الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

دليل الثغرات الأمنية في نظم إدارة المحتوى CMS المستخدمة في المواقع الإلكترونية على شبكة الإنترنت

الإصدار الأول
دمشق في ٢٠١٢/٤/١١

Tel: +963 11 3937032 Fax: +963 11 3937079 E-mail: isc@nans.gov.sy Website: www.nans.gov.sy

فهرس المحتويات

1. الثغرات الأمنية الموجودة في نظم إدارة المحتوى DotNetNuk :

تحتوي نظم DotNetNuk باستثناء الإصدار DotNetNuke 6.1.0 على الثغرات الأمنية التالية:

رمز الثغرة	نوع الثغرة	التوصيف	عامل الخطورة [المرجع]
DNN-18555	failure to sanitize certain xss strings	هذه الثغرة تمكّن المهاجم من إنشاء كودات خبيثة عبر محرر نصوص HTML الخاص بنظام إدارة المحتوى، ومن ثم إرسالها للموقع الإلكتروني، مما يسبب هجوم XSS.	متوسط [1]
DNN-18534	disable autoremember during registration	عند إدخال المستخدم بياناته إلى صفحة التسجيل، يستطيع المستخدم حينها استخدام اسم مستخدم تم استخدامه سابقاً، وإذا كانت ميزة تذكُر اسم المستخدم وكلمة المرور مفعلة في المستعرض فإن كلمة المرور سوف تعاد كتابتها بشكل آلي، مما يمكن المهاجم من الدخول لحساب المستخدم ومعرفة كلمة المرور الخاصة به.	منخفض [2]
DNN-18375	incorrect logic in module administration check	يحتوي نظام إدارة المحتوى على نظام لإدارة السماحيات، مما يسمح لمدير الموقع إعطاء السماحيات للمستخدمين والمجموعات، ولكن في بعض الإصدارات يستطيع المهاجم الدخول لنظام إدارة السماحيات واستغلاله لزيادة السماحيات الخاصة به.	منخفض [3]
DNN-15379	Module Permissions Editable by anyone with the URL	يدعم نظام إدارة المحتوى تطبيق سماحيات مختلفة للصفحات والـ modules، ولكن بعض الإصدارات تحتوي على ثغرة تمكّن المهاجم من تعديل سماحياته الخاصة بـ module معين إلى السماحيات التي يريدها، وبالتالي تمنحه تحكماً كاملاً بهذا الـ module.	متوسط [4]
DNN-16484	Cached failed passwords could theoretically be retrieved from browser cache	إذا تم إدخال اسم مستخدم وكلمة مرور خاطئتين، سيتم إعادة تحميل الصفحة من أجل إعادة المحاولة، ولكن هذه الصفحة يتم تخزينها من قبل المستعرض (وهي تحتوي على اسم المستخدم وكلمة المرور) وبالتالي إذا تمكن المهاجم من الدخول إلى	منخفض [5]

		جهاز الضحية يمكنه الحصول على هذه البيانات بسهولة.	
DNN-16535	User management mechanisms can be executed by invalid users	نظام إدارة المتحوى يحتوي على عدد من التوابع (الدوال) التي تستخدم لإدارة سماحيات المستخدم، ولكنها مكشوفة لكلٍ من المستخدم ومدير الموقع، إلا أنه يوجد قواعد يمكن تعريفها لتحديد أي هذه التوابع تكون مكشوفة للمستخدم. يوجد ثغرة في بعض الإصدارات يستطيع للمهاجم من خلالها تخطي هذه القواعد وتنفيذ الوظائف الخاصة بمدير الموقع.	حرج [6]
DNN-14587	XSS	يمكن للمهاجم استغلال هذه الثغرة بإطلاق هجوم XSS عن طريق تمرير html tag .	منخفض [7]
VULN044	Unauthenticated user can install/uninstall modules	هذه الثغرة تمكّن المهاجم الذي يملك سماحيات المستخدم العادي من تنصيب أو حذف الـ modules وبالتالي التحكم الكامل بموديولات الموقع.	حرج [8]
DNN-14540	Edit Level Users have Admin rights to modules	مدير النظام هو المسؤول عن إضافة وتعديل الصفحات في الموقع وكذلك إضافة الـ modules، ولكن بعض الإصدارات تحتوي على ثغرة تمكّن المستخدم الذي يملك سماحيات التعديل على الصفحات فقط من الدخول لإعدادات الـ modules والتحكّم بها.	حرج [9]

2. الثغرات الأمنية الموجودة في نظم إدارة المحتوى Platinum :

تحتوي نظم Platinum باستثناء الإصدار Platinum 4.x على الثغرات الأمنية التالية:

رمز الثغرة	نوع الثغرة	التوصيف	عامل الخطورة [المرجع]
10.21.56 - CVE	SQL injection vulnerability	هذه الثغرة تمكّن المهاجم من حقن استعلامات SQL والحصول على معلومات قاعدة البيانات .	لم يتم تقييمها
CVE-2008-1539		توجد هذه الثغرة في includes/dynamic_titles.php في الإصدار Platinum 7.6.b.5 حيث تسمح للمهاجم البعيد بتنفيذ تعليمات SQL عن طريق تمرير متغيّرات لـmodules.php عند استخدام الـmodule الخاص بالمنتدى.	عالي [10]
CVE-2006-2121	vulnerability in admin/config_settings.tpl.php	هذه الثغرة تسمح للمهاجم بتنفيذ التعليمات الخبيثة عن طريق إعطاء متغيّرات خاصة للرابط الخاص بـ include_path .	متوسط [11]
CVE-2006-1929	PHP remote file inclusion vulnerability in include/common.php	هذه الثغرة موجودة في include/common.php وتمكّن المهاجم البعيد من إرسال ملفات PHP خبيثة عن طريق الرابط الخاص بالمتغيّر include_path وتنفيذها على المخدم.	متوسط [12]
CVE: 2007-5676	Remote File Inclusion Vulnerability	هذه الثغرة موجودة في modules/Forums/favorites.php وهي تسمح للمهاجم البعيد بتنفيذ تعليمات PHP عشوائية عن طريق الرابط الخاص بالمتغيّر nuke_bb_root_path	متوسط [13]
–	platinum-id-sql-injection (58262)	هذه الثغرة تسمح للمهاجم بحقن تعليمات SQL حيث تسمح له بإضافة وتعديل وحذف واستعراض البيانات التي تحتوي عليها بيانات الموقع.	لم يتم تقييمها
Bugtraq ID: 1773	Platinum Config_settings.TPL.PHP Remote File Include Vulnerability	هذه الثغرة يمكن استغلالها من قبل المهاجم البعيد بارسال ملفات تحتوي على كودات خبيثة وتنفيذ هذه الملفات بما تحتويه من كودات على مخدم الويب الخاص بالموقع مما يعرّض النظام للخطر.	لم يتم تقييمها

3. الثغرات الأمنية الموجودة في نظم إدارة المحتوى Drupal :

تحتوي نظم Drupal باستثناء الإصدارين Drupal 7.5 و Drupal 7.7 على الثغرات الأمنية التالية:

رمز الثغرة	نوع الثغرة	التوصيف	عامل الخطورة [المرجع]
SA-CORE-2011-003 – Drupal core – Access bypass	Access bypass	هذه الثغرة تمكّن المستخدم الذي لا يملك سماحيات من تبادل الملفات مع الموقع بمجرد معرفة الرابط URL إلى مكان محدد على المخدّم.	منخفض [14]
SA-CORE-2011-002 – Drupal core – Access bypass			عالي [14]
SA-CORE-2011-001 - Drupal core - Multiple vulnerabilities	cross site scripting vulnerability in error handler	هذه الثغرة موجودة في معالج الأخطاء الخاص بـDrupal، حيث يمكن للمهاجم استغلالها بحقن كودات خبيثة إلى الموقع.	حرج [14]
	Cross site scripting vulnerability in Color module	عند استخدام re-colorable themes يمكن استخدام قيمة خبيثة للون، وعن طريق هذه القيمة يمكن للمهاجم حقن كودات خبيثة إلى المخدّم.	حرج [14]
	Access bypass in File module	هذه الثغرة يمكن استغلالها من قبل المهاجم للنفاذ إلى ملفات على مخدّم الموقع لا يملك سماحيات النفاذ إليها.	حرج [14]
SA-CONTRIB-2011-058 - Support Timer	Cross Site Scripting (XSS)	هذه الثغرة من نوع XSS ويمكن استغلالها من قبل المهاجم البعيد للحصول على سماحيات تمكّنه من إرسال كودات إلى المخدم الذي يحتوي على ملفات الموقع.	متوسط [15]
SA-CONTRIB-2011-057 - Support Ticketing System			
SA-CONTRIB-2011-056 - Webform Validation			
SA-CONTRIB-2011-055 - Webform CiviCRM Integration	Access bypass	هذه الثغرة موجودة في Webform CiviCRM module، حيث يمكن للمهاجم استغلالها للنفاذ إلى قواعد بيانات الموقع وحقن استعلامات SQL.	متوسط [15]
	SQL Injection		
SA-CONTRIB-2011-054 - CKEditor	Access bypass	هذه الثغرة موجودة في CKEditor module ويمكن استغلالها من قبل المهاجم للحصول على ملفات الإعداد الخاصة بالموقع بمجرد الحصول	حرج [15]

		على الرابط الخاص بها.	
SA-CONTRIB-2011-052 – Views	SQL Injection	هذه الثغرة موجودة في Views module الذي يساعد مدير الموقع بعرض محتويات الموقع بطرق مختلفة، حيث يمكن للمهاجم استغلال هذه الثغرة بحقن استعلامات SQL.	متوسط [15]
SA-CONTRIB-2011-049 - Cumulus	Cross Site Scripting (XSS)	هذه الثغرة موجودة في Cumulus module الذي يساعد في عرض ملفات الفلاش، حيث يمكن للمهاجم استغلال الثغرة عند دخول مستخدم بسماحيات مدير الموقع، حيث يستطيع المهاجم عندئذ من استغلال هذه الجلسة لإطلاق كوداته الخاصة أو جمع المعلومات الخاصة بسماحيات مدير الموقع.	متوسط [15]
SA-CONTRIB-2011-040 Author Pane	access bypass	هذه الثغرة موجودة في Author Pane module الذي يساعد على جمع معلومات عن مستخدمين الموقع. هذه الثغرة تسبب ظهور معلومات المستخدمين لمتصفحي الموقع العاديين.	منخفض [15]
SA-CORE-2010-001 - Drupal core	cross site scripting	هذه الثغرة تمكّن المهاجم من إطلاق هجوم XSS.	حرج [14]
SA-CORE-2010-001 - Drupal core	Open redirection	يمكن هذه الثغرة استغلالها من قبل المهاجم لإعادة توجيه مستخدم الموقع إلى روابط مختلفة عن الروابط الأصلية للموقع.	حرج [14]
SA-CORE-2009-007 - Drupal core	Cross-site scripting	Forum module لايعالج الروابط بشكل صحيح مما يمكّن المهاجم من إطلاق هجوم XSS وإدخال كودات HTML أو كودات script إلى صفحات المنتدى.	حرج [14]

الحل المقترح لتلافي الثغرات الموجودة في الـ Module's :

module	الحل المقترح	رابط التحميل
Support Timer module	الترقية إلى Support Timer 6.x-1.4	http://drupal.org/node/1357278
Support Ticketing System module	الترقية إلى support 6.x-1.7	http://drupal.org/node/1357300
Webform Validation module	من أجل Drupal 6.x يجب الترقية إلى Webform Validation 6.x-1.5	http://drupal.org/node/1357354
	من أجل الإصدار Drupal 7.x يجب الترقية إلى Webform Validation 7.x-1.1	http://drupal.org/node/1357356
Webform CiviCRM Integration module	من أجل الإصدار Drupal 6.x يجب الترقية إلى Webform CiviCRM Integration 6.x-2.2	http://drupal.org/node/1336044
	من أجل الإصدار Drupal 7.x يجب الترقية إلى Webform CiviCRM Integration 7.x-2.2	http://drupal.org/node/1336046
CKEditor module	الترقية إلى CKEditor 7.x-1.5	http://drupal.org/node/1336272
Views module	الترقية إلى Views 6.x-2.13	http://drupal.org/node/1329842
Cumulus module	الترقية إلى Cumulus 6.x-1.5	http://drupal.org/node/1304616
Author Pane module	الترقية إلى Author Pane 6.x-2.2	http://drupal.org/node/1271388

4. الثغرات الأمنية الموجودة في نظم إدارة المحتوى Xoops :

تحتوي نظم Xoops باستثناء الإصدار Xoops 2.5.4 على الثغرات الأمنية التالية:

رمز الثغرة	نوع الثغرة	التوصيف	عامل الخطورة [المرجع]
CVE-2006-4417	SQL injection	هذه الثغرة تسمح للمهاجم بحقن استعلامات SQL واستخلاص البيانات من قاعدة بيانات الموقع.	عالي [16]
CVE-2005-0911			عالي [17]
CVE-2006-3363	PHP remote file inclusion	هذه الثغرة تسمح للمهاجم بتنفيذ كودات PHP عشوائية وهي موجودة في Glossaire module 1.7.	متوسط [18]
CVE-2006-3341	SQL injection	هذه الثغرة موجودة في annonces-p-f.php عند استخدام الموديول MyAds، وهي تسمح للمهاجم بتنفيذ استعلامات SQL.	عالي [19]
CVE-2006-2516	–	هذه الثغرة تمكّن المهاجم البعيد من التعديل على المتغيرات مثل $xoopsOption['nocommon'] أو التسبب بهجمات مثل directory traversal attacks أو include PHP files.	متوسط [20]
CVE-2006-2516	Cross-site scripting (XSS)	هذه الثغرة تسمح للمهاجم بحقن web script عشوائية وبالتالي التسبب بهجوم XSS.	متوسط [21]
CVE-2006-2516	SQL injection	هذه الثغرة موجودة في viewcat.php في الموديول WF-Downloads وهي تسمح للمهاجم بتنفيذ استعلامات SQL عشوائية.	متوسط [21]
CVE-2005-3680	File inclusion	هذه الثغرة تسمح للمهاجم بقراءة أو الحصول على الملفات الخاصة بالموقع، وبالتالي تمكّنه من الحصول على ملفات الإعداد الخاصة بالموقع.	متوسط [22]
CVE-2005-2338	cross-site scripting (XSS)	هذه الثغرة تسمح للمهاجم بحقن web script عشوائية وهي موجودة في forum module.	متوسط [23]
CVE-2005-2113	SQL injection	هذه الثغرة تسمح للمهاجم بتنفيذ استعلامات SQL عشوائية كما تمكّنه من تخطي عملية المصادقة authentication عن طريق ملف XML .	عالي [24]

CVE-2002-1802	Cross-site scripting (XSS)	هذه الثغرة تسمح للمهاجم بحقن secript web وبالتالي التسبب بهجوم XSS.	متوسط [25]
CVE-2005-2112			متوسط [26]
CVE-2005-0910			متوسط [27]
CVE-2004-1640			متوسط [28]
CVE-2005-1031	–	هذه الثغرة تمكّن المهاجم من تحميل ملفات عشوائية إلى مخدم الموقع.	متوسط [29]
CVE-2005-0828	–	هذه الثغرة تسمح للمهاجم بالاطلاع على ملفات PHP الخاصة بالموقع بمجرد معرفة مسار الملف.	متوسط [30]
CVE-2005-0743	–	هذه الثغرة تسمح للمهاجم بتحميل وحقن كودات PHP عشوائية إلى ملفات الموقع.	عالي [31]
CVE-2002-0216	SQL injection	هذه الثغرة تمكن المهاجم من تحسس وجمع المعلومات وذلك عن طريق حقن استعلامات SQL	متوسط [32]

5. الثغرات الأمنية الموجودة في نام إدارة المحتوى Impress :

تحتوي نظم Impress باستثناء الإصدار Impress 1.2.5 على الثغرات الأمنية التالية:

رمز الثغرة	نوع الثغرة	التوصيف	عامل الخطورة [المرجع]
CVE-2010-4616	Cross-site scripting (XSS)	هذه الثغرة تسمح للمهاجم بحقن websecript أو كود Html وتنفيذها على المخدم الخاص بالموقع	متوسط [33]
CVE-2008-2035			متوسط [34]
HTB22766		هذه الثغرة تسمح للمهاجم بإنشاء رابط يمكن من تنفيذ كودات عن طريق مستعرض الانترنت وذلك لأنه ينشئ علاقة موثوقة بين المستعرض الخاص به وبين المخدّم.	لم يتم تقييمها
SA31259	ImpressCMS "modules/admin.php" Unspecified Vulnerability	هذه الثغرة يسببها خطأ غير معروف في modules/admin.php، وقد تمكّن المهاجم من تحسس معلومات مهمة تمكّنه من النفاذ إلى المخدّم.	حرج [35]
CVE-2008-3453			
CVE-2008-5964	hijack web sessions	هذه الثغرة تمكّن المهاجم من إطلاق هجوم hijack web sessions وذلك عن طريق تفعيل المتغيّر PHPSESSID.	متوسط [36]
CVE-2010-4271	SQL injection	هذه الثغرة تسمح للمهاجم بتنفيذ استعلامات QSL عشوائية على قاعدة البيانات الخاصة بالموقع.	عالي [37]
CVE-2005-4259			عالي [38]
CVE-2010-2936	Integer overflow	هذه الثغرة تمكّن المهاجم من إطلاق هجوم منع تقديم الخدمة في نمط (application crash) كما يستطيع أيضاً تنفيذ كود خبيث يتسبب بحالة طفحان الذاكرة المؤقتة buffer overflow.	حرج [39]
CVE-2010-2935			حرج [40]

6. الثغرات الأمنية الموجودة في نظم إدارة المحتوى Joomla :

تحتوي نظم Joomla باستثناء الإصدار Joomla 1.7.3 على الثغرات الأمنية التالية:

رمز الثغرة	نوع الثغرة	التوصيف	عامل الخطورة [المرجع]
[20110601]	XSS Vulnerabilitie	هذه الثغرة تُمكّن المهاجم من حقن أوامر معينة عن طريق متصفح الانترنت للحصول على معلومات مهمة.	متوسط [41]
[20110602]	Information Disclosure		منخفض [42]
NS-11-009	XSS Vulnerabilitie		عالي [43]
Bugtraq ID: 49853	Multiple Cross Site Scripting Vulnerabilities		لم يتم تقييمها
Bugtraq ID: 49855	'com_search' Component Cross Site Scripting Vulnerability		متوسط [44]
[20110603]	Unauthorised Access	هذه الثغرة تؤدي إلى نقص في سماحيات النفاذ، مما يؤدي إلى استغلالها من قبل المهاجم للحصول على سماحيات النفاذ إلى المخدّم.	متوسط [45]
Bugtraq ID: 50664	Password Enumeration Weakness	يمكن للمهاجم أن يستغل هذه الثغرة بتطبيق هجوم brute-force من أجل الحصول على نفاذ إلى النظام. كما تمكّنه من تنفيذ كودات عشوائية على المخدّم عن طريق مستعرض الإنترنت، وهذا يمكّنه من الحصول على نفاذ مصادق عليه وبالتالي إطلاق هجمات أخرى.	عالي [46]
Bugtraq ID: 47159	Unspecified Information Disclosure Vulnerability	هذه الثغرة تسمح للمهاجم البعيد بتحسس تدفق البيانات من وإلى المخدّم، وبالتالي حصوله على معلومات مهمة	منخفض [47]
CVE-2011-2488			متوسط [48]
Bugtraq ID:46846	Multiple SQL Injection Vulnerabilities	هذه الثغرة تمكّن المهاجم من حقن استعلامات SQL والنفاذ إلى البيانات وتعديلها.	متوسط [49]
CVE-2011-1151	DoS	هذه الثغرة تمكّن المهاجم من إطلاق هجوم منع تقديم الخدمة.	متوسط [50]
Bugtraq ID: 48939	Clickjacking	هذه الثغرة تمكّن المهاجم من إطلاق هجوم	متوسط [51]

	Vulnerability	Clickjacking والنفاذ إلى نظام الضحية والحصول على معلومات مهمة من خلال تحسس تدفق هذه البيانات.	
CVE-2011-2892			متوسط [52]

7. الثغرات الأمنية الموجودة في نظم إدارة المحتوى Kentico:

تحتوي نظم Kentico باستثناء الإصدار kentico 6 على الثغرات الأمنية التالية:

رمز الثغرة	نوع الثغرة	التوصيف	عامل الخطورة [المرجع]
-	XSS Vulnerabilitie	هذه الثغرة تُمكّن المهاجم من حقن أوامر عشوائية عن طريق متصفح الانترنت للحصول على معلومات مهمة وقد تؤدي إلى سرقة بيانات المستخدم وبالتالي إطلاق هجمات أخرى.	منخفض [53]
kenticocms-usersviewer-xss (67776)			متوسط [54]
SA44785	Kentico CMS 'userContextMenu_parameter' Parameter Cross Site Scripting Vulnerability		منخفض [55]

8. الثغرات الموجودة في نظم إدارة المحتوى Wordpress:

تحتوي نظم Wordpress باستثناء الإصدار Wordpress cms 3.3.1 على الثغرات الأمنية التالية:

رمز الثغرة	نوع الثغرة	التوصيف	عامل الخطورة [المرجع]
CVE-2004-1584	CRLF injection vulnerability	هذه الثغرة تمكّن المهاجم من تعديل محتويات صفحات الـHTML على المخدّم عن طريق متغيّرات نصية.	متوسط [56]
CVE-2004-1559	cross-site scripting (XSS) vulnerabilities	هذه الثغرات تمكّن المهاجم من حقن كودات Javasecript أو كودات HTML خبيثة إلى ملفات الموقع.	متوسط [57]
CVE-2007-1894	cross-site scripting (XSS) vulnerabilities		متوسط [58]
CVE-2007-1732			منخفض [59]
CVE-2007-1622			متوسط [60]
CVE-2007-1049	cross-site scripting (XSS) vulnerabilities		متوسط [61]
CVE-2007-0106			متوسط [62]
CVE-2007-1897	SQL injection vulnerability	هذه الثغرة تسمح للمهاجم بتنفيذ استعلامات SQL على قاعدة البيانات الخاصة بالموقع.	متوسط [63]
CVE-2007-0233			عالي [64]
CVE-2007-0107			متوسط [65]
CVE-2007-1599	–	هذه الثغرة تمكّن المهاجم من توجيه المستخدم إلى موقع آخر وسرقة بياناته الشخصية.	متوسط [66]
CVE-2007-1409	–	هذه الثغرة تمكّن المهاجم من تحسس المعلومات الخاصة بالموقع عن طريق طلبات يقوم بإرسالها.	متوسط [67]
CVE-2007-1277	Commands injection	هذه الثغرة تمكّن المهاجم من حقن أوامر خبيثة عشوائية وتنفيذها على المخدم.	عالي [68]
CVE-2007-1244	Cross-site request forgery (CSRF) vulnerability	هذه الثغرة تمكّن المهاجم من الحصول على سماحيات مدير النظام وإطلاق هجوم XSS.	متوسط [69]
CVE-2007-0541	Files injection	هذه الثغرة تمكّن المهاجم من تفحص وجود ملفات	متوسط [70]

		معينة على المخدم كما تمكنه من الاطلاع على محتويات الملفات الموجودة.	
CVE-2007-0540	DOS	هذه الثغرة تمكّن المهاجم من إطلاق هجوم منع تقديم الخدمة DoS.	متوسط [71]
CVE-2007-0539			عالي [72]
CVE-2007-0109	–	هذه الثغرة تمكّن المهاجم من تحسس المعلومات وإطلاق هجوم brute force .	متوسط [73]

9. الثغرات الأمنية الموجودة في نظم إدارة المحتوى Umbraco:

تحتوي نظم Umbraco باستثناء الإصدار Umbraco 4.7.1 على الثغرات الأمنية التالية:

رمز الثغرة	نوع الثغرة	التوصيف	عامل الخطورة [المرجع]
SA34209	Privilege Escalation Vulnerability	هذه الثغرة تمكّن المهاجم من تعديل إعدادات أو كلمات مرور المستخدمين.	منخفض [74]
SA200901234			منخفض [75]
Bugtraq ID: 34166	Unauthorized Access Vulnerability	هذه الثغرة تمكّن المهاجم من الحصول على نفاذ غير مصادق عليه إلى صفحات مدير الموقع في التطبيق المصاب بهذه الثغرة.	لم يتم التقييم

10. الثغرات الأمنية الموجودة في نظم إدارة المحتوى OpenPHPNuke:

تحتوي نظم OpenPHPNuke باستثناء الإصدار OpenPHPnuke 2.4.16 على الثغرات الأمنية التالية:

رمز الثغرة	نوع الثغرة	التوصيف	عامل الخطورة [المرجع]
CVE-2006-2137	Remote File Include Vulnerability	هذه الثغرة تمكّن المهاجم من حقن ملف يحتوي كود PHP خبيث و تنفيذه على مخدم الموقع.	عالي [76]
Bugtraq ID: 17772			لم يتم تقييمها
CVE-2006-1602			عالي [77]
Bugtraq ID: 34088	SQL Injection Vulnerability	هذه الثغرة تمكّن المهاجم من النفاذ إلى بيانات التطبيق المصاب بها و تعديلها.	لم يتم تقييمها

11. الثغرات الأمنية الموجودة في نظم إدارة المحتوى Bitflux:

تحتوي نظم Bitflux باستثناء الإصدار Bitflux cms 1.6 على الثغرات الأمنية التالية:

رمز الثغرة	نوع الثغرة	التوصيف	عامل الخطورة [المرجع]
CVE-2006-6361	Dos	هذه الثغرة تمكّن المهاجم من إطلاق هجوم منع تقديم الخدمة أو تنفيذ أوامر وذلك عن طريق طلبات HTTP POST.	حرج [78]
Bugtraq ID: 21417	Buffer Overflow Vulnerability	هذه الثغرة تمكّن المهاجم من تنفيذ أوامر تعرّض مخدّم الويب للخطر وإذا فشل في استغلالها فإنه يتسبب بمنع تقديم الخدمة.	لم يتم تقييمها

12. الثغرات الأمنية الموجودة في لوحة التحكم Plesk:

تحتوي لوحة التحكم Plesk باستثناء الإصدار Parallels Plesk Panel 9.5 على الثغرات الأمنية التالية:

رمز الثغرة	نوع الثغرة	التوصيف	عامل الخطورة [المرجع]
CVE-2006-3737	Cross-site scripting (XSS)	هذه الثغرة تمكّن المهاجم من حقن كودات Javasecript أو كودات HTML خبيثة إلى ملفات الموقع.	متوسط [79]
CVE-2004-2702			متوسط [80]
CVE-2001-1222	PHP Source Disclosure Vulnerability	هذه الثغرة تسمح للمهاجم البعيد بالحصول على كود المصدر PHP للموقع وذلك عن طريق طلب HTTP يحتوي على عنوان الIP لمخدم الموقع.	متوسط [81]
Bugtraq ID: 3737			لم يتم تقييمها
Bugtraq ID: 23639	Login.PHP3 Directory Traversal Vulnerability	هذه الثغرة تمكّن المهاجم من التعديل على ملفات الموقع المصاب بها.	لم يتم تقييمها
Bugtraq ID:	Filemanager.PHP Directory Traversal Vulnerability		لم يتم تقييمها
Bugtraq ID: 21067	HTML Injection Vulnerabilities	هذه الثغرة تمكن المهاجم من تنفيذ كود Html أو javascripte لسرقة البيانات الشخصية أو التحكّم في كيفية استجابة الموقع للمستخدم.	لم يتم تقييمها

13. المراجع العلمية:

http://www.secunia.com
http://www.f-secure.com/
http://www.securityfocus.com
http://cve.mitre.org
http://www.impresscms.org
http://www.dotnetnuke.com
http://drupal.org/security
http://osvdb.org
http://www.exploitsearch.net
http://cxsecurity.com/wlb
http://www.iss.net/index.html
http://www.security-database.com
http://nvd.nist.gov

14. مراجع تقييم عامل الخطورة:

[1] http://www.dotnetnuke.com/News/Security-Policy/Security-bulletin-no.59.aspx
[2] http://www.dotnetnuke.com/News/Security-Policy/Security-bulletin-no.58.aspx
[3] http://www.dotnetnuke.com/News/Security-Policy/Security-bulletin-no.57.aspx
[4] http://www.dotnetnuke.com/News/Security-Policy/Security-bulletin-no.56.aspx
[5] http://www.dotnetnuke.com/News/Security-Policy/Security-bulletin-no.54.aspx
[6] http://www.dotnetnuke.com/News/Security-Policy/Security-bulletin-no.53.aspx
[7] http://www.dotnetnuke.com/News/Security-Policy/Security-bulletin-no.49.aspx
[8] http://www.dotnetnuke.com/News/Security-Policy/Security-bulletin-no.46.aspx
[9] http://www.dotnetnuke.com/News/Security-Policy/Security-bulletin-no.45.aspx
[10] http://www.security-database.com/detail.php?alert=CVE-2008-1539
[11] http://www.security-database.com/detail.php?alert=CVE-2006-2121
[12] http://www.security-database.com/detail.php?alert=CVE-2006-1929
[13] http://www.security-database.com/detail.php?alert=CVE-2007-5676
[14] http://drupal.org/security
[15] http://drupal.org/security/contrib?page=3
[16] http://www.security-database.com/detail.php?alert=CVE-2006-4417
[17] http://www.security-database.com/detail.php?alert=CVE-2005-0911
[18] http://www.security-database.com/detail.php?alert=CVE-2006-3363
[19] http://www.security-database.com/detail.php?alert=CVE-2006-3341
[20] http://www.security-database.com/detail.php?alert=CVE-2006-2516
[21] http://www.security-database.com/detail.php?alert=CVE-2006-2516
[22] http://www.security-database.com/detail.php?alert=CVE-2005-3680
[23] http://www.security-database.com/detail.php?alert=CVE-2005-2338
[24] http://www.security-database.com/detail.php?alert=CVE-2005-2113
[25] http://www.security-database.com/detail.php?alert=CVE-2002-1802
[26] http://www.security-database.com/detail.php?alert=CVE-2005-2112
[27] http://www.security-database.com/detail.php?alert=CVE-2005-0910
[28] http://www.security-database.com/detail.php?alert=CVE-2004-1640
[29] http://www.security-database.com/detail.php?alert=CVE-2005-1031
[30] http://www.security-database.com/detail.php?alert=CVE-2005-0828
[31] http://www.security-database.com/detail.php?alert=CVE-2005-0743
[32] http://www.security-database.com/detail.php?alert=CVE-2002-0216
[33] http://www.security-database.com/detail.php?alert=CVE-2010-4616
[34] http://www.security-database.com/detail.php?alert=CVE-2008-2035
[35] http://www.security-database.com/detail.php?alert=CVE-2008-3453
[36] http://www.security-database.com/detail.php?alert=CVE-2008-5964
[37] http://www.security-database.com/detail.php?alert=CVE-2010-4271
[38] http://www.security-database.com/detail.php?alert=CVE-2005-4259
[39] http://www.security-database.com/detail.php?alert=CVE-2010-2936
[40] http://www.security-database.com/detail.php?alert=CVE-2010-2935
[41] http://developer.joomla.org/security/news/367-20110901-core-xss-vulnerability
[42] http://developer.joomla.org/security/news/369-20110903-core-information-disclosure
[43] http://www.mavitunasecurity.com/xss-vulnerability-in-joomla-163/
[44] http://developer.joomla.org/security/news/367-20110901-core-xss-vulnerability
[45] http://developer.joomla.org/security/news/350-20110603-unauthorised-access
[46] http://developer.joomla.org/security/news/374-20111102-core-password-change1.7.3
[47] http://developer.joomla.org/security/news/9-security/10-core-security/340-20110401-core-informationdisclosure.html
[48] http://www.security-database.com/detail.php?alert=CVE-2011-2488
[49] http://secunia.com/advisories/45230
[50] http://www.security-database.com/detail.php?alert=CVE-2011-3389

[51] http://developer.joomla.org/security/news/347-20110409-core-clickjacking.html
[52] http://www.security-database.com/detail.php?alert=CVE-2011-2892
[53] http://www.naked-security.com/nsa/200208.htm
[54] http://xforce.iss.net/xforce/xfdb/67776
[55] http://secunia.com/advisories/44785
[56] http://www.security-database.com/detail.php?alert=CVE-2004-1584
[57] http://www.security-database.com/detail.php?alert=CVE-2004-1559
[58] http://www.security-database.com/detail.php?alert=CVE-2007-1894
[59] http://www.security-database.com/detail.php?alert=CVE-2007-1732
[60] http://www.security-database.com/detail.php?alert=CVE-2007-1622
[61] http://www.security-database.com/detail.php?alert=CVE-2007-1049
[62] http://www.security-database.com/detail.php?alert=CVE-2007-0106
[63] http://www.security-database.com/detail.php?alert=CVE-2007-1897
[64] http://www.security-database.com/detail.php?alert=CVE-2007-0233
[65] http://www.security-database.com/detail.php?alert=CVE-2007-0107
[66] http://www.security-database.com/detail.php?alert=CVE-2007-1599
[67] http://www.security-database.com/detail.php?alert=CVE-2007-1409
[68] http://www.security-database.com/detail.php?alert=CVE-2007-1277
[69] http://www.security-database.com/detail.php?alert=CVE-2007-1244
[70] http://www.security-database.com/detail.php?alert=CVE-2007-0541
[71] http://www.security-database.com/detail.php?alert=CVE-2007-0540
[72] http://www.security-database.com/detail.php?alert=CVE-2007-0539
[73] http://www.security-database.com/detail.php?alert=CVE-2007-0109
[74] http://secunia.com/advisories/34209/
[75] http://www.f-secure.com/vulnerabilities/SA200901234
[76] http://www.security-database.com/detail.php?alert=CVE-2006-2137
[77] http://www.security-database.com/detail.php?alert=CVE-2006-1602
[78] http://www.security-database.com/detail.php?alert=CVE-2006-6361
[79] http://www.security-database.com/detail.php?alert=CVE-2006-3737
[80] http://www.security-database.com/detail.php?alert=CVE-2004-2702
[81] http://www.security-database.com/detail.php?alert=CVE-2001-1222