CVEs más relevantes de la semana

Del 27/12/2025 al 03/01/2026

Porque el primer paso para defender es conocer las amenazas.

CVE-2025-15165

Descripción: A vulnerability has been found in itsourcecode Online Cake Ordering System 1.0. The impacted element is an unknown function of the file /updatecustomer.php?action=edit. 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: 2025-12-29

CVE-2025-15166

Descripción: A vulnerability was found in itsourcecode Online Cake Ordering System 1.0. This affects an unknown function of the file /updatesupplier.php?action=edit. The manipulation of the argument ID results in sql injection. 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-74

Tecnología: No especificado

Publicado el: 2025-12-29

CVE-2025-15167

Descripción: A vulnerability was determined in itsourcecode Online Cake Ordering System 1.0. This impacts an unknown function of the file /detailtransac.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. 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: 2025-12-29

CVE-2025-15226

Descripción: WMPro developed by Sunnet has a Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.

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: 2025-12-29

CVE-2025-15228

Descripción: BPMFlowWebkit developed by WELLTEND TECHNOLOGY has a Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.

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: 2025-12-29

CVE-2025-15181

Descripción: A security flaw has been discovered in code-projects Refugee Food Management System 1.0. The impacted element is an unknown function of the file /home/pagenateRefugeesList.php. Performing manipulation of the argument rfid 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: 2025-12-29

CVE-2025-15182

Descripción: A weakness has been identified in code-projects Refugee Food Management System 1.0. This affects an unknown function of the file /home/served.php. Executing manipulation of the argument refNo 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: 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: 2025-12-29

CVE-2025-15183

Descripción: A security vulnerability has been detected in code-projects Refugee Food Management System 1.0. This impacts an unknown function of the file /home/viewtakenfd.php. The manipulation of the argument tfid leads to sql injection. The attack is possible to be carried out 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: 2025-12-29

CVE-2025-15184

Descripción: A vulnerability was detected in code-projects Refugee Food Management System 1.0. Affected is an unknown function of the file /home/refugeesreport2.php. The manipulation of the argument a results in sql injection. The attack may be performed from remote. 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: 2025-12-29

CVE-2025-15185

Descripción: A flaw has been found in code-projects Refugee Food Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /home/refugeesreport.php. This manipulation of the argument a causes sql injection. It is possible to initiate the attack 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: 2025-12-29

CVE-2025-15186

Descripción: A vulnerability has been found in code-projects Refugee Food Management System 1.0. Affected by this issue is some unknown functionality of the file /home/addusers.php. Such manipulation of the argument a 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: 2025-12-29

CVE-2025-57460

Descripción: File upload vulnerability in machsol machpanel 8.0.32 allows attacker to gain a webshell.

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: 2025-12-29

CVE-2025-68929

Descripción: Frappe is a full-stack web application framework. Prior to versions 14.99.6 and 15.88.1, an authenticated user with specific permissions could be tricked into accessing a specially crafted link. This could lead to a malicious template being executed on the server, resulting in remote code execution. Versions 14.99.6 and 15.88.1 fix the issue. No known workarounds are available.

CVSS: 9.0 (CRITICAL)

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

Tipo: CWE-1336

Tecnología: No especificado

Publicado el: 2025-12-29

CVE-2025-15194

Descripción: A vulnerability was found in D-Link DIR-600 up to 2.15WWb02. Affected by this vulnerability is an unknown functionality of the file hedwig.cgi of the component HTTP Header Handler. The manipulation of the argument Cookie results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been made public and could be used. This vulnerability only affects produc...

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-119

Tecnología: No especificado

Publicado el: 2025-12-29

CVE-2024-25182

Descripción: givanz VvvebJs 1.7.2 suffers from a File Upload vulnerability via save.php.

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: 2025-12-29

CVE-2024-27480

Descripción: givanz VvvebJs 1.7.2 is vulnerable to Insecure File Upload.

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: 2025-12-29

CVE-2025-15209

Descripción: A weakness has been identified in code-projects Refugee Food Management System 1.0. This affects an unknown part of the file /home/editfood.php. This manipulation of the argument a/b/c/d 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: 2025-12-29

CVE-2025-15210

Descripción: A security vulnerability has been detected in code-projects Refugee Food Management System 1.0. This vulnerability affects unknown code of the file /home/editrefugee.php. Such manipulation of the argument a/b/c/sex/d/e/nationality_nid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly 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: 2025-12-30

CVE-2025-15211

Descripción: A flaw has been found in code-projects Refugee Food Management System 1.0. Impacted is an unknown function of the file /home/refugee.php. Executing manipulation of the argument refNo/Fname/Lname/sex/age/contact/nationality_nid can lead to sql injection. The attack can be executed remotely. The exploit has been published 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: 2025-12-30

CVE-2025-15212

Descripción: A vulnerability was detected in code-projects Refugee Food Management System 1.0. This issue affects some unknown processing of the file /home/regfood.php. Performing manipulation of the argument a results in sql injection. Remote exploitation of the attack is possible. The exploit is now 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: 2025-12-30

CVE-2025-15243

Descripción: A flaw has been found in code-projects Simple Stock System 1.0. This affects an unknown function of the file /market/login.php. Executing manipulation of the argument Username can lead to sql injection. The attack can be launched 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: 2025-12-30

CVE-2025-15353

Descripción: A vulnerability was detected in itsourcecode Society Management System 1.0. Impacted is the function edit_admin_query of the file /admin/edit_admin_query.php. Performing manipulation of the argument Username 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: 2025-12-30

CVE-2025-15354

Descripción: A flaw has been found in itsourcecode Society Management System 1.0. The affected element is an unknown function of the file /admin/add_admin.php. Executing manipulation of the argument Username can lead to sql injection. It is possible to launch the attack 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: 2025-12-30

CVE-2022-50695

Descripción: SOUND4 IMPACT/FIRST/PULSE/Eco versions 2.x contains a network vulnerability that allows unauthenticated attackers to send ICMP signals to arbitrary hosts through network command scripts. Attackers can abuse ping.php, traceroute.php, and dns.php to generate network flooding attacks targeting external hosts.

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-770

Tecnología: No especificado

Publicado el: 2025-12-30

CVE-2022-50790

Descripción: SOUND4 IMPACT/FIRST/PULSE/Eco versions 2.x and below contain an unauthenticated vulnerability that allows remote attackers to access live radio stream information through webplay or ffmpeg scripts. Attackers can exploit the vulnerability by calling specific web scripts to disclose radio stream details without requiring authentication.

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-306

Tecnología: No especificado

Publicado el: 2025-12-30

CVE-2022-50792

Descripción: SOUND4 IMPACT/FIRST/PULSE/Eco versions 2.x and below contain an unauthenticated file disclosure vulnerability that allows remote attackers to access sensitive system files. Attackers can exploit the vulnerability by manipulating the 'file' GET parameter to disclose arbitrary files on the affected device.

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: 2025-12-30

CVE-2022-50794

Descripción: SOUND4 IMPACT/FIRST/PULSE/Eco versions 2.x and below contain an unauthenticated command injection vulnerability in the username parameter. Attackers can exploit index.php and login.php scripts by injecting arbitrary shell commands through the HTTP POST 'username' parameter to execute system commands.

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-78

Tecnología: No especificado

Publicado el: 2025-12-30

CVE-2022-50803

Descripción: JM-DATA ONU JF511-TV version 1.0.67 uses default credentials that allow attackers to gain unauthorized access to the device with administrative privileges.

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-1392

Tecnología: No especificado

Publicado el: 2025-12-30

CVE-2025-14998

Descripción: The Branda plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.4.24. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gain access to their...

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: 2026-01-02

Resumen del Reporte

CVEs analizados: 29

Promedio CVSS: 8.26

Fuente: nvd.nist.gov

Nos vemos la próxima semana. Hack the Cat □