Web Design and Development

Week 8

Web Security

Introduction

Security

- Authentication
- Authorization
- Encryption
- Threats
- Tools
- ASP.NET Authentication

Baked In
Not Bolted On

Authentication

- Ensure that person accessing your site is:
  - A registered user
  - Who they say they are
- Mechanisms
  - Username/Password (Passphrase)
  - Social Logins
  - Two Factor
  - Others

Authentication
Username/Password

- Original mechanism
- Still most common
- Relies on password only being known by registered user
- Problems
  - Sticky notes
  - Simple passwords (dictionary)
  - Easy for computers to discover by brute force

Authentication
Username/Password

- Password security
  - During transmission (TSL/SSL)
  - When stored (salted hash)
- Password expiration (can’t reuse)
- Password policy
  - Length
  - Content (special characters, digits, uppercase)

Authentication
Username/Password

- Password reset
- Login lockout
  - Number of failed logins
  - How long before user can retry
  - How does user reset
    - Call
    - Email (time limited)
    - Security questions
- Bot (not human) protection
  - CAPCHAs

Authentication
Social Logins

- Facebook, Twitter, LinkedIn, Google, GitHub, etc.
- Users may prefer to login with an existing login
- App can ask for permissions to access various items of information from the social site

Authentication
Social Logins

- Requires access application keys from each social site
- Redirected to social site to authenticate
- Social site passes verification and claims to Web site
- Site can now retrieve user information from site used for authentication
- Based upon OAUTH2 standard

Authentication
Two Factor

- Requires additional code beyond login credentials
- Code is generated:
  - by system and sent to user
  - by device user has (time based)
    - UbiKey (https://www.yubico.com/)
    - An app (Google Authenticator)

Authorization

- Ensure that person accessing your site:
  - Has permissions to perform an action
- Mechanisms
  - Roles
  - Claims

Encryption

- Types
  - Symmetric (Secret key)
  - Asymmetric (Public/private key combination)
- Different algorithms (Triple DES, RSA, BlowFish, TwoFish, AES)
- Key Length (256 bits)
- Key management
- Where to apply
  - Transport
    - SSL (Secure Socket Layer)
    - TLS (Transport Layer Security)
  - Storage
    - Sensitive information at rest
- Two Way

Hashing

- One Way
- Different algorithms (MD5, SHA, others)
- Used to store passwords
- Can be vulnerable to brute force by computers
  - Pre-computed lookup tables
  - https://crackstation.net/
- Salted hashes

Threats

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Components with Known Vulnerabilities
- A10 Unvalidated Redirects and Forwards

Tools

- Threat Modeling
- Code reviews
- Static code scanning
- Penetration tests
- OWASP (https://www.owasp.org/)
  Open Web Application Security Project

ASP.NET MVC
Version 5 (.NET 4.6.x)

- New **Identity** Framework (formerly membership)
- OWIN (Open Web Interface for .NET)
- Out of the box support (NuGet) for:
  - two factor authentication
  - social logins
- .NET has libraries for encryption
- OWASP .NET Project
- Third party open source
  - Encryption
  - Social login providers

Web Design and Development

Week 9

REST/WebAPI

Introduction