

Forum:[Hack Forums](#)

Thread: [Joomla website hack](#)

RiaanN - January 15, 2019, 7:10 am

Good Day

Normally when you do a scan, one is quite happy seeing 1 or 2 vulnerabilities. So when I saw the following I was quite excited. However it did not last very long because I am still not able to get into the site.

I will give the URL to people who are interested in helping me, and in the process maybe give me a couple of pointers.

The following vulnerabilities were detected

[+] Detecting Joomla Version

[++] Joomla 1.5

[+] Core Joomla Vulnerability

[++] Joomla! 1.5 Beta 2 - 'Search' Remote Code Execution

EDB : 4212/

Joomla! 1.5 Beta1/Beta2/RC1 - SQL Injection

CVE : CVE-2007-4781

EDB : 4350/

Joomla! 1.5.x - (Token) Remote Admin Change Password

CVE : CVE-2008-3681

EDB : 6234/

Joomla! 1.5.x - Cross-Site Scripting / Information Disclosure

CVE: CVE-2011-4909

EDB : 33061/

Joomla! 1.5.x - 404 Error Page Cross-Site Scripting

EDB : 33378/

Joomla! 1.5.12 - read/exec Remote files

EDB : 11263/

Joomla! 1.5.12 - connect back Exploit

EDB : 11262/

Joomla! Plugin 'tinybrowser' 1.5.12 - Arbitrary File Upload / Code Execution (Metasploit)

CVE : CVE-2011-4908

EDB : 9926/

Joomla! 1.5 - URL Redirecting

EDB : 14722/

Joomla! 1.5.x - SQL Error Information Disclosure
EDB : 34955/

Joomla! - Spam Mail Relay
EDB : 15979/

Joomla! 1.5/1.6 - JFilterInput Cross-Site Scripting Bypass
EDB : 16091/

Joomla! < 1.7.0 - Multiple Cross-Site Scripting Vulnerabilities
EDB : 36176/

Joomla! 1.5 < 3.4.5 - Object Injection Remote Command Execution
CVE : CVE-2015-8562
EDB : 38977/

Joomla! 1.0 < 3.4.5 - Object Injection 'x-forwarded-for' Header Remote Code Execution
CVE : CVE-2015-8562 , CVE-2015-8566
EDB : 39033/

Joomla! 1.5.0 Beta - 'pcltar.php' Remote File Inclusion
CVE : CVE-2007-2199
EDB : 3781/

Joomla! Component xstandard editor 1.5.8 - Local Directory Traversal
CVE : CVE-2009-0113
EDB : 7691/

Abruptum - January 15, 2019, 10:48 am

(Jan 15, 2019 08:10 AM)RiaanN Wrote: [\[CITE\]](#) Good Day

Normally when you do a scan, one is quite happy seeing 1 or 2 vulnerabilities. So when I saw the following I was quite excited. However it did not last very long because I am still not able to get into the site.

I will give the URL to people who are interested in helping me, and in the process maybe give me a couple of pointers.

The following vulnerabilities were detected

[+] Detecting Joomla Version
[++] Joomla 1.5

[+] Core Joomla Vulnerability
[++] Joomla! 1.5 Beta 2 - 'Search' Remote Code Execution
EDB : 4212/

Joomla! 1.5 Beta1/Beta2/RC1 - SQL Injection
CVE : CVE-2007-4781
EDB : 4350/

Joomla! 1.5.x - (Token) Remote Admin Change Password

CVE : CVE-2008-3681
EDB : 6234/

Joomla! 1.5.x - Cross-Site Scripting / Information Disclosure
CVE: CVE-2011-4909
EDB : 33061/

Joomla! 1.5.x - 404 Error Page Cross-Site Scripting
EDB : 33378/

Joomla! 1.5.12 - read/exec Remote files
EDB : 11263/

Joomla! 1.5.12 - connect back Exploit
EDB : 11262/

Joomla! Plugin 'tinybrowser' 1.5.12 - Arbitrary File Upload / Code Execution (Metasploit)
CVE : CVE-2011-4908
EDB : 9926/

Joomla! 1.5 - URL Redirecting
EDB : 14722/

Joomla! 1.5.x - SQL Error Information Disclosure
EDB : 34955/

Joomla! - Spam Mail Relay
EDB : 15979/

Joomla! 1.5/1.6 - JFilterInput Cross-Site Scripting Bypass
EDB : 16091/

Joomla! < 1.7.0 - Multiple Cross-Site Scripting Vulnerabilities
EDB : 36176/

Joomla! 1.5 < 3.4.5 - Object Injection Remote Command Execution
CVE : CVE-2015-8562
EDB : 38977/

Joomla! 1.0 < 3.4.5 - Object Injection 'x-forwarded-for' Header Remote Code Execution
CVE : CVE-2015-8562 , CVE-2015-8566
EDB : 39033/

Joomla! 1.5.0 Beta - 'pcltar.php' Remote File Inclusion
CVE : CVE-2007-2199
EDB : 3781/

Joomla! Component xstandard editor 1.5.8 - Local Directory Traversal
CVE : CVE-2009-0113
EDB : 7691/

An incredible old website or an honeypot, i am sure this one is hacked allready if this is not an honeypot :D

RiaanN - January 16, 2019, 5:55 am

(Jan 15, 2019 11:48 AM)Abruptum Wrote: [\[CITE\]](#) An incredible old website or an honeypot, i am sure this one is hacked allready if this is not an honeypot :D

Old maybe, but not a honeypot that is for sure. The only reason I am having a hard time getting access is because of ModSecurity

NoTspecified - January 17, 2019, 2:10 pm

Try encoding your payloads in Hex,unicode,base64 or similar. I don't know if it will work with OS commands(I believe it should passed thru the webapp) but I have done this with SQL to defeat WAFs however newer versions of mod_sec have gotten a lot better at catching these rule bypasses with their reward program. But I agree with above post it's intentionally vulnerable or been hacked already,but I've been wrong before. Stay safe

RiaanN - January 18, 2019, 2:17 am

This is a site in South Africa - co.za domain

I know it is old, because I know the people who own the business. It is a site where you can book a SPA session, nothing fancy. And it was not hacked before.

(Jan 17, 2019 03:10 PM)NoTspecified Wrote: [\[CITE\]](#) Try encoding your payloads in Hex,unicode,base64 or similar. I don't know if it will work with OS commands(I believe it should passed thru the webapp) but I have done this with SQL to defeat WAFs however newer versions of mod_sec have gotten a lot better at catching these rule bypasses with their reward program. But I agree with above post it's intentionally vulnerable or been hacked already,but I've been wrong before. Stay safe

mircel - January 25, 2019, 5:51 am

find the joomla version and check for exploits for that version

RiaanN - January 25, 2019, 9:05 am

(Jan 25, 2019 06:51 AM)mircel Wrote: [\[CITE\]](#) find the joomla version and check for exploits for that version

Nah - Done that with the first scan. It is an old version, but with every attack (guided by the vulnerability database) I came off second best. I know the site is protected by MOD security, because I get a message about that the moment I try to do SQL injection.

My problem now is that I start to lose faith in some of the vulnerability scanners out there.

Boolie - January 25, 2019, 9:41 am

Here are some pointers.

0xF2D0C6E2

0x23C5F013

0x563FFBC0

I hope you like them.

Please gib rep ++