Assessing Password Policy Compliance on Ohio County and City Websites

Annika Hall, Benjamin Purdum

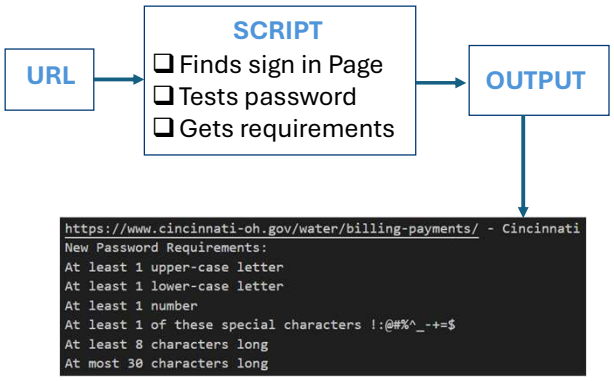
Advised by Dr. Raiful Hasan

Abstract

- State, county, and city government websites in Ohio provide residents with online access to services such as utility payments, account management, and other public interactions. These platforms rely heavily on **password based authentication**, making adherence to current security guidance essential.
- **Project Goal**: Evaluate whether residents facing Ohio government websites comply with **password policy recommendations** outlined in NIST Special Publication 800-63B.
  - minimum password length, composition requirements, and whether policies appropriately reflect authentication context.
- **Strategy**: create a script to parse county and city websites and record their password policies for analysis.

Methodology - Script

- Built a **script** in Python using the Selenium library to extract password requirements



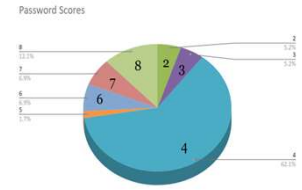
Methodology - Analysis

- Collected password policies from 60 Ohio municipal websites using the script
- Evaluated: minimum length, character requirements, MFA
- Scoring system:
- **Complexity** (0–4): uppercase, lowercase, number, special
- **Length** (0–4): scaled to 12-character baseline
- Combined into 0–8 strength score
- Benchmarked against National Institute of Standards and Technology SP 800-63B

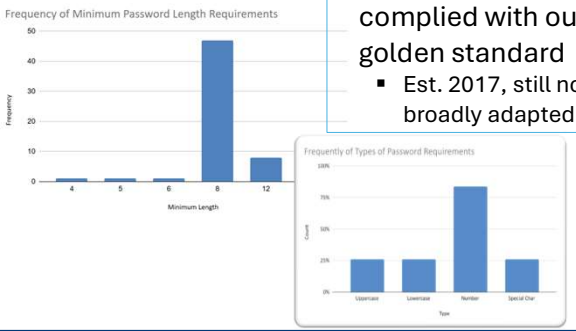
Our Golden Standard

- Providers that use a **single-factor authentication** method should have **minimum password length** of **15 characters**
- Any providers using a **multi-factor authentication** method may have a reduced **minimum password length** of **8 characters**
- All **ASCII** and **Unicode** characters should be accepted, including the space character.
- A period password change requirement should **NOT** be enforced, unless the password has been **compromised**
- The password should be compared against a known list of **leaked** or **insecure** passwords.
- Providers should **NOT** impose any other **composition rules** on passwords
  - Derived from NIST SP 800-63B

Results



- 55% share identical policy (8-character, minimal complexity)
- **0%** of Ohio city and county websites complied with our golden standard
  - Est. 2017, still not broadly adapted



Future Work

- Expand **beyond** Ohio (regional / national comparison)
- Deeper analysis of MFA strength and deployment
- Identify shared vendor platforms
- Track policy evolution over time

References

•National Institute of Standards and Technology. *Digital Identity Guidelines: SP 800-63B (Rev. 4, 2025)*
•https://pages.nist.gov/800-63-4/sp800-63b.html
•https://www.nist.gov/cybersecurity/how-do-i-create-good-password
•USENIX (2022). *Password policies of most top websites fail to follow best practices* — Kevin Lee, Sten Sjöberg, Arvind Narayanan https://www.usenix.org/conference/soups2022/presentation/lee
•USENIX (2023). *A Large-Scale Measurement of Website Login Policies* — Suood Al Roomi, Frank Li https://www.usenix.org/conference/usenixsecurity23/presentation/al-roomi