WhiteHat Security

Jim Manico – VP Security Architecture

When is a web security assessment tool effective for your web application security program?
Jim Manico

- VP Security Architecture, WhiteHat Security
- 15 years of web-based, database-driven software development and analysis experience
- Over 7 years as a provider of secure developer training courses for SANS, Aspect Security and others
- **OWASP Connections Committee Chair**
  - *OWASP Podcast Series Producer/Host*
  - *OWASP Cheat-Sheet Series Manager*
Website Security Strategies are Evolving…

FROM

• Checkbox Compliance
• Point in time assessments
• Tactical efforts to secure specific websites
• Taking precautions and accepting a certain level of risk

TO THIS

• Security throughout the SDLC
• Continuous Monitoring
• Strategic program to secure all Web assets
• Adopt “Hack Yourself First” methodology in all stages of the SDLC
Web Security Program Details

Characteristics of a “mature” website vulnerability assessment program:

- **Continuous Monitoring** (because the bad guys are)
- **Automated Assessment, DAST and SAST**
- **Manual Assessment, Business Logic and Vulnerability Triage**
- **Testing of Both Development AND Production Systems**
- **Developer Remediation Assistance**
- **Feedback Loop for Developer Training and SDLC Improvement**
- **Ability to scale all of these activities!**
All “Real Solutions” Must Combine…

- **People**: Cognitive ability, operate and interpret tool results
- **Process**: Organize and make efficient use of resources
- **Technology**: To scale the people and the process
Tool are good when...

- The organization has a sufficient number of “qualified people” to operate the tools and carry out the process. Calculate how often testing should be performed and to what depth.
- The collective costs of the “people, process, and technology” program are less expensive to perform in-house rather than outsource.
- When development teams do not challenge the credibility or validity of the tools output, and that of the tool operator.

• Failure to account for these issues may result in:
  - Expensive shelf-ware
  - Inability to scale to an enterprise-wide deployment
  - Runaway costs
  - Compliance Failure
  - Breach
Thank You!

Questions?

Jim.Manico@WhiteHatSec.com