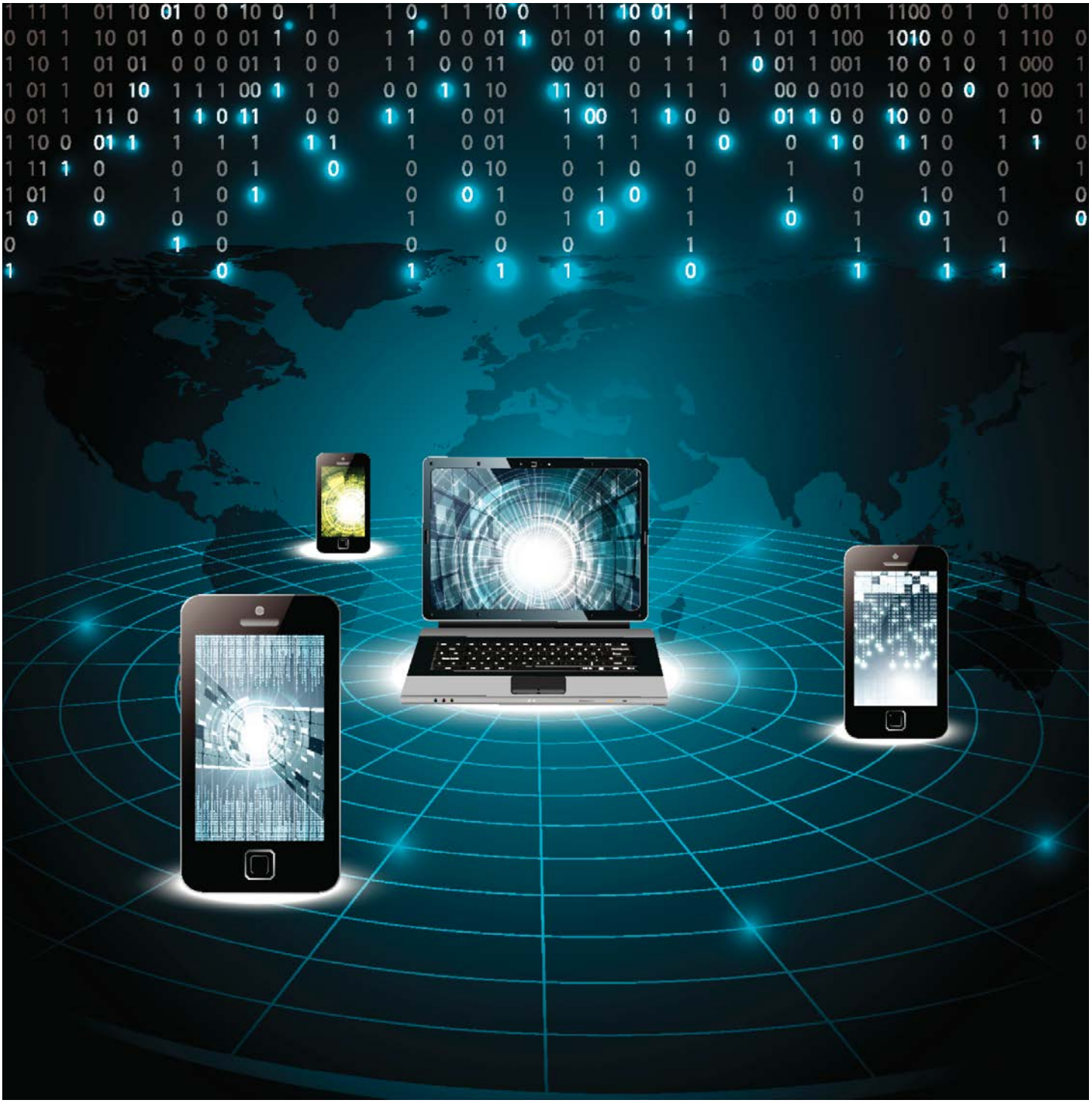
Enterprise Application Security Workshop Series



THE SAGE GROUP

Phil Costanzo
Phone 877-697-2434 x746
fax 877-697-2434
philc@thesagegrp.com

Defending JAVA Applications (3 Days)

In The Sage Group's Defending JAVA Applications workshop, participants will gain valuable insight into developing secure Java applications. The workshop will assist participants in understanding web application attacks and how they occur due to insecure coding practices. Participants will then see how to employ Java secure coding techniques to defend against these coding defects. Participants will learn to define and identify secure code, differentiate between secure coding methods, employ secure code in practice, and design and judge effectiveness of secure coding practice. Participants completing this class will find their secure coding abilities materially sharpened and able to integrate these techniques in your organization.

Introduction

- What is information security?
- Software security trends

Defending CSRF

- Review of the problem
- Non-tokenizer pattern
- CSRF in JAVA
- ESAPI Anti-CSRF tokens
- Generating an ESAPI CSRF token
- Implementing Anti-CSRF
- Solution

Defending Forced Browsing

- Review of the problem
- Downloading arbitrary files
- Forced browsing
- Declarative authorization
- Implementing web.xml
- Solution

Defending Insecure Storage

- Review of the problem
- Storing information
- Hashing
- Salted hash
- Adding a salt
- Solution
- Cipher block chaining
- EBC vs. CBC
- Solution
- AES encryption
- Encrypting files
- Decrypting files

Defending Parameters

- Review of the problem
- Buying a cheap TV
- HMACs
- Implementing HMAC
- Solution
- Regular expressions

Defending Session Hijacking

- Timeouts
- Configuring web.xml
- Solution
- Issuing new session IDs
- New session after login
- Solution
- Secure cookies
- Configuring web.xml
- Solution

Defending SQL Injection

- Review of the problem
- Accessing customers
- SQL injection
- Parameterized queries
- Implementing bind parameters
- Solution

Defending Redirects

- Review of the problem
- Redirect parameter
- Unchecked redirects
- Random access maps
- Using ESAPI access maps
- Solution
- Server side redirects
- Solution

Defending XSS

- Review of the problem
- How XSS happens
- XSS
- EASPI escaping
- The importance of context
- Using ESAPI Escaping
- Solution

Web Application Exploiting and Defending (3 Days)

The Sage Group's Web Application Exploiting and Defending workshop will help participants learn key concepts in web application security, the vulnerabilities that exist and how hackers exploit modern day applications for their own gain. Participants will be well-versed in describing common attacks and will be able to express how these scenarios could affect their own business applications. This workshop covers compliance requirements for PCI DSS 6.3.7 and 6.5.

Introduction

- What is information security?
- Software security trends

Authentication

- Authentication 101
- Factors of authentication
- Authentication weaknesses

Authorization and Access Control

- Authorization 101
- Horizontal & vertical privilege escalation
- Access controls common techniques

Session Management

- Session 101
- Hijacking sessions
- Session ID weaknesses
- CSRF
- Session management best practices

Data Validation

- Methods of validation
- Cross-site scripting
- SQL injection
- Data encoding issues
- Parameter manipulation

Cryptography

- Basics of cryptography
- Random numbers
- Hashing of data
- About SSL and weak encryption

Misc. Topics in Security

- Leakage and error handling
- Accountability
- 3rd party code
- File references

Defending .NET Applications (3 Days)

In The Sage Group's Defending .NET Applications workshop, participants will gain valuable insight into developing secure Microsoft .NET applications for the .NET framework up to 4.5. The workshop will assist participants in understanding web application attacks and how they occur due to insecure coding practices. Participants will then see how to employ .NET secure coding techniques to defend against these coding defects. Participants will learn to define and identify secure code, differentiate between secure coding methods, employ secure code in practice, and design and judge effectiveness of secure coding practice.

Participants completing this class will find their secure coding abilities materially sharpened and able to integrate these techniques in your organization.

Topics covered

- Defending CSRF
- Review of the problem
- Non-tokenizer pattern
- CSRF in .NET
- Anti-CSRF tokens
- Generating a token
- Implementing Anti-CSRF
- Solution

Defending Forced Browsing

- Review of the problem
- Downloading arbitrary files
- Forced Browsing
- Indirect Access Maps
- Creating mappings
- Implementing access maps
- Solution

Defending Insecure Storage

- Review of the problem
- Storing information
- Managing keys

Defending .NET Applications (cont)

- Salting Hashses
- Problem with hashes
- Adding a salt
- Solution
- PBKDF2
- Deriving a key from password
- Implementing RFC2898
- AES encryption
- Encrypting files with PBKDF2
- Decrypting files

Defending Redirects

- Review of the problem
- Tampered query strings
- Unchecked redirect
- URL mapping
- GUIDs mapped to URLs
- Solution

Defending SQL Injection

- Review of the problem
- Listing customer tables
- SQL injection tampering
- Bind parameters
- Changing the secure query
- Implementing bind parameter
- Solution

Defending XSS

- Review of the problem
- Insecure output
- XSS
- Escaping
- AntiXSS and encoder
- Importance of context
- Solution

Defending Authorization/Sessions

- Review of the problem
- Sessions
- Session timeout
- Configuring timeouts
- Solution
- Contained based authorization
- Modifying web config
- Solution
- Autocomplete

Defending PHP Applications (2 Days)

In The Sage Group's Defending PHP Applications workshop, participants will gain valuable insight in to developing secure PHP5 applications. The workshop will show participants the latest in web-based threats and how participants should go about defending them. Participants will learn to define and identify secure code, differentiate between secure coding methods, employ secure code in practice, and build safer web applications from the start. Participants completing this class will find their secure coding abilities materially sharpened and able to integrate these techniques in your organization.

Introduction

- OWASP Top 10
- Defending PHP5

SQL Injection

- About SQL injection
- Real-time example
- Newsflash
- Parameterized queries

Cross-site Scripting

- About XSS
- Blacklist validation
- Whitelist validation
- Safe re-encoding
- Safe vs unsafe
- HTTPonly

Session Hijacking

- About session hijacking
- Stealing credentials
- Encryption
- Short session timeouts

Parameter Manipulation

- About parameter manipulation
- Server-side validation
- Session variables

Insecure Storage

- About insecure storage
- Sensitivity of information
- Threat modeling
- Hashing passwords

Forcible Browsing

- About forcible browsing
- Page level authorization
- Programmed authorization

Cross-site Request Forgery

- About XSRF
- Meg goes shopping
- Decreasing timeouts
- XSRF tokens
- Re-authentication

Insecure Configuration

- About insecure configuration
- Users, software
- Hardening
- Standardized builds
- Patch management
- Updates and audits
- Unchecked redirects
- About unchecked redirects
- Newsflash
- Validating parameters
- Server-side checks

Clear-Text Communication

- About clear-text communication
- Eavesdropping
- Newsflash
- Encryption in transit
- Proper SSL implementations

SQL Injection Defenses

- Common pitfalls in PHP
- Parameterized queries in PHP
- MySQL
- PHP data objects

XSS Defenses

- Common pitfalls in PHP
- Whitelisting
- Output re-encoding in PHP
- HTTP Only in PHP

Session Hijacking Defenses

- Common pitfalls in PHP
- SSL Encryption
- Shorter session timeouts

Parameter Manipulation Defenses

- Common pitfalls in PHP
- Security logic
- Regular expressions
- Centralized validation

Insecure Storage Defenses

- Common pitfalls in PHP
- MCrypt library
- Hashing
- Storing passwords with Bcrypt

Forcible Browsing Defenses

- Common pitfalls in PHP
- Access controls
- Programmed authorization

XSRF Defenses

- Common pitfalls in PHP
- Best practices
- XSRF tokens

Insecure Configuration Defenses

- Common pitfalls in PHP
- Register globals
- Error reporting and trace
- Logging
- Safe mode
- Magic quotes
- Session management

Unchecked Redirects

- Common pitfalls in PHP
- PHP header redirects
- Indirect object mapping in PHP

Clear-Text communication

- Common pitfalls in PHP
- Enabling encryption
- Enforcing strong ciphers

Mobile Hacking and Securing (2 Days)

In The Sage Group's Mobile Hacking and Securing workshop, participants will discover mobile hacking techniques for Android and iOS. They will understand the platform security models, device security models, app analysis, file system analysis and runtime analysis for these popular mobile operating systems. This workshop will provide participants with the knowledge necessary to assess mobile app security including what hackers look for in mobile apps. Hacking apps themselves will equip them with the skills required to protect their own apps from attacks. Participants will come out with an understanding of the pitfalls to mobile device security and the importance of developing mobile apps securely. They will learn the concepts necessary to securely develop mobile in your organization.

Introduction

- The mobile landscape

Device Security Model

- Mobile OS security models
- App distribution models
- Sandboxing and permissions structure
- Differences from iPhone/Android platforms
- The risk of users who trust apps too much
- Common attack vectors in mobile security

Protocol Analysis

- Proxying Android / iPhone
- Handling SSL certificate trust
- Emulator & simulator proxying
- Physical device proxying
- Tools required for intercepting traffic
- LAB: Proxying mobile app traffic
- LAB: Mobile traffic manipulation

Device File System Analysis

- Android file system analysis
- Using android debugging bridge
- Retrieving files from the device
- iPhone file system analysis
- SSH access to iPhone
- SCP to retrieve files from device
- LAB: Insecure file storage
- Common data storage types for mobile OS
- Logging for developers
- Assessing logs on Android/iPhone
- LAB: Insecure logging

Mobile App Decompilation

- Android APK packaging
- Application layout
- Android manifest and permissions
- Disassembly and decompilation
- LAB: Basic encryption
- iPhone IPA packaging

Mobile Hacking and Securing (cont)

- Handling plists
- Assessing the binary
- LAB: Advanced encryption

Mobile Run-time Analysis

- Why runtime analysis?
- Debugging as an attack vector
- Rooting and jailbreak of devices
- Accessing Android memory at runtime
- DDMS and MAT
- LAB: Dumping memory
- iPhone debugging

Other Mobile Topics

- Mobile cryptography
- Password based key derivation
- LAB: Password complexity
- Jailbreak detection
- State of mobile malware
- Mobile malware defense

Mobile Run-time Analysis

- Why runtime analysis?
- Debugging as an attack vector
- Rooting and jailbreak of devices
- Accessing Android memory at runtime
- DDMS and MAT
- LAB: Dumping memory
- iPhone debugging

Multi-platform Development

- Why multiplatform?
- How wrapper APIs work
- HTML5 codebase concerns
- PhoneGap example
- Implications to JavaScript bridging
- Native features through JS
- JS to native API in iOS/Android
- Dynamic loading and minification
- LAB: HTML at rest

Mobile HTML5 Web

- HTML5 mobile apps
- Clickjacking
  - *Framebusting*
  - *X-FRAME-OPTIONS*
- Tapjacking
  - *Android defenses*
- SQL Injection (local vs mobile)
  - *Parameterized SQL*
- XSS
  - *Existing XSS mobile exploits*
  - *JS bridging concerns*
  - *Safe output encoding*
  - *Securing WebView*
- Local storage
  - *Use of local storage*
  - *Securing local storage*

Device API Weaknesses

- SSL
  - *Android / iOS SSL best practice*
  - *Weak ciphers*
- XML Parsing
  - *Prevalence in Android/iOS*
  - *External entity references*
- Virtual Keyboards
  - *iOS keyboard cache*
  - *Android 3rd party keyboards*
  - *PIN entry*
- Copy and Paste
  - *iOS UIPasteboard*
  - *Android ClipboardManager*
  - *Trouble with WebView*
- iOS Snapshots
  - *Preventing insecure snapshots*
  - *Good backgrounding*
- Geolocation
  - *iOS / Android geolocation management*
- Address Book API
  - *Privacy*
- URL Handlers / IPC
  - *iOS URL schemes*
  - *Skype vulnerability*
  - *Android intent filters / IPC*
- LAB: URLs handlers to XSS

Other Mobile Topics

- Endpoint Security
  - *Weak SSL*
  - *Securing cookies*
- Mobile Cryptography
  - *Password based key derivation*
  - *LAB: Password complexity*
  - *Jailbreak detection*
  - *State of mobile malware*
  - *Mobile malware defense*

THE SAGE GROUP

Phil Costanzo
Phone 877-697-2434 x746
fax 877-697-2434
philc@thesagegrp.com