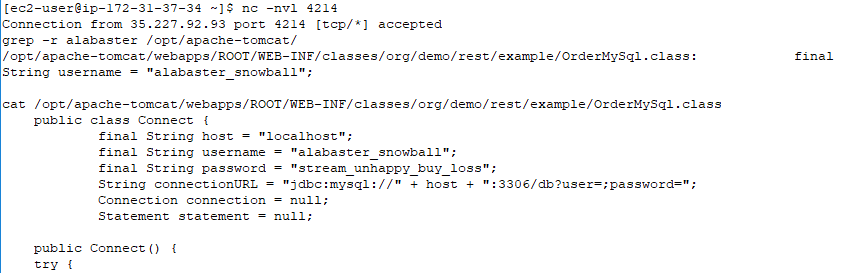
# Letters to Santa--a real world attack Part 8, Wrapping Up

In the last part, the assignment was to find a password in Alabaster’s code on the dev server. Once we had it we were asked to see if it allowed us to SSH to the dev server and the Letters to Santa (l2s) server.

To find Alabaster’s password, we reestablished a Netcat reverse shell to the dev server (web or BASH shells would have worked also.) The commands are the same as those we used in previous parts. The web server runs Apache-Tomcat and most likely, the code is in /opt or /opt/apache-tomcat. A search for alabaster in the /opt/apache-tomcat may work.  
grep -r alabaster /opt/apache-tomcat

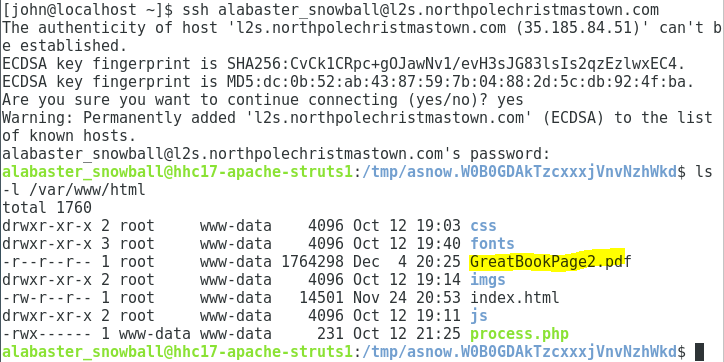


Note that the search found String username = “alabaster\_snowball”; in the file /opt/apache-tomcat/webapps/ROOT/WEB-INF/classes/org/demo/rest/example/OrderMySql.class. It did not show a password, but maybe it is in the file. Sure enough, when we cat the file we see that his password is stream\_unhappy\_buy\_loss.

## Password Reuse

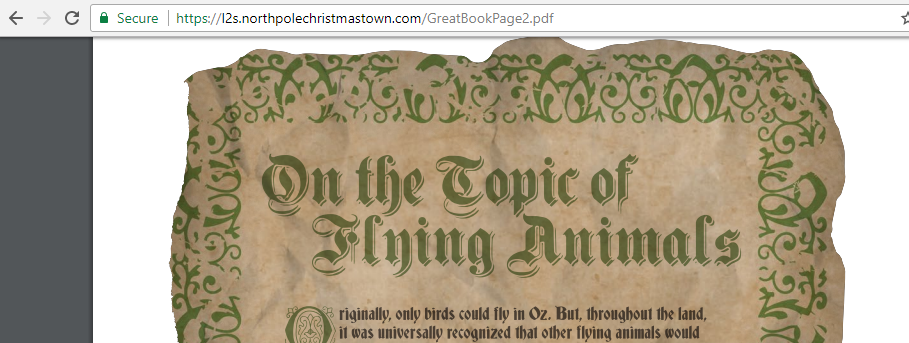
It is a major security problem when users employ the same password in multiple places. Surely, Santa’s engineer and security person would not be guilty of password reuse…

When we use alabaster\_snowball and stream\_unhappy\_buy\_loss to log in to the dev server (or l2s, as they are the same server) with SSH from our CentOS VM, we see this.



Well, we won’t have to mess with the exploit and reverse shell any more. Now that we have valid credentials, we can enter through the front door.

Just for fun, I got a directory listing of /var/www/html. The page we were looking for, GreatBookPage2.pdf, is right there on the l2s web root.



We didn’t need to exfiltrate the file from dev! (It was good practice with Netcat, though.) If you put a web shell on the l2s server, you probably discovered this a long time ago.

## Questions

1. What mistakes did Alabaster make that allowed us to compromise this server, and how could he fix them? List at least three mistakes and solutions.