Bruce Phommaly

INFOTC 2910 – Cyber Security

Aaron Scantlin

Overview

My project is the integration of two-factor authentication into a current website of mine.

I have commented out most of the functionality of the code within each file as clearly as I could.

However, I did not comment much of the css, html (form fields), or jquery (mainly error message and one button)

(Progress tracking - <https://github.com/PoacherNews/PoacherNews>)

The files which I have created / modified regarding the two-factor authentication are as follows:

index.php (modified lines 3-4)

TFA.php (created)

recoveryCode.php (created)

doc/CreateTables.sql (modified lines 24-26)

includes/header.php (modified lines 2-11)

includes/settingsAccount.php (modified lines 115-132, 176-181)

includes/settingsTFA.php (created)

util/GoogleAuthenticator.php (open source courtesy of Michael Kliewe - <https://github.com/PHPGangsta/GoogleAuthenticator>)

util/tfaCheck.php (created)

util/handleLogin.php (modified lines 109-122)

util/settingsHandler.php (modified lines 137-238)

util/userUtils.php (modified lines 355-377)

Report

Initially, I was presented with two options of either integrating two-factor authentication through the use of an app or a physical token. I opted to go with the app route for a few reasons: the open source GoogleAuthenticator.php functions were easy to implement as my website is built on php, there were more resources provided on app-based 2fa, access to a phone and apps, and I’m too poor to buy a physical token.

As I began testing the with the Google Authenticator app I realized that the GoogleAuthenticator.php functions also supported other apps as well. So far, I have tested LastPass Authenticator, Google Authenticator, and Authy and they all work. After the QR Code was functional I added a recovery code as a backup measure. Using the php function password\_hash() to store the recovery code in the database and password\_verify() to verify the hash against inputted plaintext. Overall, I am pleased with the progress of the two-factor authentication and if I were to continue to add on to it then next would be safety measures to prevent brute-force attacks perhaps.

Testing

1. Login to PoacherNews.com

2. Hover over your username in the upper right of the header for a dropdown menu

3. Click Settings

4. Click Account on the left on the left side of the settings page

5. There will be a section designated for two-factor authentication near the bottom portion of the Account tab

6. P.S. If you find any bugs please let me know!

For testing purposes, the live site should be updated by Sunday (12/03/18) afternoon ([PoacherNews.com](https://poachernews.com/)).

Also, here is a premade account if you do not wish to make one:

Username – Aaron / Password – Password1234

Although, the submitted code may be subject to change.

However, if you would like to test the submitted code locally then please email me (bypxtd@mail.missouri.edu) for the database information. As I would rather not give out that information out if I do not have to.