Dodatni zadatak – SV70/2020

Uvod

Cilj ovog projekta bio je da se podigne server sa ranjivom web aplikacijom, a zatim istraži i eksploatiše ranjivost. U okviru ovog zadatka, odlučila sam se za ranjivost pod oznakom CVE-2007-4559, koristeći Python.

Koraci

Napravila sam Flask server koji omogućava otpremanje tar fajlova i ekstrakciju istih, koji ima 3 osnovna endpointa:

- Ruta "/" – početna stranica, prikazuje jednostavnu HTML formu za otpremanje fajlova.
- Ruta "/upload" – prihvata otpremljeni tar fajl, čuva ga na serveru i vrši ekstrakciju.
- Ruta "/uploads/<filename>" – omogućava prikaz otpremljenog fajla.

app.py

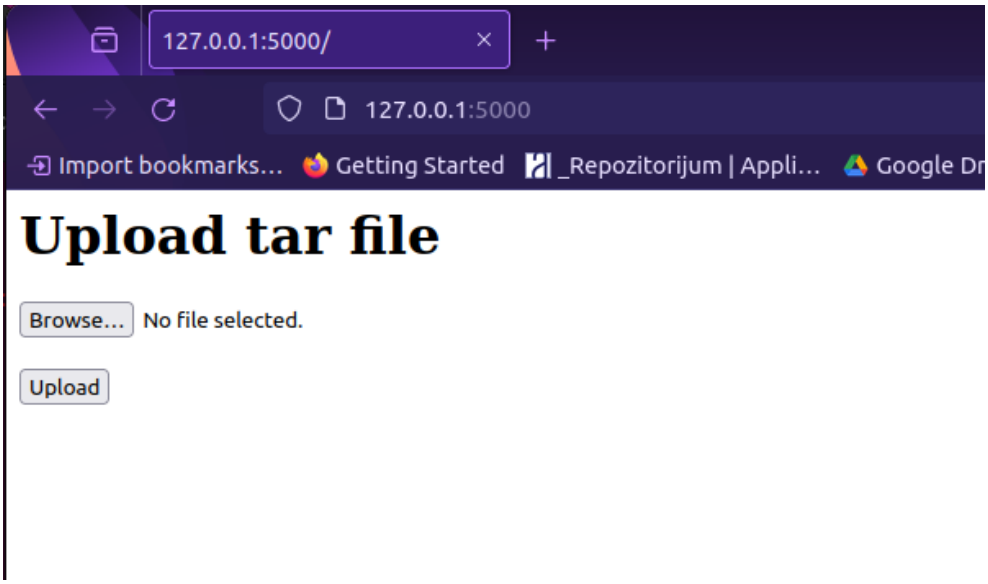
app.py > upload

```python
from flask import Flask, request, send_file
import tarfile
import os

app = Flask(__name__)

UPLOAD_FOLDER = './uploads'
if not os.path.exists(UPLOAD_FOLDER):
    os.makedirs(UPLOAD_FOLDER)

@app.route('/')
def home():
    return '''
        <html><body>
        <h1>Upload tar file</h1>
        <form action="/upload" method="post" enctype="multipart/form-data">
            <input type="file" name="file"><br><br>
            <input type="submit" value="Upload">
        </form>
        </body></html>
    '''

@app.route('/upload', methods=['POST'])
def upload():
    if 'file' not in request.files:
        return 'No file part'
    file = request.files['file']
    if file.filename == '':
        return 'No selected file'
    filepath = os.path.join(UPLOAD_FOLDER, file.filename)
    file.save(filepath)
    with tarfile.open(filepath) as tar:
        tar.extractall(path=UPLOAD_FOLDER)  # CVE-2007-4559
    return 'File uploaded and extracted successfully'

@app.route('/uploads/<filename>')
def get_uploaded_file(filename):
    file_path = os.path.join(UPLOAD_FOLDER, filename)
    if not os.path.exists(file_path):
        return 'File not found', 404
    return send_file(file_path, mimetype='text/plain')

if __name__ == '__main__':
    app.run(debug=True)

```

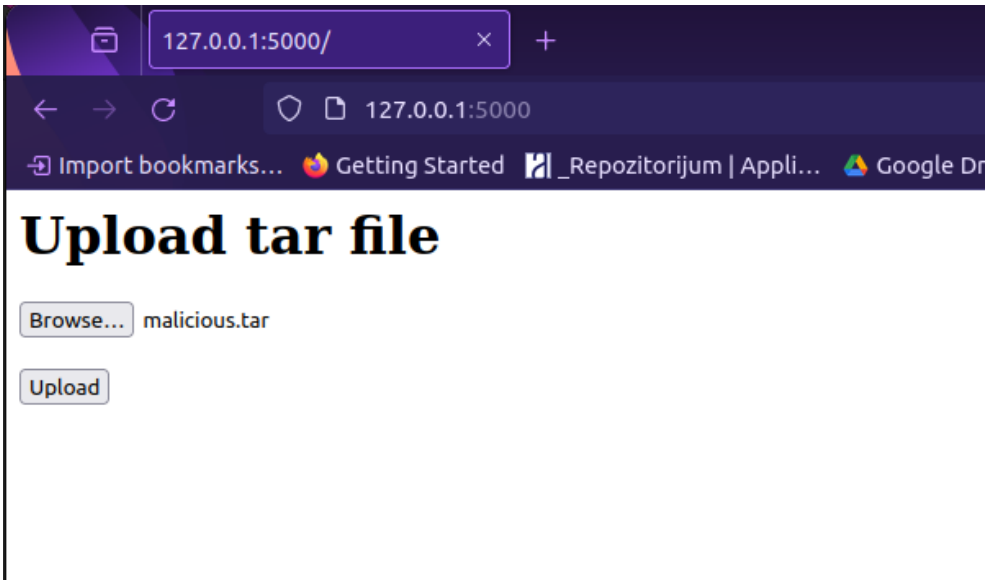
Podigla sam server:

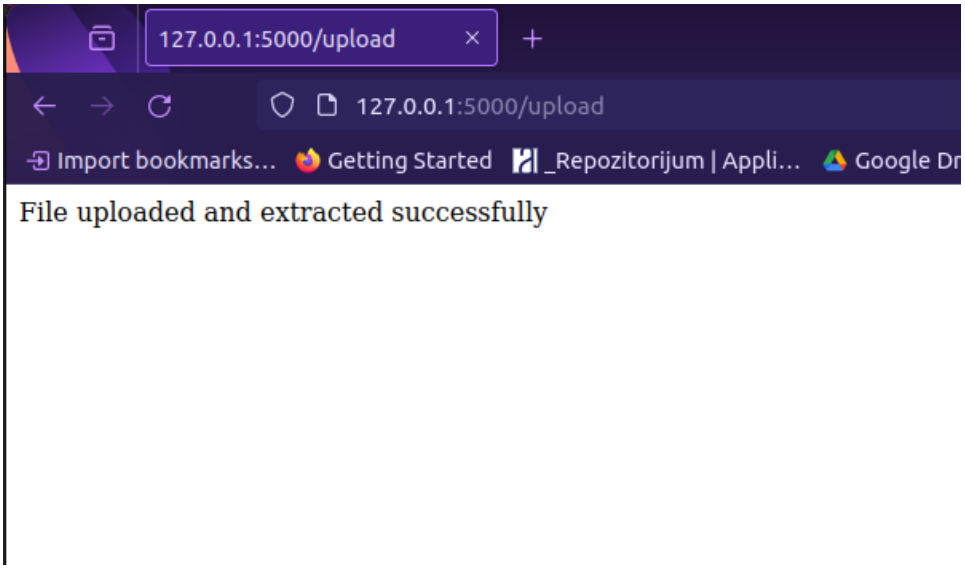
```
(venv) computer@computer-IdeaPad-3-15ITL6:~/Desktop/vulnerable_app$ python app.py
 * Serving Flask app 'app'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a product
ion WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 699-322-381
```

Pristupila http://127.0.0.1:5000



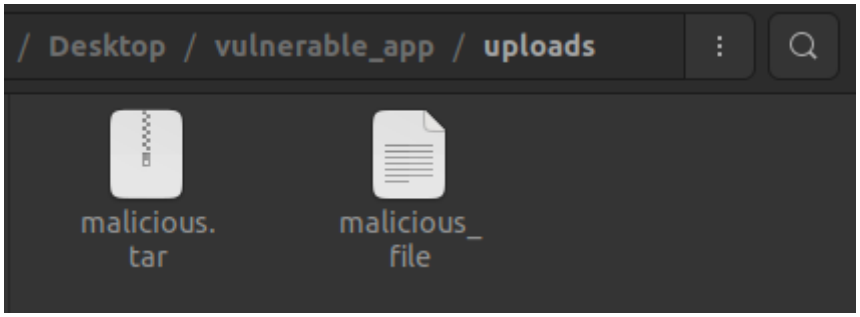
Kreirala jedan malicious_file i napravila od njega tar, pa ga uploadovala u formi.



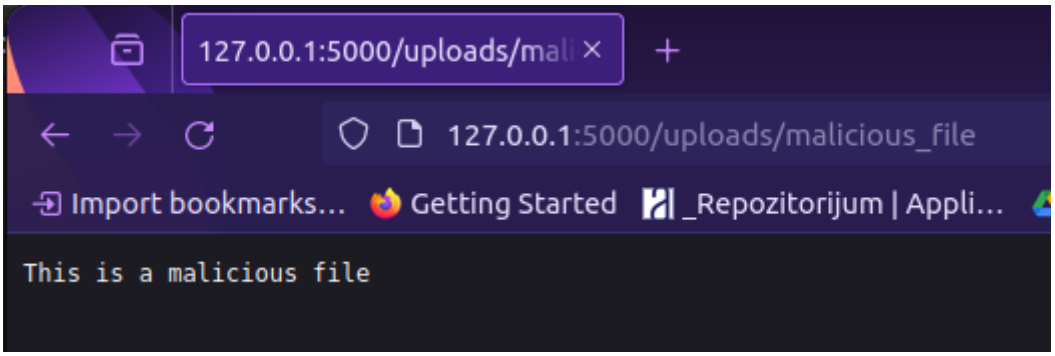


Zatim sledi provera da li je ekstrahovan.

Unutar fajl sistema:



Pomoću endpointa:



Zaključak

Kroz ovaj projekat, uspešno sam razvila Flask aplikaciju koja omogućava korisnicima da otpreme tar fajlove putem web interfejsa, a zatim vrši ekstrakciju istih na serveru. Istraživanje i eksploatacija ranjivosti CVE-2007-4559 dodatno su demonstrirali važnost implementacije sigurnosnih mehanizama u web aplikacijama. Ovaj projekat mi pružio je uvid u proces razvoja i testiranja web aplikacija, kao i identifikaciju potencijalnih sigurnosnih rizika i načina zaštite od istih.