EC-Council

CENTER FOR ADVANCED SECURITY TRAINING

CAST 613

Hacking and Hardening your Corporate Web Application

A Developer Perspective

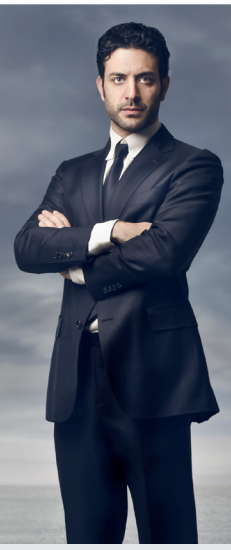
Make The Difference

About EC-Council Center of Advanced Security Training (CAST)

The rapidly evolving information security landscape now requires professionals to stay up to date on the latest security technologies, threats and remediation strategies. CAST was created to address the need for quality advanced technical training for information security professionals who aspire to acquire the skill sets required for their job functions. CAST courses are advanced and highly technical training programs co-developed by EC-Council and well-respected industry practitioners or subject matter experts. CAST aims to provide specialized training programs that will cover key information security domains, at an advanced level.

Hacking and Hardening your Corporate Web Application

A Developer Perspective

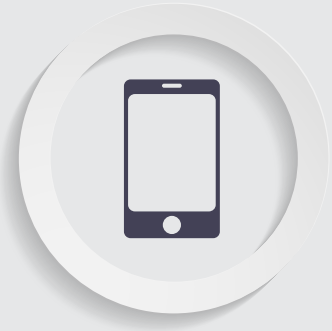


Course Description

A well thought out course designed with the average security unaware programmer in mind. Your developers will be astonished at the things they do every day that turn out to have security flaws in them. To drive the point home, the course is designed with more than 50% involving hands-on coding labs. The ideal participant should have a development background, coding or architecting background either currently or previously. The candidate currently could be a developer trying to raise his or her cyber awareness. Or the Candidate may either now or have moved into a managerial position perhaps making them even more responsible for any security breach. In today's world, there is not one day that goes by that the national evening news mentions a break in. While that may not seem that ground breaking in and of itself, the truth of the matter is much more staggering. Studies have not only shown but have proven that for every record compromised it can cost the company well over a $1000 in costs to repair. Those costs may be hard $ costs as well as costs of reputation. So if 10, 000 records were compromised. Well do the math! This can be not only a job limiting oversight but a career limiting one as well. And every manager knows after Sarbanes Oxley the finger points back to the man in charge.

CAST

EC-Council



Much thought was put into the course to be sure it worked and could be taught as a language agnostic course providing both the developer as well as management types to be exposed to how their own web site/web app could be compromised.

The course will require no special pen testing tools that are normally used during a course similar to this. The author expects that you simply understand program logic. And if you know development techniques and have an architecture background you will walk away with a heightened sense of awareness about the things you do on a day to day basis.

Regardless if you are the developer, the architect or even the project manager each will walk away with an astonishing clarity of how things could be easily improved and secured. To get the most from the course all participants should have at least some programming experience.

This course is NOT language specific although program logic and design concepts both are an absolute must have! Most of the entire course will be not only enlightening but also entertaining and easily well worth the time allocated to take. You will instantly find yourself suggesting this course to other developers, project managers and architects on your team and at your company!

Why You Should Attend

If you have taken secure coding courses in the past you may think this is going to be the same. Nothing can be further from the truth. This course is a completely different approach. Most developers will tell you that if I knew how the Hackers could get in, it is usually easy to fix. That is just it. The developers have never tried to break in to their own code or someone else's code. Perhaps they don't have the skills to do so. Does that make them just an honest person? Perhaps, but in today's world that is not a good thing but a very bad thing. You must we aware of the things that can happen to you or you will not be able to protect yourself. The hackers actually have it very easy they only need to find 1 hole to get in. The developer must plug all the holes. The developer must keep up to date with the latest security threats.

Some developers may argue that it is not the developer's job to secure the enterprise, that is the security department's job. That is pure rubbish. Each has a hand in protecting the corporate environment. Each shares this responsibility. While the finger pointing goes on the hacker is enjoying himself with all of your intellectual property, Human Resource Information, or anything else he can monetize.

This course is designed so if you understand programming logic you can benefit from this course.

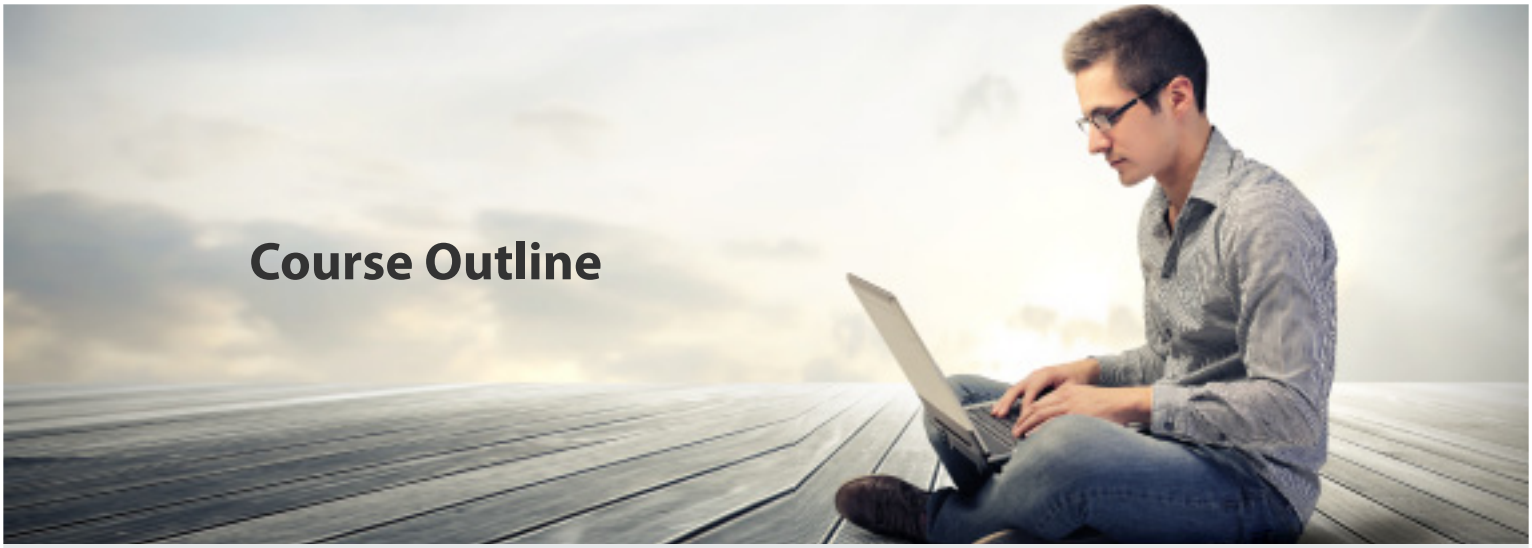
Who Should Attend

Practically information security personnel from any organization with the responsibility of handling important data would find this course beneficial, examples are:

- Government agencies
- Universities
- Hospitality
- Retail
- Banking and Financial institutions
- Brokerage and Trading firms
- Insurance
- Scientific institutions & research agencies
- Telecommunication
- Computer design firms
- Consulting firms
- Science and Engineering firms
- Those involved with online related businesses & transactions
- Card related businesses

NOTE: Students must be familiar with IT Security best practices, and have a good understanding of programming logic and common web technologies Course is designed for Developers but Most It Personnel will benefit, anyone with these minimum skills:

- Basic Windows administration for servers and workstations
- Basic command line proficiency on both Windows



Course Outline

1. Introduction

- About the course and Author Tim Pierson
- Why I developed Hacking and Hardening your Corporate Website/WebApp: A developer Perspective
- A Tip of the Hat to Troy Hunt and Jerimiah Grossman for the original concept!
- Introducing the vulnerable website
- Using very Expensive Pen testing tools high priced tools like Firefox/Firebug or Chrome's developer tools (Comes with Chrome).
- Introducing a few Free Add-ons to Chrome and Firefox, Did I mention they were Free?
- Monitoring and composing requests using a common proxy like Fiddler, Paros or Burp Suite.
- Modifying requests and responses in Fiddler to change what goes out and what comes in before Browser Renders it.
- Browser simply reads code from the top to the bottom. No idea what is good, bad, malicious or otherwise.
- Surfing the Web is like giving every website you go to a shell on your box!

2. Cryptography Decrypted

- Introduction
- For 10 Bonus Points…Who is this man?
- Encryption – A Definition
- Encryption Algorithm
- Symmetric Encryption
- Asymmetric Encryption
- Crack Times
- Password Policies and why they simply don't work!
- Don't use a Pass Word Every Again! Use a Pass Phrase Instead!
- Hashing
- Hash Collisions
- Common Hash Algorithms
- Digital Signatures – Proving who we say we are.
- Digital Certificate Levels – It comes down to Cost!
- Working with SSL Certificates.
- We Trust what we Know – True Story.
- IPSec – Will this solve it all?
- Public Key Infrastructure
- HeartBleed – What's all the Hype? Should we care?
- Laptop and Portable Encryption: TrueCrypt – BYOB is here or is Coming!
- Summary

3. Account Management – The Key to it all?

- Introduction
- Understanding How Important password strength and attack vectors are
- My Favorite Slide in the World
- Passing the Monkey Wrench Technique!
- Limiting characters in passwords
- Providing (Emailing credentials) on account creation
- Account enumeration
- Denial of service via password reset
- Correctly securing the reset processes
- Wall of Shame – Plain Text Offenders
- How to spot a Secure Web Site – Everyone should try this on their Family.
- Establishing insecure password storage
- Testing for risks in the 'remember me' feature
- Re-authenticating before key actions
- Testing for authentication brute force
- Summary

4. Parameter Diddling

- Introduction
- Identifying untrusted data in HTTP request parameters
- Capturing requests and using easy tools to manipulating parameters
- Manipulating application logic via parameters
- Testing for missing server side validation, if you don't do it, it's like having the fat kid watch the pie!
- Understanding model binding
- Executing a mass assignment attack
- HTTP verb tampering – What's a Verb? Post, Get etc. Are they interchangeable you'd be surprised?
- Fuzz testing – Spraying that App like a fireman's sprays a fire with his fire hose, then see if it Hiccups!
- Summary

5. Transport Layer Protection – Safety During the Commute

- Introduction
- The three objectives of transport layer protection
- Understanding a man in the middle attack, and we all fall victim to it every day!
- Protecting sensitive data in transit, and at Rest.
- The risk of sending cookies over insecure connections
- How loading login forms over HTTP is risky
- What's the Solution? Http Everywhere? What about the overhead?
- Exploiting mixed-mode content
- The HSTS header
- Summary

6. Cross Site Scripting (XSS) - Truth Is I just do what I am told.

- Introduction
- Understanding untrusted data and sanitization
- Establishing input sanitization practices – Keep it Clean going in
- Understanding XSS and output encoding
- Identifying the use of output encoding - and coming back out!
- 3 types of XSS, Reflected, Stored and DOM
- Delivering a payload via reflected XSS
- Testing for the risk of persistent XSS
- The X-XSS-Protection header
- Summary

7. Cookies – Not Just for Hansel and Gretel

- Introduction
- Cookies 101 – Everything you wanted to know but were afraid to Ask!
- Session Management – HTTP is like an Alzehemiers Patient – Like the Movie, 50 First Dates!
- Understanding Http Only cookies, what are they and why we should use them?
- Understanding secure cookies. No not putting Grandmas Cookies in a locked Cookie Jar!
- Disabling Cookies – Do we really need them?
- Restricting cookie access by path – Now there's an Idea!
- Reducing risk with cookie expiration – Keep it short!
- Using session cookies to further reduce risk
- Summary

8. Internal Implementation Disclosure - What's going on inside the Beast

- Introduction
- How an attacker builds a website risk profile, Make sure you don't fit that profile.
- Server response header disclosure – Tell it like it is, or is that not what you intended?
- Locating at-risk websites – Making Sure Yours is not one of them
- HTTP fingerprinting of servers – Determining what your WebApp WebSite is running
- Disclosure via robots.txt – Tell the World Where not to Look!
- The risks in HTML source – What your HTML is telling Everyone, whether you know it or not!
- Internal error message leakage – Error messages that say Way Too Much!
- Lack of access controls on diagnostic data – First things Hackers Try is to Put the sight in Debug Mode
- Summary

9. SQL Injection - SQL Injection- What's a Command, What's Data?

- Outline
- Understanding SQL injection
- Testing for injection risks – "Using Very High Priced Expensive tools like Chrome and FireFox!"
- Discovering database structure via injection
- Harvesting data via injection. Simply print out the Entire Schema under the right conditions.
- Automating attacks with Havij
- Blind SQL injection – How the Blind Man can still find Holes
- Secure app patterns
- Summary

10. Cross Site Attacks – Same Origin Policy. Everyone Else Breaks it why shouldn't we?

- Introduction
- Understanding cross site attacks – Leveraging the Authority of an approved User
- Testing for a cross site request forgery risk
- The role of anti-forgery tokens – A few Things that will help
- Testing cross site request forgery against APIs
- Mounting a clickjacking attack – What are you clicking on anyway?
- Summary

Master Trainer:

Tim Pierson

Tim Pierson is one of the World's leading trainers in technology networks and security with credentials including ongoing selection to author training courses and manuals for global corporations. He conducts high-level security evaluations and delivers seminars before professional conventions. He is endowed with exceptional skills in communicating sophisticated information to sophisticated and non-sophisticated clientele.

Tim has been a technical trainer for the past 23 years and is an industry leader in both Security and Virtualization. He has been the noted speaker at many industry events including, Lectures at/for Savannah River & Los Alamos Nuclear Power Plant, Innotech, GISSA, many military venues including the Pentagon, and numerous Military facilities addressing security both in the US and Europe, Including but not limited to Numerous Army Bases in Germany and Belgium with both the US and Foreign Military organizations.

Tim is currently Senior Consultant and Trainer at Data Sentry, Inc. with special responsibilities to initiate, develop and validate training programs for current security practices and procedures. Tim possesses formidable knowledge in these areas and the years ahead will see Tim transcribe his know-how into authoring many certification training classes, often times completing self-certification on new and emerging products in advance of teaching or writing courseware or books on related subjects.

Tim's training stints have taken him to many parts of the world - most major US cities, Europe and Asia. Having been exposed to a variety of students and audiences has given him the added advantage of being able to pitch his commitment at the appropriate level. It is therefore not surprising that he consistently receives accolades bearing testimony to his training prowess.

Tim's projects include being contributing author of "VMware Virtual Infrastructure Security: Securing ESX and the Virtual Environment". Moreover, he has done work for the bi-monthly Virtualization Security Roundtable Podcast available as a download on iTunes and Talk Shoe. Tim was Featured Speaker on Secure Coding and Virtualization Practices at Hacker-Halted in Miami September 2009 and the Hacker-Halted in Kuala Lumpur Malaysia in November 2009.

EC-Council