Drupal

Status	PRE-RELEASE
CISO owner	Frédéric Charpentier
Last update	12 Dec 2018

Security starter checklist

This document aims at providing a one stop shop "**checklist**" entry for project managers and developers involved in the usage of Drupal

Standard reference	Requirement	Check
Users management		
Access Control / Back-office	All Drupal back-offices users accounts must be tied to a real person (i.e. nominative) and accounts are not shared between people.	☐
Access Control / Back-office	All Drupal user accounts must use a professional email address (i.e. @loreal.com).	☐
Access Control / Back-office	Drupal accounts not used within **90 days** must be automatically disabled.	☐
Access Control / Back-office	A L'Oréal employee must be accountable to perform a review every **6 months**.	☐
Hosting		
Infrastructure / Hosting	Drupal instance must be hosted by L'Oréal IT Global (managed by Castelis Offre Colorée). Drupal instance must never be hosted on a shared server hosting other instances.	☐
Infrastructure / Domain names	Domain name must be registered by L'Oréal legal (malika.tighiouaret@loreal.com)	☐
Asset Management	Production URL must be registered in L'Oréal **Service Now** asset inventory.	☐
Infrastructure / Database	Database (e.g. MySQL) must restrict access from Internet and allow only access from the web server. Acceptable methods: 1. Firewalling 2. ACL on the database	☐

Infrastructure / Database	The database service must be run with a limited system service account (not root).	☐
Infrastructure / Web server	Run the HTTP server with a limited system service account	☐
Infrastructure / Web server	Configure the HTTP server to server XSS Protection header • `On Apache: header always set x-xss-protection "1; mode=block"`	☐
Infrastructure / PHP	Ensure PHP is properly hardened using the following directives in php configuration files: expose_php = Off error_reporting = E_ALL display_errors = Off display_startup_errors = Off log_errors = On allow_url_fopen = Off allow_url_include = Off disable_functions = system, exec, shell_exec, passthru, phpinfo, show_source, popen, proc_open disable_functions = fopen_with_path, dbmopen, dbase_open, putenv, move_uploaded_file disable_functions = chdir, mkdir, rmdir, chmod, rename disable_functions = filepro, filepro_rowcount, filepro_retrieve, posix_mkfifo	☐
Infrastructure / Web Application Firewall	Production websites must be protection by the Cloudflare WAF The following Cloudflare WAF rulesets must be enabled : • Security Level : High • Cloudflare Specials: On • Cloudflare PHP : On • Cloudflare Drupal : On • OWASP : Low + Block	☐
Infrastructure / Web Application Firewall	Origin web server must be denied all incoming Internet traffic, unless traffic from the Cloudflare IPs ranges.	☐
Infrastructure / Web admin interfaces	WP back-office interface URL must be protected by the LOFI protection (ex: */user/login*). Ask L'Oréal CISO for setup.	☐
Infrastructure / Staging	Dev/UAT/staging websites exposed on Internet must be restricted using the LOFI protection or HTTP Pre-Authentication.	☐
Development		
Development / Best practices	Development, Staging, QA, and production environments should all be configured identically, with different credentials used in each environment (e.g. different DB credentials).	☐

Development / Best practices	Do not expose source code to anonymous users on the Internet. Use L'Oréal validated source repository (i.e. L'Oréal Bitbucket)	
Development / Best practices	**Clean** source package from any unnecessary files and software components before delivery on production Examples of unnecessary files: • Unused Drupal plugins and themes • Configuration files: install.php, upgrade.php, phpinfo.php • database creations scripts are cleaned from testing data/accounts/passwords • Backup files: index.php.bak, file.php~ • Old pages: page2.php, test.php • Development synchronization traces: .git, .cvs, .svn • Passwords files • Libraries • Old folders: /test/, /staging/, … • Database dumps / imports files • Passwords • API access keys / certificates / token	
Drupal specials	During code customization, never concatenate data directly into SQL queries. Always use argument substitution with db_query.	
Drupal specials	During code customization, when manipulating URI, sanitize the received URI using UrlHelper::stripDangerousProtocols	
Drupal specials	During code customization, escape all user's input using Html::escape() to remove HTML tags.	
Drupal specials	Rename Drupal 'admin' account.	
Drupal specials	Define the trusted_host_patterns directive in settings.php	

Drupal specials	Disallow access to authorize.php, cron.php, install.php and upgrade.php using .htaccess:
	
	`<FilesMatch "(authorize|cron|install|upgrade)\.php">`
	
	`Order deny, allow`
	`deny from all`
	`Allow from 127.0.0.1`
	`</FilesMatch>`	

Security testing

Security testing	A penetration test or a bug bounty must be launched before GO LIVE. Contact Digital CISO at least 1 month before end of UAT.	

Patch management

Patch management	The responsibility of installing Drupal **core + plugins + themes security hotfixes** must be formally assigned by contract. Monitoring and installation delays SLAs must be comply with L'Oréal Patch Management requirements. Note: Leveraging Drupal auto-update feature is highly recommended.	☐
Patch management	Minimum Drupal branch version is **8.x** with latest security update.	☐