CVEs más relevantes de la semana

Del 16/09/2025 al 23/09/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-10562

Descripción: A flaw has been found in Campcodes Grocery Sales and Inventory System 1.0. This affects an unknown function of the file /ajax.php?action=save_product. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-16

CVE-2025-10563

Descripción: A vulnerability has been found in Campcodes Grocery Sales and Inventory System 1.0. This impacts an unknown function of the file /ajax.php?action=save_category. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-16

CVE-2025-10564

Descripción: A vulnerability was found in Campcodes Grocery Sales and Inventory System 1.0. Affected is an unknown function of the file /ajax.php?action=delete_category. Performing manipulation of the argument ID results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-16

CVE-2025-10565

Descripción: A vulnerability was determined in Campcodes Grocery Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=delete_receiving. Executing manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-16

CVE-2025-10439

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Yordam Informatics Yordam Library Automation System allows SQL Injection.This issue affects Yordam Library Automation System: from 21.5 & 21.6 before 21.7.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-89

Tecnología: No especificado

Publicado el: 2025-09-17

CVE-2025-10596

Descripción: A vulnerability was found in SourceCodester Online Exam Form Submission 1.0. This affects an unknown part of the file /index.php. The manipulation of the argument usn results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-17

CVE-2025-10598

Descripción: A vulnerability was identified in SourceCodester Pet Grooming Management Software 1.0. This issue affects some unknown processing of the file /admin/search_product.php. Such manipulation of the argument group_id leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-17

CVE-2025-10599

Descripción: A security flaw has been discovered in itsourcecode Web-Based Internet Laboratory Management System 1.0. Impacted is the function User::AuthenticateUser of the file login.php. Performing manipulation of the argument user_email results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be exploited.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-17

CVE-2025-10600

Descripción: A flaw has been found in SourceCodester Online Exam Form Submission 1.0. This impacts an unknown function of the file /register.php. This manipulation of the argument img causes unrestricted upload. It is possible to initiate the attack remotely. The exploit has been published and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-284

Tecnología: No especificado

Publicado el: 2025-09-17

CVE-2025-10601

Descripción: A vulnerability has been found in SourceCodester Online Exam Form Submission 1.0. Affected is an unknown function of the file /admin/index.php. Such manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-17

CVE-2025-10603

Descripción: A vulnerability was determined in PHPGurukul Online Discussion Forum 1.0. Affected by this issue is some unknown functionality of the file /admin/admin_forum/search_result.php. Executing manipulation of the argument Search can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-17

CVE-2025-35434

Descripción: CISA Thorium does not validate TLS certificates when connecting to Elasticsearch. An unauthenticated attacker with access to a Thorium cluster could impersonate the Elasticsearch service. Fixed in 1.1.2.

CVSS: 4.2 (MEDIUM)

Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

Tipo: CWE-295

Tecnología: No especificado

Publicado el: 2025-09-17

CVE-2025-10604

Descripción: A vulnerability was identified in PHPGurukul Online Discussion Forum 1.0. This affects an unknown part of the file /admin/edit_member.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-17

CVE-2025-59352

Descripción: Dragonfly is an open source P2P-based file distribution and image acceleration system. Prior to 2.1.0, the gRPC API and HTTP APIs allow peers to send requests that force the recipient peer to create files in arbitrary file system locations, and to read arbitrary files. This allows peers to steal other peers' secret data and to gain remote code execution (RCE) capabilities on the peer's machine....

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-09-17

CVE-2025-10621

Descripción: A vulnerability was determined in SourceCodester Hotel Reservation System 1.0. The affected element is an unknown function of the file editroomimage.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-17

CVE-2025-10623

Descripción: A vulnerability was identified in SourceCodester Hotel Reservation System 1.0. The impacted element is an unknown function of the file deleteuser.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-17

CVE-2025-10624

Descripción: A security flaw has been discovered in PHPGurukul User Management System 1.0. This affects an unknown function of the file /login.php. Performing manipulation of the argument emailid results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be exploited.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-17

CVE-2025-10662

Descripción: A vulnerability has been found in SeaCMS up to 13.3. The impacted element is an unknown function of the file /admin_members.php?ac=editsave. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. This affects another injection point than CVE-2025-25513.

CVSS: 4.7 (MEDIUM)

Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-18

CVE-2025-10663

Descripción: A vulnerability was found in PHPGurukul Online Course Registration 3.1. This affects an unknown function of the file /my-profile.php. Performing manipulation of the argument cgpa results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-18

CVE-2025-10664

Descripción: A vulnerability was determined in PHPGurukul Small CRM 4.0. This impacts an unknown function of the file /create-ticket.php. Executing manipulation of the argument subject can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-18

CVE-2025-10666

Descripción: A security flaw has been discovered in D-Link DIR-825 up to 2.10. Affected by this vulnerability is the function sub_4106d4 of the file apply.cgi. The manipulation of the argument countdown_time results in buffer overflow. The attack can be executed remotely. The exploit has been released to the public and may be exploited. This vulnerability only affects products that are no longer supported b...

CVSS: 8.8 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-119

Tecnología: No especificado

Publicado el: 2025-09-18

CVE-2025-10667

Descripción: A weakness has been identified in itsourcecode Online Discussion Forum 1.0. Affected by this issue is some unknown functionality of the file /members/compose_msg.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be exploited.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-18

CVE-2025-10668

Descripción: A security vulnerability has been detected in itsourcecode Online Discussion Forum 1.0. This affects an unknown part of the file /members/compose_msg_admin.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-18

CVE-2025-10670

Descripción: A flaw has been found in itsourcecode E-Logbook with Health Monitoring System for COVID-19 1.0. This issue affects some unknown processing of the file /check_profile.php. Executing manipulation of the argument profile_id can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-18

CVE-2025-10673

Descripción: A vulnerability was determined in itsourcecode Student Information Management System 1.0. The impacted element is an unknown function of the file /admin/modules/class/index.php. This manipulation of the argument classId causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-18

CVE-2025-10687

Descripción: A vulnerability was found in SourceCodester Responsive E-Learning System 1.0. This affects an unknown part of the file /admin/add_teacher.php. The manipulation of the argument Username results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-18

CVE-2025-10688

Descripción: A vulnerability was determined in SourceCodester Pet Grooming Management Software 1.0. This vulnerability affects unknown code of the file /admin/operation/paid.php. This manipulation of the argument inv_no/insta_amt causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.

CVSS: 7.3 (HIGH)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-18

CVE-2025-10690

Descripción: The Goza - Nonprofit Charity WordPress Theme theme for WordPress is vulnerable to unauthorized arbitrary file uploads due to a missing capability check on the 'beplus_import_pack_install_plugin' function in all versions up to, and including, 3.2.2. This makes it possible for unauthenticated attackers to upload zip files containing webshells disguised as plugins from remote locations to achieve ...

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-862

Tecnología: No especificado

Publicado el: 2025-09-19

CVE-2025-5948

Descripción: The Service Finder Bookings plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 6.0. This is due to the plugin not properly validating a user's identity prior to claiming a business when using the claim_business AJAX action. This makes it possible for unauthenticated attackers to login as any user including admins. Please note th...

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-639

Tecnología: No especificado

Publicado el: 2025-09-19

CVE-2025-26399

Descripción: SolarWinds Web Help Desk was found to be susceptible to an unauthenticated AjaxProxy deserialization remote code execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. This vulnerability is a patch bypass of CVE-2024-28988, which in turn is a patch bypass of CVE-2024-28986.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-502

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-9321

Descripción: The WPCasa plugin for WordPress is vulnerable to Code Injection in all versions up to, and including, 1.4.1. This is due to insufficient input validation and restriction on the 'api_requests' function. This makes it possible for unauthenticated attackers to call arbitrary functions and execute code.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-94

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-9588

Descripción: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Iron Mountain Archiving Services Inc. EnVision allows Command Injection.This issue affects enVision: before 250563.

CVSS: 10.0 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Tipo: CWE-78

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10147

Descripción: The Podlove Podcast Publisher plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'move_as_original_file' function in all versions up to, and including, 4.2.6. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-434

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-10412

Descripción: The Product Options and Price Calculation Formulas for WooCommerce – Uni CPO (Premium) plugin for WordPress is vulnerable to arbitrary file uploads due to misconfigured file type validation in the 'uni_cpo_upload_file' function in all versions up to, and including, 4.9.54. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make...

CVSS: 9.8 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Tipo: CWE-434

Tecnología: No especificado

Publicado el: 2025-09-23

CVE-2025-9846

Descripción: Unrestricted Upload of File with Dangerous Type vulnerability in TalentSys Consulting Information Technology Industry Inc. Inka.Net allows Command Injection.This issue affects Inka.Net: before 6.7.1.

CVSS: 10.0 (CRITICAL)

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Tipo: CWE-434

Tecnología: No especificado

Publicado el: 2025-09-23

Resumen del Reporte

CVEs analizados: 35

Promedio CVSS: 7.91

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat □