CVEs más relevantes de la semana

Del 30/08/2025 al 06/09/2025

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-9691

Descripción: A vulnerability has been found in Campcodes Online Shopping System 1.0. This impacts an unknown function of the file /login.php. Such manipulation of the argument Password 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: 2025-08-30

CVE-2025-9692

Descripción: A vulnerability was found in Campcodes Online Shopping System 1.0. Affected is an unknown function of the file /product.php. Performing manipulation of the argument p 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: 2025-08-30

CVE-2025-9740

Descripción: A vulnerability was found in code-projects Human Resource Integrated System 1.0. This affects an unknown part of the file /log_query.php. The manipulation of the argument ID 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: 2025-08-31

CVE-2025-9743

Descripción: A security flaw has been discovered in code-projects Human Resource Integrated System 1.0. Impacted is an unknown function of the file login_attendance2.php. Performing manipulation of the argument employee_id/date 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: 2025-08-31

CVE-2025-9744

Descripción: A weakness has been identified in Campcodes Online Loan Management System 1.0. The affected element is an unknown function of the file /ajax.php?action=login. Executing manipulation of the argument Username can lead to sql injection. The attack can be launched 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: 2025-08-31

CVE-2025-9748

Descripción: A vulnerability was determined in Tenda CH22 1.0.0.1. Affected by this issue is the function fromIpsecitem of the file /goform/IPSECsave of the component httpd. Executing manipulation of the argument ipsecno can lead to stack-based buffer overflow. The attack may be performed from remote.

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: 2025-08-31

CVE-2025-9749

Descripción: A vulnerability was identified in HKritesh009 Grocery List Management Web App up to f491b681eb70d465f445c9a721415c965190f83b. This affects an unknown part of the file /src/update.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. This product is using a rolling release to provide c...

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: 2025-08-31

CVE-2025-9752

Descripción: A security vulnerability has been detected in D-Link DIR-852 1.00CN B09. Impacted is the function soapcgi_main of the file soap.cgi of the component SOAP Service. Such manipulation of the argument service leads to os command injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer support...

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-77

Tecnología: No especificado

Publicado el: 2025-09-01

CVE-2025-9767

Descripción: A vulnerability was determined in itsourcecode Sports Management System 1.0. This affects an unknown function of the file /Admin/sporttype.php. Executing manipulation of the argument code can lead to sql injection. The attack can be executed 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: 2025-09-01

CVE-2025-9768

Descripción: A vulnerability was identified in itsourcecode Sports Management System 1.0. This impacts an unknown function of the file /Admin/mode.php. The manipulation of the argument code leads to sql injection. The attack is possible to be carried out remotely.

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: 2025-09-01

CVE-2025-9770

Descripción: A weakness has been identified in Campcodes Hospital Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/ of the component Admin Dashboard Login. This manipulation of the argument Password causes sql injection. It is possible to initiate the attack 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: 2025-09-01

CVE-2025-9771

Descripción: A security vulnerability has been detected in SourceCodester Eye Clinic Management System 1.0. Affected by this issue is some unknown functionality of the file /main/search_index_Diagnosis.php. Such manipulation of the argument Search leads to sql injection. It is possible to launch the attack 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: 2025-09-01

CVE-2025-9772

Descripción: A vulnerability was detected in RemoteClinic up to 2.0. This affects an unknown part of the file /staff/edit.php. Performing manipulation of the argument image results in unrestricted upload. The attack can be initiated remotely. The exploit is now public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.

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: 2025-09-01

CVE-2025-9775

Descripción: A vulnerability was found in RemoteClinic up to 2.0. Impacted is an unknown function of the file /staff/edit-my-profile.php. The manipulation of the argument image results in unrestricted upload. The attack may 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-284

Tecnología: No especificado

Publicado el: 2025-09-01

CVE-2025-9786

Descripción: A vulnerability was found in Campcodes Online Learning Management System 1.0. Affected is an unknown function of the file /teacher_signup.php. Performing manipulation of the argument firstname results in sql injection. The attack can be initiated remotely. The exploit has been made public and could 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: 2025-09-01

CVE-2025-9788

Descripción: A vulnerability was determined in SourceCodester/Campcodes School Log Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/admin_class.php. Executing manipulation of the argument id_no 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: 2025-09-01

CVE-2025-9789

Descripción: A vulnerability was identified in SourceCodester Online Hotel Reservation System 1.0. Affected by this issue is some unknown functionality of the file /admin/edituser.php. The manipulation of the argument userid 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: 2025-09-01

CVE-2025-9790

Descripción: A security flaw has been discovered in SourceCodester Hotel Reservation System 1.0. This affects an unknown part of the file /admin/updateabout.php. The manipulation of the argument address 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: 2025-09-01

CVE-2025-9791

Descripción: A weakness has been identified in Tenda AC20 16.03.08.05. This vulnerability affects unknown code of the file /goform/fromAdvSetMacMtuWan. This manipulation of the argument wanMTU causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be exploited.

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: 2025-09-01

CVE-2025-9792

Descripción: A security vulnerability has been detected in itsourcecode Apartment Management System 1.0. This issue affects some unknown processing of the file /e_dashboard/e_all_info.php. Such manipulation of the argument mid leads to sql injection. The attack can be executed 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: 2025-09-01

CVE-2025-9793

Descripción: A vulnerability was detected in itsourcecode Apartment Management System 1.0. Impacted is an unknown function of the file /setting/admin.php of the component Setting Handler. Performing manipulation of the argument ddlBranch results in sql injection. The attack is possible to be carried out 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: 2025-09-01

CVE-2025-9794

Descripción: A flaw has been found in Campcodes Computer Sales and Inventory System 1.0. The affected element is an unknown function of the file /pages/pos_transac.php?action=add. Executing manipulation of the argument cash/firstname can lead to sql injection. The attack may be performed from remote. The exploit has been published 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: 2025-09-01

CVE-2024-28988

Descripción: SolarWinds Web Help Desk was found to be susceptible to a Java Deserialization Remote Code Execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. This vulnerability was found by the ZDI team after researching a previous vulnerability and providing this report.
The ZDI team was able to discover an unauthenticated attack during their research.

...

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: 2025-09-01

CVE-2025-9811

Descripción: A vulnerability was found in Campcodes Farm Management System 1.0. This affects an unknown part of the file /reviewInput.php. Performing manipulation of the argument rating 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: 2025-09-02

CVE-2025-9814

Descripción: A security flaw has been discovered in PHPGurukul Beauty Parlour Management System 1.1. Impacted is an unknown function of the file /admin/contact-us.php. The manipulation of the argument mobnumber results in sql injection. It is possible to launch 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: 2025-09-02

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-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-2025-9927

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-2025-41032

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

Resumen del Reporte

CVEs analizados: 44

Promedio CVSS: 7.80

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat □