Account Management

Troy Hunt
troyhunt.com
@troyhunt

pluralsight
hardcore developer training

Outline

- Understanding password strength and attack vectors
- Limiting characters in passwords
- Emailing credentials on account creation
- Account enumeration
- Denial of service via password reset
- Correctly securing the reset processes
- Establishing insecure password storage
- Testing for risks in the “remember me” feature
- Re-authenticating before key actions
- Testing for authentication brute force

Understanding password security

- **Password security is driven by two primary factors**
    - Strength
    - Uniqueness
- **The more of each, the better!**

Sources of attacks against passwords

- **Remote**
  - Man in the middle attack against the transport layer
  - Password retrieved after being sent in an email
  - Accounts brute-forced via HTTP posts
  - Admin facility compromised
  - SQL injection risk exploited
- **Local**
  - Passwords retrieved from a backup
  - Admins with direct access to password storage
  - Brute force attacks against password cryptography

Common password storage practices

- **Plain text**
  - There’s no cryptography, everything is immediately exposed if the password storage is breached
- **Encrypted**
  - Encryption (usually via a symmetric key) exists, but… there’s also *de*cryption
- **Hashed**
  - A one-way, deterministic algorithm which means that passwords can’t be *un*hashed

Protecting against authentication brute force

- **Account lockout**
  - Disable the account after X failed login attempts
  - …but then you need a mechanism to re-enable it
- **Restrict logon attempts by IP address**
  - Set an allowable “rate” for the same IP to attempt to login
  - …but attackers may have many IPs and legitimate users may share IPs
- **Fingerprint the client and scale the rate**
  - Uniquely identify the client based on request attributes then slow the rate at which they can attempt to logon
  - …but the fingerprint can be manipulated by an attacker

Summary

- **Help customers maximise their password strength**
  - No arbitrary length limits, there are no “special” characters!
- **Credentials never go into email. Ever.**
- **Account enumeration risks can disclose account holder identities**
- **Be conscious of a DoS on user accounts**
  - Always verify ownership before resetting
- **Always provide a reset link to set a new password**
  - Make it a time-limited, one time token keyed to the user
- **Look for practices which disclose improper password storage**
  - If you can get a plain text password, the storage is insufficient
- **Ask for re-authentication before key actions are performed**
- **Don’t allow endless attempts to authenticate to the system**
  - Lockouts, throttling and client fingerprinting are all potential mitigations