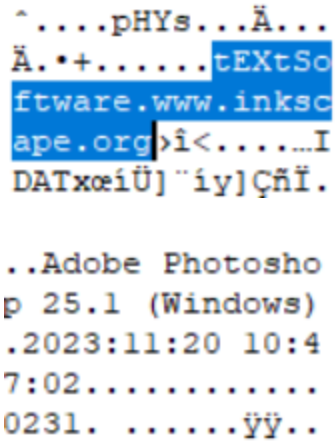
Python Executor

태그	웹해킹
상태	진행 중

```python
from flask import Flask, request
import os, subprocess, string


app = Flask(__name__)
app.config["SECRET_KEY"] = os.urandom(32)



@app.route("/",methods=["GET"])
def index():
    base_command = ["python"]
    file = list(request.args.keys())

    bannlist = []
    for i in string.ascii_lowercase:
        bannlist += ["-"+i+" "]


    base_command += file
    base_command[1] += ".py"

    My_Injection_filter = ['$','{','}','|','&',';','₩n','!','?','=','*','`',',','"','flag','system']+bannlist

    for i in My_Injection_filter:
        if i in ' '.join(base_command):
            return "NOPE! XD"+i, 500

    if not os.path.exists(base_command[1]):
        return "?", 404

    res = subprocess.run(base_command,capture_output=True,text=True)

    return res.stdout[:5]

app.run(host="0.0.0.0", port=9999)
```

우선 app.py

버프 스위트를 써볼까? 사실 이쪽 관련해 아는 툴이 그것밖에 없음.



차례로 플래그/탕후루 이미지 속 스트림.

```
async function buy_realitem(item){
    var res =  await fetch(`/api/buy/${item}/1`, {
        method: "GET",
    })

    return await res.json();
}

async function buy_item(item){
    var res =  await fetch(`/buy/${item}/1`, {
        method: "GET",
    })

    var j_res = await res.json()

    if (j_res.result == 1){
        var p = await buy_realitem(item);
        var j_p = p;

        if(j_p.result == 1){
            alert("SUCCESS!");
            location.href="/";
        }else{
            alert(j_res.result);
        location.href="/";
        }


    }else{
        alert(j_res.result);
        location.href="/";
    }
```

동봉된 js 코드.

탕후루와 플래그를 “buy”하는 시스템인 것 같다.

Login

guest

PASSWORD login

Registration

{% endblock %}

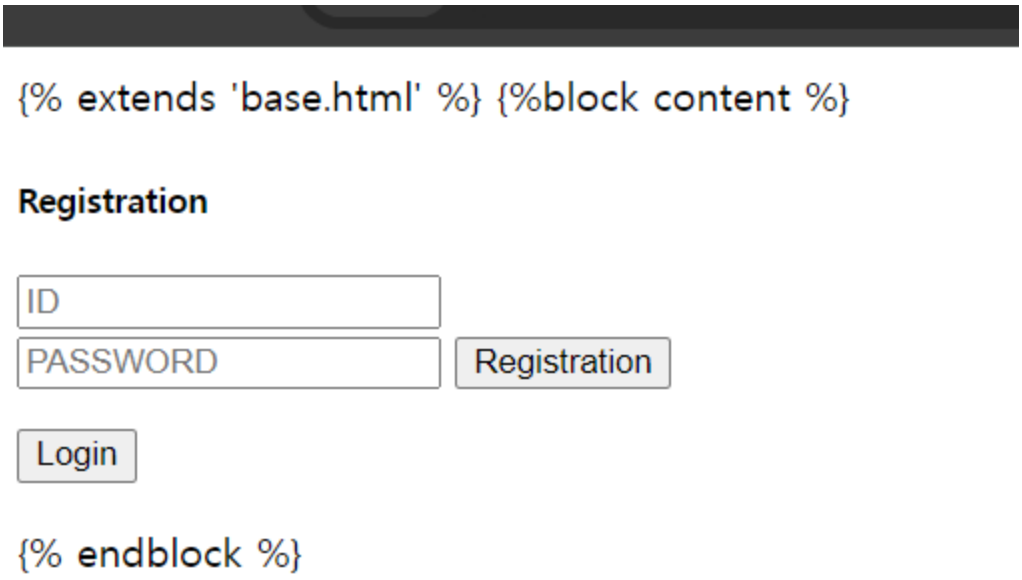
로그인 화면.

어떤 값을 입력하건 오류 페이지 출력.

```
<h3 class="card-title">Login</h3>
<p class="card-text">
  <form action="/login" method="POST">
      <input type="text" class="form-control mb-3" name="user_id" placeholder="ID" id="id">
      <input type="password" class="form-control mb-1" name="user_pw" placeholder="PASSWORD" id="pw">

      <input type="submit" id="go" class="btn btn-primary float-end" value="login">
  </form>
  <button class="btn btn-primary float-end me-1" onclick="location.href='/regis'">Registration</button>
</p>
```

페이지 소스 코드. input값이 어느 클래스로 향하는지 표기되어 있다.

버튼 onclick이 향한다는 regis 페이지




```
<div class= card-body p-lu >
  <h5 class="card-title">Registration</h5>
  <p class="card-text">
    <form action="/regis" method="POST">
        <input type="text" class="form-control mb-3" name="user_id" placeholder="ID" id="id">
        <input type="password" class="form-control mb-1" name="user_pw" placeholder="PASSWORD" id="pw">

        <input type="submit" id="go" class="btn btn-primary float-end" value="Registration">
    </form>
    <button class="btn btn-primary float-end me-1" onclick="location.href='/login'">Login</button>
  </p>
</div>
</div>
```

페이지/코드 모두 큰 차이점은 없다.

인덱스.

{% extends 'base.html' %} {%block conte


Strawberry Tanghuru

BUY


FLAG

BUY
{% endblock %}

이미지 소스가 같은 상위폴더에 속해 있는데 왜 로딩이 안 되는걸까? 코드의 결함일지도 모르겠다. 아무튼 BUY를 클릭해도 변화는 없다. 코드를 수정해서 이 페이지를 기능하게 하는 게 해법일지도.