Hacking and Hardening Your Websites/Web Apps
S-2500
Length: 5 days
Price: $ 3,895.00

Course Description

This course was 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. 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 unusual approach is that the course is 100% language independent. It makes no difference if you write in PHP, .NET, Java, Flash/Flex or the 100 other variants or mashups. If you drive your application from a Browser, and it returns angle brackets, then you are in the right place. 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.

Course Audience

This course is designed for IT personnel of all levels from all organizations/industries including: • Mid-level technology managers • Infrastructure / Network Specialists • Software Development Specialists • Information Security Officers • Executive Level Managers Students must be familiar with IT Security best practices, and have a good understanding of programming logic and common web technologies.

babbage simmel

Course Outline

Introduction

- Why Hacking and Hardening Your Websites/WebApps: A developer Perspective?
- 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!Introduction

Cryptography Decrypted

- Introduction
- 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

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

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

Transport Layer Protection – Safety During the Commute

- IntroductionThe 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

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

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 Alzheimer's 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

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

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

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

Available Dates

Request a Course Date