

<Forgot password? - web>

일단 파일을 다운 받고 압축을 풀어보았다.

✓ deploy	🔄	2024-07-24 오후 11:11	파일 폴더	
📄 Dockerfile	🔄	2024-07-24 오후 11:10	파일	1KB

deploy 폴더를 들어가봤다. app이랑 config는 파이썬 코드인 것 같다.

📁 static	🔄	2024-07-18 오후 12:40	파일 폴더	
📁 templates	🔄	2024-07-24 오후 2:43	파일 폴더	
📄 app	🔄	2024-07-24 오후 11:05	Python File	8KB
📄 config	🔄	2024-07-24 오후 11:25	Python File	1KB
📄 requirements	🔄	2024-07-24 오후 10:12	텍스트 문서	1KB

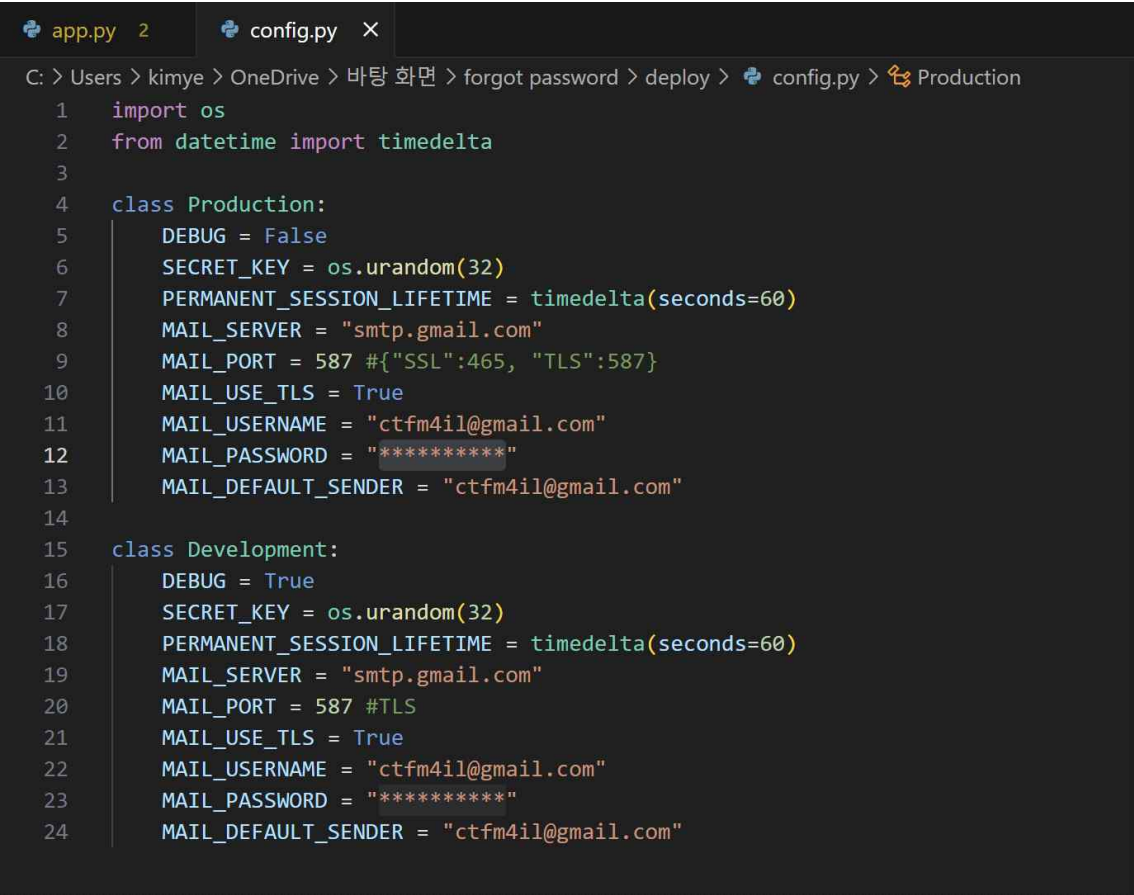
app 파일을 visual code로 열어보았다.

```
@app.route("/")
def flag_page(FLAGS="3S{FAKE FLAG}"):
    if "user" in session:
        if session["user"] == "admin@3sctf.admin.com":
            FLAG=os.getenv("FLAG")
            return render_template("flag.html", FLAG=FLAG)
        else:
            return redirect("/login")

if __name__=="__main__":
    app.run(host="0.0.0.0", port=5555, debug=True)
```

단축키로 flag 단어를 찾아보니 일치하는 결과가 있다고 해서 살짝 기대했다. 근데 자세히 보니 FAKE라고 적혀 있어서 실망스러웠다.


config 파일도 동일하게 visual studio로 들어가봤다.



```
app.py 2 config.py X
C: > Users > kimye > OneDrive > 바탕 화면 > forgot password > deploy > config.py > Production
1 import os
2 from datetime import timedelta
3
4 class Production:
5     DEBUG = False
6     SECRET_KEY = os.urandom(32)
7     PERMANENT_SESSION_LIFETIME = timedelta(seconds=60)
8     MAIL_SERVER = "smtp.gmail.com"
9     MAIL_PORT = 587 #{ "SSL":465, "TLS":587}
10    MAIL_USE_TLS = True
11    MAIL_USERNAME = "ctfm4il@gmail.com"
12    MAIL_PASSWORD = "*****"
13    MAIL_DEFAULT_SENDER = "ctfm4il@gmail.com"
14
15 class Development:
16     DEBUG = True
17     SECRET_KEY = os.urandom(32)
18     PERMANENT_SESSION_LIFETIME = timedelta(seconds=60)
19     MAIL_SERVER = "smtp.gmail.com"
20     MAIL_PORT = 587 #TLS
21     MAIL_USE_TLS = True
22     MAIL_USERNAME = "ctfm4il@gmail.com"
23     MAIL_PASSWORD = "*****"
24     MAIL_DEFAULT_SENDER = "ctfm4il@gmail.com"
```

자세히 보니까 로그인 이메일과 비밀번호가 있다. 로그인 창에 입력해볼까 싶은 생각이 들었다.

template 폴더를 들어가봤다. Html 코드를 분석하기 위해 visual code로 열어보고자 한다.

	base		2024-07-24 오후 10:33	Microsoft Edge HTM...	1KB
	flag		2024-07-24 오후 10:33	Microsoft Edge HTM...	1KB
	login		2024-07-24 오후 10:33	Microsoft Edge HTM...	2KB
	register		2024-07-24 오후 10:34	Microsoft Edge HTM...	2KB
	reset_password		2024-07-24 오후 10:34	Microsoft Edge HTM...	2KB

우선 위에서 찾았던 로그인 아이디와 비번을 login 창에 입력해보았다.

← ↻ ⓘ 파일 | C:/Users/kimye/OneDrive/바탕%20화면/forgot%20password/deploy/templates/login.html

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

Login

[Forgot Password?](#)

```
{% with messages = get_flashed_messages() %} {% if messages %}
```

{{messages[0]}}

```
{% endif %} {% endwith %}
```

Not a member? [Sign Up](#)

```
{% endblock %}
```

아무런 변화가 일어나지 않았다. 이건 아닌가 보다.

flag 웹을 visual code로 열어서 html 코드를 보려고 한다.

```
app.py 2  config.py  flag.html X
C: > Users > kimye > OneDrive > 바탕 화면 > forgot password > deploy > templates > <> flag.html > ...
1  {% extends 'base.html' %}
2  {% block content %}
3
4  <h1>FLAG</h1>
5  <div class="content">
6      <div class="input-field">
7          <p>{{ FLAG }}</p>
8          <p></p>
9      </div>
10 </div>
11 <div class="btn-box">
12     <input type="button" value="Log out" onclick="logout()">
13 </div>
14
15 <script>
16     function logout(){
17         location.href="/logout";
18     }
19 </script>
20
21 {% endblock %}
22
```

아무런 의미가 없는 것 같다.