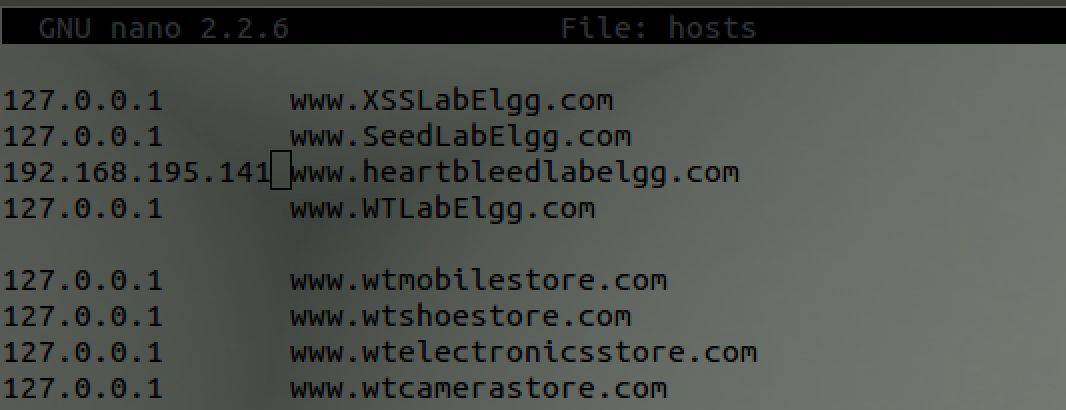
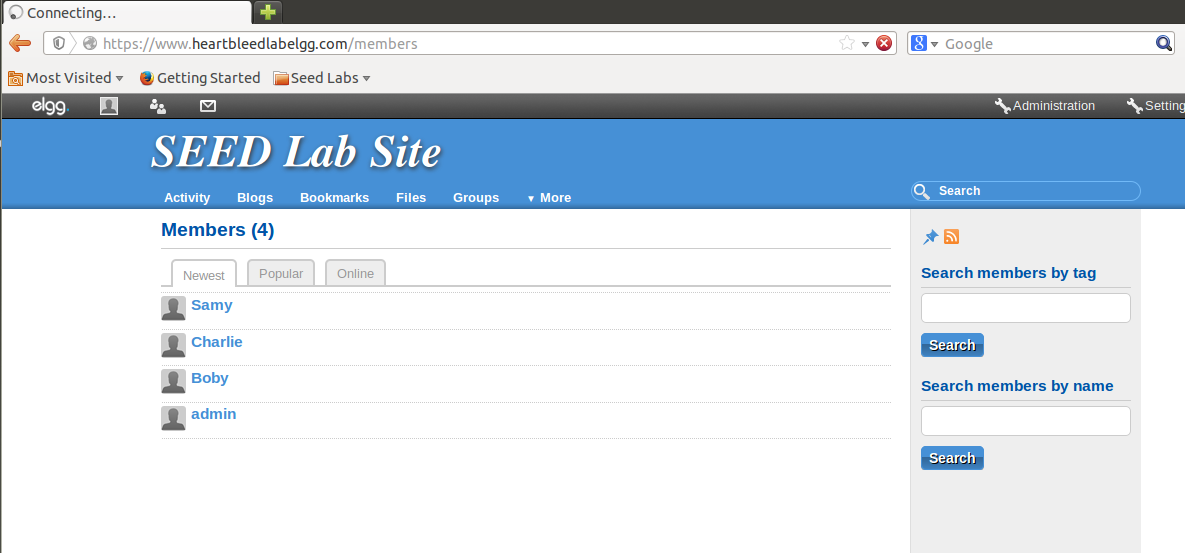
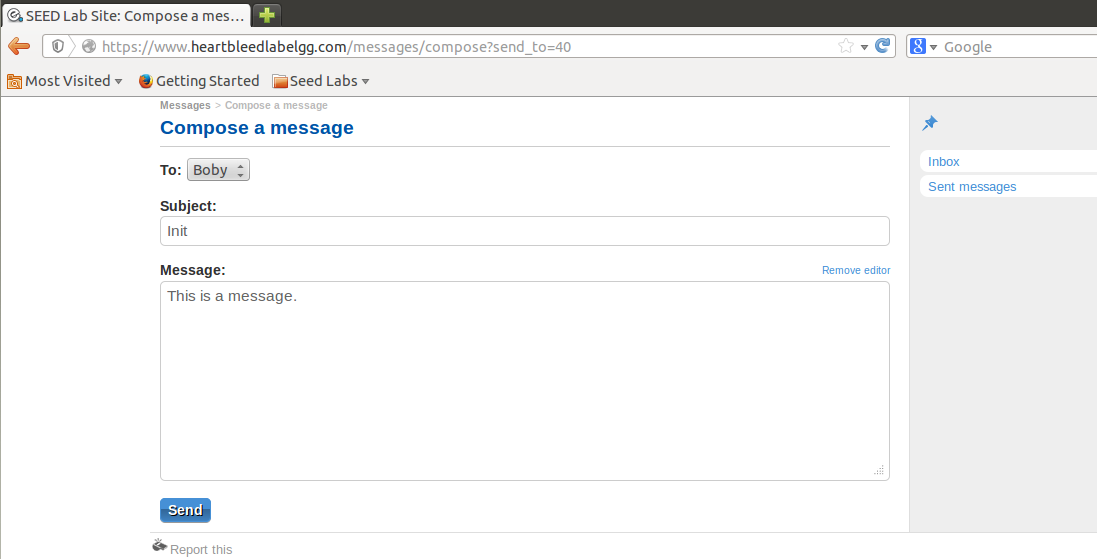
Ran ifconfig on victim, pulled IP address, changed hosts file for attacker.



Browsed to site and logged in as “admin”, and sent Boby a message:

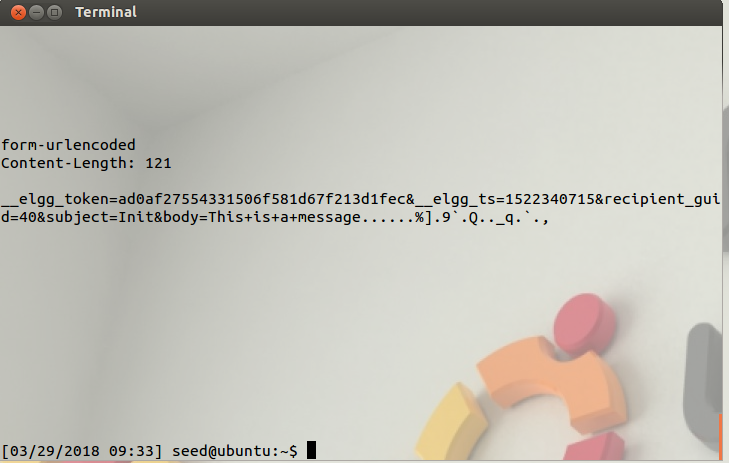






In our first attempt, we received credentials for the username and password.

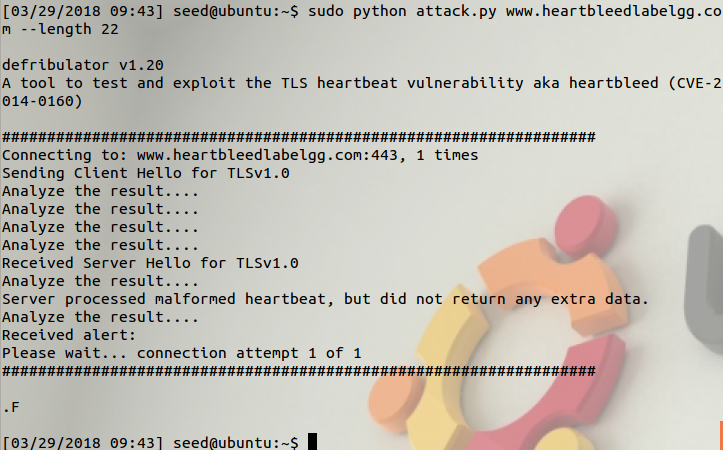
Running the attack a few more times resulted in the message being discovered:



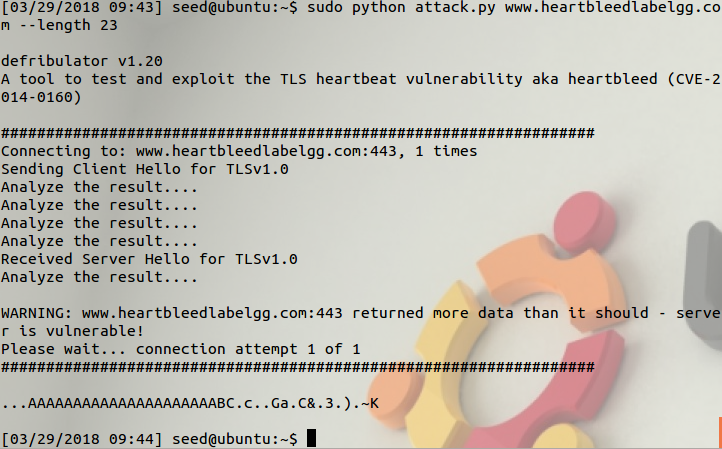
Task 2  
2.1 *As the length variable decreases, what kind of difference can you observe?*

As the length variable decreases, we receive less data than those with a higher length variable.

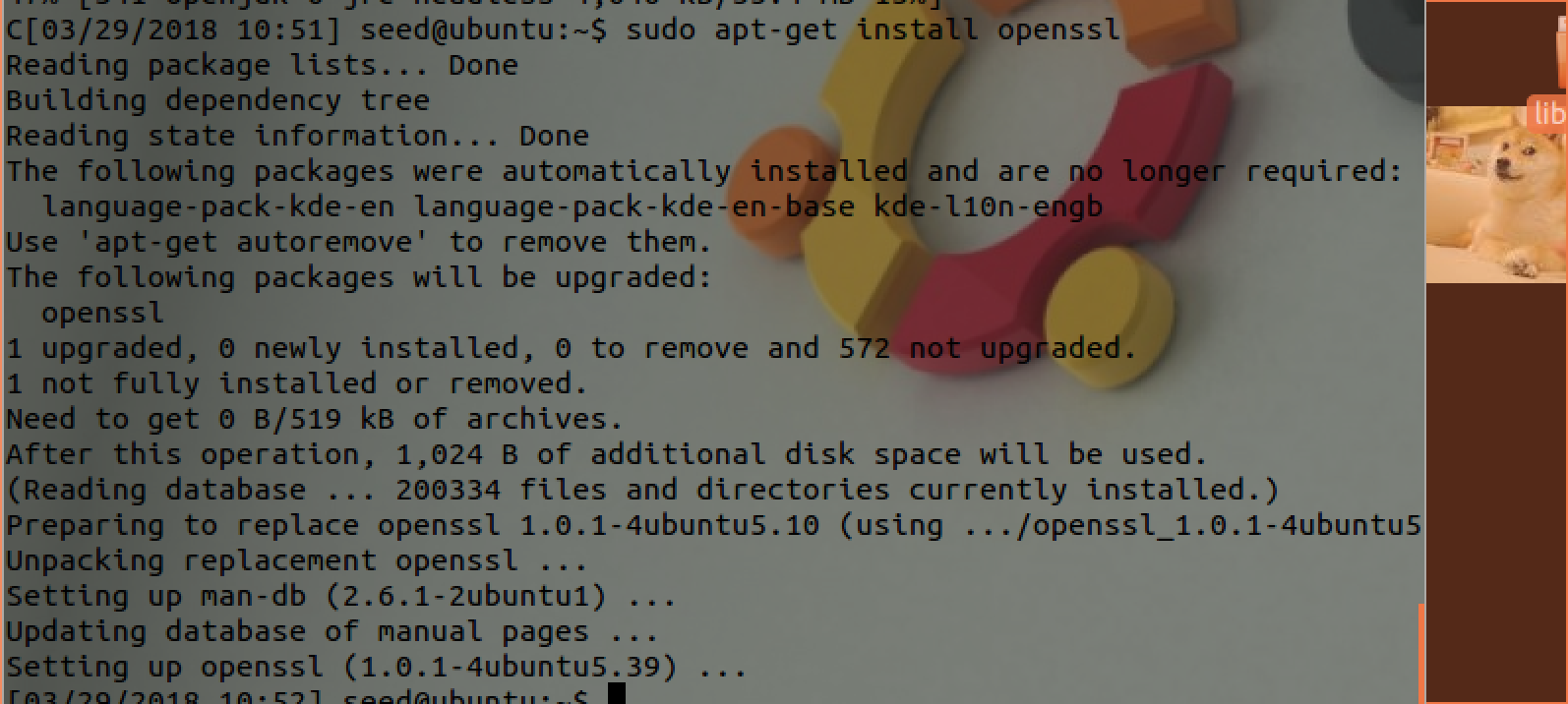
2.2: Using an attack length of 22 bytes results in an empty response:



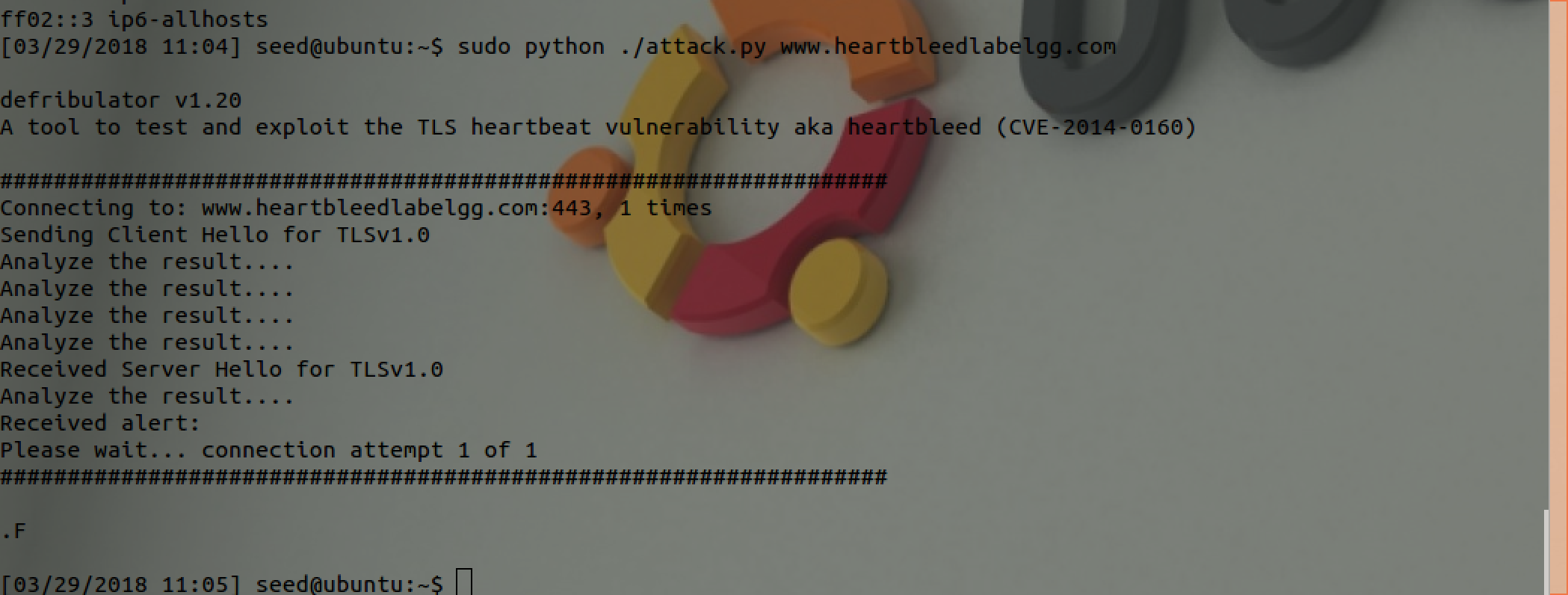
However, using length 23 results in data being returned:



Upgraded openssl

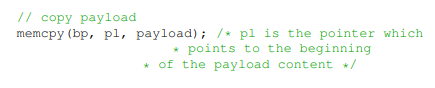


3.1: After the upgrade, when performing the attack we were not able to infiltrate the system.



3.2

The problematic section of code is below:



Because there isn’t any check to determine whether or not ‘pl’ is a valid value, a memory breach can occur. Three solutions are proposed:

Alice’s solution requires the program to know the allowed boundary while performing the copy, which could be difficult to implement.

Eva’s solution requires the server to calculate the packet size at runtime, and although this entails overhead in the server application, it is less computationally demanding than Bob’s proposal, which requires both calculation and comparison to validate the packet length.