

Home Files News About Contact &[SERVICES_TAB]

Add New

Search .

DotNetNuke CMS 9.5.0 Cross Site Scripting

Posted Feb 24, 2020

Cross site scripting attacks can be launched against DotNetNuke CMS version 9.5.0 by uploading a malicious XML

tans | exploit xss

Related Files

Share This

LinkedIn Reddit Digg StumbleUpon Like TWO

Change Mirror Download

Exploit Title: File upload vulnerability through bypassing client-side file extension check
Date: 23 Feb 2020
Exploit Author: Sajjad Pourali
Vendor Romepage: http://dnnsoftware.com/
Software Link:
https://github.com/dnnsoftware/Dnn.Platform/releases/download/v9.5.0/DNN_Platform_9.5.0_Install.zip
Version: < 9.5
Version: < 9.5
Version: < 9.5 Version: <- 9.5 CVE : CVE-200-5166 More Info: https://medium.com/8SajjadPourali/dnn-dotnetnuke-cms-not-as-secure-as-you-think-e8516f789175

DNN allows normal users to upload XML files by using journal tools in their profile. An attacker could upload XML files which may execute malicious scripts in the user's browser.

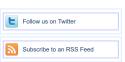
In XML, a namespace is an identifier used to distinguish between XML element names and attribute names which might be the same. One of the standard namespaces is "http://www.w3.org/1999/xhtml" which permits us to run XMTML tags such as <<cri>cript.

For instance, uploading the following code as an XML file executes javascript and shows a non-harmful 'XSS' alert.

<?xml version="1.0" encoding="UTF-8"?>
<script xmlns="http://www.w3.org/1999/xhtml">
alert('XSS');
</script>

Though stealing of authentication cookies are not possible at this time (because the authentication's cookies are set as HttpOnly by default), XSS attacks are not limited to stealing users' cookies. Using XSS vulnerability, an attacker can perform other more damaging attacks on other or high privileged users, for example, bypassing CSRF protections which allows uploading "aspx" extension files through settings page which leads to upload of backboor files.

Login or Register to add favorites





Top Authors In Last 30 Days

Red Hat 150 files	
Ubuntu 68 files	
LiquidWorm 23 files	
Debian 16 files	
malvuln 11 files	
nu11secur1ty 11 files	
Gentoo 9 files	
Google Security Research 6 files	
Julien Ahrens 4 files	
T. Weber 4 files	

File Tags File Archives December 2022 Advisory (79,754) Arbitrary (15.694) October 2022 BBS (2.859) September 2022 August 2022 Bypass (1,619) CGI (1,018) July 2022 Code Execution (6,926) June 2022 Conference (673) May 2022 April 2022 Cracker (840) CSRF (3,290) March 2022 DoS (22.602) February 2022 Encryption (2,349) January 2022 Exploit (50,359) Older File Inclusion (4,165) File Upload (946) Systems Firewall (821) AIX (426) Info Disclosure (2,660) Apple (1,926) Intrusion Detection (867) BSD (370) Java (2,899) CentOS (55) JavaScript (821) Cisco (1.917) Kernel (6,291) Debian (6,634) Local (14,201) Magazine (586) FreeBSD (1.242) Overflow (12,419) Gentoo (4.272) Perl (1.418) PHP (5.093) iOS (330) Proof of Concept (2,291) iPhone (108) Protocol (3,435) IRIX (220) Python (1.467) Juniper (67) Remote (30.044) Linux (44,315) Root (3,504) Mac OS X (684) Ruby (594) Mandriva (3.105) Scanner (1.631) Security Tool (7,777) OpenBSD (479) Shell (3,103) RedHat (12,469) Shellcode (1,204) Slackware (941)

Sniffer (886)

Solaris (1,607)

Spoof (2,166) SUSE (1,444) SQL Injection (16,102) Ubuntu (8,199) TCP (2,379) UNIX (9,159) Trojan (686) UnixWare (185) UDP (876) Windows (6,511) Virus (662) Other Vulnerability (31,136) Web (9,365) Whitepaper (3,729)



x86 (946) XSS (17,494)

Site Links About Us

News by Month History & Purpose Contact Information News Tags

Files by Month Terms of Service File Tags
File Directory Privacy Statement

Copyright Information

Hosting By Rokasec

Follow us on Twitter

