E-Arogya - Bug #71

Feature # 65 (New): Security Audit

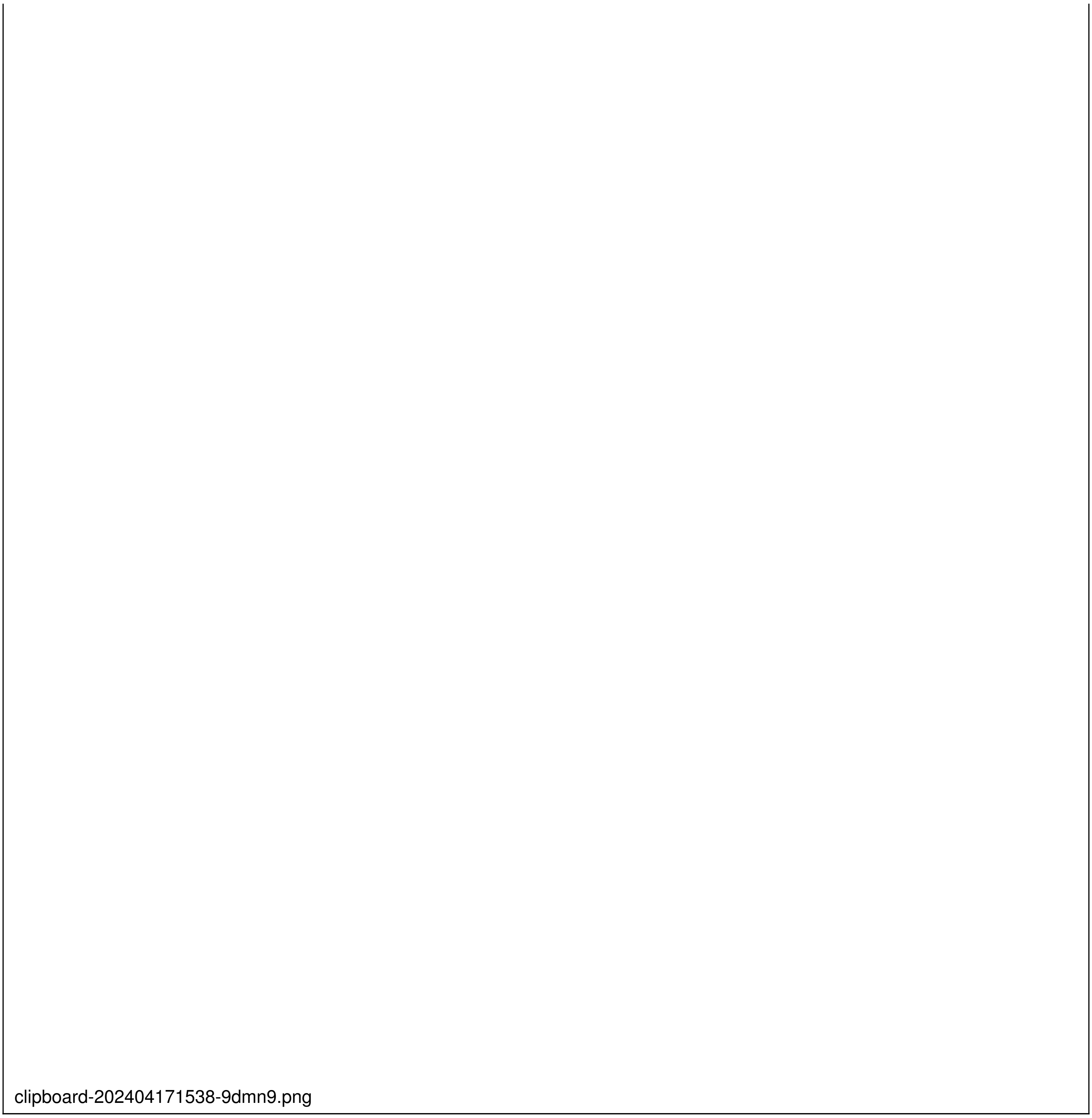
[Security Audit] 6- Unrestricted File Upload

17/04/2024 03:39 PM - Kalyan Battula

Status:	Closed	**Start date:**	17/04/2024
Priority:	High	**Due date:**	
Assignee:	Karthik Daram	**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:	Security Audit	**Spent time:**	0:00 hour
Deployed In:		**Category:**	

Description

6- Unrestricted File Upload
CWE : CWE-434
Description :
The application fails to restrict the file types that the user uploads. The application accepted the files with the double extension when tried to upload. If tshe uploaded file contains any malicious content such as macros it may cause an adversary result in the server.
Affected Path(s) :
https://earogya.satragroup.in/patient/0/patient-Registration *-Applicable to entire application
Impact :
An attacker can upload the malicious files that can be used as the backdoor for the later attacks in an attempt to compromise the whole server.
Recommendation :
1. List allowed extensions. Only allow safe and critical extensions for business functionality. Ensure that input validation is applied before validating the extensions. 2. Validate the file type, don't trust the Content-Type header as it can be spoofed 3. Change the filename to something generated by the application 4. Set a filename length limit. Restrict the allowed characters if possible 5. Set a file size limit 6. Only allow authorized users to upload files 7. Store the files on a different server. If that's not possible, store them outside of the webroot. In the case of public access to the files, use a handler that gets mapped to filenames inside the application (someid -> file.ext) 8. Run the file through an antivirus or a sandbox if available to validate that it doesn't contain malicious data 9. Ensure that any libraries used are securely configured and kept up to date 10. Protect the file upload from CSRF attacks Reference:
https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html
Evidence/Proof Of Concept :
Step 1: Login to the application with "test1_fd" Credentials and Now go Source and Destination entry form and fill form.Details saved successfully with malicious file as shown as below screenshot.



clipboard-202404171538-9dmn9.png

History

#1 - 23/04/2024 03:01 AM - Uma Maheswarachari Melpati

- Assignee set to Karthik Daram

#2 - 23/04/2024 03:48 AM - Karthik Daram

- Status changed from New to Resolved

#3 - 03/05/2024 05:24 AM - Sivakanth Kesiraju

- Target version set to Sprint 1 (29th April - 3rd May)

#4 - 03/05/2024 05:28 AM - Sivakanth Kesiraju

- Target version changed from Sprint 1 (29th April - 3rd May) to Security Audit

#5 - 30/09/2024 05:22 PM - Gautam Kumar

- Status changed from Resolved to Closed

Files

clipboard-202404171538-9dmn9.png	134 KB	17/04/2024	Kalyan Battula