Tokens (TOTP & HOTP)

## Summary

This lab investigates using 2FA tokens. Specifically Time-based one-time password (TOTP) and hash-based one-time password (HOTP) standards. TOTP is commonly seen in phone apps providing 2FA.

## Tools/Resources

Parrot: browser, python

Phone app: QR code reader, 2FA token provider.

Background resources: <https://jacob.jkrall.net/totp> and <https://2fa.glitch.me/>

## Tasks

1. Download and run a python app:

curl https://raw.githubusercontent.com/kengraf/TOTP/master/google\_authenticator.py -o tokens.py

python3 tokens.py 80

1. Review the function get\_otp\_token(secret, counter). It does all of the calculations for OTP.

Resources

1. Open <http://localhost>

A screenshot of a qr code

Description automatically generated

1. Register a new user. Any name is fine, as well as picking a new 32 hexdigit secret. Click “RegisterUser”

A screenshot of a computer

Description automatically generated

1. Capture the QR code value. Using your phone’s OTP 2FA app or this page should generate the same results.
2. Test the functionality of valid and invalid names and tokens. Refreshing the page will give you a new TOTP. The program is written with a zero-time skew to more readily show validation errors. Every time you used HOTP the counter will increment.

A screenshot of a computer

Description automatically generated A screenshot of a qr code

Description automatically generated

## Submission

Upload to Canvas a docx or pdf containing your QR code URI and a screenshot showing a valid OTP entry.

## Additional Thoughts

TOTP works on a 30 second window. Some time skew is to be expected. How we can handle faster/slower machines? The standard allows for accepting the time periods before and after the current window, thus creating a 90 window.

Can HOTP counters get out of sync? Yes, failed communications, multiple devices, and server load are all possible. Like TOTP a window of values is recommended. Out side that a device reset is required.

Is TOTP/HOTP “A new Google thing”? No IETF standards have been around for decades.