

## <Python executors - web>

파일을 다운 받고 압축을 풀어봤다.

 src		2024-07-21 오후 4:26	파일 폴더	
 docker-compose		2024-07-05 오후 3:01	Yaml 원본 파일	1KB
 Dockerfile		2024-07-19 오후 4:19	파일	1KB

src 파일을 들어가봤다.

 static		2024-07-21 오후 4:26	파일 폴더	
 templates		2024-07-21 오후 4:26	파일 폴더	
 app		2024-07-21 오후 4:25	Python 원본 파일	1KB

다른 web 문제에서도 static이랑 template 폴더가 있었던 것 같다.

먼저 static 폴더에 들어가봤다.



 common



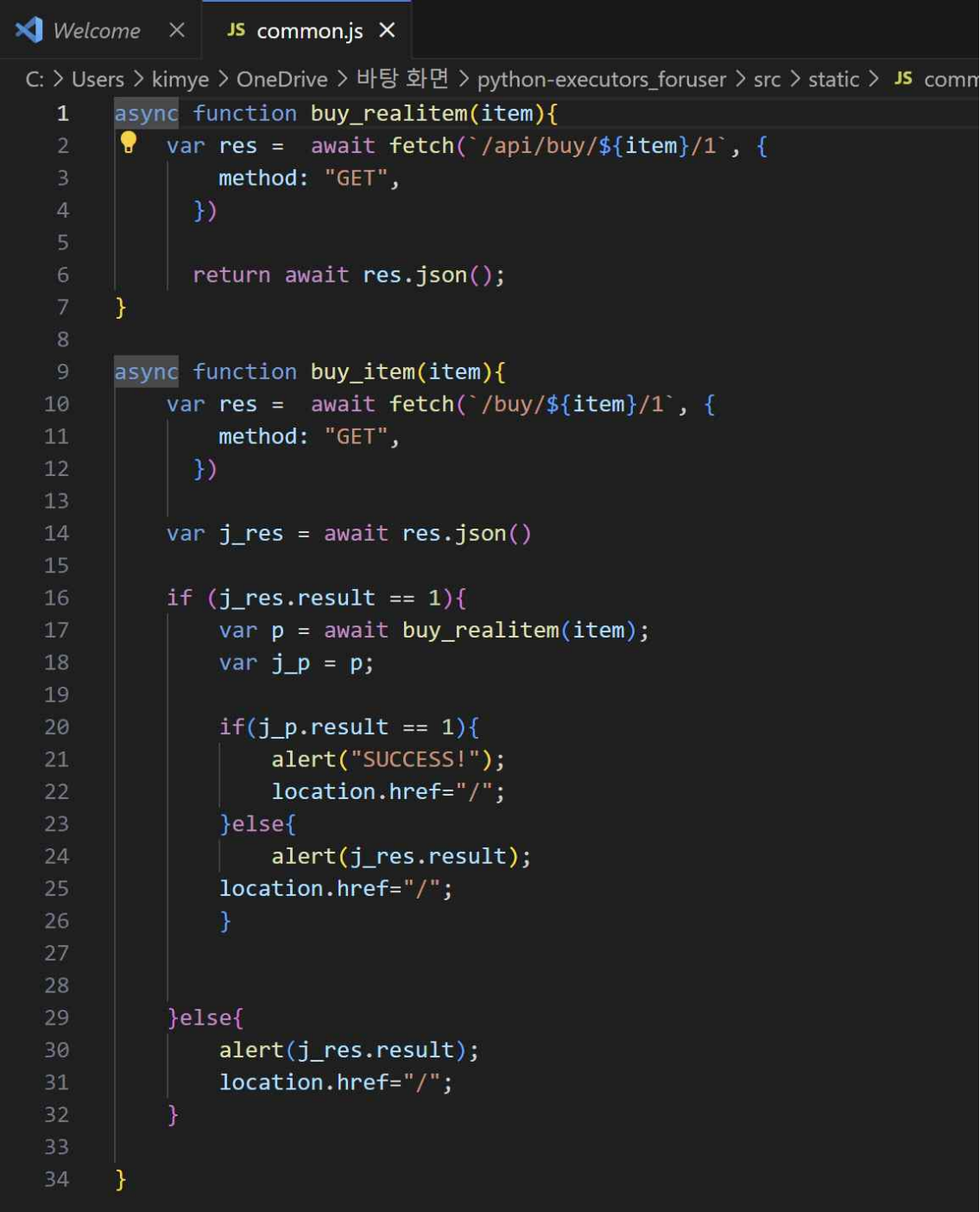
 flag



 tanghuru

이렇게 3개의 사진이 존재했다.

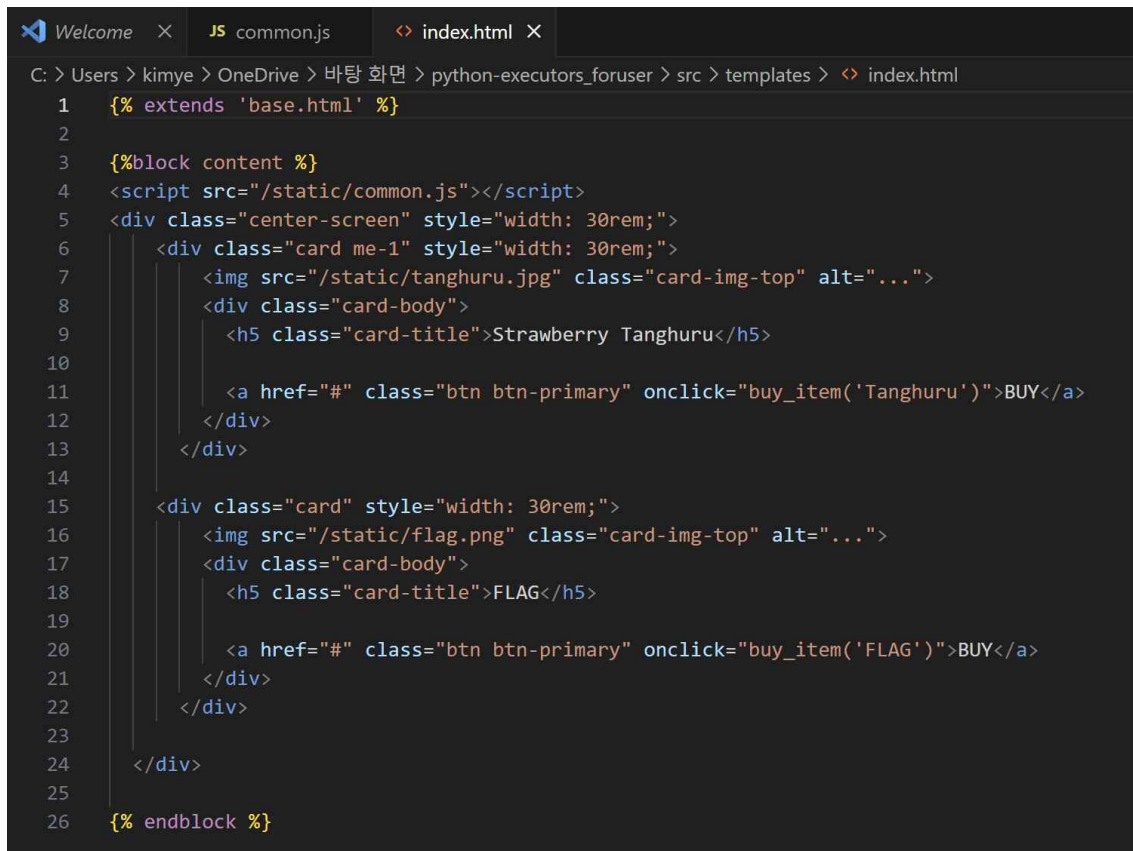
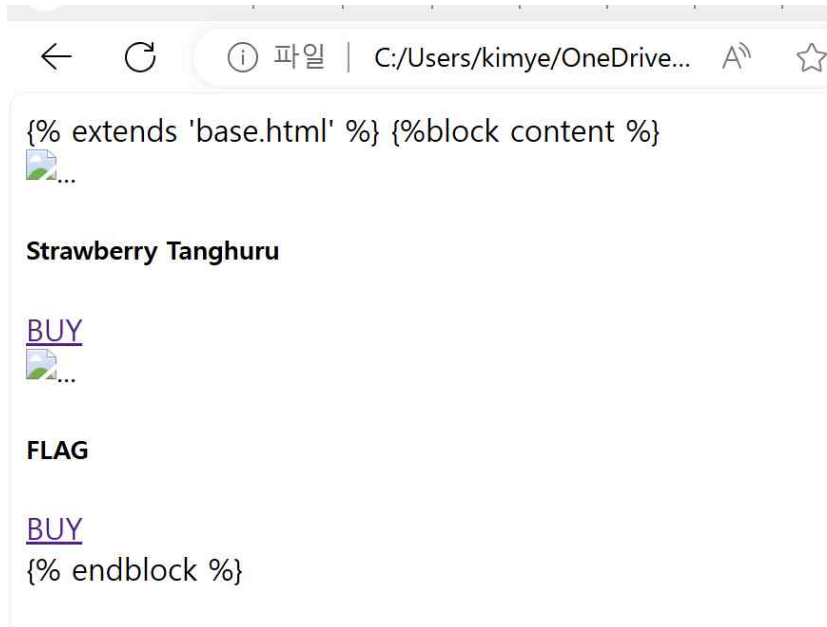
먼저 common 파일을 visual code로 열어 봤는데 자바 스크립트인 것 같았다.



```
1  async function buy_realitem(item){
2      var res = await fetch(`/api/buy/${item}/1`, {
3          method: "GET",
4      })
5
6      return await res.json();
7  }
8
9  async function buy_item(item){
10     var res = await fetch(`/buy/${item}/1`, {
11         method: "GET",
12     })
13
14     var j_res = await res.json()
15
16     if (j_res.result == 1){
17         var p = await buy_realitem(item);
18         var j_p = p;
19
20         if(j_p.result == 1){
21             alert("SUCCESS!");
22             location.href="/";
23         }else{
24             alert(j_res.result);
25             location.href="/";
26         }
27
28     }else{
29         alert(j_res.result);
30         location.href="/";
31     }
32 }
33
34 }
```

flag 사진이랑 tanghuru 사진은 왜 들어있는지 잘 모르겠다. 웹 문제에서 이미 포렌식을 할 것 같지는 않다고 생각했다.

index 파일에 정보들이 들어있었던 것 같아서 index를 웹으로 열어본 뒤 해당 웹을 visual code로 열어 보았다.



잘 모르겠지만 중간에 strawberry tanghuru라고 적혀 있는 걸 보니까 사진이 무의미 한 것 같지는 않다고 생각했다.

login 웹을 열어보니 로그인 창이 뜬다.

```
{% extends 'base.html' %} {%block content %}
```

**Login**

```
{% endblock %}
```

html 코드에 아이디와 비번이 숨겨져 있지는 않을까 해서 마찬가지로 visual code로 열어보았다.

```
C: > Users > kimye > OneDrive > 바탕 화면 > python-executors_foruser > src > templates > login.html
1  {% extends 'base.html' %}
2
3  {%block content %}
4  <div class="center-screen card" style="width: 18rem;">
5      <div class="card-body p-10">
6          <h5 class="card-title">Login</h5>
7          <p class="card-text">
8              <form action="/login" method="POST">
9                  <input type="text" class="form-control mb-3" name="user_id" placeholder="ID" id="id">
10                 <input type="password" class="form-control mb-1" name="user_pw" placeholder="PASSWORD" id="pw">
11
12                 <input type="submit" id="go" class="btn btn-primary float-end" value="login">
13             </form>
14             <button class="btn btn-primary float-end me-1" onclick="location.href='/regis'">Registration</button>
15         </p>
16     </div>
17 </div>
18
19 {% endblock %}
```

별다른 정보가 보이지는 않는다.

app.py 파일을 열어서 파이썬 코드를 보니 flag 형식이 나와 있는 것 같다.

```
C: > Users > kimye > OneDrive > 바탕 화면 > python-executors_foruser > src > app.py > ...
1  from flask import Flask, request
2  import os, subprocess, string
3
4
5  app = Flask(__name__)
6  app.config["SECRET_KEY"] = os.urandom(32)
7
8
9
10 @app.route("/", methods=["GET"])
11 def index():
12     base_command = ["python"]
13     file = list(request.args.keys())
14
15     bannlist = []
16     for i in string.ascii_lowercase:
17         bannlist += ["-"+i+" "]
18
19
20     base_command += file
21     base_command[1] += ".py"
22
23     My_Injection_filter = ['$','{','}','|','&',';','\n','!','?','=','*','(',')','(',')','(',')','flag','system']+bannlist
24
25     for i in My_Injection_filter:
26         if i in ' '.join(base_command):
27             return "NOPE! XD"+i, 500
28
29     if not os.path.exists(base_command[1]):
30         return "?", 404
31
32     res = subprocess.run(base_command, capture_output=True, text=True)
33
34     return res.stdout[:5]
35
36 app.run(host="0.0.0.0", port=9999)
```

웹 문제는 html 코드를 수정해서 숨겨진 정보를 찾아내는 건가 싶기도 한데, 아직은 잘 모르겠다. 다른 사람들의 라이터업을 보고 완전한 풀이를 보면 조금 감을 잡을 수 있을까?