Vulnerability analysis

The darkpoetry application accepts titled poems uploaded by users. It saves the title on a SQL database and the content of the poem in a txt file inside the folder /poems/[poemtitle]/. If the poem title is new (i.e., not present in the database), the server creates the corresponding folder. Otherwise, it uses the existing folder and adds or overwrites a new txt file inside suh a folder. The client can also see all the uploaded poems through the page "poems.php". The flag is inside a "file.txt" file inside a folder /flag/. The browser is not allowed to download the flag directly. It is possible to insert javascript code in the txt file containing the poem, thus realizing a stored XSS. However, this attack does not allow the attacker to capture the flag.

In order to capture the flag, the attacker must exploit a path traversal vulnerability on the title of the poem. It is possible to do that since the poem title is not checked to contain dangerous characters, such as "." or "/", and the folder name is not checked to effectively be a subfolder of /poems/. We can test this by uploading a poem titled "testpoem" and another one titled "../poems/testpoem", and checking that they are considered parts of the same poem by the server.