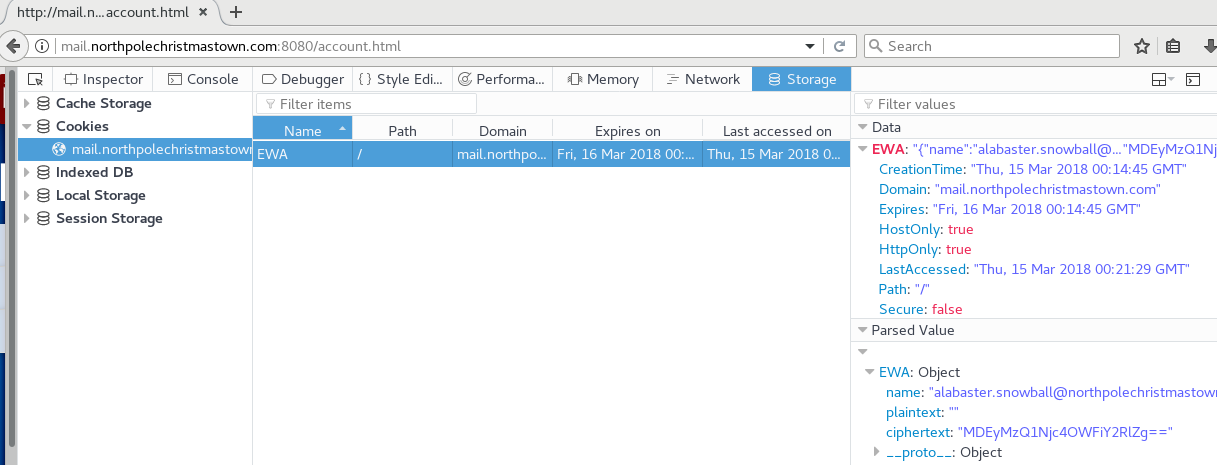
# Elf Web Access--Encryption Gone Wrong Part 5, Wrapping Up

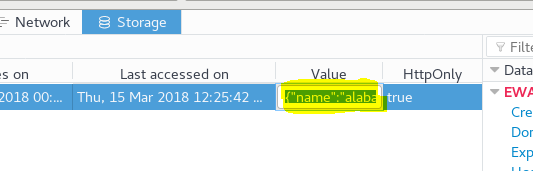
Once you learn how they work, the developer tools in both Chrome and Firefox make it easy to manipulate the cookies the browser sends to the web site.

## Firefox

Access Developer through the menu icon and select Toggle Tools, if they aren’t on already. Select Storage (hopefully you enabled it in Part 2.)

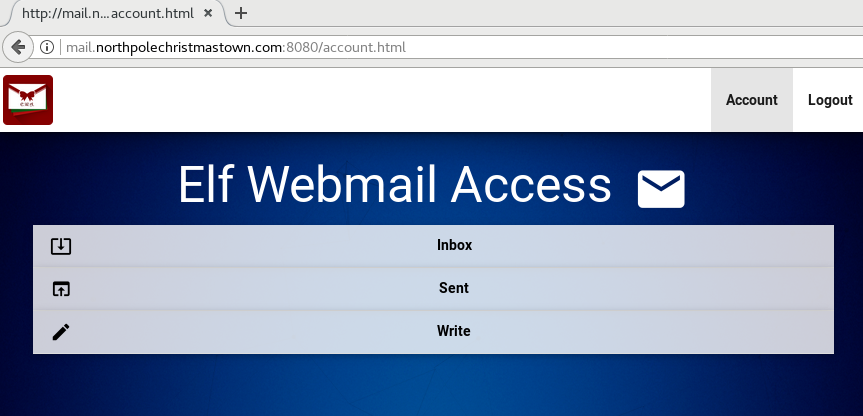


You can change the cookie by double-clicking in the Value area, and then editing the value. I could never get the Value column to be as wide as I wanted, but it is useable. I usually copy the contents and paste them into a text editor. Once I’ve made the changes I want, I paste it back into the tool



Edit the cookie so that name is [alabaster.snowball@northpolechristmastown.com](mailto:alabaster.snowball@northpolechristmastown.com) and ciphertext is a 16-byte string that is encoded in base64, like MDEyMzQ1Njc4OWFiY2RlZg==. Leave plaintext empty.

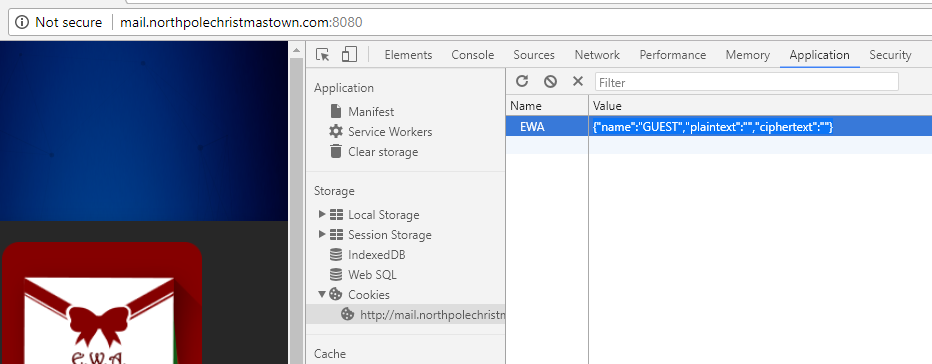
Then just go to the navigation bar and click enter to cause the page to reload.



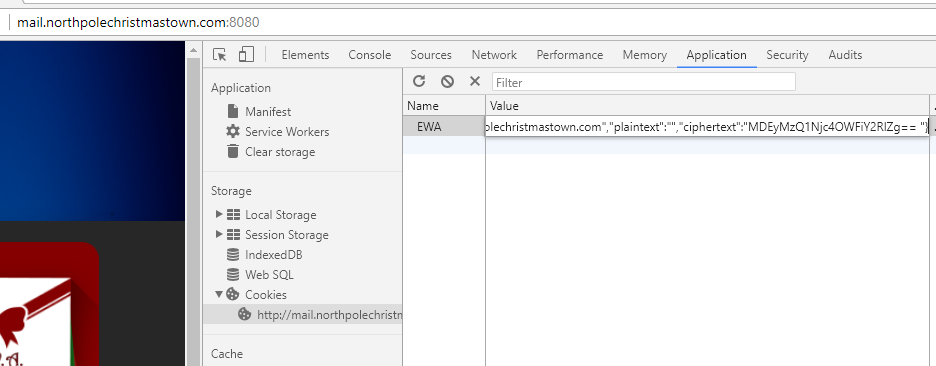
Success!

## Chrome

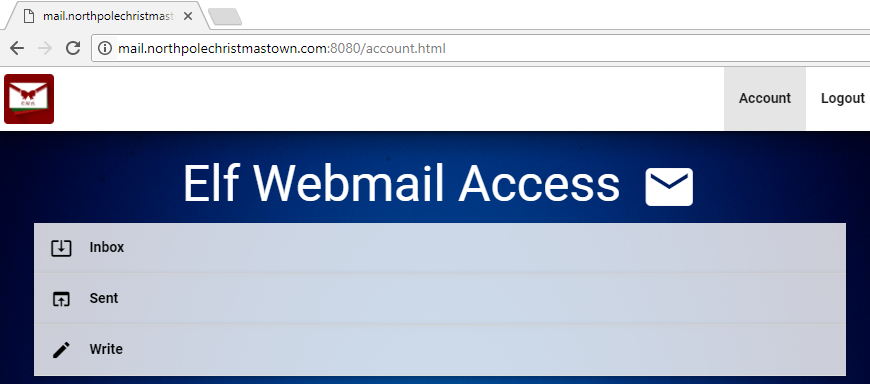
Access Developer Tools and select Application, Cookies. Double-click in the Value area to edit the cookie.



Edit the cookie so that name is [alabaster.snowball@northpolechristmastown.com](mailto:alabaster.snowball@northpolechristmastown.com) and ciphertext is a 16-byte string that is encoded in base64, like MDEyMzQ1Njc4OWFiY2RlZg==. Leave plaintext empty.



Cause the page to reload, and…



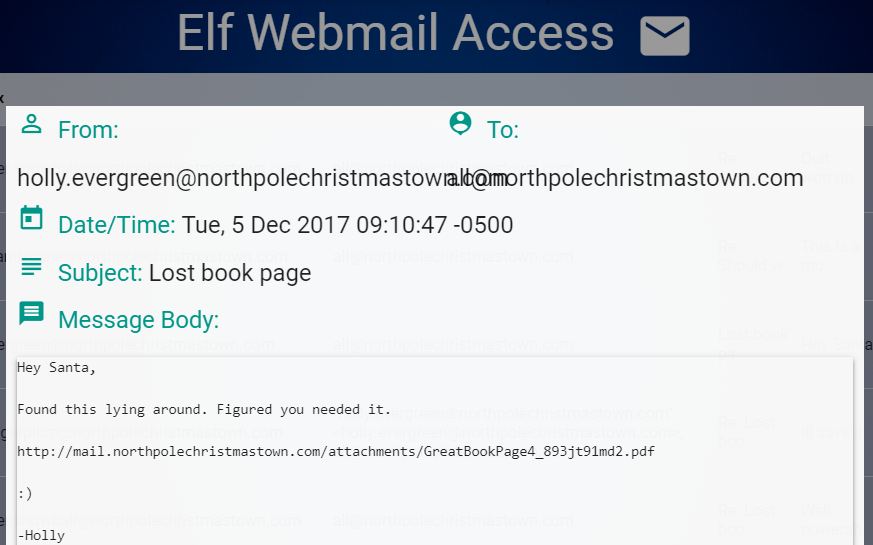
Break-in complete!

## The Great Book Page

If you peruse Alabaster’s email you will find an email from Holly Evergreen with the subject, Lost book page.

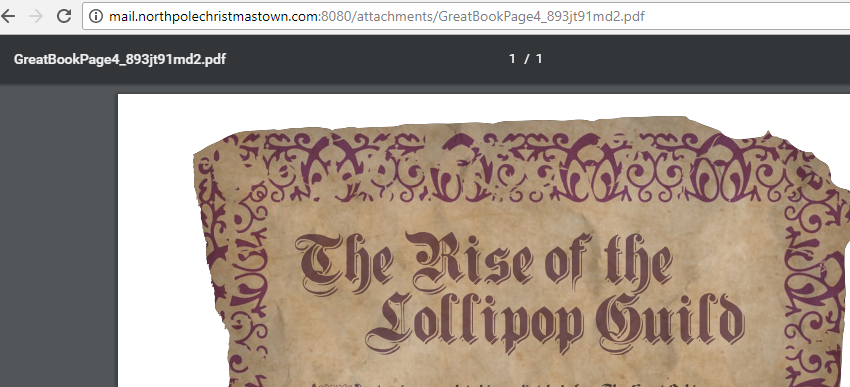


Holly has attached the page to her email. EWA handles attachments by creating links.

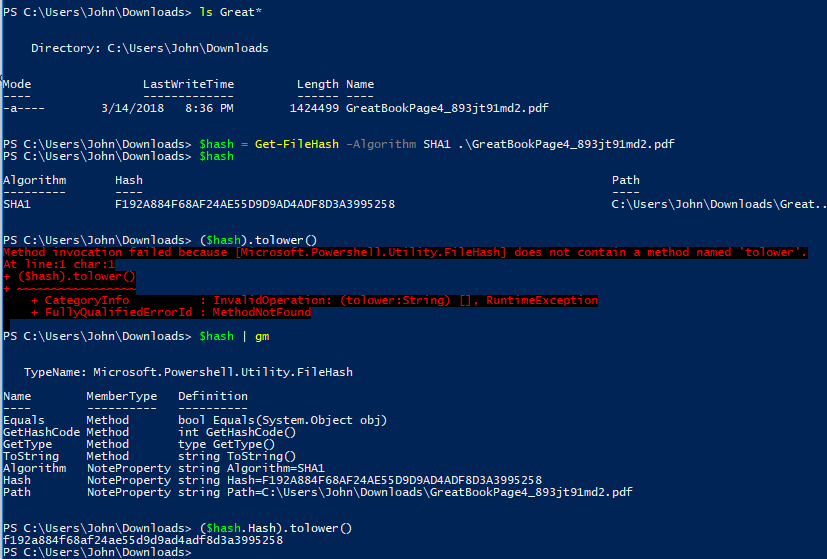


If we go to that link (<http://mail.northpolechristmastown.com/attachments/GreatBookPage4_893jt91md2.pdf> or in my case,

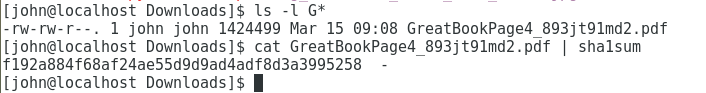
<http://mail.northpolechristmastown.com:8080/attachments/GreatBookPage4_893jt91md2.pdf> ) we find the Great Book Page.



Once we have downloaded the page, we can get the SHA1 hash by using PowerShell in Windows. If you want to enter the hash in your stocking on the Holiday Hack site it will only take lower case, so we need to convert it to lower case.



In Linux, it is a little simpler.



In either case, the SHA1 hash is f192a884f68af24ae55d9d9ad4adf8d3a3995258.

## Questions

1. How could fix his cookie scheme to prevent the vulnerability that we exploited?
2. What other things can Alabaster do to protect his server?