COSC 366 Course Project

Due Tuesday Nov. 15 @ 11:59 PM

In this project, you will make a phishing website independently.

Description:

> Make a phishing website that looks like a popular website out there but with false information, e.g., a fake news site. Your phishing website should include a login page that is used to steal the username and password upon user login. For demo purposes, you can trick yourself using the defined methods described below and pretend that you fall victim. For fun, you can trick your friends into going to your phishing site. Remember to let them know afterwards. Keep in mind that there are risks associated with making your phishing website go live. You may be hunted down by the admin of the webhost you use or have your personal WAN IP blacklisted online. So, I do not recommend you do that. You do not need to publish the website for demo purposes. **Do not** publish your site on any UT machines or using any UT IP addresses. You can run the website on your local machine using a WAMP, MAMP, or LAMP stack for example.

You should implement the following features for your phishing website:

1. Have two defined methods of tricking victims into using the phishing site, e.g., shortened URL sent via email, or posted on social media, etc.

2. Store credentials in a database to prove validity of attack, but passwords should be slightly obfuscated before storage, so that no real credentials are stored, e.g., only store the first and/or last two characters of the password.

3. Redirect from phishing site to the real site, without leaving evidence to the victim that they were at a phishing site. There are multiple ways to accomplish this using JavaScript among other languages.

4. Use a TLS certificate so that the site appears even more legitimate. You can set up a self-signed certificate to achieve this. Please read this article: https://letsencrypt.org/docs/certificates-for-localhost/ and be sure to pay attention to the section at the end, “Making and trusting your own certificates.”

5. Implement two SQL injection vulnerabilities for your website using the tricks covered in class, e.g., ’ or 1=1--, ’; Drop Table Users--, and show how to exploit them.

6. Have a download link to “malware” on the site. You can use any benign file or program on your site for download. Include a SHA-256 hash of the “malware” visible on the site so that victims trust it.

Deliverables:

1. A comprehensive report that clearly describes the project goal, your overall plan, the challenging issues you encountered, the approaches and techniques you tried, the tools you used, the results (failure is acceptable but you need to show all the steps you have gone through), and your conclusion including what you have learned, what you would like to improve if given more time, and the experiences you want to share. Use diagrams, figures, tables, and screenshots where you see fit. Attach your code if applicable.

2. A demo video with the link provided in the report. The video should start with a brief introduction of yourself. You will show all the necessary tools, techniques, steps, and results, just like in a “How to make blueberry muffins” video.