网络与信息安全课内实验四报告

Web安全

### 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

### 实验原理

实验基于常见的Web安全漏洞进行探究，通过搭建DVWA靶场和使用专业工具，深入了解以下攻击方式的原理。DVWA（Damn Vulnerable Web Application）是一个用来进行安全脆弱性鉴定的PHP/MySQL Web应用，旨在为安全专业人员测试自己的专业技能和工具提供合法的环境，帮助web开发者更好的理解web应用安全防范的过程。

1. **Brute Force 暴力破解**

攻击者借助计算机的高速计算不停枚举所有可能的用户名和密码，直到尝试出正确的组合，成功登录系统。理论上，只要字典足够大，破解总是会成功的。阻止暴力破解的最有效方式是设置复杂的密码（英文字母大小写、数字、符号混合）。

1. **SQL注入**

SQL注入是另一种很常见的攻击方式，主要的攻击方式是通过把SQL命令插入到Web表单或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。

引起SQL注入漏洞的原因，一般是由于web服务没有对传递的数据中的关键词过滤导致的。在用户的输入有转义字符时，它会被传递给一个SQL语句。这样就会导致应用程序的终端用户对数据库上的语句实施操纵 。

1. **基于ARP协议漏洞的中间人攻击**

ARP（Address Resolution Protocol，地址解析协议）是一个位于TCP/IP协议栈中的网络层，负责将某个IP地址解析成对应的MAC地址。以太网（局域网）进行信息传输时，不是根据IP地址进行通信，因为IP地址是可变的，用于通信是不安全的。然而MAC地址是网卡的硬件地址，一般出厂后就具有唯一性。ARP协议就是将目标IP地址解析成MAC地址进行验证通信。

每台主机都会在自己的ARP缓冲区建立一个ARP列表（生命周期二十分钟），用于表示IP地址和MAC地址的对应关系。主机A若想和主机B通信，首先主机A会查询Arp缓存表（后面称ip-mac缓存表）是否有B主机对应的ip-mac，有的话就将B主机的mac地址封装到数据包发送。若没有的话，主机A会向以太网发送一个Arp广播包，告诉以太网内的所有主机自己的ip-mac，并请求B主机（以ip来表示B主机）的mac地址。当B主机收到Arp广播包后，确认A主机是想找自己的mac地址，就会对A主机进行回应一个自己的mac地址。A主机就会更新自己的ip-mac缓存表，同时B主机也会接收A主机的ip-mac对应关系到自己的ip-mac缓存表。

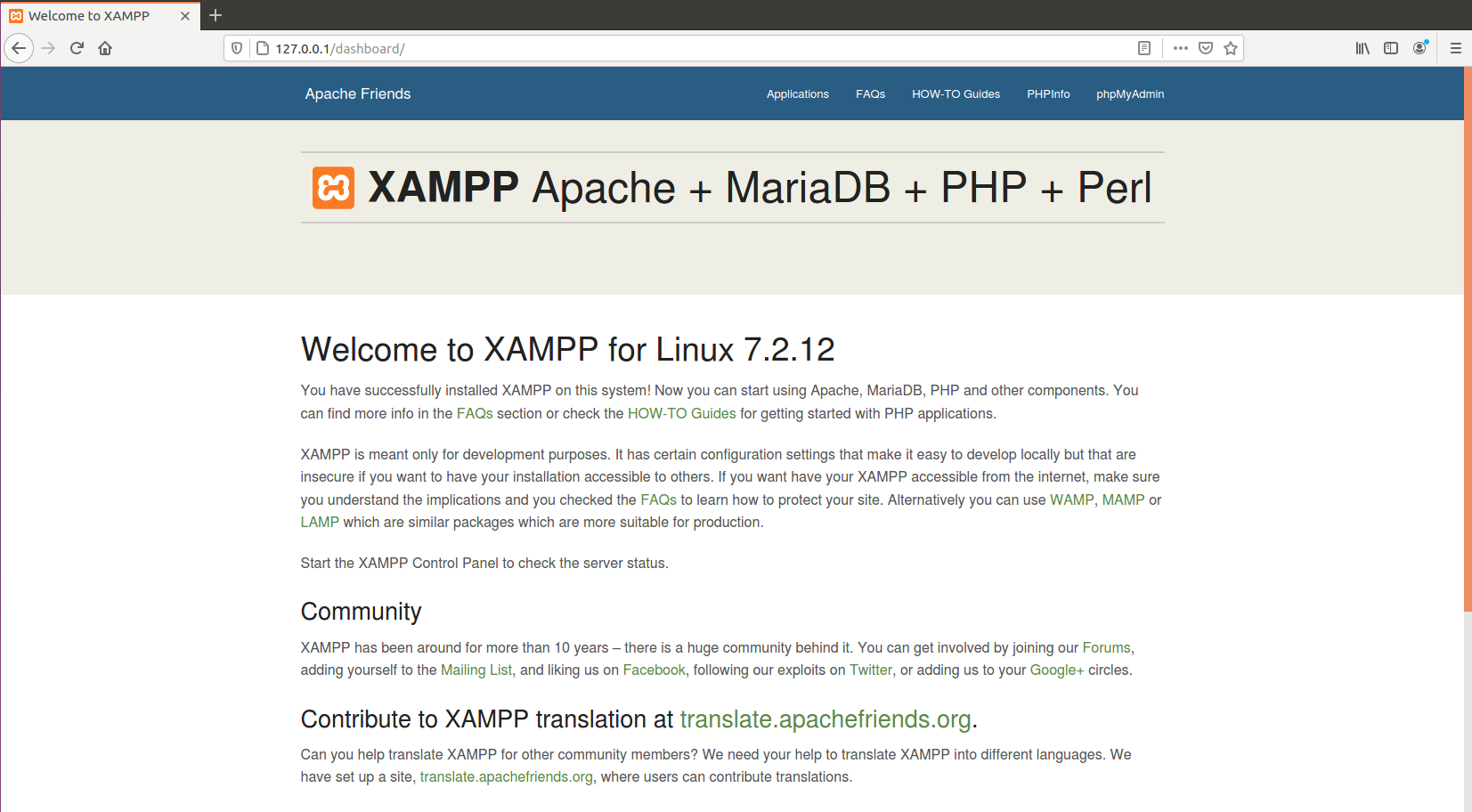
ARP协议信任以太网所有的节点，效率高但是不安全。这份协议没有其它字协议来保证以太网内部信息传输的安全，它不会检查自己是否接受或发送过请求包，只要它就收到的arp广播包，他就会把对应的ip-mac更新到自己的缓存表。

根据以上说的arp协议缺陷，如果我们冒充网关主机C，不停的向以太网发送自己的ARP广播包，告知自己的ip-mac，此时其它主机就会被欺骗，更新我们C的ip-mac为网关主机的ip-mac，那么其它主机的数据包就会发送到C主机上，因为没有发给真正的网关，就会造成其它主机的网络中断。

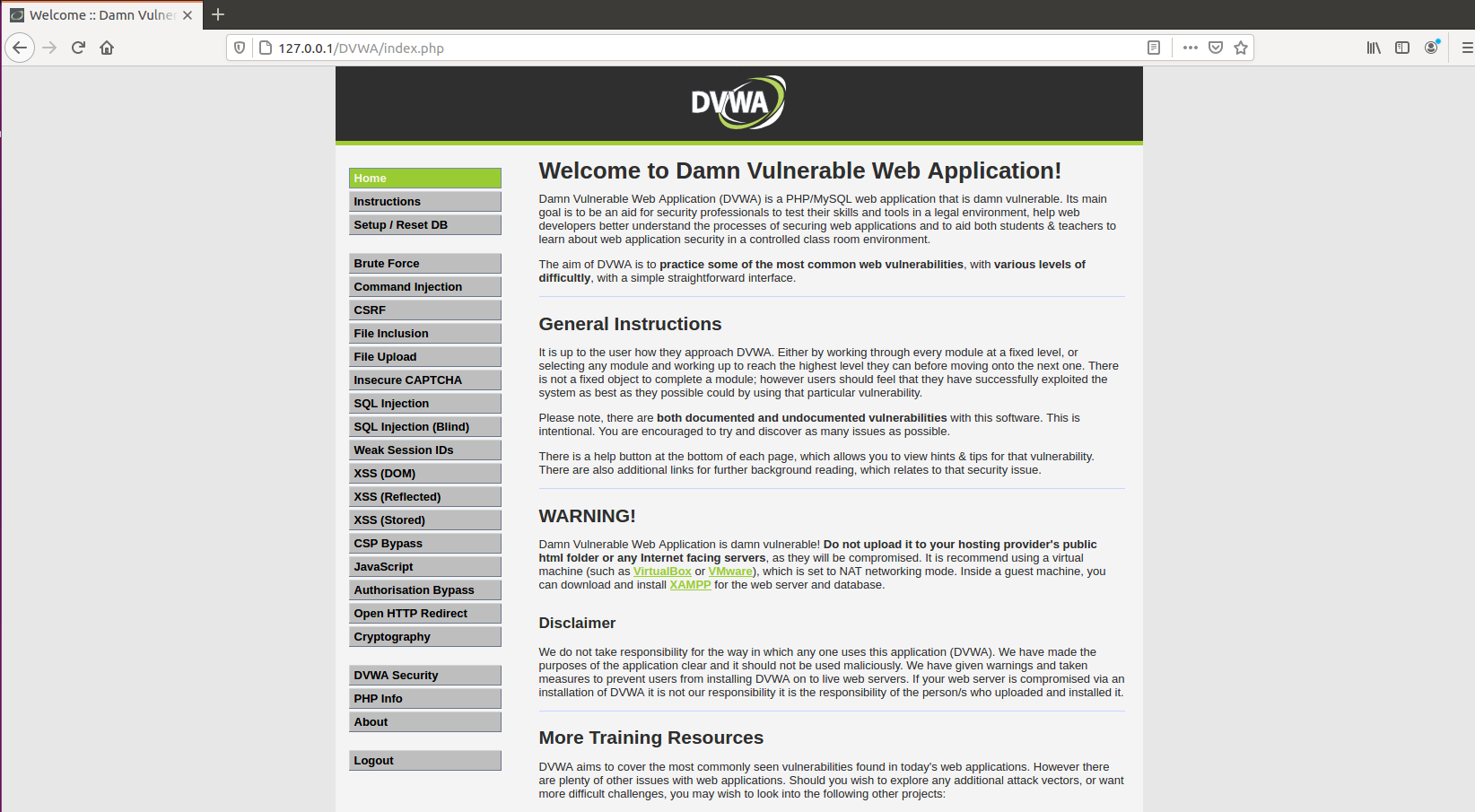
### 实验内容

1. **DVWA靶场搭建**

xampp安装成功

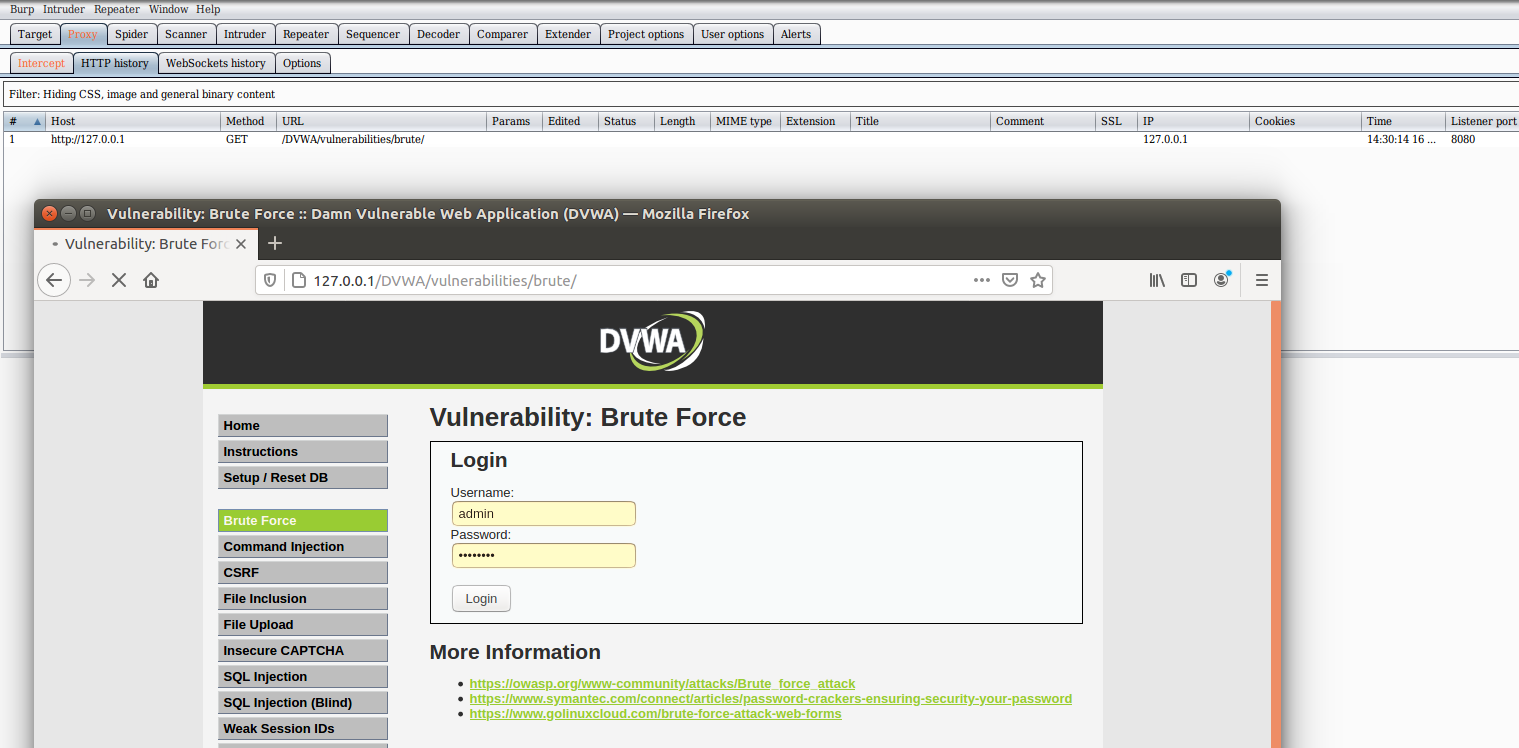


打开靶场，创建数据库，登陆成功，

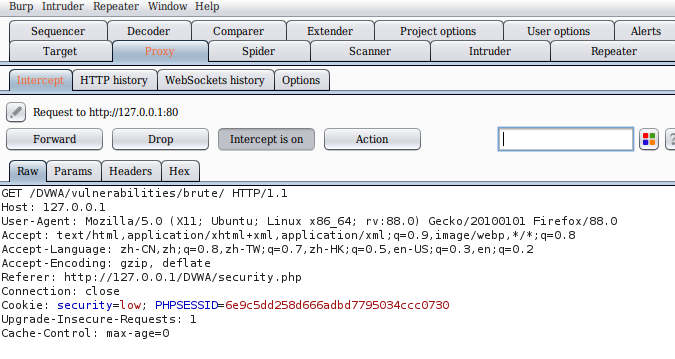


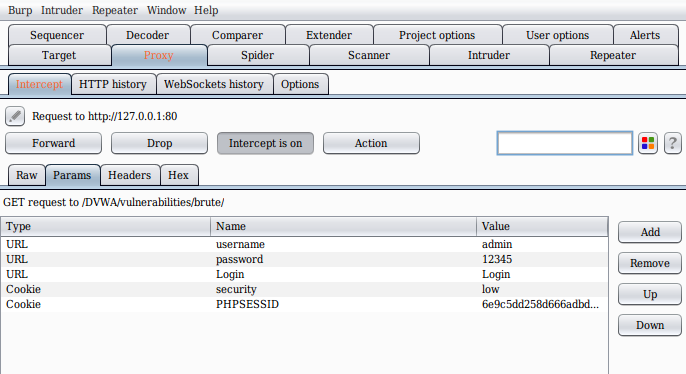
1. **Brute Force 暴力破解**

使用burp suite工具成功拦截到了包

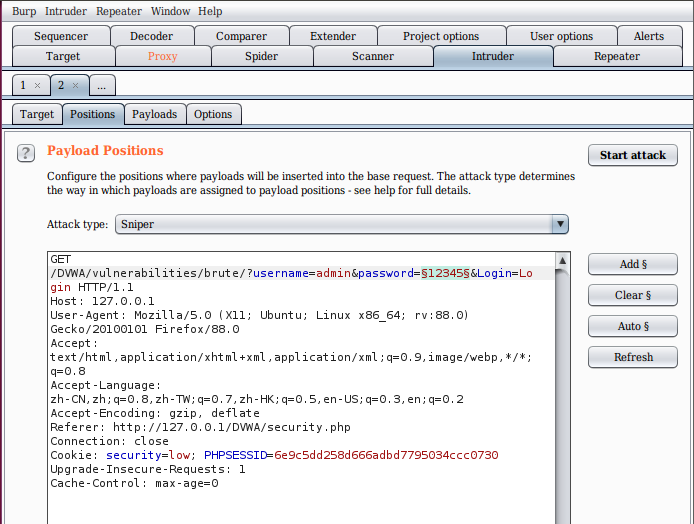


发现账号和密码是明文传输的

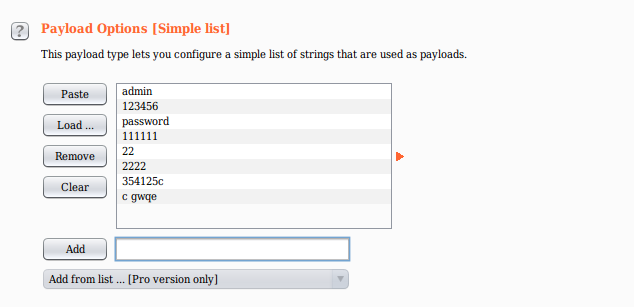




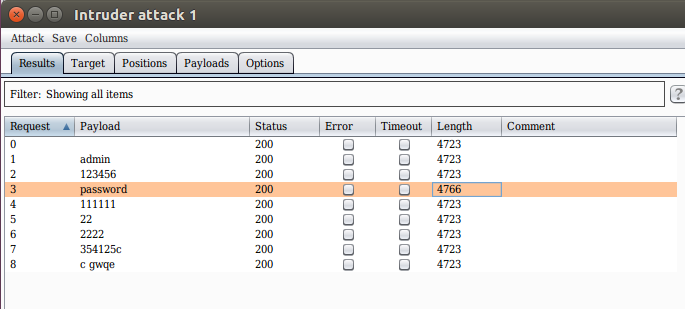
清除自动标记的参数，然后手动选中密码



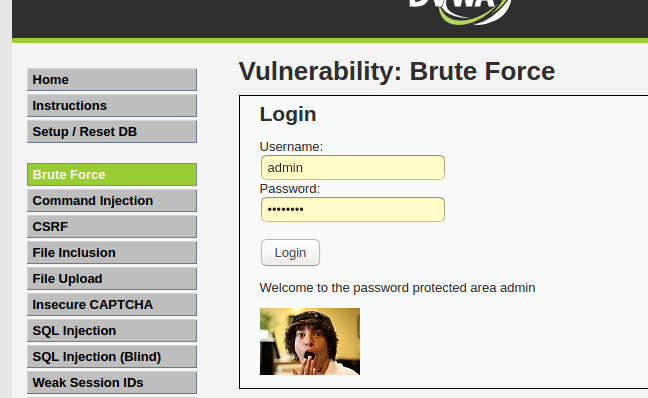
点击payload标签，在simple list中添加字典



点击start attack.查看结果，发现有一个包返回的长度跟别的不一样，就是爆破正确的密码

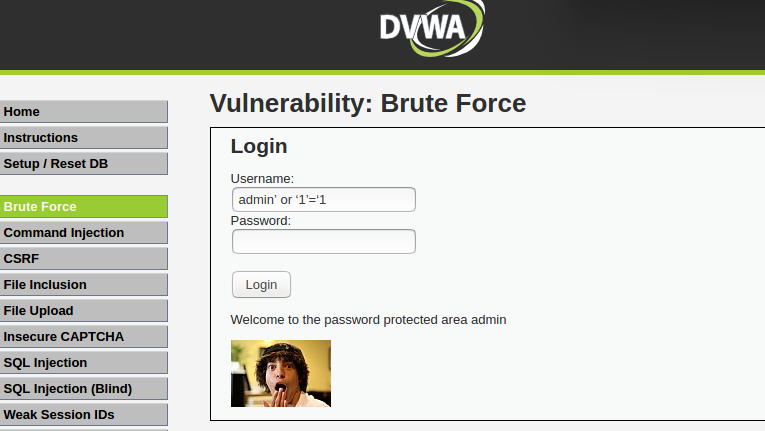


输入密码，登陆成功



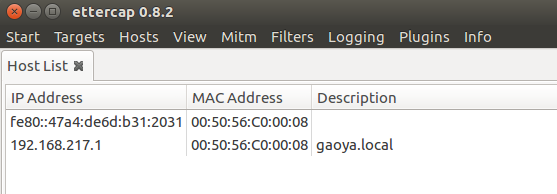
1. **SQL注入**

在用户名一栏输入 admin’ or ‘1’=‘1，密码留空，可以成功登陆

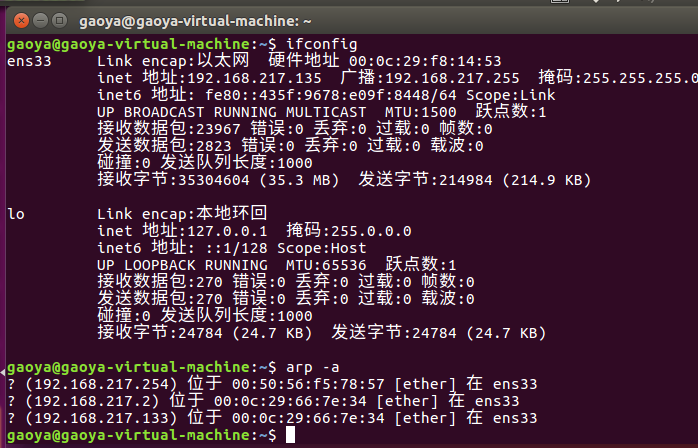


**四、基于ARP协议漏洞的中间人攻击**

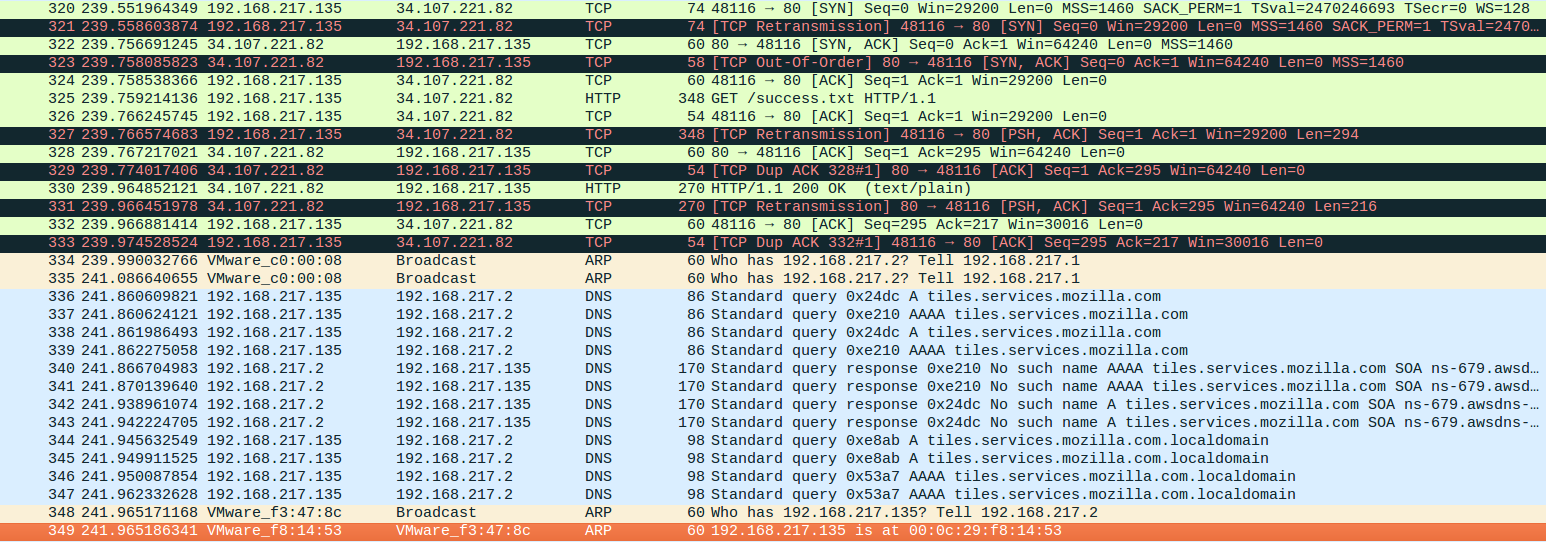
选择host 下的scan for hosts 扫描主机，完成后选择hosts list打开



在受害主机上查看arp缓存表，主机攻击成功

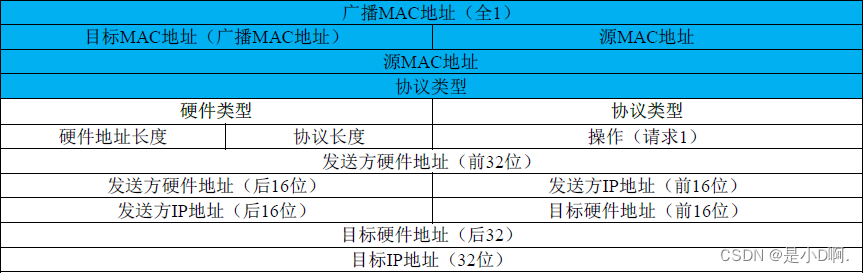


在攻击者主机上打开wireshark进行抓包



查看arp协议数据包的内容

**ARP请求协议报文格式**



蓝色的部分是以太网的帧头部

第一个字段是广播类型的MAC地址，其目标是网络上的所有主机

第二个字段是源MAC地址，即请求地址解析的的主机MAC地址

第三个字段是协议类型

硬件类型：表明ARP协议实现在哪种类型的网络上

协议类型：表示解析协议

硬件地址长度：MAC地址长度

协议地址长度：IP地址长度

操作类型：表示ARP协议数据包类型

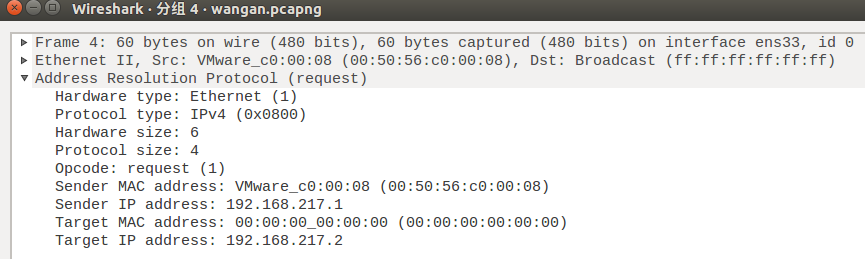
源MAC地址：发送端MAC地址

源IP地址：表示发送端协议地址

目标MAC地址：目标端MAC地址

目标IP地址：表示目的端协议地址

捕获的ARP请求包如下：



Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface ens33, id 0

这是第4帧数据包的详细信息，该包的大小为60个字节

Ethernet II, Src: VMware\_c0:00:08 (00:50:56:c0:00:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

以太网帧头部信息，源MAC地址为00:50:56:c0:00:08，目标MAC地址为ff:ff:ff:ff:ff:ff广播地址，因为主机PC2不知道PC1的MAC地址。这样，局域网中所有设备都会收到该数据包

Address Resolution Protocol (request)

地址解析协议内容，request表示该包是一个ARP请求包

Hardware type: Ethernet (1) 硬件类型

Protocol type: IPv4 (0x0800) 协议类型

Hardware size: 6 硬件地址

Protocol size: 4 协议长度

Opcode: request (1) 操作码，该值为1表示是个ARP请求包

Sender MAC address: VMware\_c0:00:08 (00:50:56:c0:00:08) 发送端MAC地址

Sender IP address: 192.168.217.1 发送端IP地址

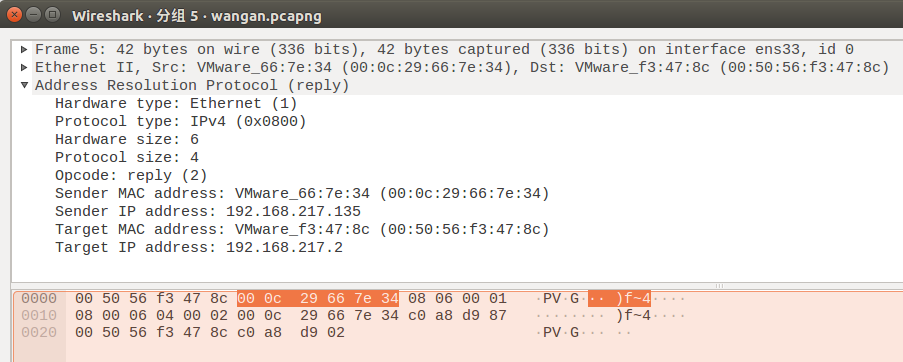
Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00) 目标MAC地址

Target IP address: 192.168.217.2 目标IP地址

**ARP请求协议报文格式**



捕获的ARP应答包如下：



Ethernet II, Src: VMware\_66:7e:34 (00:0c:29:66:7e:34), Dst: VMware\_f3:47:8c (00:50:56:f3:47:8c)以太网帧头部的信息，源MAC地址为00:0c:29:66:7e:34，目标MAC地址为00:50:56:f3:47:8c，PC2获取到了PC1主机的MAC地址，这样就可以正常通信了

Address Resolution Protocol (reply)

表示这是一个ARP应答包

Hardware type: Ethernet (1) 硬件类型

Protocol type: IPv4 (0x0800) 协议类型

Hardware size: 6 硬件长度

Protocol size: 4 协议长度

Opcode: reply (2) 操作码为2表示该包是ARP响应包

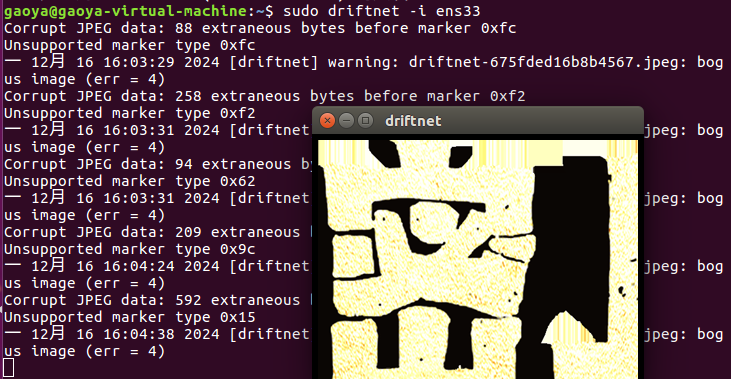
Sender MAC address: VMware\_66:7e:34 (00:0c:29:66:7e:34) 发送方MAC地址

Sender IP address: 192.168.217.135 发送方IP地址

Target MAC address: VMware\_f3:47:8c (00:50:56:f3:47:8c) 目标MAC地址

Target IP address: 192.168.217.2 目标IP地址

在受害者主机上随便打开一个未加密的http网页，比如youku，然后观察driftnet的嗅探情况，可以发现driftnet已经有嗅探到了图片，说明中间人攻击生效





### 漏洞的防御方法

**防御暴力破解攻击**

* 1. 增强密码安全性

·提升密码长度和复杂度

密码应由数字、大小写字母和特殊符号混合组成，且密码越长，破解密码的时间就会成指数增加，一旦密码超过了某个长度，基本上就不能用暴力破解了。强制用户设置复杂密码，增加字典攻击的难度。

·在不同的地方使用不同的密码

重复使用电子邮件、银行和社交媒体帐户的密码更可能导致身份被盗用。

·避免使用字典单词、数字组合、相邻键盘组合、重复的字符串。

避免使用名字或者非机密的个人信息（电话号码、出生日期等）作为密码，或者是亲人、孩子的名字。

·定期修改密码

* 1. 做好密码防暴力破解设计

·锁定策略

输错密码几次就锁定一段时间。

·验证码技术

要求用户完成简单的任务才能登录到系统，用户可以轻松完成，但暴力工具无法完成。例如图形验证码、短信等。

·密码复杂度限制

强制用户设置长而复杂的密码，并强制定期更改密码。

·双因子认证

结合两种不同的认证因素对用户进行认证的方法。例如密码、身份证、安全令牌、指纹、面部识别、地理信息等。

**SQL注入防御**

* 1. 使用参数化查询

在Java中，可以使用PreparedStatement来实现参数化查询，sql注入只对sql语句的准备（编译）过程有破坏作用，而PreparedStatement已经准备好了,执行阶段只是把输入串作为数据处理，而不再对sql语句进行解析,准备,因此也就避免了sql注入问题。

* 1. 最小权限原则

用户被授予最小必需的权限，只能访问和执行他们工作所需的数据库对象和操作，而不是拥有对整个数据库的完全访问权限。通过限制用户的权限，可以防止他们对数据库中的敏感数据进行未经授权的访问、修改或删除。

* 1. 定期安全测试

定期进行静态和动态的安全测试可以帮助发现和修复SQL注入漏洞。这包括使用自动化工具扫描代码中的安全漏洞，以及进行渗透测试来模拟攻击者的行为。

**中间人攻击防御**

·避免不安全的公共 Wi-Fi 网络：公共 Wi-Fi 网络通常未加密，容易受到 MiTM 攻击。连接到此类网络时最好避免访问敏感信息或使用安全帐户。

·使用虚拟专用网络 (VPN)：VPN 会加密您的互联网流量，提供额外的安全和隐私层，尤其是在使用公共网络时。

·使用安全和加密的通信渠道：确保您访问的网站使用 HTTPS 加密，尤其是在传输密码或财务详细信息等敏感信息时。

·保持您的设备和软件最新：定期更新您的操作系统、网络浏览器和安全软件，以减

少攻击者可能利用的漏洞。

·验证数字证书：访问需要身份验证的网站或服务时，请确保所提供的数字证书有效且由受信任的证书颁发机构颁发。

·警惕可疑链接和附件：避免点击来自未知或不受信任来源的链接或下载附件，因为它们可能会导致恶意网站或触发恶意软件的安装。

### 遇到问题及解决方法

问题：软件没有拦截到包

解决：

浏览器代理中显示如下



打开about:config页面，搜索network.proxy.allow\_hijacking\_localhost双击变为true,再重新打开配置页面，就没有localhost、127.0.01永不经过代理这一提醒。

### 心得体会

通过本次实验，我学习了Web安全漏洞产生的根本原因和危害。安全漏洞常常是在开发过程中因为疏忽大意而产生的，比如没有充分检查用户的输入，或者没有启用加密通信来保障数据传输的安全性。像Burp Suite、Ettercap这样的工具，虽然为攻击者提供了便利，简化了攻击流程，但也提醒我们要加强对这些工具使用的监管，防止它们被用于非法用途。要想有效防范安全漏洞，必须从开发阶段就开始重视，结合后续的测试和运维工作，共同构建一个全面的安全防护体系。