# CVEs más relevantes de la semana

Del 26/04/2025 al 03/05/2025

Porque el primer paso para defender es conocer las amenazas.

# CVE-2025-3969

Descripción: A vulnerability was found in codeprojects News Publishing Site Dashboard 1.0. It has been rated as critical. This issue affects some unknown processing of the file /edit-category.php of the component Edit Category Page. The manipulation of the argument category_image leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.

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-284

Tecnología: No especificado

Publicado el: 2025-04-27

# CVE-2025-3200

Descripción: An unauthenticated remote attacker could exploit the used, insecure TLS 1.0 and TLS 1.1 protocols to intercept and manipulate encrypted communications between the Com-Server and connected systems.

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-327

Tecnología: No especificado

Publicado el: 2025-04-28

# CVE-2025-4020

Descripción: A vulnerability was found in PHPGurukul Old Age Home Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /contact.php. The manipulation of the argument fname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may 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: 2025-04-28

# CVE-2025-4024

Descripción: A vulnerability classified as critical has been found in itsourcecode Placement Management System 1.0. Affected is an unknown function of the file /add_drive.php. The manipulation of the argument drive_title leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may 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: 2025-04-28

# CVE-2025-4025

Descripción: A vulnerability classified as critical was found in itsourcecode Placement Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /registration.php. The manipulation of the argument Name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may 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: 2025-04-28

# CVE-2025-4026

Descripción: A vulnerability, which was classified as critical, has been found in PHPGurukul Nipah Virus Testing Management System 1.0. This issue affects some unknown processing of the file /profile.php. The manipulation of the argument adminname leads to sql injection. The attack may be initiated 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: 2025-04-28

# CVE-2025-4027

Descripción: A vulnerability, which was classified as critical, was found in PHPGurukul Old Age Home Management System 1.0. Affected is an unknown function of the file /admin/rules.php. The manipulation of the argument pagetitle 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: 2025-04-28

# CVE-2025-4039

Descripción: A vulnerability was found in PHPGurukul Rail Pass Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/search-pass.php. The manipulation of the argument searchdata 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: 2025-04-28

# CVE-2025-30390

Descripción: Improper authorization in Azure allows an authorized attacker to elevate privileges over a network.

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-285

Tecnología: No especificado

Publicado el: 2025-04-30

# CVE-2025-30392

Descripción: Improper authorization in Azure Bot Framework SDK allows an unauthorized attacker to elevate privileges over a network.

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-285

Tecnología: No especificado

Publicado el: 2025-04-30

# CVE-2025-3746

Descripción: The OTP-less one tap Sign in plugin for WordPress is vulnerable to privilege escalation via account takeover in versions 2.0.14 to 2.0.59. This is due to the plugin not properly validating a user's identity prior to updating their details, like email. This makes it possible for unauthenticated attackers to change arbitrary users' email addresses, including administrators, and leverage that to r...

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: 2025-05-02

# CVE-2025-3708

Descripción: Le-show medical practice management system from Le-yan has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.

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: 2025-05-02

# CVE-2025-3709

Descripción: Agentflow from Flowring Technology has an Account Lockout Bypass vulnerability, allowing unauthenticated remote attackers to exploit this vulnerability to perform password brute force attack.

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: 2025-05-02

# CVE-2025-2812

Descripción: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mydata Informatics Ticket Sales Automation allows Blind SQL Injection.This issue affects Ticket Sales Automation: before 03.04.2025 (DD.MM.YYYY).

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: 2025-05-02

# CVE-2025-3918

Descripción: The Job Listings plugin for WordPress is vulnerable to Privilege Escalation due to improper authorization within the register_action() function in versions 0.1 to 0.1.1. The plugin's registration handler reads the client-supplied $_POST['user_role'] and passes it directly to wp_insert_user() without restricting to a safe set of roles.  This makes it possible for unauthenticated attackers to ele...

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-285

Tecnología: No especificado

Publicado el: 2025-05-03

# Resumen del Reporte

CVEs analizados: 15

Promedio CVSS: 8.53

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat