中南大学

Heart Bleed 实验

学　　院：信息科学与工程学院

专业班级：信安 1401

指导老师：王伟平

学　　号：0906140127

姓　　名：袁魁

目　　录

Heart Bleed 实验

1.实验描述

【实验背景】

Heartbleed 漏洞（CVE-2014-0160）是 OpenSSL 库中的严重实现缺陷，它使攻击者能够从受害服务器的内存窃取数据。 被盗数据的内容取决于服务器内存中的内容。 它可能包含私钥，TLS 会话密钥，用户名，密码，信用卡等。此漏洞是存在 Heartbeat 协议中，SSL / TLS 使用它来保持连接活动。

【实验目的】

使用 Heart Bleed 对目标服务器进行攻击，了解 Heart Bleed 漏洞的危害。

2.实验步骤

2.1 环境搭建

这里攻击者和受害站点可以使用一台虚拟机，需要的站点在虚拟机里已经搭建完成，使用同一台机器可以省去配置 IP 的步骤。

2.2 实验内容

Heartbleed 漏洞之所以得名，是因为用于安全传输层协议(TLS)及数据包传输层安全协议(DTLS)的 Heartbeat 扩展存在漏洞。Heartbeat 扩展为 TLS/DTLS 提供了一种新的简便的连接保持方式，但由于 OpenSSL 1.0.2-beta 与 OpenSSL 1.0.1 在处理 TLS heartbeat 扩展时的边界错误，攻击者可以利用漏洞披露连接的客户端或服务器的存储器内容，导致攻击者不仅可以读取其中机密的加密数据，还能盗走用于加密的密钥。

该漏洞发生在 OpenSSL 对 TLS 的心跳扩展(RFC6520)的实现代码中，由于遗漏了一处边界检查，使攻击者无需任何特权信息或身份验证，就能够从内存中读取请求存储位置之外的多达 64 KB 的数据，可能包含证书私钥、用户名与密码、聊天消息、电子邮件以及重要的商业文档和通信等数据。

实验过程我们按如下步骤进行

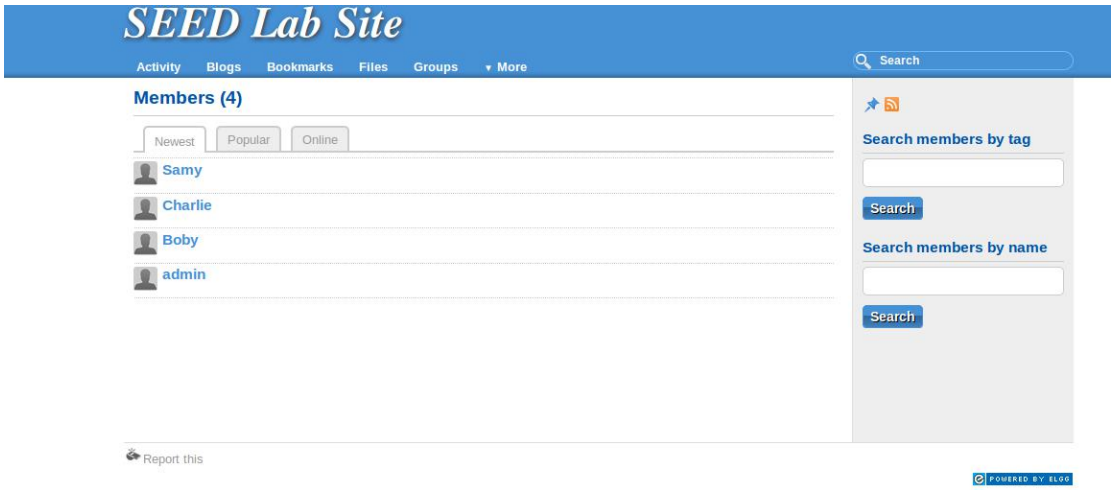
1、登陆事先搭好的站点 www.heartbleedlabelgg.com

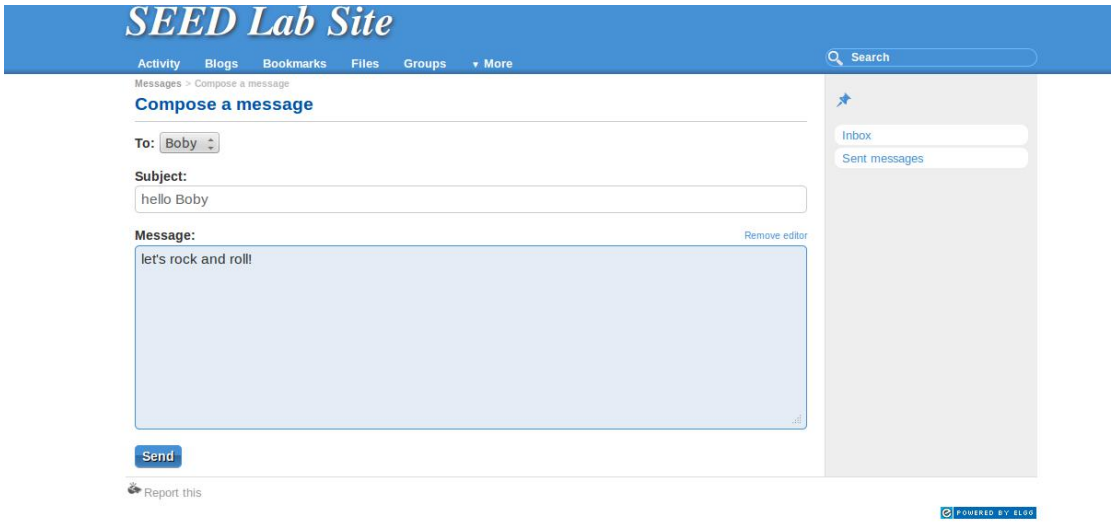
2、以管理员身份登陆

3、进行操作，例如添加 Boby 为好友

4、给 Boby 发送一条信息

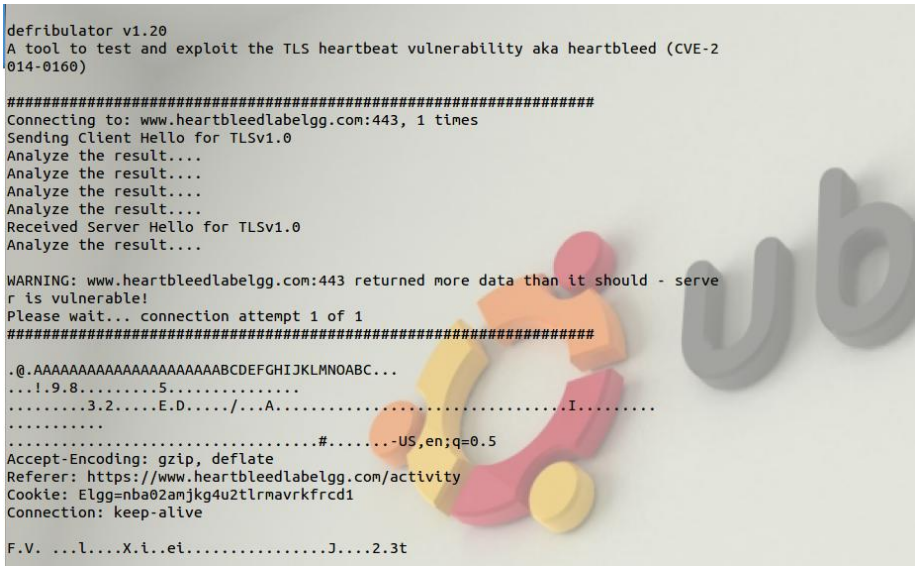
如图所示：



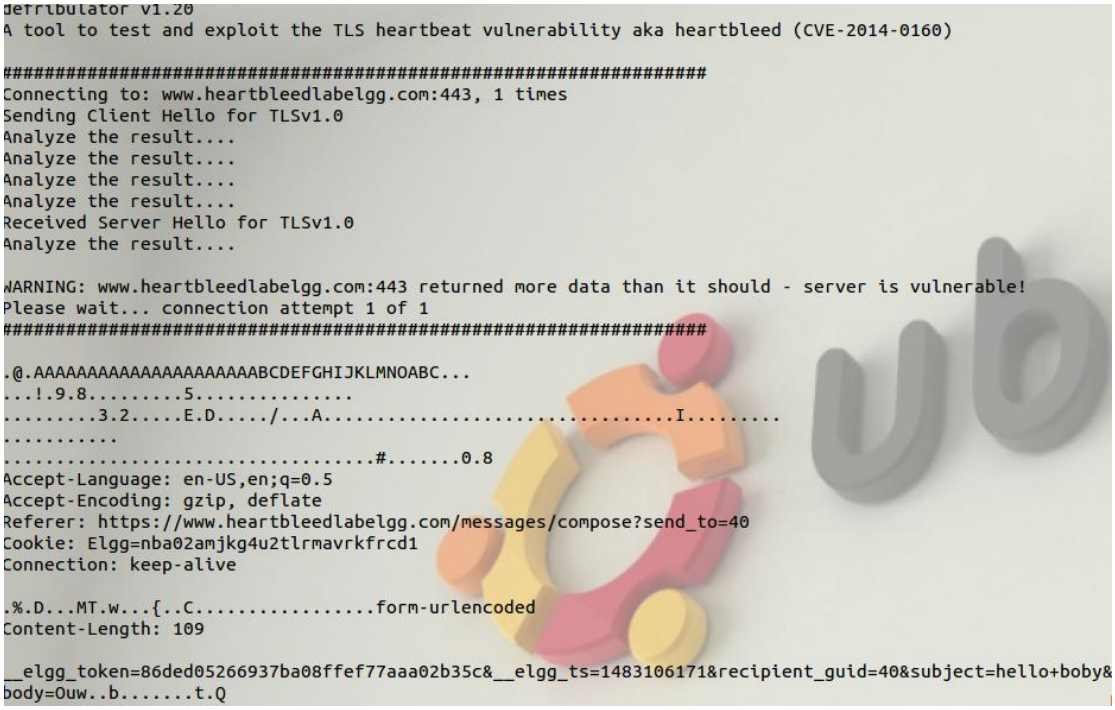


之后，我们再用 heartbleed 漏洞，对站点服务器进行攻击，这里需要用到一段攻击代码 attack.py，在攻击端执行操作

./attack.py www.heartbleedlabelgg.com



多进行几次操作，直到得到有用的信息，如下图所示：



可以看到，攻击方得到了管理员刚才发送给 Boby 的消息。

3. 总结

通过此次 HeartBleed 攻击实验，我了解到：早期版本的 OpenSSL 协议还是存在一些致命的漏洞，由于忽略了对心跳包大小的边界检查，而导致了服务器内存的数据泄露，这将会造成很大的威胁和损失。而解决 HeartBleed 漏洞的方式也十分重要，关键在于对心跳包返回长度大小的限制，在相关代码中加入对心跳包大小的边界检查，即可防止被 HeartBleed 攻击，或者，升级到最新的 OpenSSL 协议，也可以防止 HeartBleed 攻击。