Agenda

- Subdomain Takeover

Subdomain

- a smaller part of a larger domain.
- e.g., cs.boisestate.edu is a subdomain of boisestate.edu; coen.boisestate.edu is also a subdomain of boisestate.edu.
- e.g., boisestate.edu is a subdomain of .edu
- every domain is a subdomain of some other domain, except the root (.) domain.

Subdomain Takeover Vulnerability

- Very popular type of website vulnerbility.
- Occurs when an attacker claims the ownership of your subdomain

When Subdomain Takeover is possible

- Cloud IP reuses (Amazon EC2, Microsoft Azure)
- Third-party services (e.g., Github Pages) abandoned
- Domain expires

Remediation

- Remove DNS records when you don't need them

References

A large portion of the material is adapted from:

- "All Your DNS Records Point to Us Understanding the Security Threats of Dangling DNS Records" - by Daiping Liu, Shuai Hao, and Haining Wang