponding to the index numbers and titles in the report for reference.

1. SQL Injection

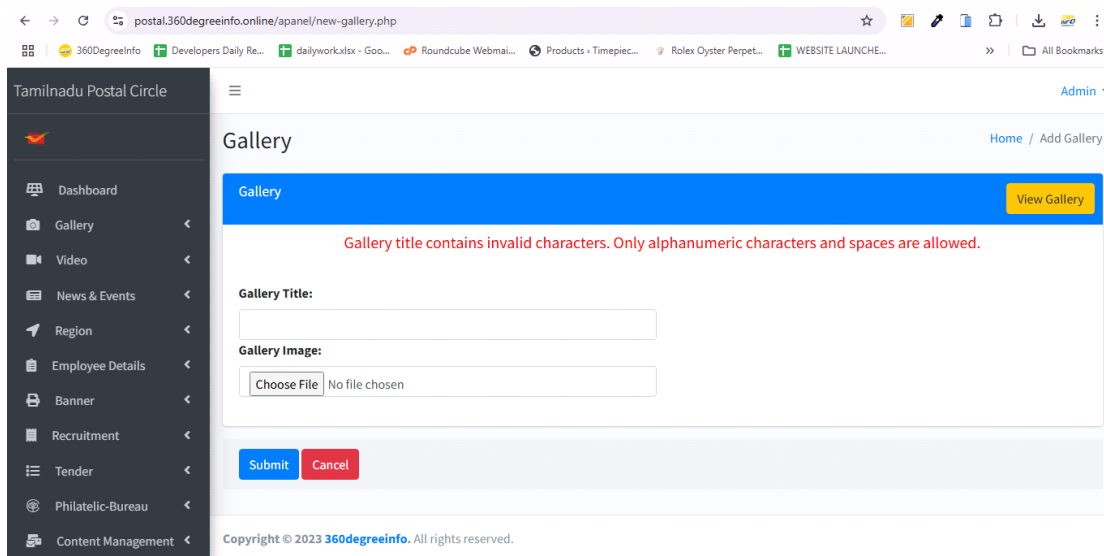
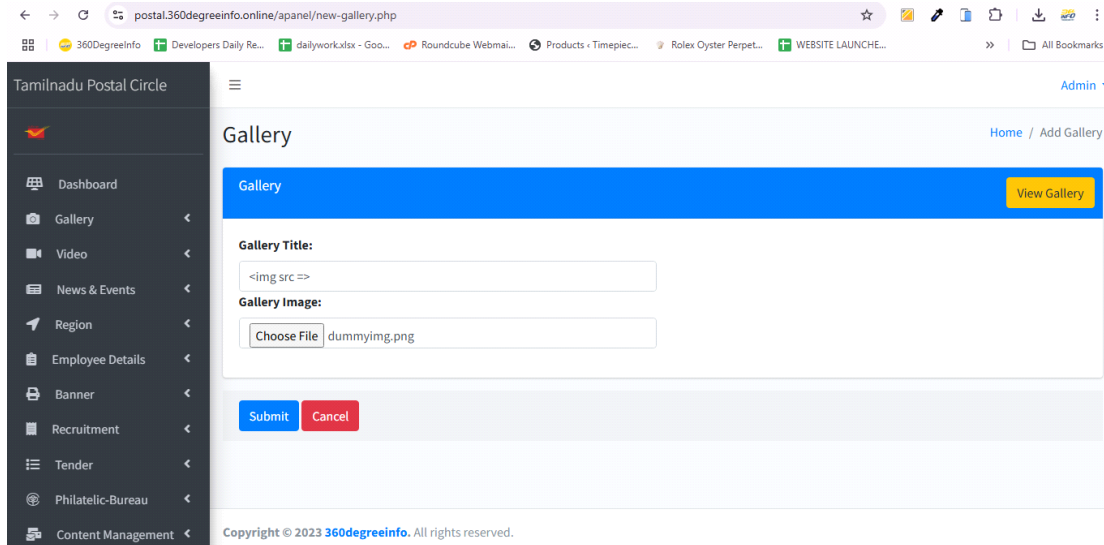
As per recommendation can add server side sql injection

2. Cross Site Scripting



The screenshot shows the 'Add Gallery' form in the Tamilnadu Postal Circle web application. The form is titled 'Gallery' and has a 'View Gallery' button. It contains two main input fields: 'Gallery Title' and 'Gallery Image'. The 'Gallery Image' field has a 'Choose File' button and a placeholder text 'No file chosen'. Below the input fields are 'Submit' and 'Cancel' buttons. The sidebar menu on the left lists various sections: Dashboard, Gallery, Video, News & Events, Region, Employee Details, Banner, Recruitment, Tender, Philatelic-Bureau, and Content Management. The footer of the page states 'Copyright © 2023 360degreeinfo. All rights reserved.'

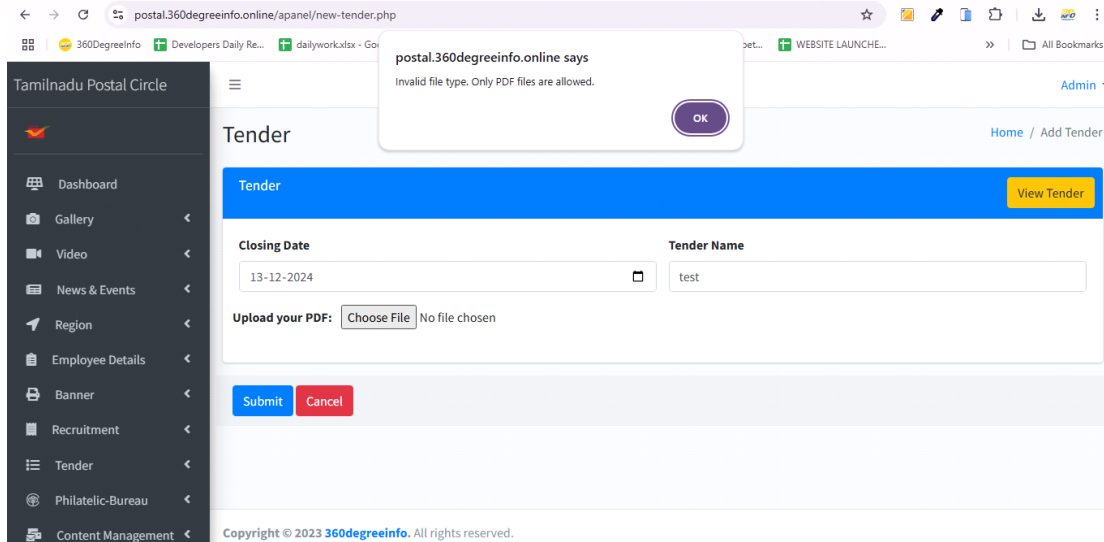
2.1 Add user side validation in add title field



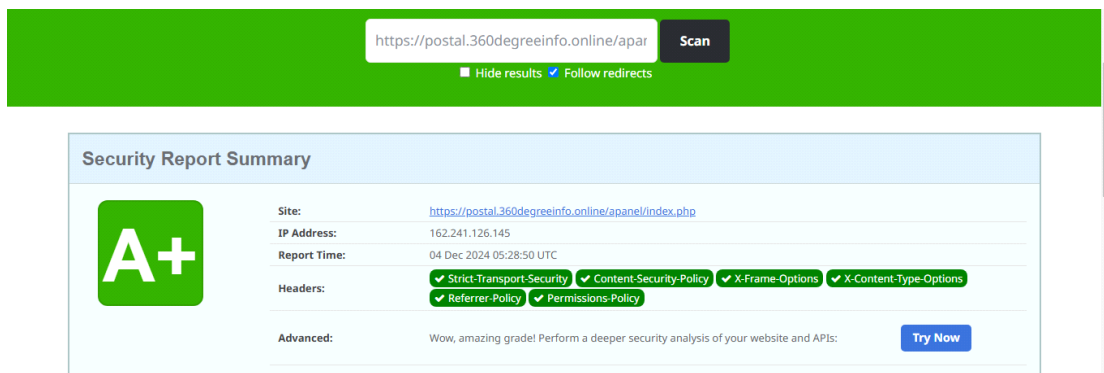
2.2 also adding a server side validation while adding a title

3.Unrestricted File Upload

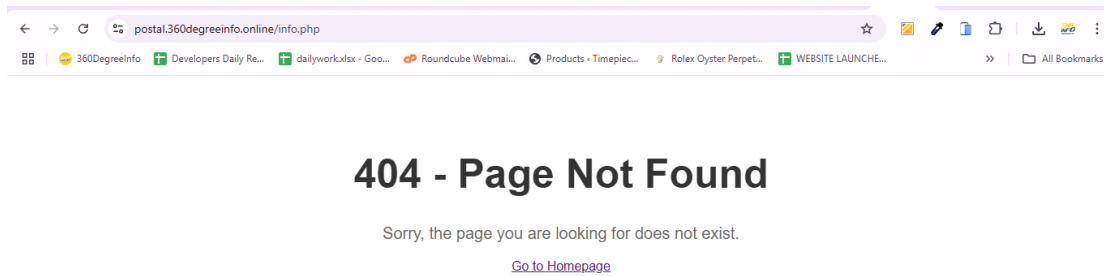
while file uploading adding both user and server side validations



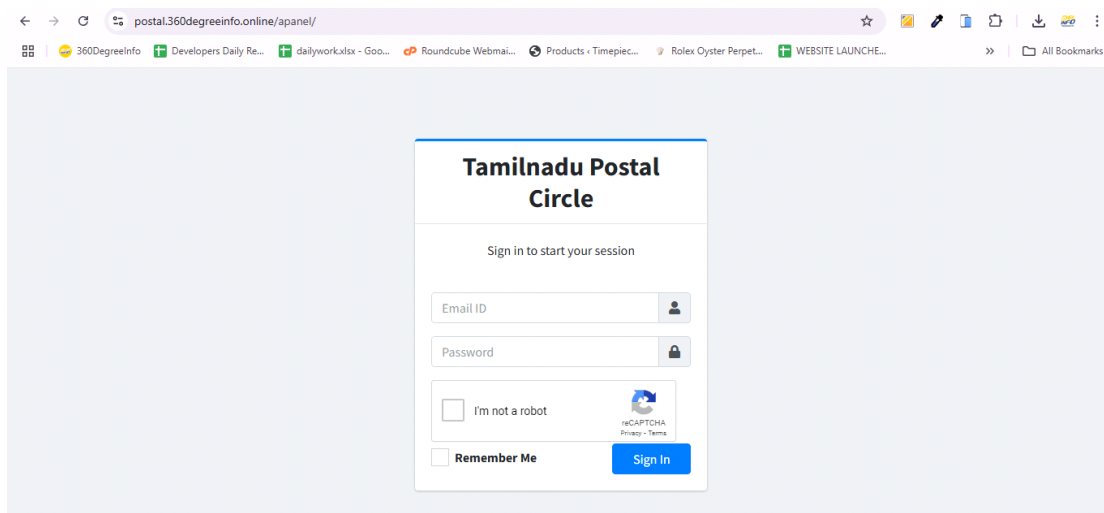
4.Missing HTTP Security Headers



5. PHP Info Page Disclosure



6. Multi Factor Authentication



7.Application allows multiple logins for same user account

postal.360degreeinfo.online/apanel/dashboard.php

360DegreeInfo Developers Daily Re... dailyworkslx - Goo... Roundcube Webmai... Products + Timepiec... Rolex Oyster Perpet... WEBSITE LAUNCE...

Tamilnadu Postal Circle

Admin

Dashboard

Dashboard

33 Gallery More info	31 News & Event More info	1 Video More info	1873 Employee More info
-----------------------------------	--	--------------------------------	--------------------------------------

Copyright © 2023 360degreeinfo. All rights reserved.

postal.360degreeinfo.online/apanel/index.php

360DegreeInfo Developers Daily Re... dailyworkslx - Goo... Roundcube Webmai... Products + Timepiec... Rolex Oyster Perpet... WEBSITE LAUNCE...

Tamilnadu Postal Circle

Sign in to start your session

Is already activated in another browser.

Email ID

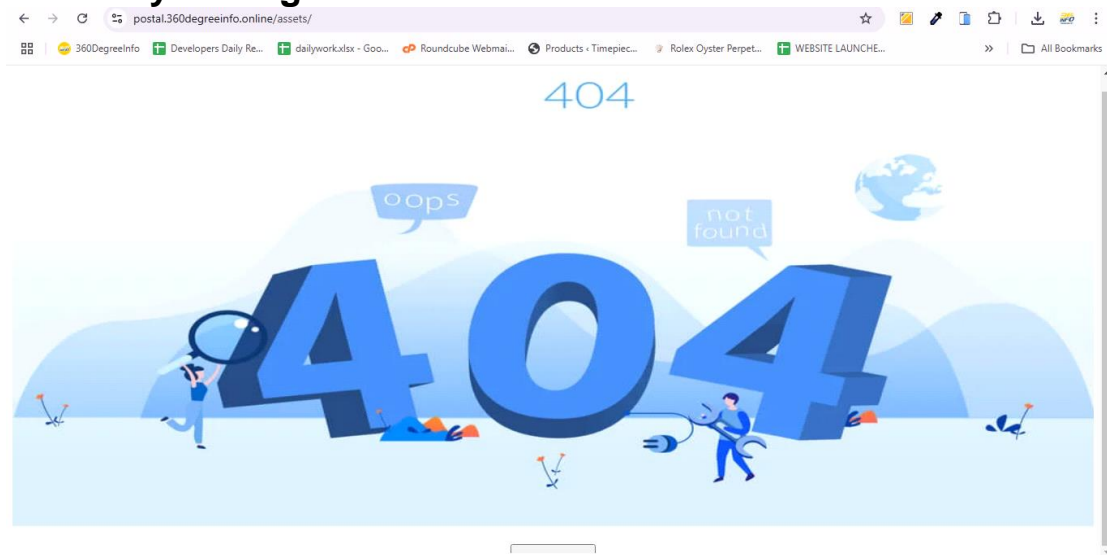
Password

☐ I'm not a robot

☐ Remember Me

Sign In

8. Directory Listing



9. Cookie Same Site Set as None

A screenshot of a web application dashboard for 'Tamilnadu Postal Circle'. The dashboard has a dark sidebar with links to 'Dashboard' and 'Gallery'. The main content area has four colored cards: '33 Gallery' (red), '31 News & Event' (teal), '1 Video' (yellow), and '1873 Employee' (green). Each card has a 'More info' link. Below the cards is a copyright notice: 'Copyright © 2023 360degreeinfo. All rights reserved.' At the bottom, a browser's developer tools are open, showing the 'Application' tab. Under 'Storage', the 'Cookies' section is expanded, showing a table of cookies for the domain 'postal.360degreeinfo.online'. The table has columns for Name, Value, Domain, Path, Expires, Size, HttpO..., Secure, SameSite, Pa..., Cross S..., and Priority. Two cookies are listed: 'cpsession' and 'custom_session_id'. The 'SameSite' attribute is set to 'Strict' for both. Below the table, there is a text prompt: 'Select a cookie to preview its value'.

10 Vulnerable / Outdated JavaScript libraries

As per your recommendation can add upgrade to the latest versions