thepiyushkumarshukla / **CVE-2025-67004-disclosure.md**

Last active last month

Code Revisions 5

CVE-2025-67004-disclosure.md

CVE-2025-67004 — Directory Traversal in CouchCMS version 2.4

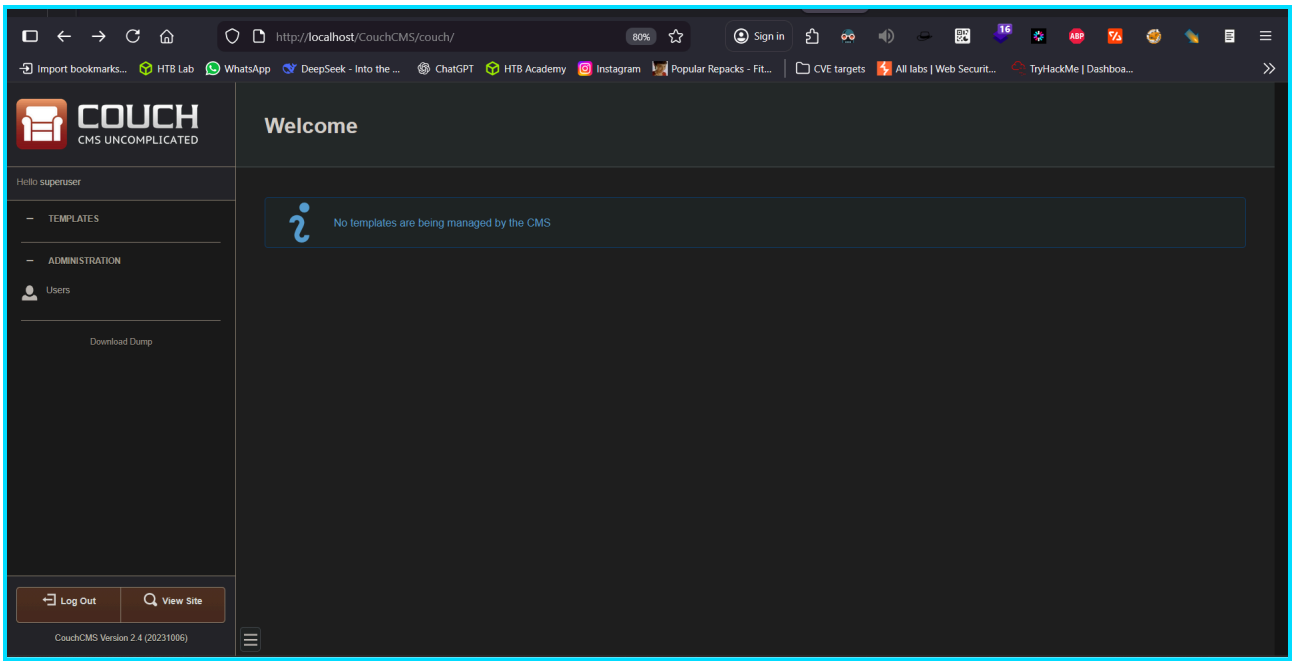
Affected product: CouchCMS 2.4

Summary:

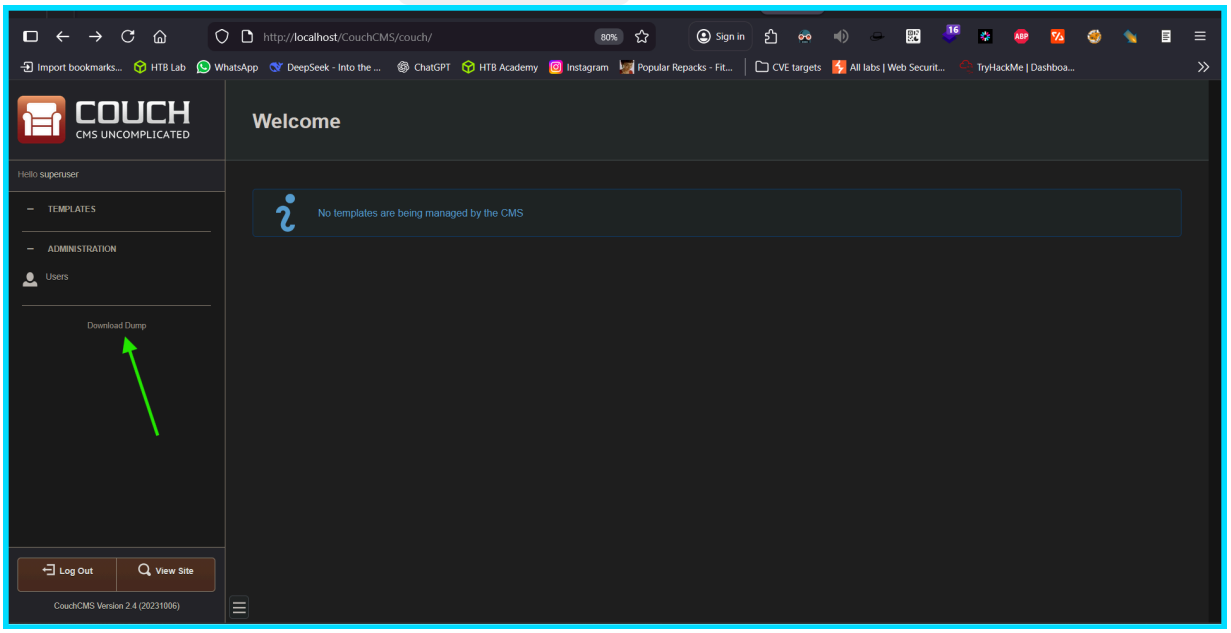
In Couch CMS 2.4, any admin user will able to read system files even outside the root directory via directory traversal (using ../../../../). Any admin user with bad intention can able to read sensitive system files via directory traversal. A Information Disclosure vulnerability in CouchCMS 2.4 allow an Admin user to read arbitrary files via traversing directories back after back. It can Disclosure the source code or any other confidential information if weaponize accordingly.

Technical details:

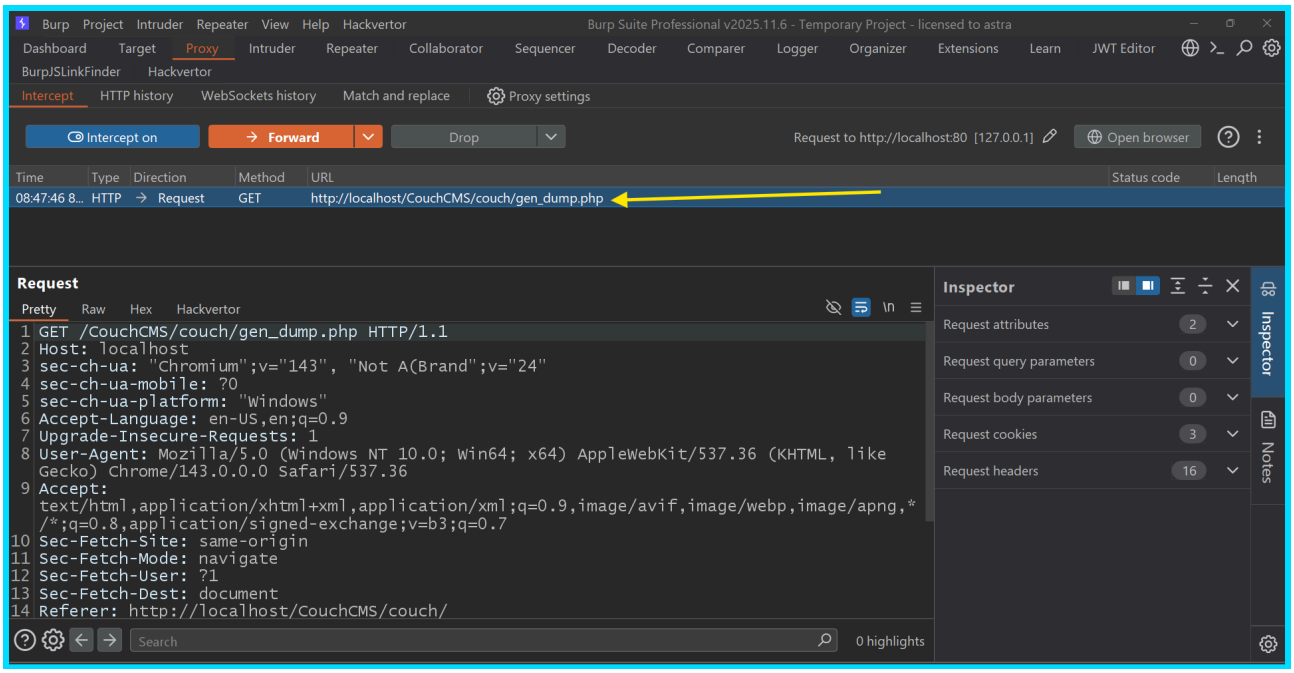
1. Fist Download and install CouchCMS 2.4 From official github
2. Log in as superuser account which you created at the time of installation !



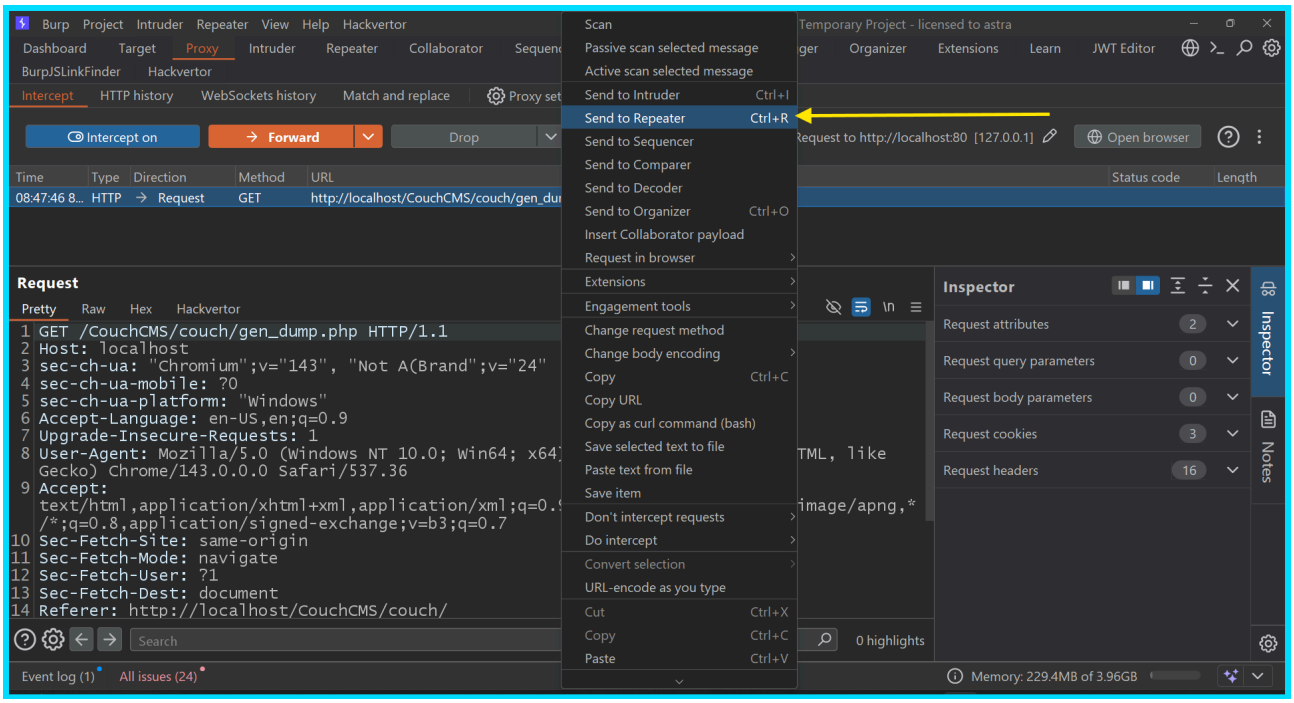
3. Now capture the request of `Download Dump` in Burp Suit

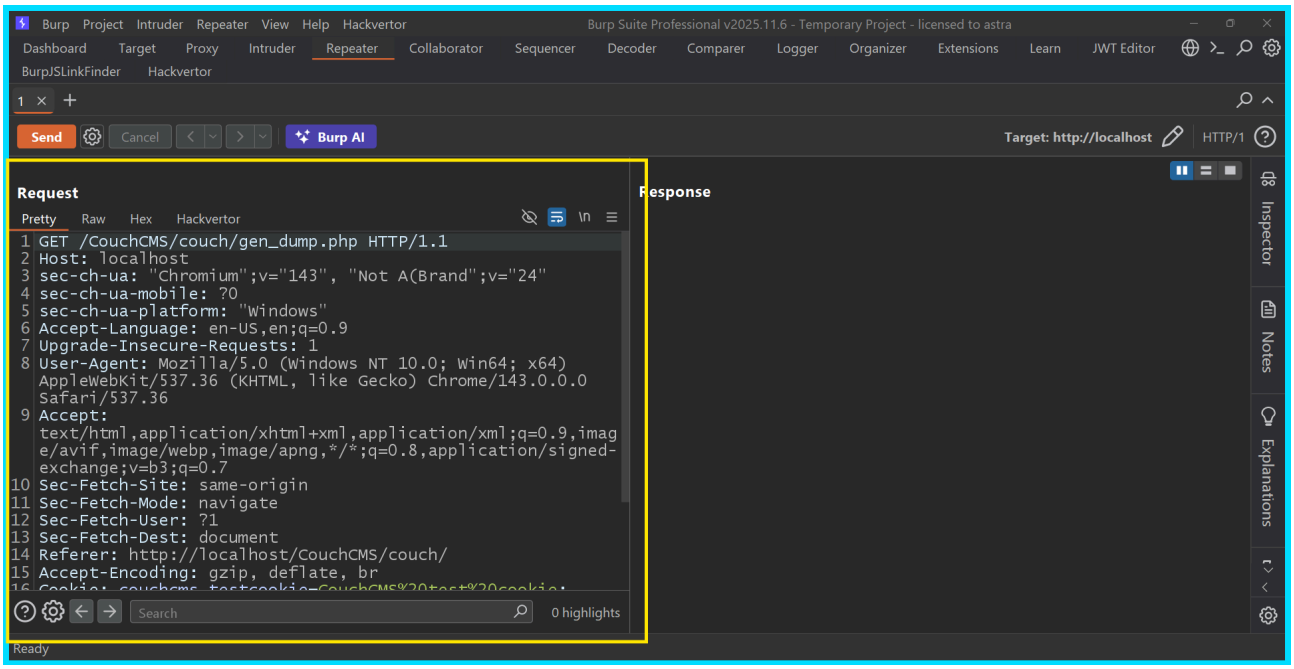


REQUEST CAPTURED :-

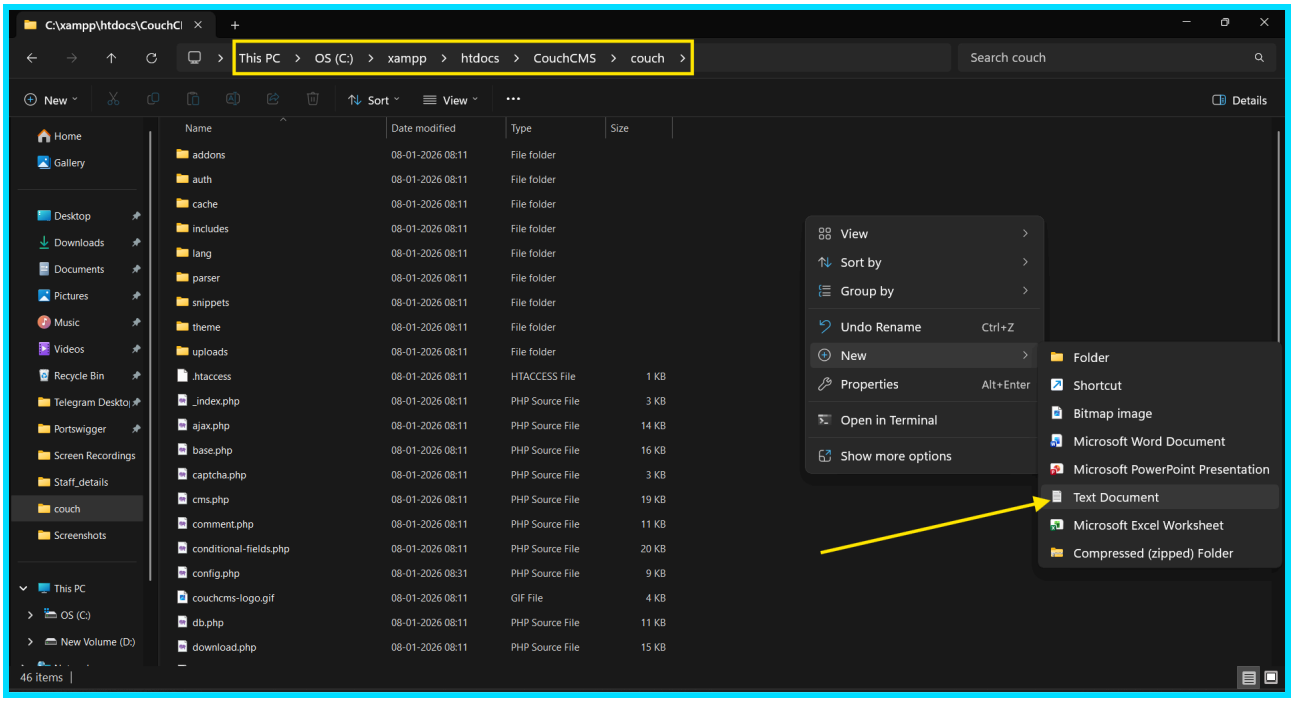


4. After capturing the request of `Download Dump` forward it to the `Repeater`

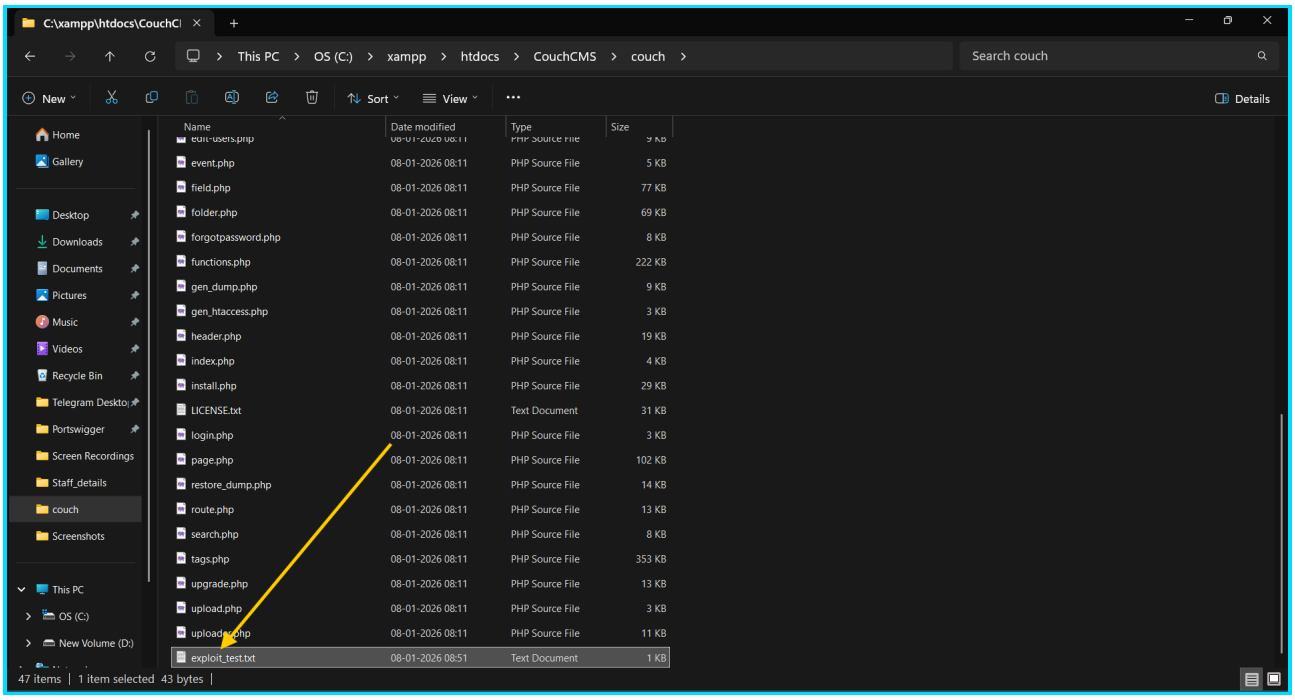




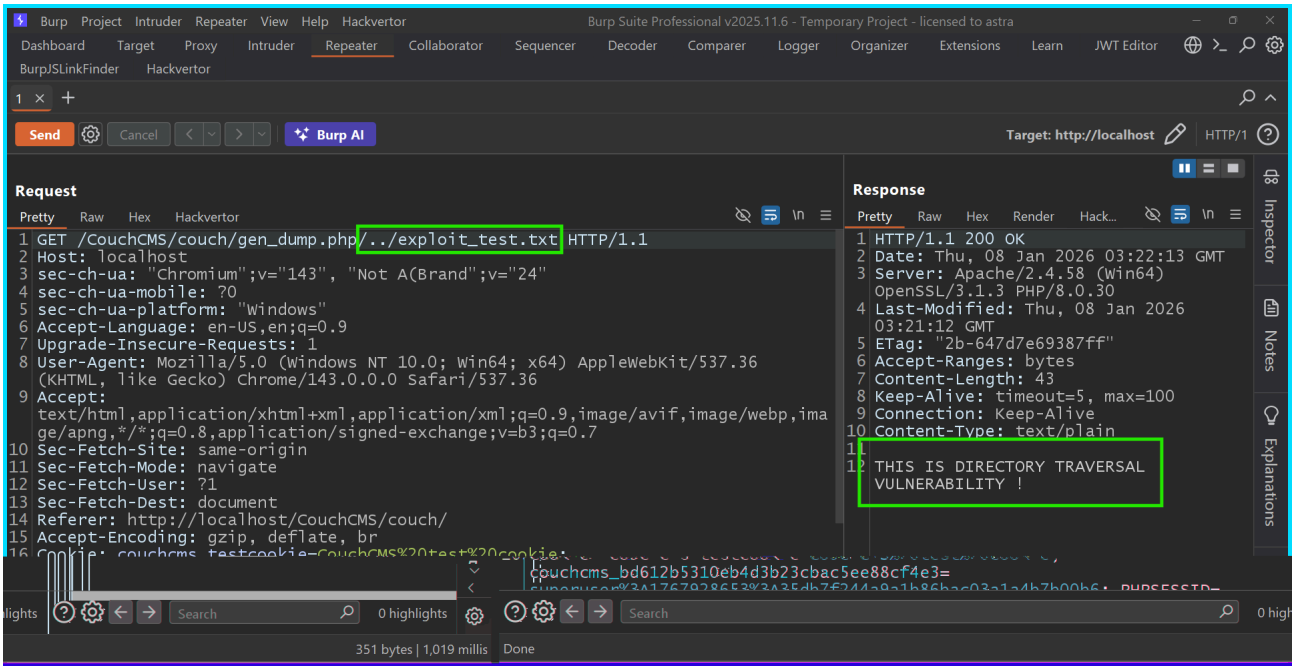
5. Now `navigate` to the couchCMS/couch folder which is root folder of the CMS and make a simple TXT file with coustom name like:- `exploit_test.txt` and write some text data into that file !



This file is made for the shake of example purpose to show how a user can access outside files by Directory Traversal



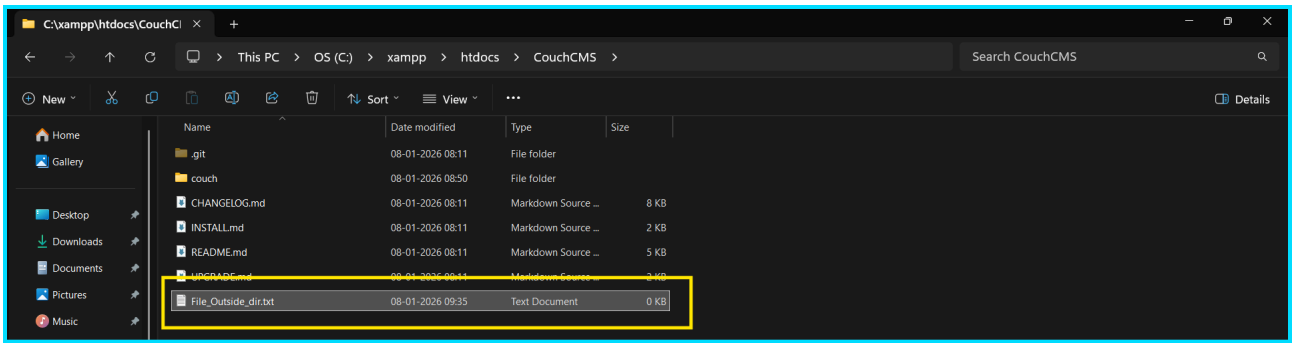
6. Now Navigate to the `Burp Repeater` and add `/../exploit_test.txt` on the path of the http request and `send` It !



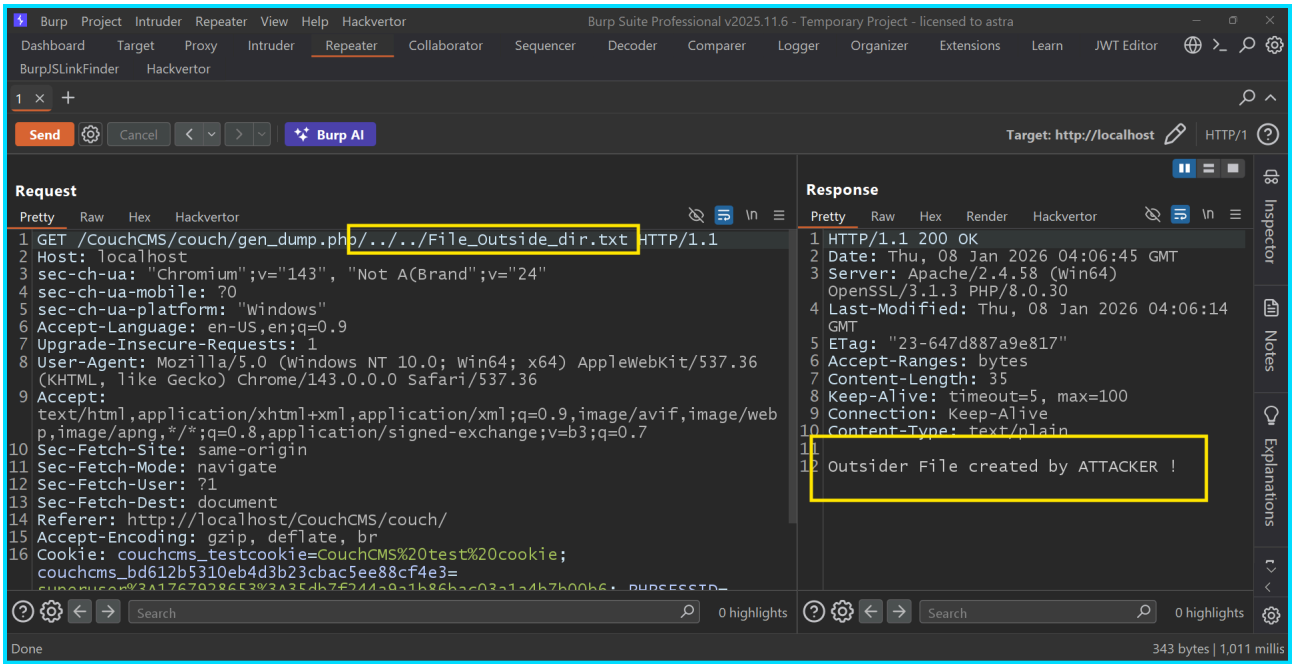
You showed up with the file data and able to read files even outside of the CouhCMS dir.

Moreover, If any the file is outside the `couch` root folder then also it can be accessed by this vulnerability. Like you seen below :-

Made a new file outside the Couch `root` folder :-



Able to accesss file with the same path traversal payload by adding one more ../



Impact:

confidentiality : High Impact

integrity : Low Impact

availability : Medium Impact

Mitigation / Fix:

Upgrade to higher version.

Timeline:

Discovery: 16 Nov 2025

CVE reserved: 07 Jan 2026

Public disclosure: 9 Jan 2026

Credits:

Reported by: Piyush Kumar Shukla

Contact:

piyushbusiness29@gmail.com

Comments are disabled for this gist.