# CVEs más relevantes de la semana

Del 02/09/2025 al 09/09/2025

Porque el primer paso para defender es conocer las amenazas.

# CVE-2025-9829

Descripción: A vulnerability was identified in PHPGurukul Beauty Parlour Management System 1.1. The impacted element is an unknown function of the file /signup.php. The manipulation of the argument mobilenumber leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. Other parameters might be affected as well.

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: 2025-09-02

# CVE-2025-9830

Descripción: A security flaw has been discovered in PHPGurukul Beauty Parlour Management System 1.1. This affects an unknown function of the file /admin/add-customer-services.php. The manipulation of the argument sids[] results in sql injection. The attack can be executed 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: 2025-09-02

# CVE-2025-9831

Descripción: A weakness has been identified in PHPGurukul Beauty Parlour Management System 1.1. This impacts an unknown function of the file /admin/edit-services.php. This manipulation of the argument sername 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: 2025-09-02

# CVE-2025-9832

Descripción: A security vulnerability has been detected in SourceCodester Food Ordering Management System 1.0. Affected is an unknown function of the file /routers/register-router.php. Such manipulation of the argument phone 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: 2025-09-02

# CVE-2025-9833

Descripción: A vulnerability was detected in SourceCodester Online Farm Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /Login/login.php. Performing manipulation of the argument uname results in sql injection. It is possible to initiate the attack remotely. The exploit is now 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: 2025-09-02

# CVE-2025-9837

Descripción: A vulnerability was determined in itsourcecode Student Information Management System 1.0. This issue affects some unknown processing of the file /admin/modules/student/index.php. This manipulation of the argument studentId 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: 2025-09-02

# CVE-2025-9838

Descripción: A vulnerability was identified in itsourcecode Student Information Management System 1.0. Impacted is an unknown function of the file /admin/modules/subject/index.php. Such manipulation of the argument 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: 2025-09-02

# CVE-2025-9839

Descripción: A security flaw has been discovered in itsourcecode Student Information Management System 1.0. The affected element is an unknown function of the file /admin/modules/course/index.php. Performing manipulation of the argument ID 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: 2025-09-02

# CVE-2025-9840

Descripción: A weakness has been identified in itsourcecode Sports Management System 1.0. The impacted element is an unknown function of the file /Admin/gametype.php. Executing manipulation of the argument code can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be exploited.

CVSS: 6.3 (MEDIUM)

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

Tipo: CWE-74

Tecnología: No especificado

Publicado el: 2025-09-02

# CVE-2023-21467

Descripción: Error in 3GPP specification implementation in Exynos baseband prior to SMR Apr-2023 Release 1 allows incorrect handling of unencrypted message.

CVSS: 4.6 (MEDIUM)

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

Tipo: CWE-287

Tecnología: No especificado

Publicado el: 2025-09-03

# CVE-2025-1740

Descripción: Improper Restriction of Excessive Authentication Attempts vulnerability in Akinsoft MyRezzta allows Authentication Bypass, Password Recovery Exploitation, Brute Force.This issue affects MyRezzta: from s2.03.01 before v2.05.01.

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-307

Tecnología: No especificado

Publicado el: 2025-09-03

# CVE-2025-9924

Descripción: A vulnerability has been found in projectworlds Travel Management System 1.0. This vulnerability affects unknown code of the file /enquiry.php. The manipulation of the argument t2 leads to sql injection. Remote exploitation of the attack is possible. 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: 2025-09-03

# CVE-2025-9925

Descripción: A vulnerability was found in projectworlds Travel Management System 1.0. This issue affects some unknown processing of the file /detail.php. The manipulation of the argument pid results in sql injection. The attack can be executed 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: 2025-09-03

# CVE-2025-9926

Descripción: A vulnerability was determined in projectworlds Travel Management System 1.0. Impacted is an unknown function of the file /viewsubcategory.php. This manipulation of the argument t1 causes sql injection. The attack is possible to be carried out 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: 2025-09-03

# CVE-2025-9927

Descripción: A vulnerability was identified in projectworlds Travel Management System 1.0. The affected element is an unknown function of the file /viewpackage.php. Such manipulation of the argument t1 leads to sql injection. The attack may be performed from remote. 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: 2025-09-03

# CVE-2025-9928

Descripción: A security flaw has been discovered in projectworlds Travel Management System 1.0. The impacted element is an unknown function of the file /viewcategory.php. Performing manipulation of the argument t1 results in sql injection. It is possible to initiate the attack 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: 2025-09-03

# CVE-2025-9930

Descripción: A security vulnerability has been detected in 1000projects Beauty Parlour Management System 1.0. This impacts an unknown function of the file /admin/contact-us.php. The manipulation of the argument mobnumber leads to sql injection. The attack can be initiated remotely. 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: 2025-09-04

# CVE-2025-9932

Descripción: A flaw has been found in PHPGurukul Beauty Parlour Management System 1.1. Affected by this vulnerability is an unknown functionality of the file /admin/update-image.php. This manipulation of the argument lid causes sql injection. The attack may be initiated 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: 2025-09-04

# CVE-2025-9933

Descripción: A vulnerability has been found in PHPGurukul Beauty Parlour Management System 1.1. Affected by this issue is some unknown functionality of the file /admin/view-appointment.php. Such manipulation of the argument viewid leads to sql injection. The attack may be launched 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: 2025-09-04

## CVE-2025-41032

Descripción: An SQL injection vulnerability has been found in appRain CMF 4.0.5. This vulnerability allows an attacker to retrieve, create, update, and delete the database, through the 'data%5BAdmin%5D%5Busername%5D' parameter in /apprain/admin/manage/add/.

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: 2025-09-04

# CVE-2025-41033

Descripción: An SQL injection vulnerability has been found in appRain CMF 4.0.5. This vulnerability allows an attacker to retrieve, create, update, and delete the database, through the 'data%5BPage%5D%5Bname%5D' parameter in /apprain/page/manage-dynamic-pages/create.

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: 2025-09-04

# CVE-2025-41034

Descripción: An SQL injection vulnerability has been found in appRain CMF 4.0.5. This vulnerability allows an attacker to retrieve, create, update, and delete the database, through the 'data%5BPage%5D%5Bname%5D' parameter in /apprain/page/manage-static-pages/create/.

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: 2025-09-04

# CVE-2025-54914

Descripción: Azure Networking Elevation of Privilege Vulnerability

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-284

Tecnología: No especificado

Publicado el: 2025-09-04

# CVE-2025-55241

Descripción: Azure Entra Elevation of Privilege Vulnerability

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-287

Tecnología: No especificado

Publicado el: 2025-09-04

# CVE-2025-55244

Descripción: Azure Bot Service Elevation of Privilege Vulnerability

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-284

Tecnología: No especificado

Publicado el: 2025-09-04

# CVE-2025-8359

Descripción: The AdForest theme for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 6.0.9. This is due to the plugin not properly verifying a user's identity prior to authenticating them. This makes it possible for unauthenticated attackers to log in as other users, including administrators, without access to a password.

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-288

Tecnología: No especificado

Publicado el: 2025-09-06

# CVE-2025-10062

Descripción: A vulnerability was determined in itsourcecode Student Information Management System 1.0. This affects an unknown part of the file /admin/login.php. Executing manipulation of the argument uname 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: 2025-09-06

# CVE-2025-10076

Descripción: A weakness has been identified in SourceCodester Online Polling System 1.0. This affects an unknown function of the file /manage-profile.php. This manipulation of the argument email causes sql injection. The attack may be initiated 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: 2025-09-08

# CVE-2025-10077

Descripción: A security vulnerability has been detected in SourceCodester Online Polling System 1.0. This impacts an unknown function of the file /registeracc.php. Such manipulation of the argument email leads to sql injection. The attack may be launched remotely. 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: 2025-09-08

# CVE-2025-9113

Descripción: The Doccure theme for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'doccure_temp_upload_to_media' function in all versions up to, and including, 1.4.8. 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: 2025-09-08

# CVE-2025-9114

Descripción: The Doccure theme for WordPress is vulnerable to Arbitrary User Password Change in versions up to, and including, 1.4.8. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for unauthenticated attackers to change user passwords and potentially take over administrator accounts.

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: 2025-09-08

## CVE-2025-42922

Descripción: SAP NetWeaver AS Java allows an attacker authenticated as a non-administrative user to use a flaw in an available service to upload an arbitrary file. This file when executed can lead to a full compromise of confidentiality, integrity and availability of the system.

CVSS: 9.9 (CRITICAL)

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

Tipo: CWE-94

Tecnología: No especificado

Publicado el: 2025-09-09

# CVE-2025-42944

Descripción: Due to a deserialization vulnerability in SAP NetWeaver, an unauthenticated attacker could exploit the system through the RMI-P4 module by submitting malicious payload to an open port. The deserialization of such untrusted Java objects could lead to arbitrary OS command execution, posing a high impact to the application's confidentiality, integrity, and availability.

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-502

Tecnología: No especificado

Publicado el: 2025-09-09

# CVE-2025-42958

Descripción: Due to a missing authentication check in the SAP NetWeaver application on IBM i-series, the application allows high privileged unauthorized users to read, modify, or delete sensitive information, as well as access administrative or privileged functionalities. This results in a high impact on the confidentiality, integrity, and availability of the application.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-250

Tecnología: No especificado

Publicado el: 2025-09-09

# CVE-2025-10134

Descripción: The Goza - Nonprofit Charity WordPress Theme theme for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the alone_import_pack_restore_data() function in all versions up to, and including, 3.2.2. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right ...

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-73

Tecnología: No especificado

Publicado el: 2025-09-09

# CVE-2025-40795

Descripción: A vulnerability has been identified in SIMATIC PCS neo V4.1 (All versions), SIMATIC PCS neo V5.0 (All versions), User Management Component (UMC) (All versions < V2.15.1.3). Affected products contain a stack-based buffer overflow vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to execute arbitrary code or to cause a denial of service condition.

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-121

Tecnología: No especificado

Publicado el: 2025-09-09

# CVE-2025-40804

Descripción: A vulnerability has been identified in SIMATIC Virtualization as a Service (SIVaaS) (All versions). The affected application exposes a network share without any authentication. This could allow an attacker to access or alter sensitive data without proper authorization.

CVSS: 9.1 (CRITICAL)

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

Tipo: CWE-732

Tecnología: No especificado

Publicado el: 2025-09-09

# Resumen del Reporte

CVEs analizados: 37

Promedio CVSS: 8.19

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat ▯