CVEs más relevantes de la semana

Del 18/11/2025 al 25/11/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-13396

Descripción: A weakness has been identified in code-projects Courier Management System 1.0. This affects an unknown function of the file /add-office.php. This manipulation of the argument OfficeName causes sql injection. The attack may be initiated 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: 2025-11-19

CVE-2025-13400

Descripción: A vulnerability was detected in Tenda CH22 1.0.0.1. Affected is the function formWrlExtraGet of the file /goform/WrlExtraGet. Performing manipulation of the argument chkHz results in buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used.

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: 2025-11-19

CVE-2025-13410

Descripción: A vulnerability has been found in Campcodes Retro Basketball Shoes Online Store 1.0. Affected is an unknown function of the file /admin/receipt.php. Such manipulation of the argument tid 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: 2025-11-19

CVE-2025-13411

Descripción: A vulnerability was found in Campcodes Retro Basketball Shoes Online Store 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/admin_football.php. Performing manipulation of the argument product_image results in unrestricted upload. The attack is possible to be carried out remotely. The exploit has been made public and could be used.

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-284

Tecnología: No especificado

Publicado el: 2025-11-19

CVE-2025-13420

Descripción: A weakness has been identified in itsourcecode Human Resource Management System 1.0. This issue affects some unknown processing of the file /src/store/EventStore.php. This manipulation of the argument eventSubject causes sql injection. The attack can 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: 2025-11-19

CVE-2025-13421

Descripción: A security vulnerability has been detected in itsourcecode Human Resource Management System 1.0. Impacted is an unknown function of the file /src/store/NoticeStore.php. Such manipulation of the argument noticeDesc leads to sql injection. The attack can 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: 2025-11-19

CVE-2025-13422

Descripción: A vulnerability was detected in freeprojectscodes Sports Club Management System 1.0. The affected element is an unknown function of the file /dashboard/admin/change_s_pwd.php. Performing manipulation of the argument login_id results in sql injection. The attack may be initiated 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: 2025-11-20

CVE-2025-13424

Descripción: A vulnerability has been found in Campcodes Supplier Management System 1.0. This affects an unknown function of the file /admin/add_product.php. The manipulation of the argument txtProductName leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.

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: 2025-11-20

CVE-2025-13445

Descripción: A flaw has been found in Tenda AC21 16.03.08.16. This affects an unknown part of the file /goform/SetIpMacBind. Executing manipulation of the argument list can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been published and may be used.

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: 2025-11-20

CVE-2025-13446

Descripción: A vulnerability has been found in Tenda AC21 16.03.08.16. This vulnerability affects unknown code of the file /goform/SetSysTimeCfg. The manipulation of the argument timeZone/time leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.

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: 2025-11-20

CVE-2025-13449

Descripción: A vulnerability was found in code-projects Online Shop Project 1.0. This issue affects some unknown processing of the file /login.php. The manipulation of the argument Password results in sql injection. The attack may be performed from remote. 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: 2025-11-20

CVE-2025-13451

Descripción: A vulnerability was identified in SourceCodester Online Shop Project 1.0. The affected element is an unknown function of the file /action.php. Such manipulation of the argument Search 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: 2025-11-20

CVE-2025-64428

Descripción: Dataease is an open source data visualization analysis tool. Versions prior to 2.10.17 are vulnerable to JNDI injection. A blacklist was added in the patch for version 2.10.14. However, JNDI injection remains possible via the iiop, corbaname, and iiopname schemes. The vulnerability has been fixed in version 2.10.17.

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-74

Tecnología: No especificado

Publicado el: 2025-11-20

CVE-2025-59245

Descripción: Microsoft SharePoint Online Elevation of Privilege Vulnerability

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: 2025-11-20

CVE-2025-13485

Descripción: A security flaw has been discovered in itsourcecode Online File Management System 1.0. This issue affects some unknown processing of the file /ajax.php?action=login. The manipulation of the argument Username results in sql injection. The attack may be launched 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: 2025-11-21

CVE-2025-11456

Descripción: The ELEX WordPress HelpDesk & Customer Ticketing System plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the eh_crm_new_ticket_post() function in all versions up to, and including, 3.3.1. 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: 2025-11-21

CVE-2025-6389

Descripción: The Sneeit Framework plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 8.3 via the sneeit_articles_pagination_callback() function. This is due to the function accepting user input and then passing that through call_user_func(). This makes it possible for unauthenticated attackers to execute code on the server which can be leveraged to inject backd...

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: 2025-11-25

CVE-2025-13559

Descripción: The EduKart Pro plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.3. This is due to the 'edukart_pro_register_user_front_end' function not restricting what user roles a user can register with. This makes it possible for unauthenticated attackers to supply the 'administrator' role during registration and gain administrator access to the site.

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-269

Tecnología: No especificado

Publicado el: 2025-11-25

Resumen del Reporte

CVEs analizados: 18

Promedio CVSS: 7.90

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat