Training on Secure Agile Software Development for JavaScript and .NET/C# Technology Stack

1. Intro

Would you like to improve security of your software products, build secure software development processes and manage security during the whole software life cycle? Our expertise both in software development and in information security serves as a solid ground for delivering professional Secure Software Development Lifecycle (Secure SDLC) consulting services.

Our Application Security Services include customizable parts of ***Secure SDLC Management*** for your company, ***Product Security Management*** *(including Security DevOps)* for your products and solutions, and ***Secure SDLC training*** for your personnel.

2. Secure SDLC Training

Like any other Secure SDLC component, *Secure SDLC training* can be and usually is combined with any other Application Security service. This description is intended to help you to define better what you want to improve in your personnel.

The service is delivered in the form of lectures, workshops, tests and consultations for:

- ***managers and team leads*** – on how to organize Secure SDCL process, procedures and artifacts, how to plan, manage and report about security activities, and how to communicate on security effectively;
- ***software architects and analysts*** – on how to derive security requirements from any business requirements and formulate them correctly, how to develop security architecture and secure design based on security requirements, and how to define security controls for software solutions;
- ***software developers*** – on how to interpret and implement security requirements, what are secure development best practices in general, what are secure practices for specific platforms, and how to avoid programming mistakes leading to security vulnerabilities;
- ***software testers*** – on how to plan and perform security testing including identification and validation of basic security bugs in applications, and how to ensure the implementation of security requirements.

You should order the Secure SDLC Training if you are concerned about security skills of your personnel.

© 2019 H-X technologies

3. Sample Training Program

Duration: 3 days

Section 1: Introduction to Secure Software Development Lifecycle

1. Secure Systems Development Lifecycle (Secure SDLC).
2. SDLC models (SAMM, BSSIMM, Microsoft).
3. SDLC practices for Agile:
   a) Trainings.
   b) Governance and metrics.
   c) Policies.
   d) Security Requirements Definitions.
   e) Quality gates/Bug bars.
   f) Security and Privacy risk assessments and reviews.
   g) Design requirements.
   h) Attack surface analysis and reviews.
   i) Threat modeling.
   j) Safe development tools.
   k) Unsafe functions.
   l) Secure coding guidelines.
   m) Static analysis.
   n) Dynamic analysis.
   o) Fuzz testing.
   p) Incident response planning.
   q) Secure configuration guidelines.
   r) Operational security practices.
   s) Secure SDLC implementation guidelines.
   t) Writing good use cases and abuse cases.
   u) Setting the right priorities.

Section 2: JavaScript and Web security.

1. JavaScript security model.
2. Same origin policy.
3. Frame sandboxing.
4. Content security policy.
5. Cross origin security sharing.
6. JavaScript signing.
7. Web-workers security.
8. Differences in the browser implementations of security features.
9. Common vulnerabilities:
    a) Cross-Site Scripting.
    b) Reflected XSS.
    c) Stored XSS.
    d) DOM XSS.
    e) Universal XSS (Flash, etc.).
    f) Vulnerable components (JavaScript libraries, Browser plugins).
    g) Lack of CSRF tokens.
    h) Lack of authentication for Ajax requests.
    i) Java applet exploits.
    j) Weak SOP configuration.
    k) Weak SSL protection. SSL stripping. Man-in-the-middle attacks.
    l) Insecure server headers.
    m) Insecure cookie flags.
    n) Insecure websockets.
    o) Privacy issues (geolocation, video recording, microphone access).
    p) Clickjacking.
    q) Unsafe coding practice: innerHTML, document.write, eval.
    r) Insecure session management. Session fixation. Weak session timeouts.
    s) Unsafe URL redirects.
    t) SQL injections.
    u) XML and Xpath injections.
    v) Other injections (LDAP, OS command, etc.).

© 2019 H-X technologies

w) Business logic flaws.
x) Concurrency and race conditions issues.
y) Unsafe deserialization.
z) Unsafe signatures (hash extension attacks).
aa) DDoS attacks and defenses.
bb) Security of SOAP and REST services.
cc) Metadata leak.
dd) Backup files.
ee) Social engineering attacks and protection measures.
ff) Password policies and account management.
gg) Admin interfaces.
hh) Improper error handling.
ii) Hardcoded credentials.
jj) Directory traversal.

Section 3: .NET and C# security.

1. Managed code.
2. .NET runtime.
3. .NET security model.
4. App domains.
5. Windows security architecture.
6. Privileges.
7. Access rights.
8. ACL management. Null DACL.
9. Service security groups.
10. Integrity levels.
11. Delegation and impersonalization.
12. Declarative and imperative application permissions.
13. Class security.
14. XSS protection.
15. CSRF tokens.
16. SQL injection protection.

17. SSL.
18. Authentication and authorization.
19. Cryptography functions.
20. Weak random number generators.
21. Secure password and key storage.
22. Auditing and logging.
23. Viewstate signing.
24. Unsafe reflection.
25. Number overflow handling.
26. Unsafe native libraries and memory corruption vulnerabilities.
27. Unsafe array access.
28. Safe resource permissions (file system, registry, mutexes, etc.).
29. Secure interprocess communication.
30. Code signing.
31. DLL hijacking.
32. Certificate PINNING.
33. Thread safety mechanisms.
34. Obfuscation.
35. Security of active browser components.
36. Windows Firewall.
37. IPv6 support note.
38. Secure service communication with desktop.
39. CardSpace.
40. Security in finalizers
41. Protected groups
42. Restricted groups for service accounts to restrict delegation between domains (Kerberos extension)

Section 4: Additional ASP.NET topics

1. ASP.NET Themes security
2. ASP.NET impersonalization
3. ASP.NET Session state data security considerations
4. ASP.NET events

5. ASP.NET routing security
6. ASP.NET validation under-posting risks
7. Filename case insensitivity warning
8. Special device names
9. Attacks in ASP.core
10. Timeouts for regular expressions
11. XXE and ASP.NET
12. Xpath and ASP.NET
13. Right URL redirects implementations
14. What do and what not to do in ASP.Net
15. Mistake: token based authentication with tokens that do not expire (requires change of the machineKey to revoke authentication)
16. Web-sockets Hijacking protection

© 2019 H-X technologies

4. Outcomes and Business Values of Application Security Services

Outcomes

- Guides for secure software development management adapted to the company's application designing and coding culture.
- Security architecture of the products and solutions.
- Security controls for all stages of software development life cycle, according to the customer's internal standards and methodologies, as well as international standards and best practices.
- Prompt and effective response to emerging application security problems and challenges.

Business values

- Security and quality of customer's applications, solutions, and products.
- Proper and mature organization of the software development projects, including the control and monitoring of development process.
- Mitigation of risks of unexpected expenses for software development and support by means of clear security requirements and architecture design, which results in the reduction of production scrap and rework.
- Increased security awareness and the establishment of a mature security culture of software development projects.

Make your software and systems secure from the beginning!

Send us your business requirements for analysis
to info@h-xtech.com, or call us +380996100702
to get security for your software products and whole organization!

5. Why us?

We are a team of cyber security professionals from Ukraine.
Highest qualification, flexibility and reliability are our main distinctions:

Experience in information security. Since 2001, our employees have gained rich information security experience in State sector, industry, pharmacy, telecom, retail, banking, IT outsourcing, etc. Late in 2015, we initiated the H-X project.

International security certifications. The specialists of H-X earned and keep up-to-date internationally recognized security certifications (OSCP, ISO 27001, CISSP, CEH, PCIP, CLPTP, etc.). These certifications cannot be obtained without confirmed years of experience and grueling exams passed. The certifications prove high professionalism and do not allow illegal or unethical behavior, otherwise they are immediately revoked.

Absolute legitimacy and confidentiality. The employees of H-X technologies strictly adhere to laws, regulations, corporate Code of Ethics and Penetration Testing Code of Ethics. We are ethical, white-hat hackers. Our legal support takes into account not only our and your rights and interests, but also the legitimate rights and interests of third parties. Our specialists sign your commitment forms personally, just like your employees.

Highest customization and flexibility. We provide professional cyber security service for any budget. We provide even free security assessment services. Our Express Pentest service is deeper than just a vulnerability scanning, but cheaper than pentests. We study every customer's needs carefully to prepare for the project. Unlike other companies, our pre-engagement documentation includes comprehensive set of detailed penetration testing parameters. Our approach allows the customer to understand more accurately what they pay for. During many projects, we have developed and continually improve our security assessment and implementation methodologies. This is our know-how and our distinction from competitors.

Highest quality. H-X uses modern comprehensive security assessment tools. Besides automatic vulnerability scanning, we actually do manual work. We do not claim that automatic vulnerability scanning is a pentest, like others do. H-X not only finds vulnerabilities and not just shows how exactly hackers can exploit them, but also helps customers eliminate the vulnerabilities and reduce risks. In every project, we develop suggestions for continuous improvement and are tracking changes in the security of our customers over the years.

6. Overview of Services

We specialize on Security Assessment and Penetration Testing services:

- External or internal wired or wireless network security assessments.
- Website, web application, web server security assessments.
- Desktop or mobile application security assessments.
- DoS/DDoS-attack modelling.
- Personnel pentest (social engineering methods).
- Industrial IT security audits, etc.

ISO 27001 and PCI DSS implementation:

- Scoping and prioritization – we provide this service free of charge.
- Initial audit, gap analysis and detailed project planning.
- Implementation of the security processes and operations.
- Certification audit.

Subscriptions and Hourly-Based Security Consulting Services:

- **Managed compliance** with GDPR, VDA, TISAX, PCI DSS, HIPAA, ITIL, ISF, NIST, COBIT, etc.
- **Application Security** and Software Engineering: Secure Software Development Lifecycle (SDLC) management and Security DevOps of specific software products.
- **Trainings and workshops** on Secure Software Development (SDLC, Secure DevOps). Personnel Security Awareness and Behavior Management. People-Centric Security.
- **Security Operations Center (SOC)** Implementation and SOC as a Service, including: technical vulnerability management, security event monitoring, security incident response and investigations, etc.
- **Development of Smart Contracts** and blockchain technologies. Software engineering.
- **Enterprise Risk Management** and IT-related Risk Management.
- **Business Continuity Management** and Disaster Recovery Planning.
- Physical security and other security areas.

7. Some of our Happy Customers

8. Conclusion

Our distinction is building real tangible security, not only security for formal compliance. At the same time, we have a considerable experience in GRC (Governance, Risks, and Compliance) services, as well as in implementation and maintenance of security management systems.

We help you to harden your security, protect your assets from cybercrime and get official recognition of your new security status.

Moreover, we train your personnel how to develop secure software and how to test its security.

Learn more about us and our services at https://h-xtech.com.

H-X

TANGIBLE CYBER SECURITY

Please ask your questions, try our free automated security assessment services, order an Express Penetration Test or get a quote for a Full-scale Penetration Test at h-xtech.com/services, or call us +380958860891