网络与信息安全课内实验2

WEB安全实验

1. 实验目的

1.搭建安全靶场，熟悉常见的WEB安全漏洞

2.了解并掌握相关工具寻找漏洞及注入点

3.掌握漏洞的保护方式

二．实验内容

1.爆破登陆

使用burp suite工具拦截包并使用字典暴力破解密码登陆

2.SQL注入

了解SQL注入原理并利用漏洞

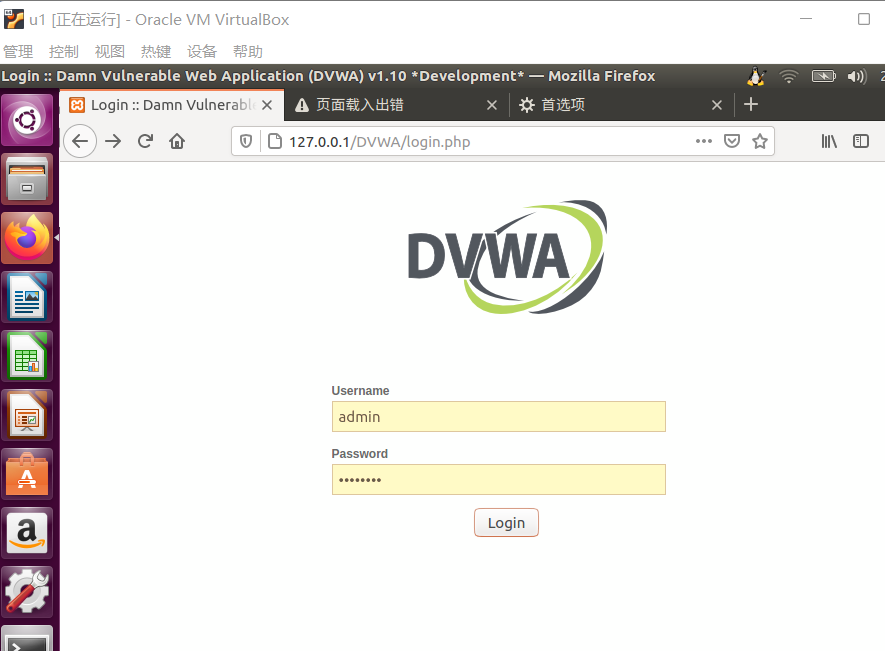
3. 中间人攻击

使用Ettercap+driftnet软件建立中间人攻击并监听图片

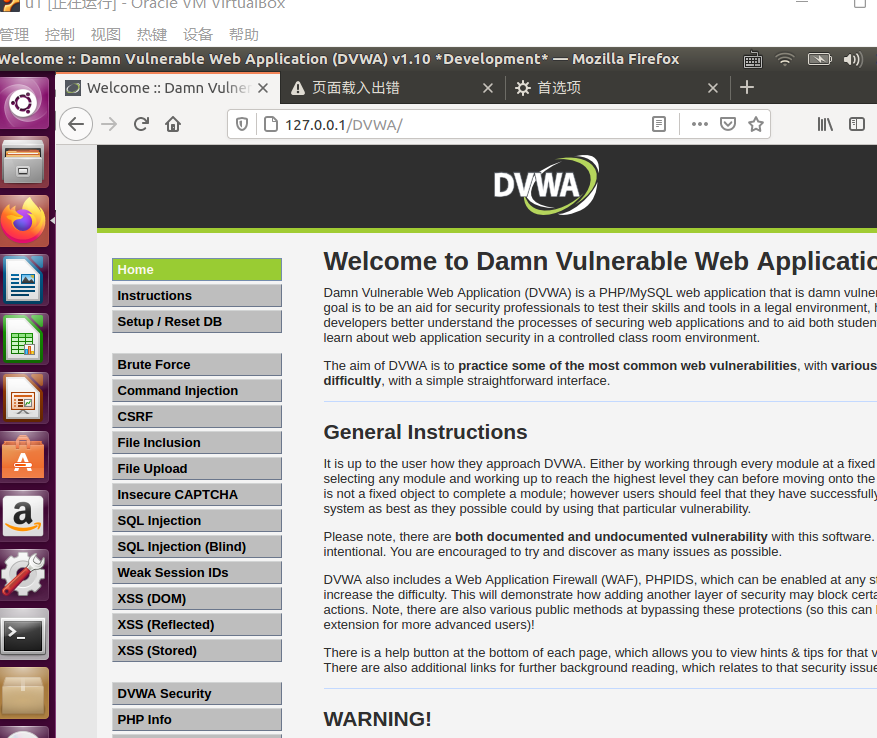
三．实验步骤

1. DVWA靶场搭建

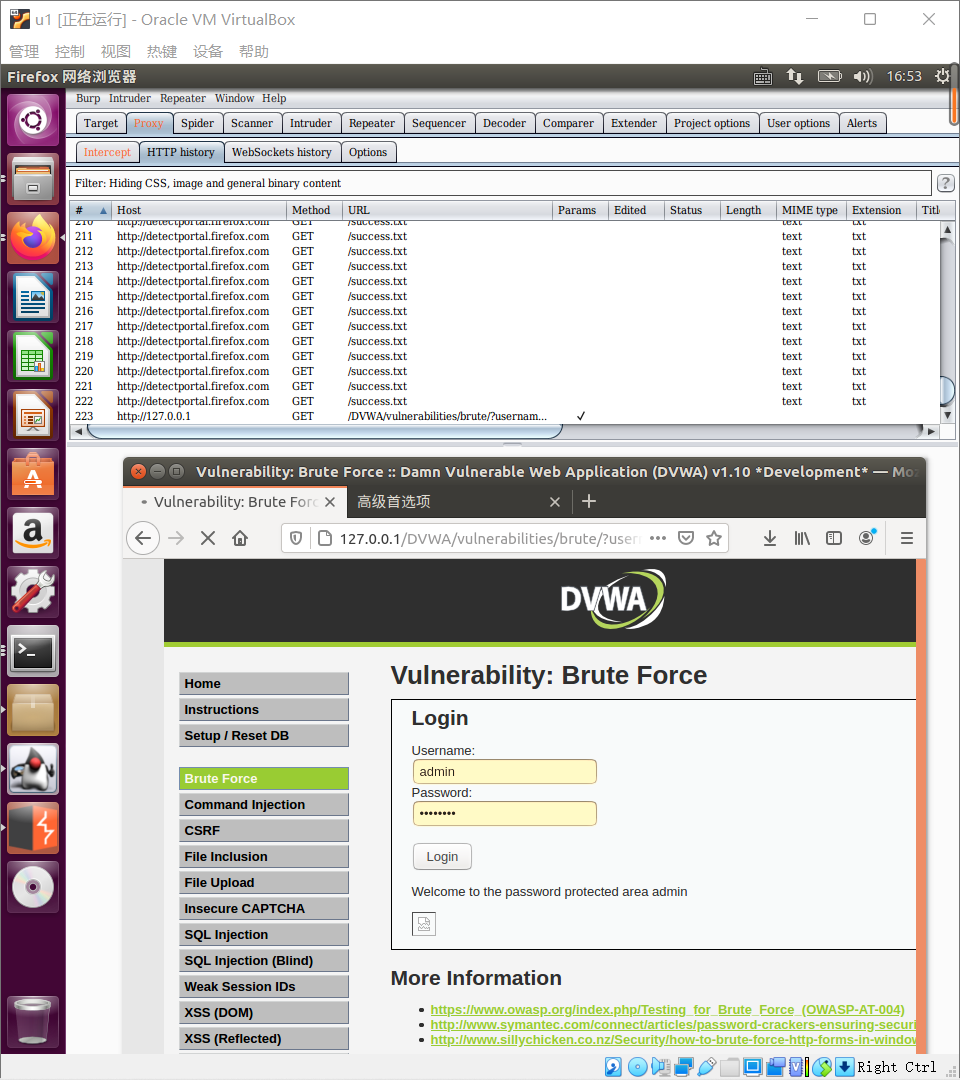
搭建好之后登陆127.0.0.1/DVWA/login.php



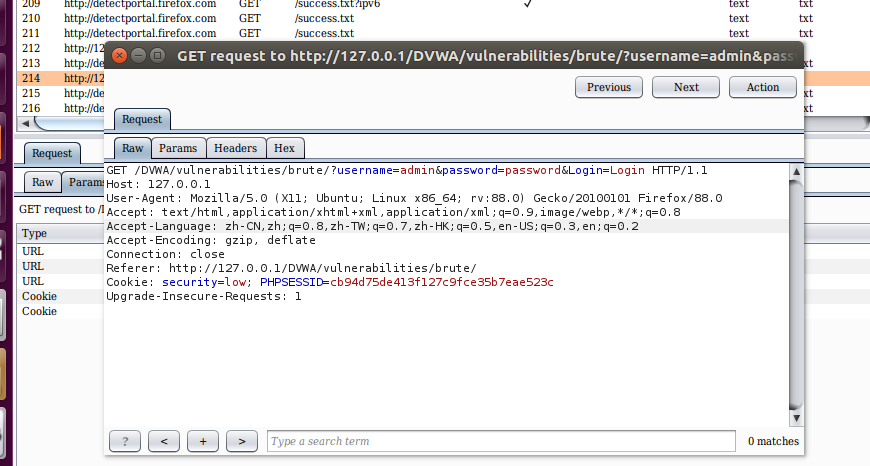
创建数据库并登录

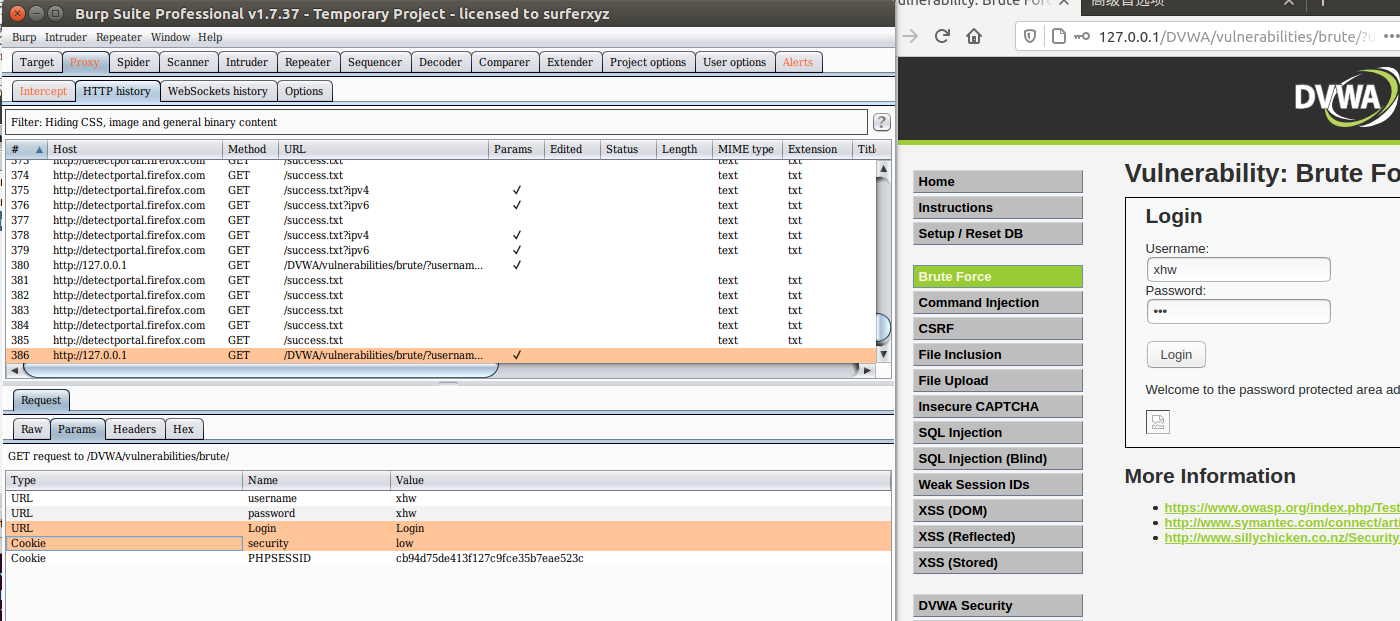


2. Brute Force 暴力破解

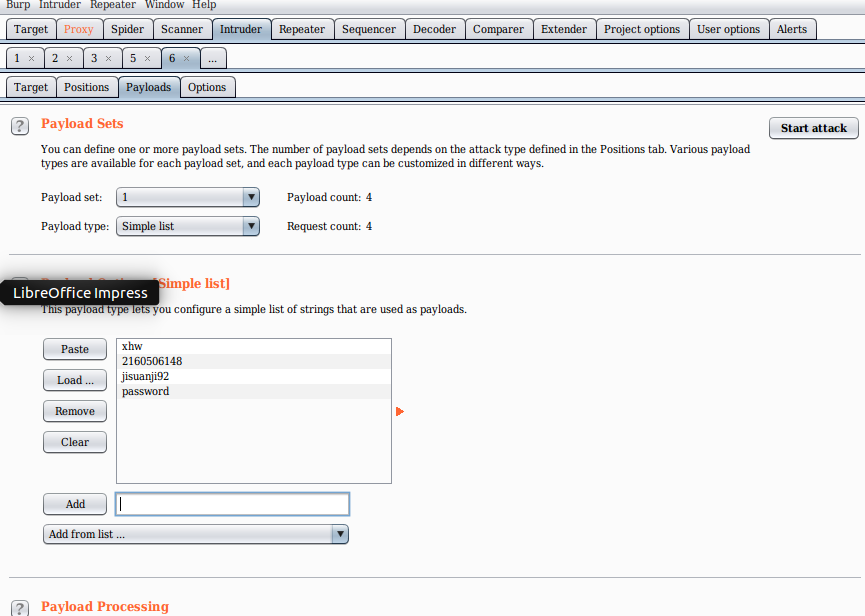


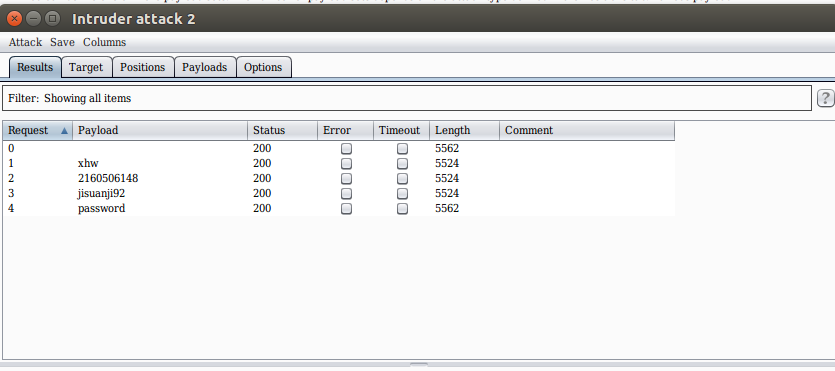
随便填写一个·账号密码，然后提交登录，软件拦截到了包，并且发现账号和密码是明文传输



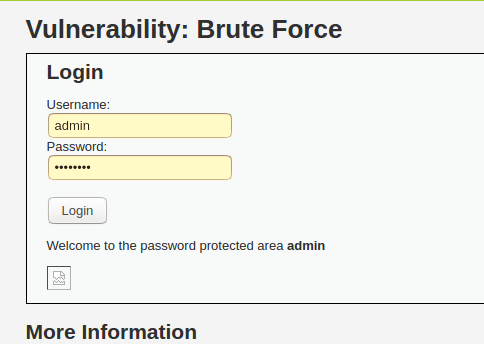


构造爆破包，在simple list中添加字典，然后start attack





然后输入密码，登陆成功！



3. 基于ARP协议漏洞的中间人攻击

两个虚拟机处于同一网段，能互相ping通

一个正常访问浏览器

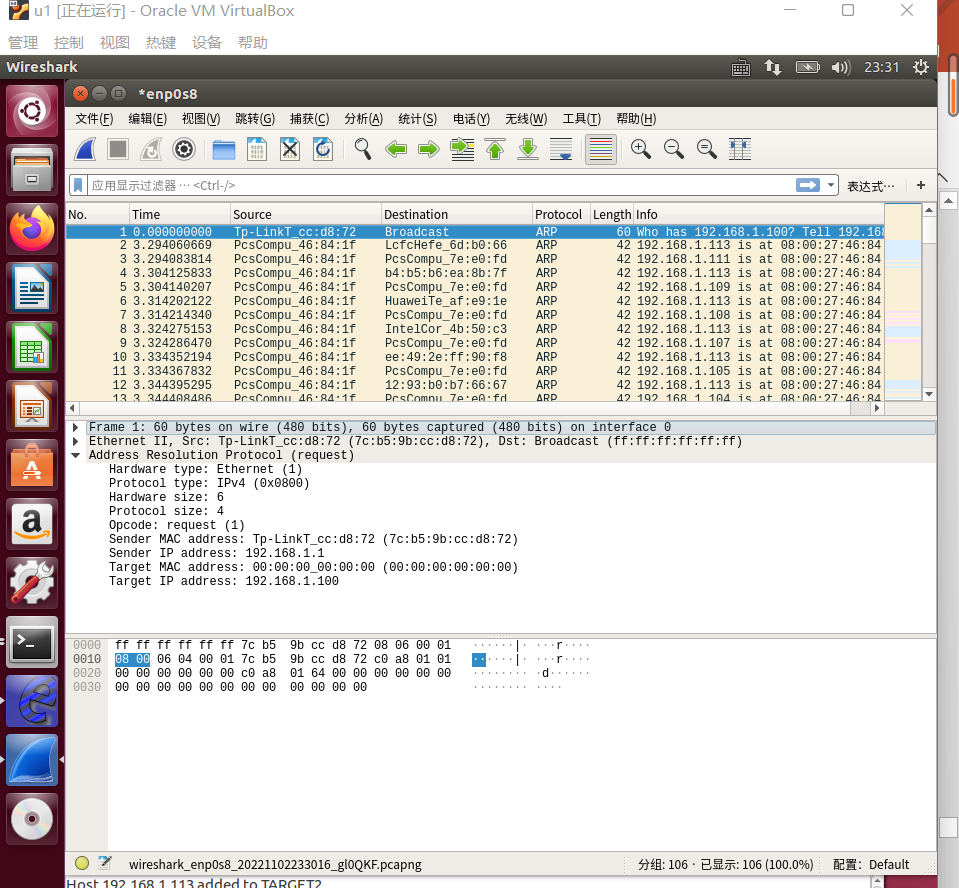
另一个用ARP攻击拦截流量，并进行分析

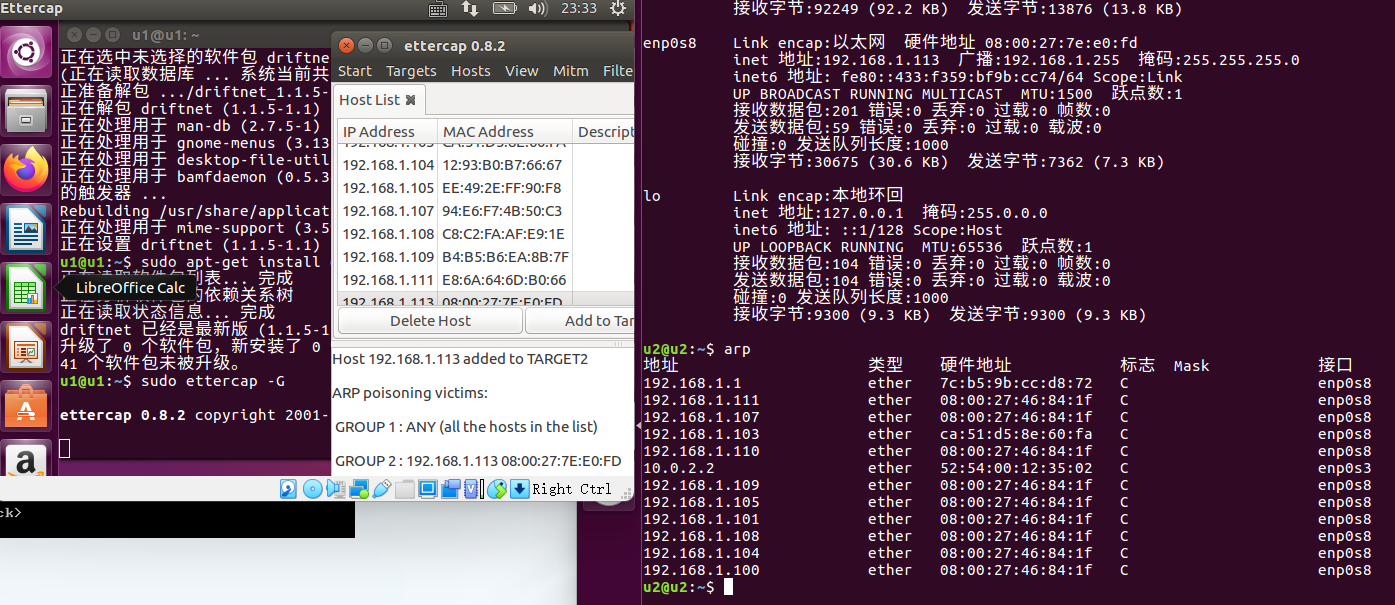
受害主机的arp缓存表

192.168.1.1110攻击成功



抓包：





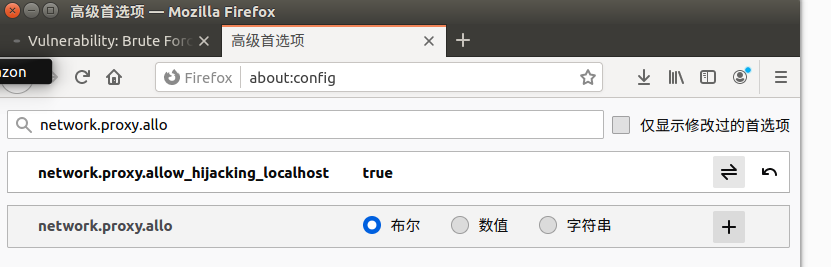
在受害者主机上随便打开youku.com. 发现driftnet已经有嗅探到了图片，说明中间人攻击生效。

****

四、实验总结

如何防御：①对于爆破登录，我们可以针对用户登录未作限制，批量爆破成功密码登陆系统的漏洞问题。将密码策略更改为输入错误规定的错误自动锁定。②对于SQL注入攻击：1、使用参数化筛选语句。为了防止SQL注入，用户输入不能直接嵌入到SQL语句中。相反，用户输入必须被过滤或参数化。参数语句使用参数，而不是将用户输入嵌入语句中。在大多数情况下，SQL语句是正确的。然后，用户输入仅限于一个参数。一般来说，有两种方法可以确保应用程序不易受到SQL注入攻击。一种是使用代码审查，另一种是强制使用参数化语句。强制使用参数化语句意味着在运行时将拒绝嵌入用户输入中的SQL语句。但是，目前对此功能的支持不多。2、避免使用解释程序，这是黑客用来执行非法命令的手段。3、防止SQL注入，但也避免一些详细的错误消息，因为黑客可以使用这些消息。标准的输入验证机制用于验证所有输入数据的长度、类型、语句和企业规则。4、使用专业的漏洞扫描工具。但是，防范SQL注入攻击是不够的。攻击者现在自动搜索和攻击目标。它的技术甚至可以很容易地应用于其他Web体系结构中的漏洞。企业应该投资于专业的漏洞扫描工具，如著名的Accunetix网络漏洞扫描程序。完美的漏洞扫描器不同于网络扫描器，它专门在网站上查找SQL注入漏洞。最新的漏洞扫描程序可以找到最新发现的漏洞。5、最后，企业在Web应用程序开发过程的所有阶段执行代码安全检查。首先，安全测试应该在部署Web应用程序之前实现，这比以前更重要、更深远。企业还应在部署后使用漏洞扫描工具和站点监控工具测试网站。③对于中间人攻击：①使用HTTPS；②不要忽略警告；③不要使用公共WiFi；④运行并更新防病毒软件。

此次实验中遇到了许多的问题，比如burpsuite的下载安装，破解问题，xampp等软件如何下载安装也困扰了许久，通过上网搜索都一一解决了。其中耗时最多的问题就是Firefox 无法抓取本地localhost数据包的问题，最后也都解决了。



夏涵文 2160506148 计算机92