247CTF – Secured Session

247CTF - Dashboard | https://63dcfe4084f2fec6.247ctf.c | https://63dcfe4084f2fec6.247ctf.c

63dcfe4084f2fec6.247ctf.com

Men Tactical Militar... | PinkDraconian - Yo... | swisskyrepo/Payloa... | XSS Filter Evasion -... | Input events | How

```
import os
from flask import Flask, request, session
from flag import flag

app = Flask(__name__)
app.config['SECRET_KEY'] = os.urandom(24)

def secret_key_to_int(s):
    try:
        secret_key = int(s)
    except ValueError:
        secret_key = 0
    return secret_key

@app.route("/flag")
def index():
    secret_key = secret_key_to_int(request.args['secret_key']) if 'secret_key' in request.args else None
    session['flag'] = flag
    if secret_key == app.config['SECRET_KEY']:
      return session['flag']
    else:
      return "Incorrect secret key!"

@app.route('/')
def source():
    return "

%s

" % open(__file__).read()

if __name__ == "__main__":
    app.run()
```

לאחר כניסה לאתר הדף מציג לנו את הקוד של האתר, באותו רגע הבנו שמדובר באתר שרץ על flask
ואנחנו רואים שיש לו דף בflag/ לאחר מכן הבחנו שהדגל נשמר ב Session['flag'] אז הלכנו לבדוק מה יש שם:

Name	Value
session	eyJmbGFnIjp7IiBiIjoiTWpRM1ExUkdlMlJoT0RBM09UVm1PR0UxWTJGaU1tVXdN...

מצאנו Cookie שנראה כאילו הוא מכיל Base64 אז ניסינו לראות ב Cyber Chef לראות מה נקבל:

lines: 2

```
eyJmbGFnIjp7IiBiIjoiTWpRM1ExUkdlMlJoT0RBM09UVm1PR0UxWTJGaU1tVXdNemRrTnpNNE5UZ3dOMkk1WVRreGZRPT0ifX0
MjQ3Q1RGe2RhODA3OTVmOGE1Y2FiMmUwMzdkNzM4NTgwN2I5YTkxfQ==
```

Output

start: 75 end: 115 length: 40 | time: 1ms length: 115 lines: 2

```
{"flag":{" b":"MjQ3Q1RGe2RhODA3OTVmOGE1Y2FiMmUwMzdkNzM4NTgwN2I5YTkxfQ=="}}
247CTF{da80795f8a5cab2e037d7385807b9a91}
```

בהתחלה מצאנו Json של Flag ב-Base64 ולאחר פיענוח את הדגל.