UPCOMING EVENTS

AFCEA Luncheon
September 23, 2010 (11:30 am - 1:00 pm)
WIIG Network Social
September 23, 2010 (5:00 pm - 7:00 pm)
Fall Golf Outing
October 01, 2010 (All Day)
AFCEA Luncheon
October 28, 2010 (11:30 am - 1:00 pm)
YAC Bull & Oyster Roast
November 06, 2010 (2:00 pm - 6:00 pm)
AFCEA Luncheon
November 18, 2010 (11:30 am - 1:00 pm)
AFCEA Luncheon
January 27, 2011 (11:30 am - 1:00 pm)
View Full Calendar

ANNOUNCEMENTS

AFCEACMD Google Group
Luncheon - new location - MARTIN'S CROSSWINDS in Greenbelt
Luncheon Speaker - next Thusday!
IT'S NOT TOO LATE - Sign up Now for the WIIG Fundraiser - THIS SUNDAY!!
Fall Golf Outing, October 1st (all the details)
Fall 2010 NSA Acquisition/Industry Symposium, November 3rd
Fall Golf Outing, October 1st
Bull & Oyster Roast - November 6, 2010
Night at Camden Yards, purchase deadline: Tuesday 9/7!
WIIG Fundraiser on 9/12, RSVP by 9/9
Cyber Training
View All Items

OFFICER LOGIN

Officer Login

Training Week

PRINT EMAIL

AFCEA Central Maryland Presents Cyber Training Week. Training Week is a developing program for local delivery of professional development courses. The deeply discounted rates provided to members are representative of AFCEA Central Maryland Chapter and its partner's commitment to the community and ensuring critical skills are accessible.

Windows Exploits | CEH | SCADA | Adv Ethical Hacking | App Security | Rev Engineering | CISSP

Writing Windows Exploits (Sept 14-16)

Syllabus (pdf)

The Expert Penetration Testing course provides an in-depth and hands-on review of the most current exploit development strategies and techniques for the Microsoft Windows platform. This course is designed to provide a hands-on, interactive learning experience. To the end, the course includes approximately 30 minutes of lab work after each hour of lecture and Q&A time.

Price: $2,149

Registration: If you would like additional information on this training or if you would like to register, please contact Jamie Lichon at InfoSec Institute at 866-471-0059 ext. 7188 or jamie.lichon@infosecinstitute.com.

Location: 8161 Maple Lawn Blvd, Suite 300 Fulton MD 20759

Certified Ethical Hacker (CEH) (Sept 20-24)

The CEH Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.

Syllabus (pdf)

SCADA Security (Sept 27- Oct 1)

SCADA controls our nation's mission critical infrastructure, everything from the power grid to water treatment facilities. Gain homeland security skills, by learning to assess and secure SCADA systems. This course covers everything from field based attacks to automated vulnerability assessments for SCADA networks.

Syllabus (pdf)

Advanced Ethical Hacking (Oct 4-8)

InfoSec Institute's Advanced Ethical Hacking: Advanced Penetration Testing Training comprehensive 5 day program designed to bring you to the next level in terms of software exploitation skills. Very few people in the world have these skills, after completing the course, youw ill be in the top 5% of all hackers and pen testers in the world.

Syllabus (pdf)

Application Security & Penetration Testing (Oct 18-22)

InfoSec Institute's Award Winning 5-Day Web Application Penetration Testing Boot Camp focuses on preparing students for the real world of Web App Pen Testing through extensive lab exercises, thought provoking lectures led by an expert instructor. We review of the entire body of knowledge as it pertains to web application pen testing through a high-energy seminar approach.

Syllabus (pdf)

Reverse Engineering (Nov 1-5)

In any hands on reverse engineer training course, it is important to have the opportunity to prove to current or potential employers that you have the skills you say you do. This course prepares you for the top reverse engineering certification in the industry, the CREA. The exam is given on-site, InfoSec Institute has achieved a 93% pass rate for this certification.

Syllabus (pdf)

Certified Information Security Professional (CISSP) (Dec 6-10)

Security is a leading concern in every organization and the CISSP Certification is the premier security certification available today for information assurance professionals looking to differentiate themselves among their colleagues. In fact, the DoD 8570 directive recognizes the CISSP as an important credential for the DoD workforce.

SPONSORS

DRC DYNAMICS RESEARCH CORPORATION

more...

TRAINING WEEK

Cyber Training

Expert Penetration Testing: Writing Windows Exploits

More info...

NEWS AND PHOTOS

5K Pics - Set 5
5K Pics - Set 4
5K Pics - Set 3
5K Pics - Set 2
5K Pics - Set 1
Awards Night Candids
Awards Night Photos
Luncheon Pics (03.25.2010)
Luncheon Pics (02.25.2010)
Valentine's Gala Pics - 2
Valentine's Gala Pics - 1
Emerging Leadership Award Winner - Beth Sheehy
DYA Award Winner - Richard Windsor
DYA Award Winner - Randy Findley
2009 Bull & Oyster Roast Pics

Securible, LLC

Certified Ethical Hacker Training

About the Program

Securible, LLC can offer your organization Certified Ethical Hacker training. If you want to stop hackers from invading your network, first you've got to invade their minds.

The goal of the ethical hacker is to help the organization take preemptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits. This philosophy stems from the proven practice of trying to catch a thief, by thinking like a thief. As technology advances and organization depend on technology increasingly, information assets have evolved into critical components of survival.

If hacking involves creativity and thinking 'out-of-the-box', then vulnerability testing and security audits will not ensure the security proofing of an organization. To ensure that organizations have adequately protected their information assets, they must adopt the approach of 'defense in depth'. In other words, they must penetrate their networks and assess the security posture for vulnerabilities and exposure.

The CEH Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.

To achieve the Certified Ethical Hacker Certification, you must pass the CEH exam 312-50

Call Securible, LLC today at 703-879-3310 to see how we can help your organization meet it high quality technical training needs.

EC-Council
Accredited Training Center

CompTIA
Learning Alliance
CompTIA Approved Training

SCP Authorized Training Partner

Program Elements

Provided Resources

- Certified Ethical Hacker Instructor
- Ec-Council Authorized Courseware
- MeasureUp Practice Test Software
- Prometric Exam Voucher
- Dedicated equipment for each student

Course Options

- Flexible schedules including day, evening, or weekend sessions
- Dedicated class for your organization
- Catering

When an organization hires Securible here is what they get:

- Security solutions that address the organization's needs
- Cost effective solutions that are the right thing at the right time
- The quality guarantee of our work - we want satisfied customers and will do what it takes to keep the client satisfied

Organization Details

Securible, LLC

3213 Duke St #220
Alexandria, VA 22314
Phone: 703-879-3310
Fax: 703-754-8215
http://www.securible.com

DUNS #: 80-778-4991
Small Business
POC: Amee Devine

SCADA Security

Protecting our Homeland Security

InfoSecInstitute.com | 866-471-0059

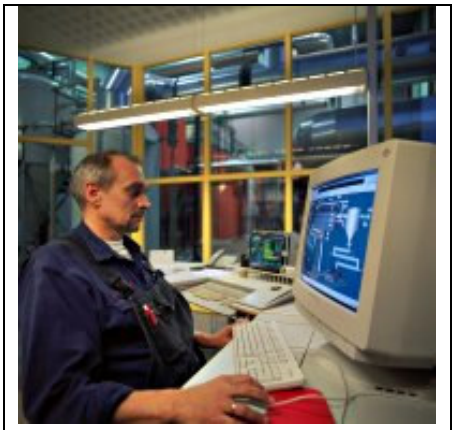
Learn to how to effectively secure your SCADA Systems

In this Brochure:

SCADA controls our nation's mission critical infrastructure, everything from the power grid to water treatment facilities. Gain homeland security skills, by learning to assess and secure SCADA systems. This course covers everything from field based attacks to automated vulnerability assessments for SCADA networks.

Learn the best practices for security SCADA networks and systems inside and out. InfoSec Institute shows you how to defend against both internal and external attackers to provide holistic security for critical industrial automation systems.

InfoSec Institute's instructors have real world hands on experience securing some of the most high profile energy delivery, water treatment and mission critical SCADA system.



Dozens of exercises in InfoSec Institute's Hands On Labs bring you up to speed with the latest threats to your SCADA systems. Learn subjects not found in books, on the internet, or taught anywhere else in any other information security class.

InfoSec Institute 1515 N. Harlem Av. Suite 205-25, Oak Park, IL 60302 USA
(866) 471-0059 www.InfoSecInstitute.com

Detailed 3 Day Syllabus

InfoSec Institute's SCADA Security: Protecting our Homeland Security comprehensive 3 day program is unique in the industry, no one else has a technical SCADA course available to the public.

Day 1: Best Practices and Perimeter Security

The first day begins with SCADA security best practices, with the rest of the day focused on properly implementing Physical and Logical perimeters. Topics Include:

- Introduction to SCADA Security Concepts
- Security Approach
- Industrial Network Policy Development
- SCADA Systems Audit
- Physical Security Considerations
- Field-Based Attacks
- Logical Security Perimeter
- DMZ Architectures for SCADA Networks
- Common DMZ Elements
- Common Rulesets
- Control Center Remote Access
- Vendor Access
- Antivirus Issues
- Security Patching Methodologies
- Compensating Controls
- Automating the Delivery of Patches to the SCADA Net

Every day includes lunch, snacks, soda, and finishes with catered dinner on InfoSec Institute!

Day 2: Access and Authorization Controls

Having learned how to properly segment, protect and assess the SCADA network, access control within SCADA systems are covered:

- Identification
- User Account Issues
- Password Policy Enforcement
- Two-Factor Authentication on Industrial Networks
- Role Based Authentication
- Location Based Auth
- System Based Auth
- SCADA Application Integration Security Issues
- Microsoft Active Directory Integration Issues
- Gold Standard Configs
- Strong Auth Support
- IPSec
- Data Security Classifications
- Current SCADA Security Standards
- Implementing Current Standards

Student Testimonials

See what previous students have to say:

"The instructor was one of the most brilliant people in the field of information security that I have met. After 2 weeks of being in his course, I feel that I have gained a great deal of knowledge in this field. Yet only about 10% of what he knows!!!"

Kawika Takayama, Verizon Federal Network Services

"This was the best course that I have ever attended. The content was perfect for keeping me interested. I've attended many courses where I didn't feel like the first few days were worth my time, but not here. I was constantly learning new things."

Seth Law, Zions Bank

Detailed 3 Day Syllabus Continued

Day 3: Intrusion Prevention and Detection

Having understood the complex nature of SCADA perimeter security, authentication and authorization models, the third day of the course focuses on detection of anomalous events that could indicate system abuse or worse.

- Vulnerable Systems Analysis
- SCADA Protocol Analysis
- SCADA Protocol Vulnerabilities
- Network Based Intrusion Detection
- Modbus/TCP specific Intrusion Detection Rules
- Log collection
- Log correlation
- Event management
- Alert Management
- Field WAN Networks
- Internet Based WAN Networks
- Wireless SCADA Security Issues
- Vulnerability Assessment
- Legacy Systems
- Exceptions
- Security Awareness Programs
- Final Exam (90 Questions)

InfoSec Institute
734 North Marion Street
Oak Park, IL 60302
(800) 305-5257
www.InfoSecInstitute.com
Sales@InfoSecInstitute.com

Advanced Ethical Hacking: Expert Penetration Testing

5 Day Detailed Syllabus

InfoSec Institute's Advanced Ethical Hacking: Advanced Penetration Testing Training comprehensive 5 day program designed to bring you to the next level in terms of software exploitation skills. Very few people in the world have these skills, after completion of the course, you will be in the top **5%** of all hackers and pen testers in the world.

Day 1: Advanced System Exploitation
Day 1 focuses on advanced exploitation techniques. A brief introduction to system exploitation will be covered, the rest of the day covers advanced topics, such as:

Introduction
System Exploitation Process
Buffer Overflows
Attacking DMZs
Port Redirection
Hiding from IDSs
Covert Channels
Windows Rootkits
Linux Rootkits
Privilege Escalation On Windows XP

Some of the instructor-led **hands-on lab** exercises:

System Exploitation
Attacking DMZs II
Covert Channels Lab
Circumventing IDS/IPS
Windows Rootkits
Linux Rootkits (LKMs)
XP Privilege Escalation

Capture the Flag exercises **every night**!

The day finishes with an all encompassing after-dinner Capture the Flag exercise. It ensures that you can put everything together that you learned during the day.

Day 2: Vulnerability Development
Having learned expert exploitation techniques in Day 1, Day 2 covers the art of vulnerability development. You will learn not how to use exploits, but how to **create** your own.

Introduction to Vuln Dev
C Language Buffer Overflows
Linux Stack Overflows
Writing Shellcode
Format String attacks
Windows Stack Overflows

InfoSec Institute
734 North Marion Street
Oak Park, IL 60302
(800) 305-5257
www.InfoSecInstitute.com
Sales@InfoSecInstitute.com

Some of the instructor-led **hands-on lab** exercises:

Overflowing Buffers
Lab Exploiting Stack Overflows
Linux Shellcode
Firewall ACL flushing shellcode
Format Strings Lab
Windows overflow lab
Windows shellcode
Overcoming Unicode Filters

Capture the Flag exercises **every night**

Day 3: Advanced Vuln Dev and Vulnerability Discovery
Having learned how to write exploits, Day 3 works on advanced concepts such as Heap Overflows and covers the vulnerability discovery process in detail.

Calculating offsets for Windows exploits
Heap Overflows
Introduction to Kernel Overflows
Advanced Vuln Dev - Heap Overflows
Windows vuln dev Security Vulnerability Genres
Fuzzing and Fault Injection
Instrumented Investigation
Binary Auditing
Source code analysis

Some of the instructor-led **hands-on lab** exercises:

Abusing the Structured Exception Handler (SEH)
Heap Overflow lab
Fuzzing Lab
Fault Monitoring Lab
Binary Auditing Lab with IDA Pro
Source Code analysis

Capture the Flag exercises **every night**!
The day finishes with an all encompassing after-dinner Capture the Flag exercise. It ensures that you can put everything together that you learned during the day.

Day 4: Reverse Engineering
This day deals specifically with the art of reverse engineering. Using tools such as IDA Pro, Softice, ProcDump, you will learn how programs are reverse engineered.

Introduction to Software Cracking
Commercial CD-ROM copy protections
Circumventing CD-ROM copy protections
Portable Executable (PE) Compression and Encoding
Using a Dissassembler
Creating Keygens
Attacking hardware/dongle protection schemes
Anti-debugging
Anti-disassembling
Detecting and Attacking SoftICE

Some of the instructor-led **hands-on lab** exercises:

InfoSec Institute
734 North Marion Street
Oak Park, IL 60302
(800) 305-5257
www.InfoSecInstitute.com
Sales@InfoSecInstitute.com

Basic software cracking
Intermediate software cracking
Removing timelimits
Manual binary decryption
Advanced software cracking
Detecting Breakpoints and Debuggers
Capture the Flag exercises **every night**!

Day 5: Advanced Web Application Hacking

Day 5 is totally dedicated to the latest frontier in hacking and information security -- web application hacking. You will come to master the advanced penetration of web applications and web enabled devices.

Attacking Java applets and applications
Web program fuzzing
Advanced SQL Injection
Proxy cache poisoning
SQL Injection in cookies
Attacking session Ids
Cross Site Scripting

Some of the instructor-led **hands-on lab** exercises:

Harvesting web application data
Web App fuzzing
SQL Injection on PHP/MySQL
Sneaky SQL Injection
Java applet hooking
Calculating the Return on Investment (ROI) for an ethical hack

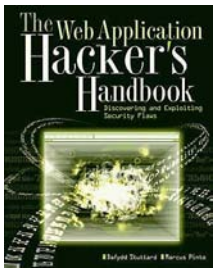
Web Application Penetration Testing Course

InfoSec Institute's 5-Day Web Application Penetration Testing Course

InfoSec Institute's Award Winning 5-Day Web Application Penetration Testing Boot Camp focuses on preparing students for the real world of Web App Pen Testing through extensive lab exercises, thought provoking lectures led by an expert instructor. We review of the entire body of knowledge as it pertains to web application pen testing through a high-energy seminar approach.

SC MAGAZINE AWARDS 2010 FINALIST Honored in the U.S.

GSA



InfoSec Institute's Web Application Penetration Testing Boot Camp - Course Description

INFOSEC INSTITUTE

Web Application Penetration Testing Course

InfoSec Institute offers this award winning Web Application Penetration Testing program to train and prepare IT Security Professionals. The highlights of this course include:

- Learn the Secrets of Web App Pen Testing in a totally **hands-on** classroom environment
- Learn how to exploit and defend real-world web apps – not just *silly* sample code
- Complete the 83 Step "Web App Pen Test Methodology", and bring a copy back to work with you
- Understand how to find Vulnerabilities in Source Code
- Take home a fully featured Web App Pen Test Toolkit
- Learn how to do OWASP Top 10 Assessments – for PCI DSS compliance and others
- Certified IACRB CWAPT (Web Application Penetration Tester) Exam delivered On-Site

Intensive Hands-On Training

The Web Application Penetration Testing course from InfoSec Institute is a totally hands-on learning experience. From the first day to the last day, you will learn the ins and outs of Web App Pen Testing by attending thought provoking lectures led by an expert instructor. Every lecture is directly followed up by a comprehensive lab exercise (we also set up and provide lab workstations so you don't waste valuable class time installing tools and apps). Typical lab exercises consist of a real-world app that demonstrates a vulnerability commonly found in a web app. You learn how to assess the app much as a black hat hacker would, exploit the app so that you can demonstrate the true risk of the vulnerability to the application owner. This can involve taking control of the application itself, downloading data the application stores, or potentially using the app as a launching pad to attack unsuspecting visitors with a malicious script. Finally, the lab will follow up with remediation steps so that the application owner can properly close down the security hole for good.

Nightly Capture The Flag (CTF) Exercises

After learning important Web App Pen Testing concepts during the day in a structured learning environment led by an expert instructor, it is important in the knowledge transfer process to attempt to apply the concepts you learned during the day in an unscripted, controlled exercise. The InfoSec Institute CTF exercises consist of a variety of web applications set up and designed to mimic the web presence of a company, a bank, a credit union, and an internal web app. You are then challenged by the instructor to capture specific flags that require you to apply your knowledge gained during the day. The CTFs are instructor-supervised, so if you get stuck, there is always a resource at hand to offer guidance.

At InfoSec Institute, we feel CTFs are a tremendous way to ensure you **leave the course with the skills needed to perform Web App Pen Tests at work after the course is completed.**

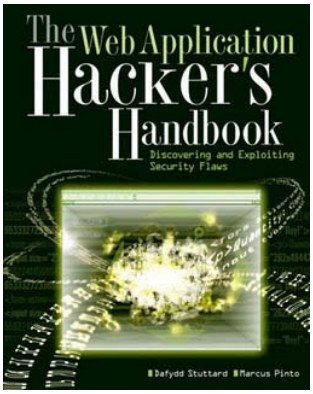
Up To Date, Current, Courseware

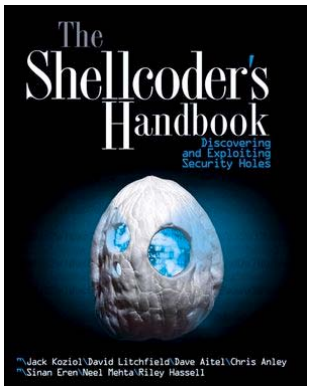
The threat landscape for Web Applications changes on a near continuous basis. Bad guys wishing to attack your applications know that they need to stay ahead of the curve in order to get in. For this reason, InfoSec Institute continuously updates our Web App Pen Testing courseware to cover the latest and greats threats, exploits and mitigation strategies.

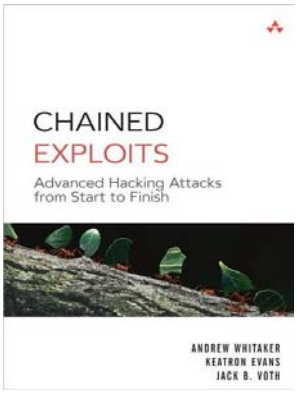
Web Application Penetration Testing Course

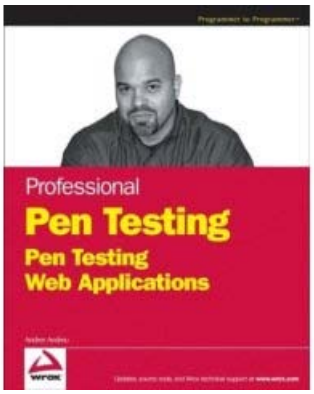
Expert Instruction

InfoSec Institute instructors that teach the Web App Pen Testing course are highly seasoned and have years of in the field pen testing experience. Not only are they active in the field of pen testing, they are industry-recognized experts that present at conferences such as DEFCON, Black Hat Briefings, RSA Security. Many of our instructors have authored some of the top Penetration Testing books on the market today:









Prerequisites

This course is a technical security course targeted at IT Security Professionals, Security Engineers, Penetration Testers, Software Developers and QA Engineers. You should have some experience with Penetration Testing, IT Security and the Software Development Life Cycle (SDLC).

Web Application Penetration Testing Course

The TOTAL Immersion Experience

During the five day program, our instructors give you 110% of their time and dedication to ensure that your time is well spent. The typical daily schedule rolls out as follows:

5 Day Web Application Pen Testing Class

Schedule	DAY 1	DAY 2	DAY 3	DAY 4	DAY 5
8:30am to 12:30pm	Web Application (In)security Core Defense Mechanisms – OWASP Top 10	Bypassing Client-Side Controls Attacking Authentication	Attacking Access Controls Attacking & Assessing Application Architectures	Exploiting Path Traversal Attacking Web App Users – Reflected Attacks	Attacking Compiled Applications Source Code Auditing
12:30pm - 1:30pm	Lunch Provided	Lunch Provided	Lunch Provided	Lunch Provided	Lunch Provided
1:30pm - 5:30pm	Web Application Technologies Relevant for Pen Testers	Attacking Session Management	Injecting Code	Exploiting Information Disclosure Vulnerabilities	Take IACRB CWAPT Certification Exam Onsite
5:30pm - 7:00pm	Break	Break	Break	Break	
7:00pm to 10PM (Approx.)	Capture The Flag Exercises	Capture The Flag Exercises	Capture The Flag Exercises	Capture The Flag Exercises	

Note: Schedule Subject to Change. Our instructors are there to see that all of your questions are addressed, even during evening labs.

Web Application Penetration Testing Course

InfoSec Institute's Web Application Penetration Testing - Course Details

Web Application (In)security
The Core Security Problem: Users Can Submit Arbitrary Input
Key Problem Factors
Immature Security Awareness
In-House Development
Deceptive Simplicity
Rapidly Evolving Threat Profile
Resource and Time Constraints
Overextended Technologies
The New Security Perimeter
The Future of Web Application Security

Core Defense Mechanisms – OWASP Top 10
Injection
Cross-Site Scripting (XSS)
Broken Authentication and Session Management
Insecure Direct Object References
Cross-Site Request Forgery (CSRF)
Security Misconfiguration
Insecure Cryptographic Storage
Failure to Restrict URL Access
Insufficient Transport Layer Protection
Unvalidated Redirects and Forwards

Web Application Technologies Relevant for Pen Testers
HTTP Requests, Responses, Methods, Headers
General, Request, Response Headers
Cookies
Status Codes
HTTPS
HTTP Proxies
HTTP Authentication
Server-Side Functionality
The Java, ASP.NET, PHP Platforms for Pen Testers
Client-Side Functionality
JavaScript
Thick Client Components
State and Sessions
Encoding Schemes, URL Encoding, Unicode Encoding

Bypassing Client-Side Controls
Transmitting Data via the Client
Auto-Discover Hidden Form Fields
HTTP Cookies
URL Parameter Injection
Manipulating The Referer Header
Tampering with Opaque Data
Hacking ASP.NET ViewState

Capturing User Data: HTML Forms
Length Limits
Script-Based Validation
Disabled Elements
Capturing User Data: Thick-Client Components
Java Applets
Decompiling Java Bytecode
Coping with Bytecode Obfuscation
Hacking ActiveX Controls
Reverse Engineering ActiveX
Manipulating Exported Functions
Fixing Inputs Processed by Controls
Decompiling Managed Code
Tampering with Shockwave Flash Objects
Handling Client-Side Data Securely
Transmitting Data via the Client
Validating Client-Generated Data
Logging and Alerting

Attacking Authentication
Authentication Technologies
Common Design Flaws in Authentication Mechanisms
Bad Passwords
Brute-Forcible Login
Exploiting Verbose Failure Messages
Exploiting Vulnerable Transmission of Credentials
Attacking Password Change Functionality & Forgotten Password Functionality
Exploiting “Remember Me” Functionality
User Impersonation Functionality
Incomplete Validation of Credentials
Non-Unique Usernames
Predictable Usernames & Initial Passwords
Insecure Distribution of Credentials
Implementation Flaws in Authentication
Fail-Open Login Mechanisms
Defects in Multistage Login Mechanisms
Insecure Storage of Credentials
Securing Authentication
Use Strong Credentials
Handle Credentials Secretively
Validate Credentials Properly
Prevent Information Leakage
Prevent Brute-Force Attacks
Prevent Misuse of the Password Change Function
Prevent Misuse of the Account Recovery Function
Log, Monitor, and Notify

Attacking Session Management
The Need for State
Alternatives to Sessions
Weaknesses in Session Token Generation
Meaningful Tokens

Hacking Predictable Tokens
Exploiting Concealed Sequences
Exploiting Time Dependency
Exploiting Weak Random Number Generation
Weaknesses in Session Token Handling
Disclosure of Tokens on the Network
Disclosure of Tokens in Logs
Vulnerable Mapping of Tokens to Sessions
Vulnerable Session Termination
Client Exposure to Token Hijacking
Liberal Cookie Scope
Cookie Domain Restrictions
Cookie Path Restrictions
Securing Session Management
Generate Strong Tokens
Protect Tokens throughout Their Lifecycle
Per-Page Tokens
Log, Monitor, and Alert
Reactive Session Termination

Attacking Access Controls
Common Vulnerabilities
Completely Unprotected Functionality
Targeting Identifier-Based Functions
Attacking Multistage Functions
Locating Static Files
Insecure Access Control Methods
Attacking Access Controls
Securing Access Controls
A Multi-Layered Privilege Model

Injecting Code
Injecting into Interpreted Languages
Injecting into SQL
Exploiting a Basic Vulnerability
Bypassing a Login
Finding SQL Injection Bugs
Injecting into Different Statement Types
The UNION Operator
Fingerprinting the Database
Extracting Useful Data
An Oracle Hack
An MS-SQL Hack
Exploiting ODBC Error Messages (MS-SQL Only)
Enumerating Table and Column Names
Extracting Arbitrary Data
Using Recursion
Bypassing Filters
Second-Order SQL Injection
Advanced Exploitation
Retrieving Data as Numbers
Using an Out-of-Band Channel

Using Inference: Conditional Responses
Beyond SQL Injection: Escalating the Database Attack
MS-SQL
Oracle
MySQL
SQL Syntax and Error Reference
SQL Syntax
SQL Error Messages
Preventing SQL Injection
Partially Effective Measures
Parameterized Queries
Defense in Depth
Injecting OS Commands
Injecting via Perl
Injecting via ASP
Finding OS Command Injection Flaws
Preventing OS Command Injection
Injecting into Web Scripting Languages
Dynamic Execution Vulnerabilities
Dynamic Execution in PHP
Dynamic Execution in ASP
Finding Dynamic Execution Vulnerabilities
File Inclusion Vulnerabilities
Remote File Inclusion
Local File Inclusion
Finding File Inclusion Vulnerabilities
Preventing Script Injection Vulnerabilities
Injecting into SOAP
Finding and Exploiting SOAP Injection
Preventing SOAP Injection
Injecting into XPath
Subverting Application Logic
Informed XPath Injection
Blind XPath Injection
Finding XPath Injection Flaws
Preventing XPath Injection
Injecting into SMTP
Email Header Manipulation
SMTP Command Injection
Finding SMTP Injection Flaws
Preventing SMTP Injection
Injecting into LDAP
Injecting Query Attributes
Modifying the Search Filter
Finding LDAP Injection Flaws
Preventing LDAP Injection

Exploiting Path Traversal
Common Vulnerabilities
Finding and Exploiting Path Traversal Vulnerabilities
Locating Targets for Attack
Detecting Path Traversal Vulnerabilities

Circumventing Obstacles to Traversal Attacks
Coping with Custom Encoding
Exploiting Traversal Vulnerabilities
Preventing Path Traversal Vulnerabilities

Attacking Web App Users – Reflected Attacks
Cross-Site Scripting
Reflected XSS Vulnerabilities
Exploiting the Vulnerability
Stored XSS Vulnerabilities
Storing XSS in Uploaded Files
DOM-Based XSS Vulnerabilities
Real-World XSS Attacks
Chaining XSS and Other Attacks
Payloads for XSS Attacks
Virtual Defacement
Injecting Trojan Functionality
Inducing User Actions
Exploiting Any Trust Relationships
Escalating the Client-Side Attack
Delivery Mechanisms for XSS Attacks
Delivering Reflected and DOM-Based XSS Attacks
Delivering Stored XSS Attacks
Finding and Exploiting XSS Vulnerabilities
Finding and Exploiting Reflected XSS Vulnerabilities
Finding and Exploiting Stored XSS Vulnerabilities
Finding and Exploiting DOM-Based XSS Vulnerabilities
HttpOnly Cookies and Cross-Site Tracing
Preventing XSS Attacks
Preventing Reflected and Stored XSS
Preventing DOM-Based XSS
Preventing XST
Redirection Attacks
Finding and Exploiting Redirection Vulnerabilities
Circumventing Obstacles to Attack
Preventing Redirection Vulnerabilities
HTTP Header Injection
Exploiting Header Injection Vulnerabilities
Injecting Cookies
Delivering Other Attacks
HTTP Response Splitting
Preventing Header Injection Vulnerabilities
Frame Injection
Exploiting Frame Injection
Preventing Frame Injection
Request Forgery
On-Site Request Forgery
Cross-Site Request Forgery
Exploiting XSRF Flaws
Preventing XSRF Flaws
JSON Hijacking
JSON

Attacks against JSON
Overriding the Array Constructor
Implementing a Callback Function
Finding JSON Hijacking Vulnerabilities
Preventing JSON Hijacking
Session Fixation
Finding and Exploiting Session Fixation Vulnerabilities
Preventing Session Fixation Vulnerabilities
Attacking ActiveX Controls
Finding ActiveX Vulnerabilities
Preventing ActiveX Vulnerabilities
Local Privacy Attacks
Persistent Cookies
Cached Web Content
Browsing History
Autocomplete
Preventing Local Privacy Attacks
Advanced Exploitation Techniques
Leveraging Ajax
Making Asynchronous Off-Site Requests
Anti-DNS Pinning
A Hypothetical Attack
DNS Pinning
Attacks against DNS Pinning
Browser Exploitation Frameworks

Exploiting Information Disclosure Vulnerabilities
Exploiting Error Messages
Script Error Messages
Stack Traces
Informative Debug Messages
Server and Database Messages
Using Public Information
Engineering Informative Error Messages
Gathering Published Information
Using Inference
Preventing Information Leakage
Use Generic Error Messages
Protect Sensitive Information
Minimize Client-Side Information Leakage

Attacking Compiled Applications
Buffer Overflow Vulnerabilities
Stack Overflows
Heap Overflows
“Off-by-One” Vulnerabilities
Detecting Buffer Overflow Vulnerabilities
Integer Vulnerabilities
Integer Overflows
Signedness Errors
Detecting Integer Vulnerabilities
Format String Vulnerabilities

Detecting Format String Vulnerabilities

Attacking & Assessing Application Architectures
Tiered Architectures
Attacking Tiered Architectures
Exploiting Trust Relationships between Tiers
Subverting Other Tiers
Attacking Other Tiers
Securing Tiered Architectures
Minimize Trust Relationships
Segregate Different Components
Apply Defense in Depth
Shared Hosting and Application Service Providers
Virtual Hosting
Shared Application Services
Attacking Shared Environments
Attacks against Access Mechanisms
Attacks between Applications
Securing Shared Environments
Secure Customer Access
Segregate Customer Functionality
Segregate Components in a Shared Application

Source Code Auditing
Approaches to Code Review
Black-Box vs. White-Box Testing
Code Review Methodology
Signatures of Common Vulnerabilities
Cross-Site Scripting
SQL Injection
Path Traversal
Arbitrary Redirection
OS Command Injection
Backdoor Passwords
Native Software Bugs
Buffer Overflow Vulnerabilities
Integer Vulnerabilities
Format String Vulnerabilities
Source Code Comments
The Java Platform
Identifying User-Supplied Data
Session Interaction
Potentially Dangerous APIs
File Access
Database Access
Dynamic Code Execution
OS Command Execution
URL Redirection
Sockets
Configuring the Java Environment
ASP.NET
Identifying User-Supplied Data

Session Interaction
Potentially Dangerous APIs
File Access
Database Access
Dynamic Code Execution
OS Command Execution
URL Redirection
Sockets
Configuring the ASP.NET Environment
PHP
Identifying User-Supplied Data
Session Interaction
Potentially Dangerous APIs
File Access
Database Access
Dynamic Code Execution
OS Command Execution
URL Redirection
Sockets
Configuring the PHP Environment
Register Globals
Safe Mode
Magic Quotes
Miscellaneous
Perl
Identifying User-Supplied Data
Session Interaction
Potentially Dangerous APIs
File Access
Database Access
Dynamic Code Execution
OS Command Execution
URL Redirection
Sockets
Configuring the Perl Environment
JavaScript
Database Code Components
SQL Injection
Calls to Dangerous Functions
Tools for Code Browsing

Reviewing the 83 Step Web Application Pen Tester Methodology

Review for CWAPT Certification Exam

InfoSec Institute's 5 Day Web Application Pen Testing Boot Camp - Schedule

To view our current course schedule and locations, visit InfoSec Institute's online at:

http://www.infosecinstitute.com/courses/web_application_hacking_training.html

Web Application Penetration Testing Course

InfoSec Institute's Pre-Class Preparation

Signing up for InfoSec Institute's Web Application Penetration Testing Class means more than just attending a 5 day program. The program starts with the following pre-class preparation materials:

- Quality, targeted prep books shipped directly to you prior to start of class

Post-Class Follow up and Support

Even after the course, we are here to provide support, including:

- Option to retake the class for up to a year (or until you obtain certification, whichever comes first)

Career Path-Related Courses

The courses below are excellent follow-on classes, once the class has been completed:

- Advanced Ethical Hacking Boot Camp
- Reverse Engineering Training

Testimonials

"I think the amount of time was appropriate, the information was relevant and well-summarized, and the test reflected the study materials well. My instructor did a great job. My Training Sales Representative has also been very helpful and I am glad that he had taken a great interest to follow up during class to with the students. I am very pleased with InfoSec Institute and the entire process."

Ryan Argomaniz
AVP, Specialist – Info Security Engr
Bank of America

Testimonials – cont.

"This class has been an outstanding experience for me. The instructor has a way of presenting material at a level that all can relate to. There is a lot of information with regards to this course, but he helps you to pinpoint your weak areas and turn them into to strengths. Thank you so much for this experience."

Phyliss Moore
Booz Allen Hamilton

Corporate On-Site Discounts

Your Company will Save Big on group on-sites of **10 or more students**. Get training FAST on-site at your location for a fraction of the price of our public scheduled classes!

InfoSec Institute's 100% Satisfaction & Human Capital Guarantee

InfoSec Institute is committed to you having the best possible training experience available. We offer students the opportunity to re-sit a Classroom-based or Live Online course tuition-free for up to one year or until the student obtains certification, whichever comes first.

Our Training School At-A-Glance

Web Application Penetration Testing Course

InfoSec Institute is the #1 accelerated IT training school in the world for good reason – our Expert Instructors are industry-recognized leaders, authors, and experts in their fields. We have mastered the accelerated method of training and certification and take pride in offering you the same quality training and certification programs that more than 45,000 satisfied clients have raved about.

InfoSec Institute's Expert Instructors possess strong consulting, implementation and training expertise. Our security professionals come from diverse roles including positions in consulting, product development, project management, information security and information technology. Our training team has supported public and private corporations, technology vendors, telecommunications companies and professional services organizations around the world.

InfoSec Institute

Reverse Engineering Detailed 5 Day Course Syllabus

Day 1: Introduction to Reverse Engineering
Day 1 focuses on the fundamental knowledge required for reverse engineering. This day is designed to build critical skills required to proceed further into deeper discussions on reversing. You will also train on special purpose reversing debuggers and disassemblers.

Foundations of Reversing
The Reversing Process
Program Structure
Common Code Constructs
Indentifying Variables & Lists
Low level data management - Stacks, Heaps and Data sections
Compiler representations
Kernel vs. User memory
Virtual Memory and Paging
Reversing threaded applications
Defining the Win32 API
Win32 executable formats and image sections
Discovering undocumented APIs in ntdll.dll
Fundamentals of IDA Pro

Day 2: Reverse Engineering
Day 2 encompasses a deep discussion with hands-on content for reversing Windows binaries. Key concepts such as identifying code paths, control functions and developing a general understanding of the code to be analyzed is covered.

Reversing file formats
Reversing encrypted file formats
Understanding conditional branching statements
Virtual machines and bytecode
System vs. Code Level reversing
Identifying variables
Compilers and branch prediction
Memory management
Advanced uses of IDA Pro
Using Ollydbg for runtime analysis
Kernel mode debugging with SoftICE

Day 3: Reverse Engineering - Malware
Detailed coverage on reverse engineering malware. Focus is on live malware reversing using examples of viruses, Trojans and rootkits collected from the wild.

Using Ollydbg for runtime analysis of malware

Kernel mode debugging with SoftICE
Dumping executables from memory with Dumpbin
Obfuscation of file formats
Understanding hashing functions
Working with encrypted binaries
Polymorphism
Metamorphism
Reversing UPX and other compression types
Reversing a Trojan backdoor
Understanding network communications

Day 4: Reverse Engineering - Anti-reversing techniques
Day 4 works with various anti-reversing techniques that software developers and malware writers put in place to make reverse engineering more difficult.

Basic anti-reversing strategies
Symbol elimination
IsDebuggerPresent API
Single Step Interrupt Detection
Softice Backdoor
Exploits for IDA Pro
IDA Pro obfuscation
Code flow transformations
Opaque Predicates
Interleaving Code
Restructuring Arrays
Encoding variables
Recursive traversal dissasemblers
Reversing .NET bytecode
Legal issues and the DMCA
CREA review

Day 5: Binary Diffing & CREA Exam

Using IDA to diff binaries
Manual patch investigation
Manual patch diffing
Building fuzzers
Using pei-mei
Using other code coverage tools
Protocol reversing

CREA Exam given on-site in afternoon

Certified Reverse Engineering Analyst:
In any hands on reverse engineer training course, it is important to have the opportunity to prove to current or potential employers that you have the skills you say you do. This course prepares you for the top reverse engineering certification in the industry, the CREA. The exam is given on-site, InfoSec Institute has achieved a 93% pass rate for this certification.

Securible, LLC

CISSP Training

About the Program

Securible, LLC is pleased to offer their proven, high quality training in the Certified Information Systems Security Professional (CISSP) Certification Preparation Program.

Security is a leading concern in every organization and the CISSP Certification is the premier security certification available today for information assurance professionals looking to differentiate themselves among their colleagues. In fact, the DoD 8570 directive recognizes the CISSP as an important credential for the DoD workforce.

To help organizations stay up to speed on security issues and help security professionals achieve the CISSP certification, Securible, LLC has developed a proven, interactive CISSP training program. This program focuses on helping security professionals understand the prevailing security issues, practices and trends, and helps them prepare for the CISSP exam.

The CISSP Training Program focuses on the 10 Common Body of Knowledge areas designated by (ISC)^2, the international non-profit organization dedicated to security and the sponsor of the CISSP and SSCP certifications.

Program Elements

10 Domains of Study

- Information Security and Risk Management
- Access Control
- Security Architecture and Design
- Physical (Environmental) Security
- Telecommunications and Network Security
- Cryptography
- Business Continuity and Disaster Recovery
- Legal, Regulations, Compliance and Investigations
- Application Security
- Operations Security

Provided Resources

- 2 Student Workbooks
- 1 All-in-One CISSP textbook
- 1 set of 750+ flashcards
- 1000's of practice exam questions
- Catering for each night of class
- 1 highly qualified and proven instructor

When an organization hires Securible here is what they get:

- Security solutions that address the organization's needs
- Cost effective solutions that are the right thing at the right time
- The quality guarantee of our work - we want satisfied customers and will do what it takes to keep the client satisfied

Our Mission

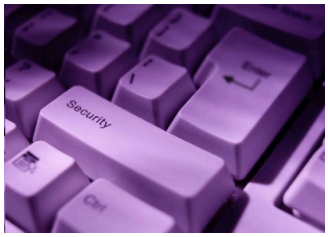
At Securible, LLC we treat each customer as our best customer and listen to their needs so we can custom design solutions that achieve their goals. By doing this we consistently meet our own goal of 100% customer satisfaction.

SCP Authorized Training Partner

EC-Council Accredited Training Center

CompTIA Learning Alliance CompTIA Approved Training

Microsoft Certified Partner | Security Solutions



Organization Details

Securible, LLC

3213 Duke St #220
Alexandria, VA 22314
Phone: 703-879-3310
Fax: 703-754-8215
http://www.securible.com

DUNS #: 80-778-4991
Small Business
POC: Amee Devine
amee.devine@securible.com