# CVEs más relevantes de la semana

Del 17/05/2025 al 24/05/2025

Porque el primer paso para defender es conocer las amenazas.

# CVE-2025-4849

Descripción: A vulnerability was found in TOTOLINK N300RH 6.1c.1390_B20191101. It has been rated as critical. Affected by this issue is the function CloudACMunualUpdateUserdata of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument url leads to command injection. The attack may be launched 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-74

Tecnología: No especificado

Publicado el: 2025-05-18

# CVE-2025-4851

Descripción: A vulnerability classified as critical was found in TOTOLINK N300RH 6.1c.1390_B20191101. This vulnerability affects the function setUploadUserData of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to command injection. The attack can 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-74

Tecnología: No especificado

Publicado el: 2025-05-18

# CVE-2025-4861

Descripción: A vulnerability classified as critical was found in PHPGurukul Beauty Parlour Management System 1.1. Affected by this vulnerability is an unknown functionality of the file /admin/admin-profile.php. The manipulation of the argument contactnumber 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 aff...

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: 2025-05-18

# CVE-2025-4864

Descripción: A vulnerability has been found in itsourcecode Restaurant Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/finished.php. The manipulation of the argument ID leads to sql injection. The attack can 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: 2025-05-18

# CVE-2025-4865

Descripción: A vulnerability was found in itsourcecode Restaurant Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/member_save.php. The manipulation of the argument last leads to sql injection. The attack may be initiated 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: 2025-05-18

# CVE-2025-4870

Descripción: A vulnerability classified as critical was found in itsourcecode Restaurant Management System 1.0. This vulnerability affects unknown code of the file /admin/menu_save.php. The manipulation of the argument menu leads to sql injection. The attack can 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: 2025-05-18

# CVE-2025-4873

Descripción: A vulnerability has been found in PHPGurukul News Portal 4.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/index.php of the component Login. The manipulation of the argument Username leads to sql injection. The attack can 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: 2025-05-18

# CVE-2025-4874

Descripción: A vulnerability was found in PHPGurukul News Portal Project 4.1 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/contactus.php. The manipulation of the argument pagetitle 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: 2025-05-18

# CVE-2025-4875

Descripción: A vulnerability was found in Campcodes Online Shopping Portal 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /forgot-password.php. The manipulation of the argument email leads to sql injection. The attack can 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: 2025-05-18

# CVE-2025-4880

Descripción: A vulnerability has been found in PHPGurukul News Portal 4.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/aboutus.php. The manipulation of the argument pagetitle leads to sql injection. The attack can 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: 2025-05-18

# CVE-2025-4881

Descripción: A vulnerability was found in itsourcecode Restaurant Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/user_save.php. The manipulation of the argument username/name 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: 2025-05-18

# CVE-2025-4882

Descripción: A vulnerability was found in itsourcecode Restaurant Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/team_update.php. The manipulation of the argument team leads to sql injection. It is possible to initiate 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: 2025-05-18

# CVE-2025-4895

Descripción: A vulnerability, which was classified as critical, has been found in SourceCodester Doctors Appointment System 1.0. This issue affects some unknown processing of the file /admin/delete-session.php. The manipulation of the argument ID 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: 2025-05-18

# CVE-2025-4899

Descripción: A vulnerability was found in Campcodes Sales and Inventory System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /pages/transaction_update.php. The manipulation of the argument ID 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: 2025-05-18

# CVE-2025-4900

Descripción: A vulnerability classified as critical has been found in Campcodes Sales and Inventory System 1.0. Affected is an unknown function of the file /pages/payment.php. The manipulation of the argument cid 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: 2025-05-18

# CVE-2025-4906

Descripción: A vulnerability was found in PHPGurukul Notice Board System 1.0. It has been classified as critical. Affected is an unknown function of the file /login.php. The manipulation of the argument Username 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: 2025-05-19

# CVE-2025-4907

Descripción: A vulnerability was found in PHPGurukul Daily Expense Tracker System 1.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file /forgot-password.php. The manipulation of the argument email 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: 2025-05-19

# CVE-2025-4908

Descripción: A vulnerability classified as critical has been found in PHPGurukul Daily Expense Tracker System 1.1. This affects an unknown part of the file /expense-datewise-reports-detailed.php. The manipulation of the argument fromdate/todate leads to sql injection. It is possible to initiate 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: 2025-05-19

# CVE-2025-4910

Descripción: A vulnerability, which was classified as critical, has been found in PHPGurukul Zoo Management System 2.1. This issue affects some unknown processing of the file /admin/edit-animal-details.php. The manipulation of the argument aname leads to sql injection. The attack may be initiated 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: 2025-05-19

# CVE-2025-4911

Descripción: A vulnerability, which was classified as critical, was found in PHPGurukul Zoo Management System 2.1. Affected is an unknown function of the file /admin/view-foreigner-ticket.php. The manipulation of the argument viewid 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: 2025-05-19

# CVE-2025-4912

Descripción: A vulnerability has been found in SourceCodester Student Result Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/core/update_student.php of the component Image File Handler. The manipulation of the argument old_photo leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the p...

CVSS: 5.4 (MEDIUM)

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

Tipo: CWE-22

Tecnología: No especificado

Publicado el: 2025-05-19

# CVE-2025-4913

Descripción: A vulnerability was found in PHPGurukul Auto Taxi Stand Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/index.php. The manipulation of the argument Username 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: 2025-05-19

# CVE-2025-4914

Descripción: A vulnerability was found in PHPGurukul Auto Taxi Stand Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/forgot-password.php. The manipulation of the argument email leads to sql injection. It is possible to initiate 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: 2025-05-19

# CVE-2025-4915

Descripción: A vulnerability was found in PHPGurukul Auto Taxi Stand Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/auto-taxi-entry-detail.php. The manipulation of the argument price leads to sql injection. The attack can 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: 2025-05-19

# CVE-2025-4916

Descripción: A vulnerability was found in PHPGurukul Auto Taxi Stand Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/admin-profile.php. The manipulation of the argument mobilenumber leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected a...

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: 2025-05-19

# CVE-2025-4917

Descripción: A vulnerability classified as critical has been found in PHPGurukul Auto Taxi Stand Management System 1.0. Affected is an unknown function of the file /admin/new-autoortaxi-entry-form.php. The manipulation of the argument drivername 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 affect...

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: 2025-05-19

# CVE-2025-4924

Descripción: A vulnerability, which was classified as critical, was found in SourceCodester Client Database Management System 1.0. Affected is an unknown function of the file /user_void_transaction.php. The manipulation of the argument order_id 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: 2025-05-19

# CVE-2025-4925

Descripción: A vulnerability has been found in PHPGurukul Daily Expense Tracker System 1.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /expense-monthwise-reports-detailed.php. The manipulation of the argument fromdate/todate leads to sql injection. The attack can 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: 2025-05-19

# CVE-2025-4927

Descripción: A vulnerability was found in PHPGurukul Online Marriage Registration System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/between-dates-application-report.php. The manipulation of the argument fromdate/todate leads to sql injection. It is possible to initiate 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: 2025-05-19

# CVE-2025-4928

Descripción: A vulnerability was found in projectworlds Online Lawyer Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /save_lawyer_edit_profile.php. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Multiple parameters might be affected.

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: 2025-05-19

# CVE-2025-4929

Descripción: A vulnerability was found in Campcodes Online Shopping Portal 1.0. It has been rated as critical. This issue affects some unknown processing of the file /my-account.php. The manipulation of the argument Name 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: 2025-05-19

# CVE-2025-4930

Descripción: A vulnerability classified as critical has been found in Campcodes Online Shopping Portal 1.0. Affected is an unknown function of the file /my-cart.php. The manipulation of the argument billingaddress 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: 2025-05-19

# CVE-2025-4933

Descripción: A vulnerability, which was classified as critical, was found in ponaravindb Hospital-Management-System 1.0. This affects an unknown part of the file /doctor-panel.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack 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-74

Tecnología: No especificado

Publicado el: 2025-05-19

# CVE-2025-4322

Descripción: The Motors theme for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 5.6.67. This is due to the theme not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user passwords, including those of administrators, and leverage that to gain access to ...

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-620

Tecnología: No especificado

Publicado el: 2025-05-20

# CVE-2025-4524

Descripción: The Madara – Responsive and modern WordPress theme for manga sites theme for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.2.2 via the 'template' parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access co...

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: 2025-05-21

# CVE-2025-4603

Descripción: The eMagicOne Store Manager for WooCommerce plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_file() function in all versions up to, and including, 1.2.5. 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 file is deleted (su...

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: 2025-05-24

# CVE-2025-5058

Descripción: The eMagicOne Store Manager for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the set_image() function in all versions up to, and including, 1.2.5. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. This is only exploitable by...

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: 2025-05-24

# Resumen del Reporte

CVEs analizados: 37

Promedio CVSS: 7.42

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat