Global Focus

Site Audit Report

Date of Report: Jan 06, 2021

Contact Person: Qusai Taha

Engagement Manager: Majdouleen Al-Nadi

Table of Content

1.0 SUMMARY

1.1 How to use this report

We produce this report by examining various aspects of your Drupal site(s) for the most common site-impacting issues. We evaluate Drupal core settings, settings of some of the commonly used modules, module selection, and perform a very surface-level review of custom code. Each section of this report identifies an aspect of the site we reviewed. We indicate the desired condition, the condition found on your site(s), and a description of why each condition should be considered. The conditions of your site(s) are highlighted based on their risk as follows:

Critical conditions appear in white text with a red background.

Significant conditions appear in white text with a yellow background.

Acceptable conditions appear in white text with a green background.

User Experience critical conditions in white text with an orange background.

1.2 Sites Evaluated

Global Focus website: https://reporting.unhcr.org/

1.3 Summary of Availability Risks

This is a summary of the most critical conditions we discovered when reviewing your site.

Issue	Severity
Drupal core and contributed module need security updates	N/A
The presence of many site admins with full admin permissions	Critical
Security Kit module is not installed	Critical
Custom code that can be improved by applying lints (PHPCS)	Significant
Password policy module is not installed.	Significant

1.4 Summary of Risk Remediation

This is a summary of steps that we recommend following to address the most critical conditions.

- Set proper permissions for each role and limit the administrator role to a **[webmaster]** user.
- Update Drupal core and modules to the recommended versions.
- Implementing the password policy module to protect users' paid accounts.
- Fix custom code coding practices issues.
- Properly address and configure all the identified Significant issues to proper recommendations

1.5 Architecture Recommendations

- Make use of the Display Suite and Field Group modules; and an admin theme for managing the form display of content types and other entities.

2.0 SITE AUDIT DETAILS

2.1 General Site Configuration

Item	Recommended Settings	Settings Found on Site
The site default country is properly set	Set the Site's default country.	Default Country is set
Is cron properly configured?	Cron to be properly configured and have a logical time interval Ultimate Cron module is preferred to be used for performance improvements. Configure PHP CLI cron task from the server's crontab.	The ultimate Cron module is configured.
Site name and site slogan are set	Site name and slogan must be set and have values related to the current website.	Site name is set but the slogan is not set.
Email sending method configuration	The site uses authenticated SMTP (not PHP mail) for sending an email.	The site is not using SMTP to send emails, and the email sending is not configured
Email from address	The site to use no-reply@domainname.com or info@domainname.com.	Site from email is configured to use: hqgars@unhcr.org
Contact Email address	Contact email address and all should be under the same domain, for example, "info@domainname.com".	The contact e-mail address is hqgars@unhcr.org
User registration	User registration settings to be only for admins if there is no registration business requirement for the site.	Users can't register on the site.

2.2 Security

Item	Recommended Settings	Settings Found on Site
PHP Filter permissions	PHP filter should be disabled. Otherwise only user (1) should have access to the PHP fields.	The PHP filter module is not installed
Site errors	Site errors must be hidden to reduce visibility into problems with your website.	Site errors are hidden
User permissions	Authenticated and Anonymous users do not have admin privileges.	No admin privileges are given to Anonymous or Authenticated
System logging and reporting	The Syslog module is enabled to log errors to the server. Alternatively, logging services such as Sentry.io are recommended.	Syslog module is disabled
Users table contains anonymous user	The anonymous user record (User ID 0), which many Drupal functions and modules use, should present in the database.	Users table contains an anonymous user records.
Ten or fewer website admins	The site must have less than 10 users with administrator-level access to your site which represents a security risk.	6 current website admins
Username Enumeration Prevention module	Enabling Username Enumeration Prevention module to addresses the most common methods of user name discovery, the password reset form and the Views module's autocomplete path	Username Enumeration Prevention module is not installed.
Security Kit module	The Security Kit module provides useful security enhancements to your website such as Clickjacking, Cross-Site Request Forgery	Security Kit module is not installed.

	(CSRF), and Cross-Site Scripting (XSS) protections among others	
Admin username is complex	Your admin username (User ID 1) must be complex. Simple usernames (including admin, administrator, and root) can represent a security vulnerability to your website.	User 1 Password complexed.
Password Policy module	The Password Policy module should be enabled and configured with a secure password policy.	Password Policy Module is not installed
Views access control is configured	The displays defined by the Views module should have access checks defined to prevent information disclosure.	Views has access control configured.
SSL is required for login	Your website should require the use of Secure Socket Layers (SSL) when users log in. This prevents attackers from gaining administrative access to your website.	SSL is required for login
Drupal root directory does not contain sensitive files and/or folders	Any sensitive files should be located outside the Drupal root directory to keep them secure and inaccessible by users.	No sensitive data is being saved in the root directory
Menu Router does not have potentially malicious entries	Database table for the menu router should not have any malicious entries.	No malicious entries found
HTTP X-XSS-Protection header is used in the response headers	Site should use X-XSS-Protection to stops pages from loading when they detect reflected cross-site scripting (XSS) attacks.	Site does not use HTTP X-XSS-Protection header
HTTP Content-Security-Policy	Site should use CSP to control resources the user agent is allowed to load which helps guard against cross-site scripting attacks.	No CSP Header found. CSP module is not installed

2.3 Performance

Item	Recommended Settings	Settings Found on Site
Page caching	Page caching must be enabled and configured properly.	Page caching is enabled (using internal page cache and Internal Dynamic Page Cache modules)
Cache lifetime	Maximum cache lifetime 60 minutes or greater.	Cache lifetime is set to 1 day
JavaScript and CSS	JavaScript and CSS are optimized for performance improvements.	JavaScript and CSS aggregated.
Views UI module	Views UI module to be disabled for performance improvements.	Views UI module is disabled.
Other UI modules	Other UI modules to be disabled for performance improvements.	Fields UI module is enabled
Modules and Development modules	(Devel, Coder, Theme Developer, SimpleTest, Database logging, Mobile tools, Statistics, Backup and Migrate module) should be disabled.	Devel Database logging modules is disabled.
Fast 404 module	Fast 404 module is enabled.	Fast 404 pages is disabled.
Active modules	No mismatch between .module files and the registered modules in the database.	A total of 144 active modules are registered in the database. No missing entries found. All *.module files are present.
Site does not have unused content types	No additional unused content types	No unused content types
Site does not have unused vocabularies	Your website should not have unused vocabularies	No unused vocabularies

Total number of fields does not exceed 75	Drupal site should be optimized and make use of the ability to reuse entity fields as well as decreasing the amount of unused fields	There are 85 total fields, which is higher than average
Unused fields	Your website should not use unused or unnecessary fields.	There are no unused fields.
Database table collation	The database tables should be using a consistent collation in order to avoid unexpected errors especially with multilingual sites.	Every table using UTF-8
Database uses InnoDB	All database tables should use the InnoDB storage engine.	All tables use InnoDB
Each project directory have less than 2,500 files	Project directories should have less than 2,500 files per directory so it does not affect the performance and stability of the site negatively.	No directories with over 2,500 files

2.4 Search Engine Optimization (SEO)

Item	Recommended Settings	Settings Found on Site
Sharing on Social media (Facebook, Twitter Cards ...etc.)	Site's information to appear well when shared on Social Media.	Metatags are configured on the site.
Site has XML Sitemap	XML Sitemap is installed and configured properly.	XML Sitemap is installed and configured
Redirect module	The redirect module is enabled and configured.	Redirect module is enabled.
Duplicate content not found	In the Global Redirect configuration, ensure that the Redirect non-clean to clean URL setting is enabled.	Clean and canonical URLs are enabled in the Redirect module.
Pathauto module	Pathauto module enabled and configured.	Pathauto module is enabled
Google Analytics module or Google Tag Manager	Google Analytics module enabled and configured,	Google tag manager script is installed and configured.
Site links do not direct to 4xx and 5xx links	Site should not have links that direct to 4xx pages and 5xx.	Site links to 500 and 502 pages. (Vardot worked to fix the 4xx links)
Images used in content are optimized	The images in the site should be resized and optimized and should not be larger than 800kb for improving performance ranking.	Site contains images larger than 800kb. EX: The header image on the homepage
Missing Description Pages	There should be at least a description for each page	Missing description found: EX: Operations node pages
Missing H1 Tag Pages	There should be one H1 tag in the page	No missing H1 tag found Vardot already worked to fix this.
Duplicate H1 Tag Pages	There should be one H1 tag in the page	Duplicate H1 tag found: EX: Homepage and situation node pages

		(/operational/situations/venezuela-situation)

2.5 General User Experience

Item	Recommended Settings	Settings Found on Site
Breadcrumbs are working fine and are visible properly	The site has breadcrumbs that are describing the current path the users are on.	Site uses breadcrumbs
CAPTCHA enabled and configured	CAPTCHA is enabled and used on all forms that are available for visitors for Spam prevention.	CAPTCHA module is installed and configured.
Antibot enabled and configured	The Antibot module is enabled and used on all forms that are visible for visitors, to prevent spam submissions and remote submissions.	Antibot module is not installed
Unwanted full-node-pages redirect to the desired place	Any unwanted full-node-pages should be redirected to the desired place. The Rabbit Hole module can be used for this.	Rabbit hole module configured.
/node page redirects to a defined place	/node page redirects to a defined landing page.	/node page does not redirect to homepage

2.6 Accessibility

Item	Recommended Settings	Settings Found on Site
Is the site navigable through keyboard	The site to be navigable through keyboard (tabs and arrows).	The site is not navigable through the keyboard (tabs and arrows) in

		the correct order and a lot of links are not navigable
Site to pass accessibility test	To get no errors back from the accessibility test.	The accessibility test fails due to several issues such as very low contrast issues, missing alternative text, empty heading, empty button, Linked image missing alternative, multiple form labels, broken ARIA menu, and contrast errors
Logical navigation and order	Site to have logical navigation order and accessible in general.	The site is not navigable through the keyboard (tabs and arrows) in the correct order

2.7 Administration Experience & Best Practices

Item	Recommended Settings	Settings Found on Site
Contextual (or equivalent)	Enabled and configured.	Enabled and configured
Field groups in content forms	Enabled and configured.	fields are not grouped inside field groups
Site uses a user-friendly administration toolbar	Admin toolbar transforms the admin menu into a drop-down menu, providing a fast access to all administration pages.	Admin toolbar installed
Rich text (WYSIWYG) editor is used for editors and admins	Enabled and configured to limited for content entry standardization	CKeditor is enabled and configured
File uploads are properly configured in meaningful upload locations	Upload file paths are properly configured for all file fields	FileField paths are configured to handle the files location
Automatically generate password when creating a user	Generate Password module is enabled and configured.	Not installed
User-friendly administration theme	Site to use a user-friendly and usable Administration Theme like (Claro).	The site uses the claro admin theme

2.8 Design & Navigation

2.8.1 Responsive Layout

The responsive mobile is working well.

2.8.2 Cross Browser

No issues were found for this category

2.8.3 Design

No issues were found for this category

2.9 Code Analysis

2.9.1 Drupal Core

Recommended setting: Drupal 9.5.9 - as of the date of this audit report

The version found on the website: 9.5.9

Keeping the Drupal codebase up to date will help to keep its site more secure while also providing performance enhancements. Keeping up to date will also make the path for applying security fixes in the future much more smooth.

Update Manager is not enable:

Enabling the update manager core module ensures tracking releases automatically and applying security updates as soon as they are released.

**This version is the recommended version at the time of applying the audit process.*

2.9.2 Contributed Modules Security Updates

Recommended setting: No contributed modules require security updates.

Settings found on the website: No contributed modules require security updates.

Keeping the Drupal modules up to date will help to keep its site more secure while also providing performance enhancements. Keeping up to date will also make the path for applying security fixes in the future much more smooth.

2.9.3 Contributed Modules Version

Recommended setting: All contributed modules are the latest released version.

Settings found on the website: All of the installed modules have the latest versions.

2.9.4 Modified or Patched Contributed Modules

Recommended setting: All contributed modules should not be modified locally. Patching a module should be done using composer.

Settings found on the website: There are no modified modules. 1 patched module found. Patch applied using composer referencing a local file:

Keeping the Drupal modules code unhacked will help to keep the site more secure while also keeping the update process in the future much more smooth.

2.9.5 Duplicate Modules in the Site Codebase

Recommended setting: There should not be any duplicate modules in the database.

Settings found on the website: No duplicate modules found.

2.9.6 Code Security

Recommended setting: No presence of poor coding practices that would impact the site security

Settings found on the website: No security issues found.

2.9.7 Code Performance and Standards

Recommended setting: No presence of poor coding practices that would impact the site Code Performance or compatibility.

Settings found on the website: Poor code practices were detected after running the Drupal coding standards checker.

There al lots of code standard that needs to follow,

The following custom modules and themes have code practice errors:

Module/Theme	Details
gfxvisu	https://drive.google.com/file/d/1lVK9jm9vwkFfjOAuJ7i20lPvbsvsSZtM/view?usp=drive_link
gfxmaps	https://drive.google.com/file/d/1xDDqffoZERfRbghGlAWfWrHAWBzuZbj7/view?usp=drive_link
gfxlegacy	https://drive.google.com/file/d/13FYoPUj6bqsZ_hD2PXl8wlJX5AW5KAMe/view?usp=drive_link