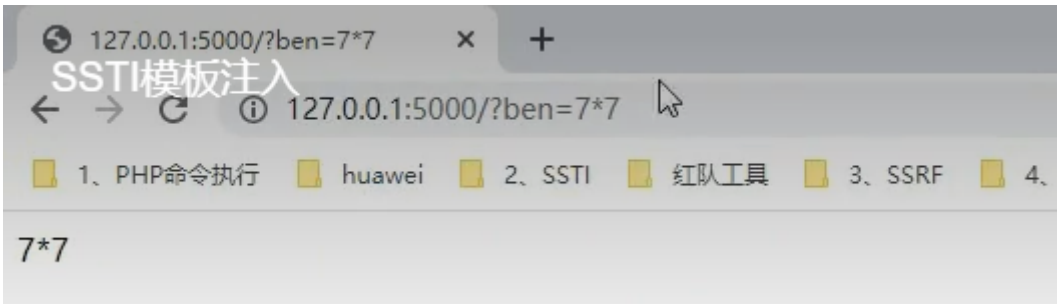
模版注入漏洞介绍

感觉ssti漏洞和sql注入和xss漏洞也是大同小异

.

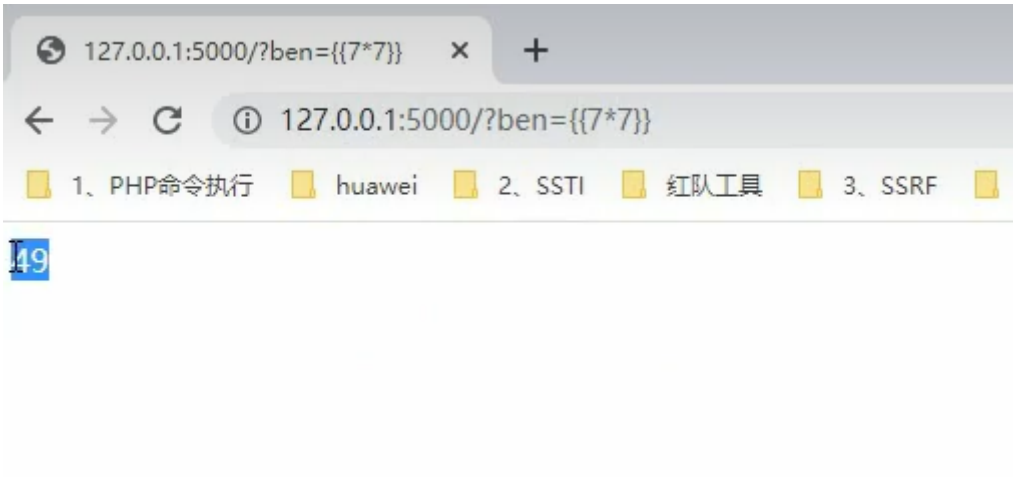
这里的str只会被输出在页面上而不会执行自己本身的意思

本来应该是输出49的，但是因为被预先渲染转义了。就会直接输出而不是渲染执行



这样的话就可能存在漏洞，我们稍微修改一下代码

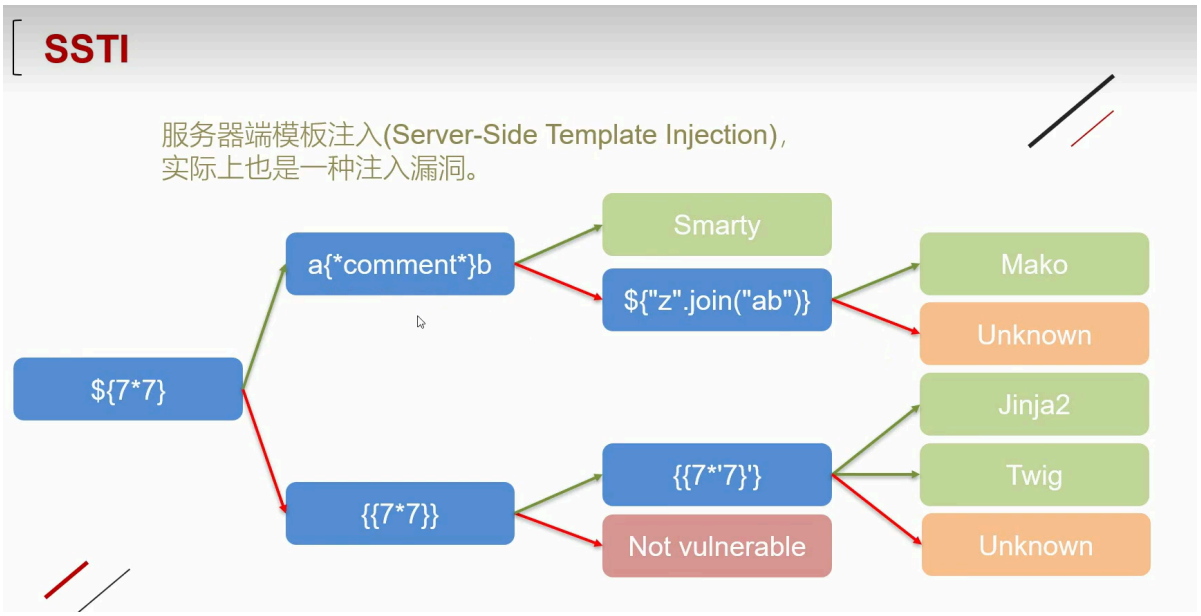
原来的str是会先通过render_template_string 进行转义后再填充到body中间，但是经过代码修改以后会直接被format函数填充到body中间，此时render_template_string函数就会将str当做代码渲染执行(说白点就是后面的代码中str没有预先被渲染转义再输出)



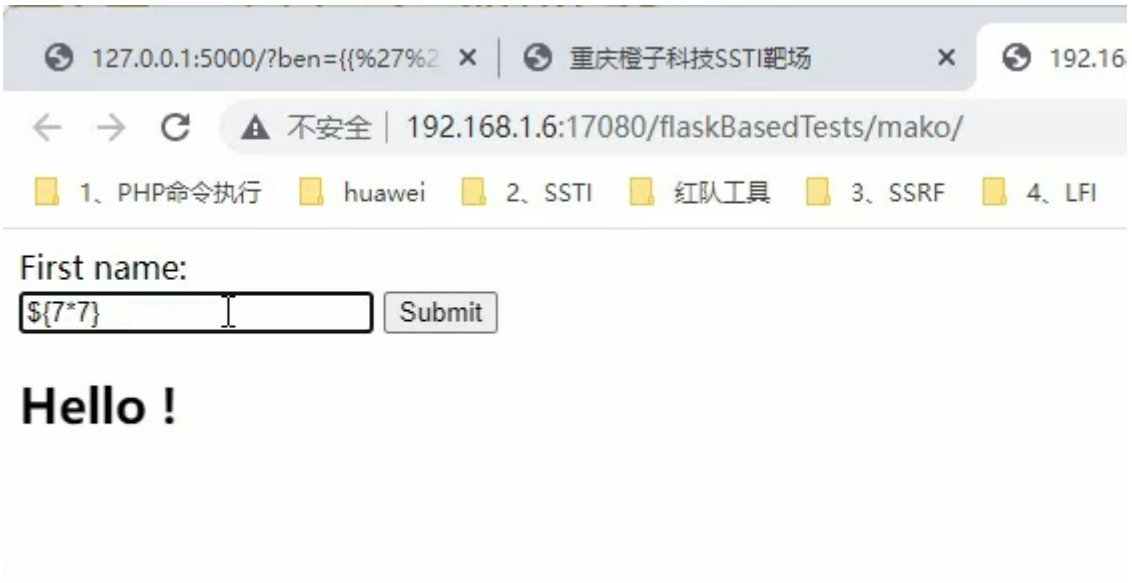
jinjia的语言：

```
控制结构 {% %}
变量取值 {{ }}
注释 {# #}
```

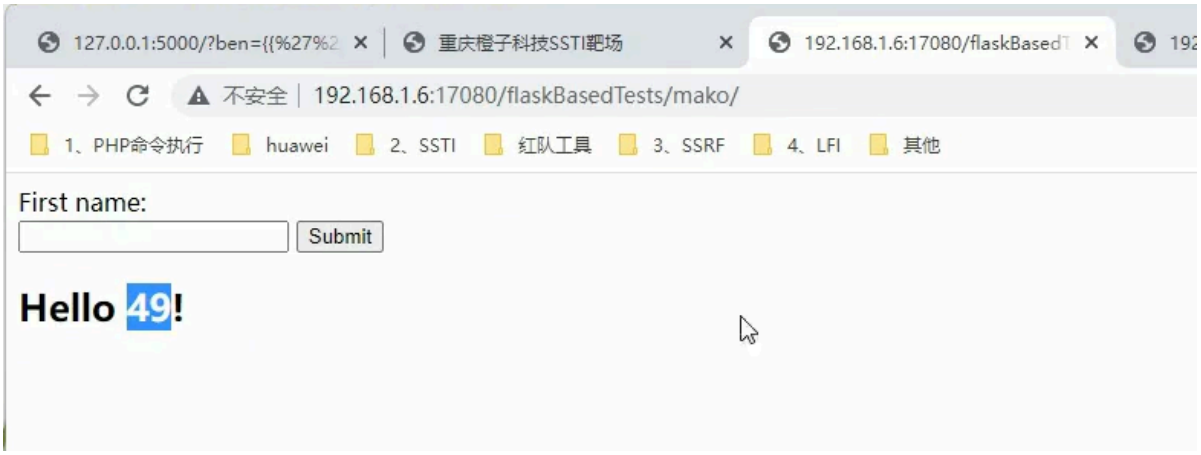
辨别不同类型模版注入的命令方法，在输入框通过输入以下蓝图中的命令，如果能执行，那么就是改命令绿色线后面的类型模版注入



比如我敲一个

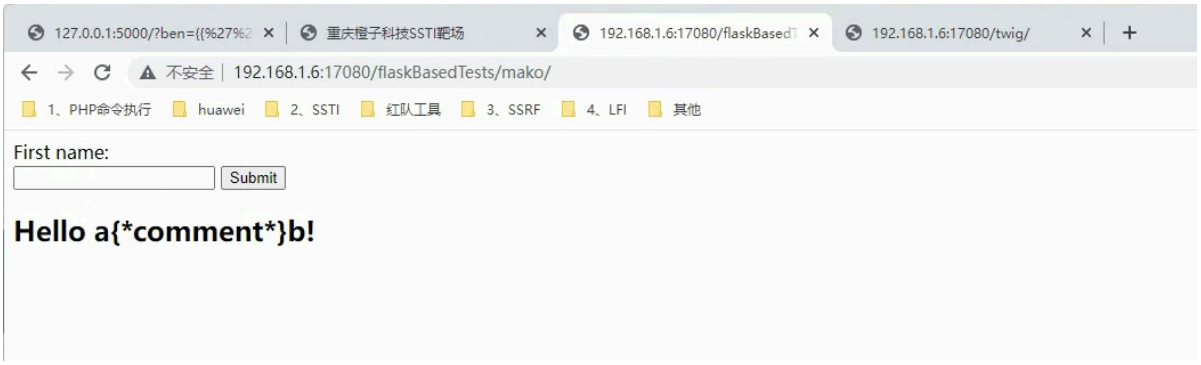


点击submit给我回显49，说明存在ssti漏洞·1但我不知道是什么类型。那么输入其他命令试试



解下来我输入第二个命令，点击submit

发现命令没有被执行，那么就不是Smarty类型注入，是mako类型注入


127.0.0.1:5000/?ben={{%27%2
重庆橙子科技SSTI靶场
192.168.1.6:17080/flaskBased
192.168.1.6:17080/twig/
不安全 | 192.168.1.6:17080/flaskBasedTests/mako/
1、PHP命令执行
huawei
2、SSTI
红队工具
3、SSRF
4、LFI
其他
First name:
Submit
Hello a{*comment*}b!