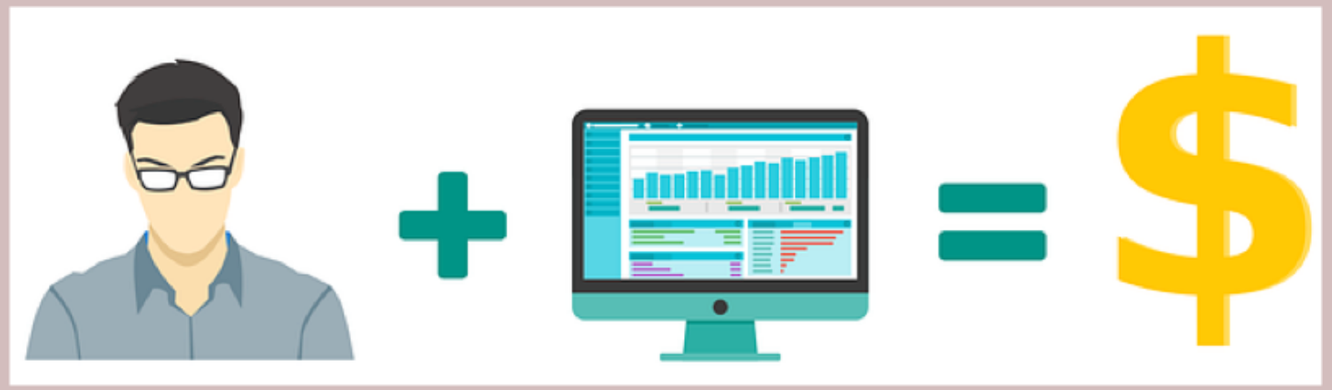
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Coding for Security

Security Architecture & Tool Sets

Coding for Security

- Security should be added in requirements
- Security is built during design and coding
- Security is *then* tested in prototypes and final products



Secure Coding Practices

- Have an organizational secure coding policy
- Conduct risk assessments (and ongoing assessments) to prioritize issues to remediate
- User input validation (prevent XSS/SQL inject)
- Consider your error messages
  - What information is being given? Too much?
- Database security in application and database
  - Prevents data leaks

Secure Coding Practices

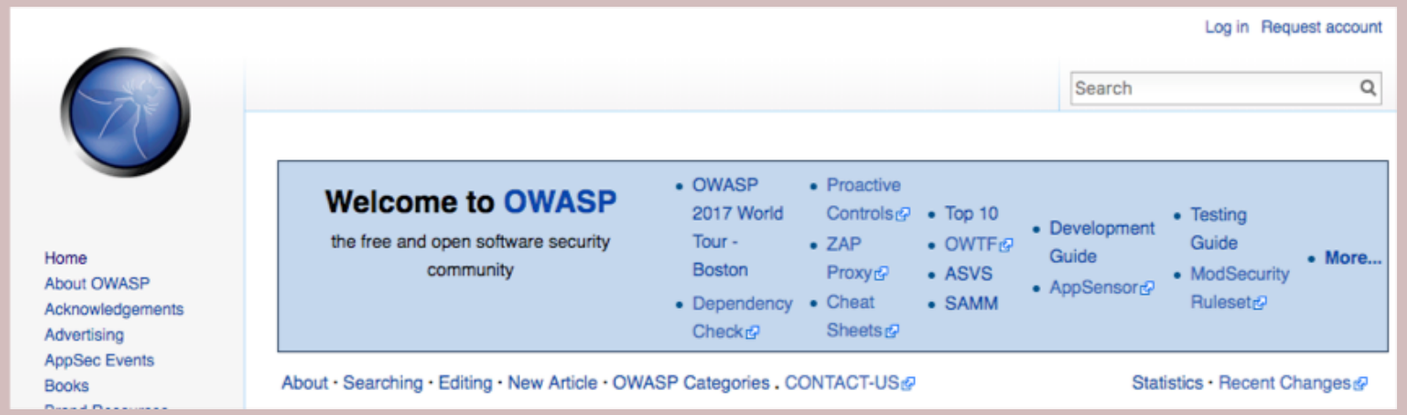
- Encrypt sensitive information being stored
- Hash passwords your applications store
- Design for availability and scalability
  - Conduct load and stress testing
- Conduct monitoring and logging
- If possible, utilize multifactor authentication

Secure Coding Practices

- Code for secure session management
  - Prevents session hijacking
- Proper cookie management
  - Secure cookies if used in web applications
- Encrypt network traffic
  - Use TLS to prevent network-based data capturing
- Secure the underlying infrastructure
  - As a cybersecurity analyst, your biggest impact will usually be on the infrastructure and not the code

Open Web Application Security Project (OWASP)

- Community hosting standards, guides, best practices, and open source tools
- Provides updated lists of proactive controls to test your web application's security
- Check out OWASP.org



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Source Code Management

- Use check-in/check-out and revision history to ensure you know what code is current version

- Source Control Management or Version Control tools, like Git, Subversion, or CVS

GitHub

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE