

# The "Easy" Button for Your Web Application Security Career

@greecs







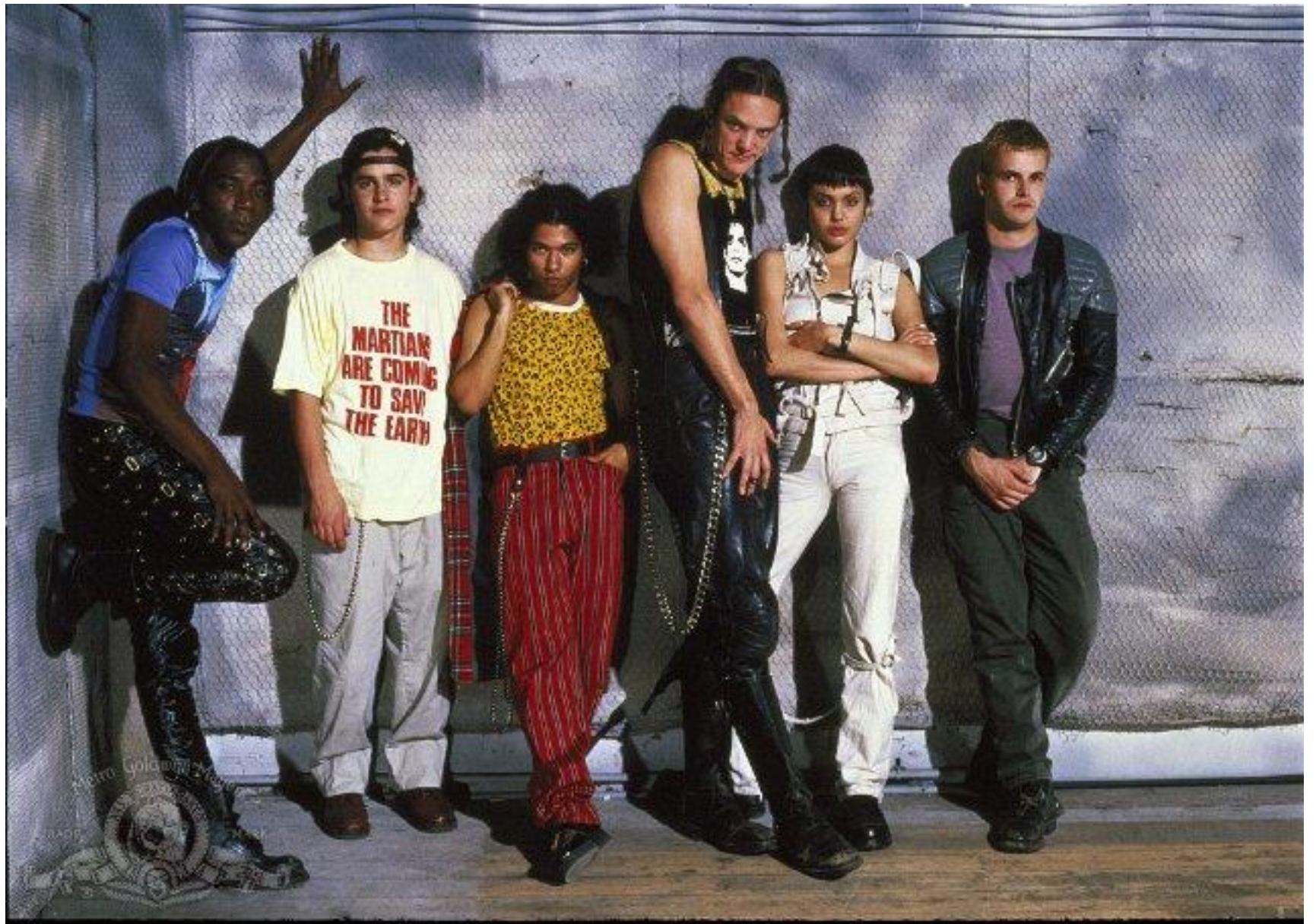


# HACKERS

You thought your  
secrets were safe.  
You were wrong.







The Ralph Macchio Homepage


http://www.geocities.com/hollywood/hills

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize

Edit Post Nettut... 53 Firefox Organi... Top 10 Reasons... The Ralph Macchi...

# The Ralph Macchio Homepage

Please take a moment to rank my site!



The Ralph Macchio Homepage

---

You are Macchio Maniac # (150,000 or so...my counter's busted) to visit The Ralph Macchio Homepage since February 25, 1997


---

Thanks to Time Magazine for the feature this month! It has motivated me to finally do some updates. You can see the article [here](#).

---

Welcome to The Ralph Macchio Homepage. This man has dedicated his life to providing millions of moviegoers with countless hours of entertainment. While it is, of course, impossible to recount every instance of Ralph's greatness and all of his contributions, this page will serve as a wholehearted tribute to the greatest actor of the 20th century.

---



Done

# The Ralph Macchio Homepage

Please take a moment to rank my site!

[Biography](#)

[Film Reviews & Summaries](#)

[Pictures](#)

[Sounds](#)

[FAQ](#)

[MP3's](#)

[Quotes](#)

[Where can I get...?](#)

[Interviews](#)

[The Eight is Enough Conspiracy](#)

[The Ties That Bind](#)

[Thanks](#)

[Assorted Stuff](#)

[Awards](#)

*"I think Ralph Macchio turned me on to the blues." - Jerry Cantrell of Alice in Chains*

You are Macchio Maniac # (150,000 or so...my counter's busted) to visit The Ralph Macchio Homepage since February 25, 1997

Thanks to Time Magazine for the feature this month! It has motivated me to finally do some updates. You can see the article [here](#).

Welcome to The Ralph Macchio Homepage. This man has dedicated his life to providing millions of moviegoers with countless hours of entertainment. While it is, of course, impossible to recount every instance of Ralph's greatness and all of his contributions, this page will serve as a wholehearted tribute to the greatest actor of the 20th century.

# HOME PAGE, DOMAIN NAME, HOSTING, WEB PAGE DESIGNING FOR THE INTERNET



**LET US HOST, DESIGN AND CREATE YOUR OWN WEB SITE FOR YOUR BUSINESS AND LET THE WORLD KNOW WHAT YOU ARE SELLING OR SERVICING AND WE WILL CREATE AND DESIGN YOUR HOME PAGE AND ADDITIONAL WEB PAGES ACCORDING TO YOUR REQUIREMENTS. OUR PAGES ARE DESIGNED USING NETSCAPE COMPOSER WHICH IS EASY FOR YOU TO MAKE ANY CHANGES.**



**\$\$\$ YOU CAN HAVE YOUR LIVE BUSINESS SITE ON THE INTERNET WITHIN 3-7 DAYS FROM DATE OF SUBMISSION AND INCREASE YOUR INCOME. WE HAVE WEB DESIGNERS WHO ARE EXPERTS IN THE FIELD AND CAN DESIGN ANY WEB SITE DESIGN REQUESTED.**

**WE PROVIDE THE FOLLOWING DESIGN SERVICES WITH TEXT, PHOTOS, IMAGES & ANIMATION**

**HOME PAGE WITH TEXT, PHOTOS, AND IMAGES**

**AND ADDITIONAL PAGES LISTED BELOW**

<b>PRODUCTS SOLD OR OFFERED</b>	<b>ORDER FORMS WITH PRODUCT PHOTOS</b>
<b>SERVICES RENDERED</b>	<b>YOUR COMPANY PROFILE</b>
<b>PRICE LISTS OF PRODUCTS OR SERVICES</b>	<b>FREE OFFERS AND GIFTS</b>
<b>CONTACT FORMS</b>	<b>ANY OTHER DETAILS AS REQUIRED</b>

## **◆ SITE REGISTRATION**

**WE WILL CARRY OUT THE FOLLOWING FOR THE SERVICES ORDERED:-**



# [HomePage](#)

**[\[Home\]](#)**

[HomePage](#) | [RecentChanges](#) | [Preferences](#)

You can [edit this page right now!](#) It's a free, community project

---

**Welcome to [Wikipedia](#)**, a collaborative project to produce a complete encyclopedia from scratch. We started in January 2001 and already have **over 8,000 articles**. We want to make over 100,000, so let's get to work--*anyone* can edit any page--copyedit, write a little, write a lot. See the [Wikipedia FAQ](#) for information on how to edit pages and other questions. If you're visiting Wikipedia for the first time, [welcome!](#) *The content of Wikipedia is covered by the [GNU Free Documentation License](#).*

---

## **Philosophy, Mathematics, and Natural Science**

[Astronomy and Astrophysics](#) -- [Biology](#) -- [Chemistry](#) -- [Earth Sciences](#) -- [Mathematics](#) -- [Philosophy](#) -- [Physics](#) -- [Science](#) -- [Statistics](#)

## **Social Sciences**

[Anomalous Phenomena](#) -- [Anthropology](#) -- [Archaeology](#) -- [Countries of the world](#) -- [Economics](#) -- [Geography](#) -- [History](#) -- [History of Science and Technology](#) -- [Language](#) -- [Linguistics](#) -- [Politics](#) -- [Psychology](#) -- [Sociology](#)

## **Applied Arts and Sciences**

[Agriculture](#) -- [Architecture](#) -- [Business and Industry](#) -- [Communication](#) -- [Computing](#) -- [Education](#) -- [Engineering](#) -- [Family and Consumer Science](#) -- [Health Sciences](#) -- [Law](#) -- [Library and Information Science](#) -- [Public Affairs](#) -- [Technology](#) -- [Transport](#)

## **Culture**

[Classics](#) -- [Critical Theory](#) -- [Dance](#) -- [Entertainment](#) -- [Film](#) -- [Games](#) -- [Hobbies](#) -- [Literature](#) -- [Music](#) -- [Opera](#) -- [Painting](#) -- [Performing Arts](#) -- [Recreation](#) -- [Religion](#) -- [Sculpture](#) -- [Sports](#) -- [Theater and Drama](#) -- [Tourism](#) -- [Visual Arts and Design](#)

---

## **Other Category Schemes**

[About Wikipedia category schemes](#) -- [Library of Congress catalog scheme](#) -- [Dewey Decimal System](#) -- [Wikipedia arranged by topic](#) -- [Year in Review](#) -- [Historical anniversaries](#) -- [Reference tables](#) -- [Biographical Listing](#)

## **International Wikipedias**

[About the International Wikipedias](#) -- [\[Catalan \(Català\)\]](#) -- [\[Chinese \(Hanyu\)\]](#) -- [\[German \(Deutsch\)\]](#) -- [\[Esperanto\]](#) -- [\[French \(Français\)\]](#) -- [\[Hebrew \(Ivrit\)\]](#) -- [\[Italian \(Italiano\)\]](#) -- [\[Japanese \(Nihongo\)\]](#) -- [\[Portuguese \(Português\)\]](#) -- [\[Russian \(Russkiv\)\]](#) -- [\[Spanish \(Castellano\)\]](#) -- [\[Swedish \(Svensk\)\]](#)

### NAVIGATION

#### About OWASP

[Mission](#)  
[Organizational Chart](#)  
[FAQ](#)  
[Get Involved](#)  
[Licensing](#)  
[Contact OWASP](#)

#### Application Security Projects

[Attack Components](#)  
[Informational](#)  
[Input Validation](#)  
[Session Management](#)  
[Parameter Manipulation](#)  
[Buffer Overflows](#)  
[Cryptographic](#)  
[Format Strings](#)  
[Race Conditions](#)  
[Testing Framework](#)  
[Project Schedule](#)

#### Resources

[Framework Tools](#)  
[Tutorials](#)  
[Links](#)  
[Books](#)

[Home](#)

### OFFICIAL LAUNCH

We are extremely pleased to finally officially launch OWASP, the "Open Web Application Security Project". For those that have been following the site and mailing list for the last 8 weeks you'll be a part of the 250,000 web hits, and this will be nothing new; but given our new technical committee it made sense to re-launch the efforts with some basic work already done.

In short the project aims to help everyone build more secure web applications and web services. We will be covering a wide range of related work over the coming years and have initially defined two areas to concentrate on.

**Attack Components** - The Application Security Attack Components project was started as an attempt to create common language and definitions for which much of the other work planned at OWASP can later benefit. When describing security issues in web applications or when attempting to model security it is very easy to describe the same issue in many different ways, seemingly creating new problems. When analyzing problems described on Bugtraq it is evident that most problems are variants of common issues, but applied to different applications or systems using different parameters or targets. The aim is definitely not to build the biggest list of problems or describe attacks like Nimda or Code Red; but to document the underlying primary attack

### NEW OWASP TECHNICAL COMMITTEE

The Technical Committee is made up of renowned application security experts who ensure that the work and ideas produced by the project are technically sound. These people have a wealth of experience and knowledge and will be guiding much of the direction of the work in various areas. As well as participating on the mailing list the technical committee has a monthly conference call to discuss progress. They are the OWASP technical think tank!

- **Elias Levy**  
- probably best known as the long-time moderator of Bugtraq at [securityfocus.com](#) and author of "Smashing the Stack for Fun and Profit"
- **Chris Wysopal**  
- formerly with the L0pht and heads up the [@Stake](#) Application Security Center of Excellence.
- **John Viega**  
- wrote 'the' book on "Building Secure Software" and is author of RATS (Rough Auditing Tool for Security) as well as hundreds of articles and several other books. John is the CTO of [Secure Software](#).
- **Greg Hoglund**  
- well known for his work on buffer overflows and his Black Hat presentations, as well a respected developer of security and fault injection

### NEWS UPDATES

**XML and metadata news**  
[webMethods Sets the Agenda for Enterprise Web Services...](#)

[Web Host Directory](#) Wed Feb 06 2002 23:33:00 GMT-0500 (EST)

[webMethods = Web Services...](#)

[line56](#) Wed Feb 06 2002 02:27:00 GMT-0500 (EST)

[Using tDOM and tDOM XSLT...](#)

[IBM](#) Tue Feb 05 2002 23:01:00 GMT-0500 (EST)

[Third Generation Native XML Database...](#)

[Content-Wire](#) Tue Feb 05 2002 22:07:00 GMT-0500 (EST)

**moreover...**

[Microsoft touts tightened security of Web services...](#)

[ZDNet](#) Tue Nov 27 2001 04:47:00 GMT-0500 (EST)

[Relaxed holiday attitudes help BadTrans worm...](#)

[ZDNet](#) Tue Nov 27 2001 04:26:00 GMT-0500 (EST)

[Symantec Firewall/VPN](#)



# US PATENT AND TRADEMARK OFFICE

General Info

Patents

Trademarks

Weekly Data

Download Forms

Order Copies

PTO Fees

Libraries-PTDLs

Site Index

Info by Org

About PTO

International

Statistics

Acquisitions

Jobs at PTO

Related Web Sites

Public Affairs

FOIA

Document Formats

Copyrights (LOC)

## New on the PTO site:

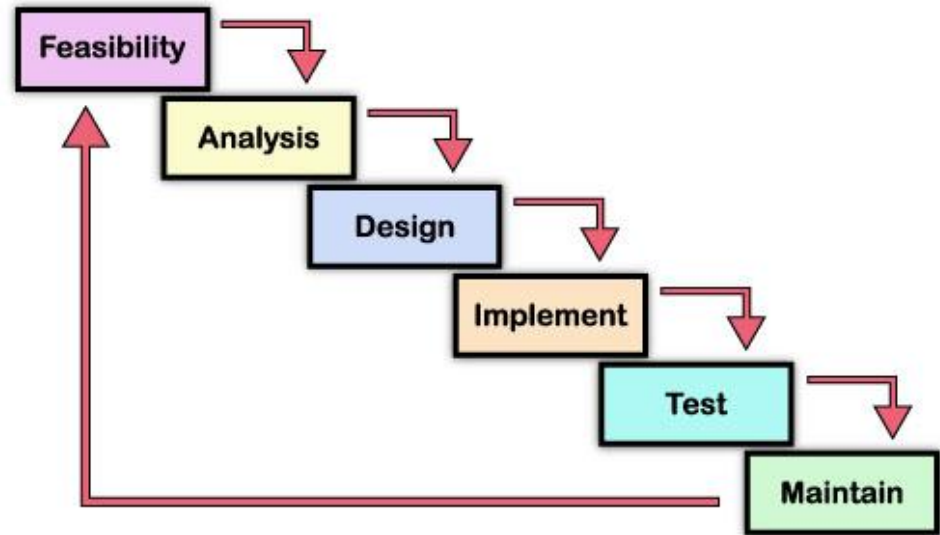
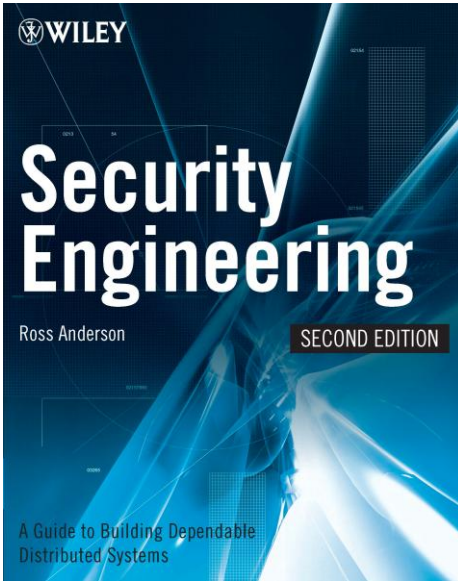
- [Biography of Q. Todd Dickinson, Acting Assistant Secretary of Commerce and Acting Commissioner of Patents and Trademarks](#) (14Jan99)
- [Job Fair, Arlington VA, Feb. 5-6](#) (13Jan99)
- [Public Comments on "Changes to Implement the Patent Business Goals \(October 27, 1998\)"](#) (13Jan99)
- [Top 10 Patenting Organizations for 1998](#) (12Jan99)
- [Public Comments on Expansion of Searchable Database Offerings](#) (7Jan99)
- [Solicitation of Applications for Membership on Public Advisory Committee for Trademark Affairs](#) (7Jan99)
- [RFC: Official Insignia of Native American Tribes; Statutorily Required Study](#) (4Jan99)
- [US Trademark Law -- Rules of Practice & Federal Statutes Updated](#) (22Dec98)
- [Manual of Patent Examining Procedure, Seventh Edition Text](#) (22Dec98)
- [Cassis Currents Optical Disk Publishing Newsletter No. 2](#) (21Dec98)
- [PTO Red Book Definition for Patent Mark-up in SGMI.](#) (18Dec98)

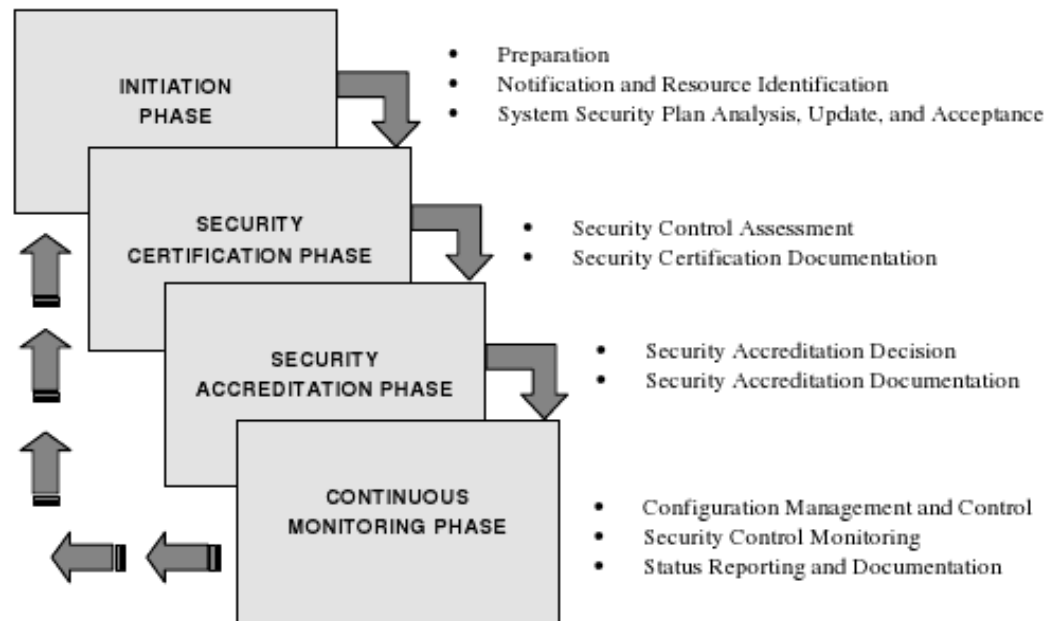
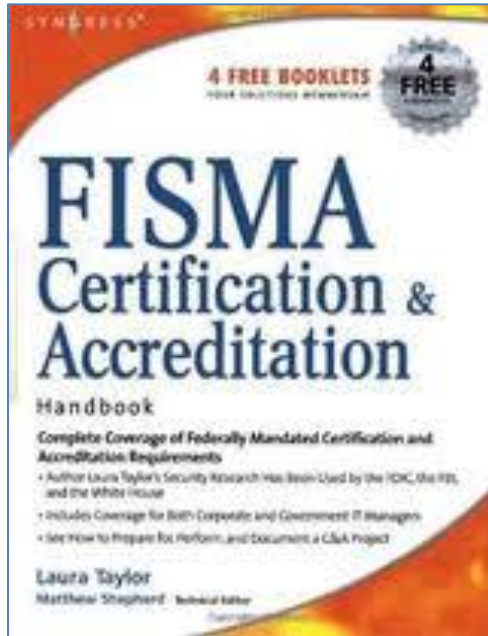
# Infosec Career Start - WebAppSec

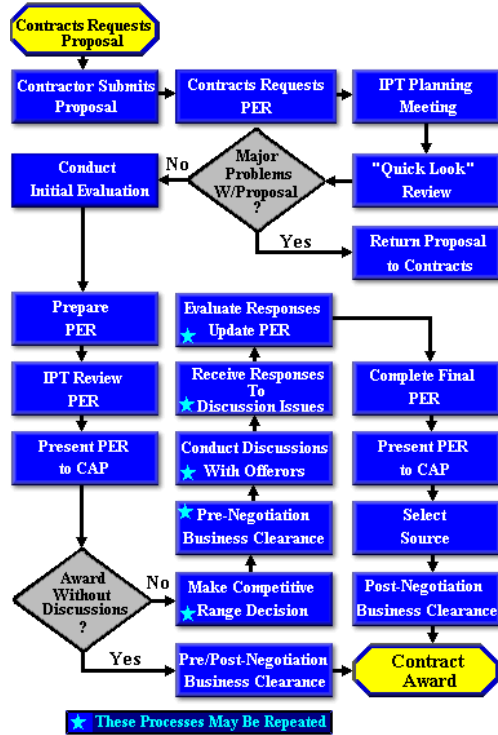
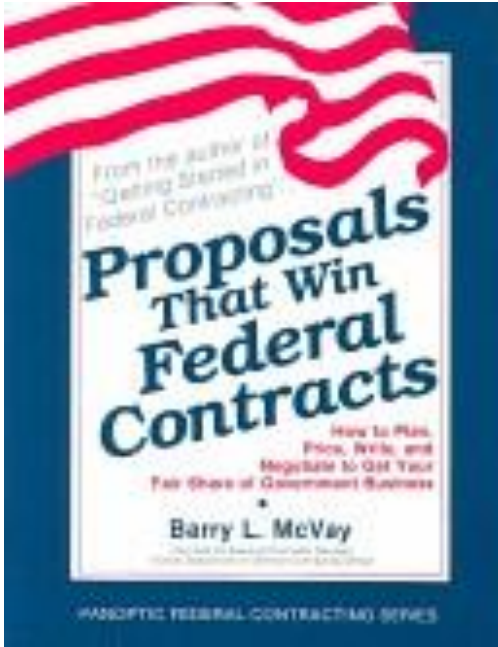
- Around 2002
- Sooo Much Simpler
  - No CSRF, Click-Jacking, ... SQLi
  - No SOAP
  - No AJAX
  - No HTML5
- Had Our Problems
  - Browser Wars Still Going On
  - Per Browser Customizations
  - No Guidance
  - Limited Security Libraries
  - Immature Tools



**move  
on**











## System Shutdown



This system is shutting work in progress and lo changes will be lost. T initiated by NT AUTHO

Time before shutdown

Message

Windows must now re Remote Procedure C terminated unexpecte

## MYDOOM INTERNET WORM

### How the MyDoom worm spreads



2. The attachment releases a program which can take over the victim's computer, sending infected e-mails to every address it can find



## LSA Shell (Export Version)

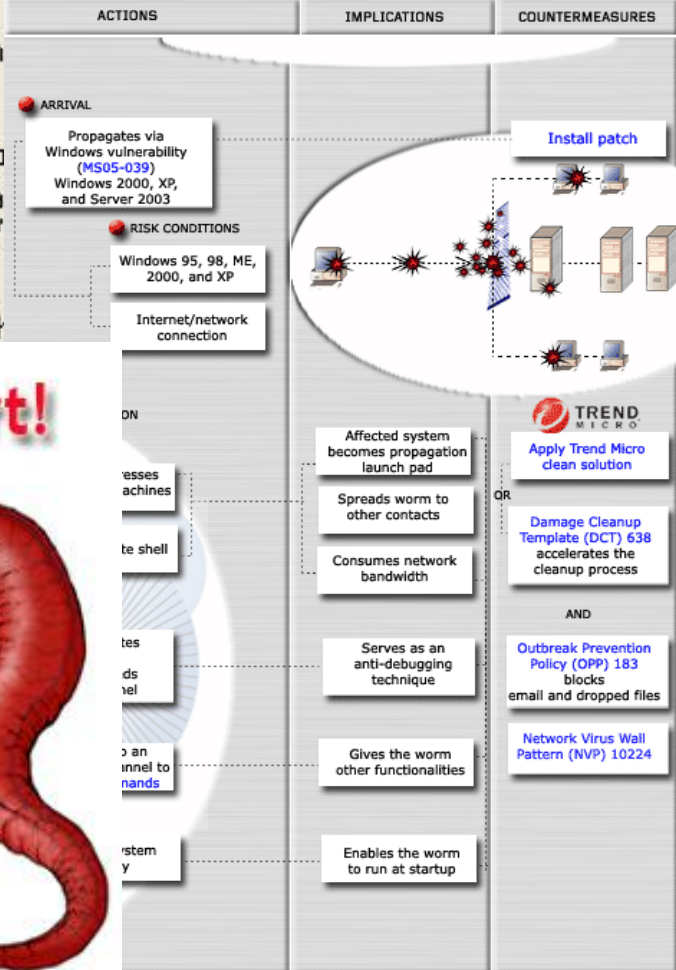
**LSA Shell (Export Version) has encountered a problem and needs to close. We are sorry for the inconvenience.**

If you were in the m might be lost.

**Please tell Micro**  
We have created a LSA Shell (Export V anonymous.

To see what data th

WORM\_ZOTOB.D Behavior Diagram



# Storm Worm Alert!





# Infosec COTS



## ~~Microcontroller vs. FPGA Trade Study~~

MCU vs. Antifuse FPGA Trade Study V1.0					
Criteria	Weight (%)	Microcontroller	Grade	Antifuse FPGA	Grade
Radiation Tolerance	30%	Logical	2	Physical (rad hard by design)	5
Programming Language	20%	C	4	VHDL or Verilog	2
Power consumption	15%	16.5 mW	4	<16.5 mW	5
Cost per unit	10%	\$15.05	4	\$30	2
Initial Cost	5%	\$0.00	5	\$500	2
In Flight Programmable	5%	Yes	5	No	1
CubeSat Legacy	15%	Extensive	3	Unknown	1
<b>Average Score</b>			<b>3.8571</b>	<b>2.57143</b>	
<b>Weighted Score</b>			<b>3.35</b>	<b>3.15</b>	

## APPLIED RESEARCH



THERESA A.  
THORKILDSEN

**HANDS ON  
HACKING**

**UNLIMITED**



# NovaInfosecPortal.com

News, events, & resources for infosec professionals in NoVA, DC, & MD

[Home](#)
[News](#)
[Events](#)
[Resources](#)
[Job Board](#)
[Contact Us](#)

## UPCOMING EVENTS

- October 9, 2011  
SANS Baltimore  
Conference  
Baltimore, MD
- October 10, 2011  
NoVA Hackers Association  
Meetup  
Fairfax, VA
- October 11, 2011  
SANS National  
Cybersecurity Innovation  
Conference  
Arlington, VA
- October 12, 2011  
ISACA CM Meetup  
Linthicum, MD
- October 13, 2011  
ISSA NoVA Meetup  
Fairfax, VA

[View All Events](#)

## MOST POPULAR

NoVA Meetups  
Infosec Conferences  
ShmooCon 2010 FireTalks  
Infosec Blogs/Podcasts  
ShmooCon 2011 FireTalks

## Latest Story

# Weekly Rewind – Top Industry News, Infosec Schools, 20 CSCs, Cybersec Awareness, & More

October 8, 2011

By grecs



[Read more »](#)

Here's another edition of the Weekly Rewind, where we post out a quick summary of industry articles you seemed to like as well as our stories from the past week. If you missed anything or happened to be offline, we hope you find this post useful as a reference. Industry Articles Steve Jobs: How...

## Top Infosec Schools in the Metro DC Area

October 7, 2011

By judykavuo

## Top 3 NoVA Infosec Blog Posts of the Week

October 7, 2011

By nathiet

## SEARCH



## FEATURED PAGES

[Advertise with Us](#)  
[Help Us Help You](#)  
[Job Board](#)  
[NovaInfosec Twits](#)

## SUBSCRIBE



## CONTRIBUTORS

Who is @greecs?  
Who is @nathiet?  
Who is @cktricky?

## NOVA BLOGGERS

# Agenda

- Introduction
- Background
- Principles & Concepts
- Career States
- Cheatsheet
- Conclusion

# Introduction

- Been Around a While
- Passion for Studying Art of Career Management
  - Hopefully Help Myself
  - Mostly for Spending Time Mentoring Others
- Derived Several Framework Concepts
  - Help Others Manage Their Career



# Introduction

- [Hacking Your Way into an Infosec Career](#) (11/10)
- [Certifications – Hey, All the Cool Kids Are Doing It](#) (7/11)
- [How to Get the Hot Jobs](#) (9/11)
- [Faring of the Top 5 Certifications for 2012](#) (3/12)
- [Top 4 Un-Certifications](#) (3/12)
- [Where to Learn More about Infosec?](#) (3/12)
- ...

# Introduction

- Personal Opinion
  - Lots of Ways to Get There
  - Just One Way Applied to Web Application Security
- Goal
  - Provide One General Track
  - Tools to Customize or Develop Your Own
  - Provides Framework to Build a Security Career Around

# Background

- Attended Many Similar Presentations
- High Expectations
  - All Bright-Eyed & Bushy Tailed
  - Discover Golden Ticket that Will Change Everything
  - Make Career Management Super Obvious & Easy
- Low Results
  - Follow Presenter Point-for-Point
  - Most Content Already Know
  - Might Pick Up One or Two Tidbits
  - But I Hold Out Judgment Until End Where Pull All Together
  - Never Comes

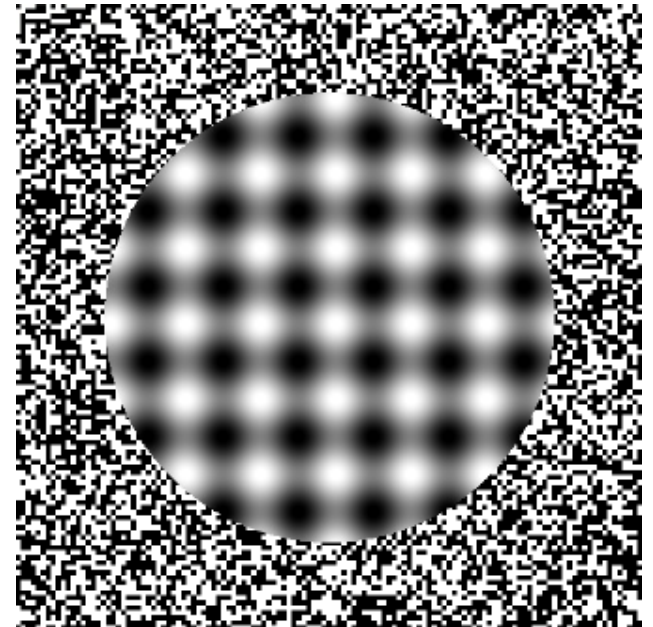


# Background

- Very Difficult
  - No One Plan
  - Presenters Tend to Stick to One Broad Standard Career Talk
  - Could Apply to Any Profession
  - Others Customize Some (e.g., on infosec) But Still too Broad
  - No Clear Link between Strategic & Tactical
- Trust Me It's Hard
  - Last Two Years Been Giving General Infosec Career Talks
  - As Presenter Often Feel Left Unsatisfied
  - Too Hard to Take Down to Practical Level
    - Diverse Nature of Infosec
    - Multitude of Different Ways of Getting Started

# Background

- Focus
  - Only Way Achieving Practical/Actionable Steps
  - Much More Narrow Approach
  - Web Application Security



# **PRINCIPLES & CONCEPTS**

# Overarching Principle

## Why?

- How Many Have a Career Plan?
  - Why?
  - What's Look Like?
- Allows You to Most Efficiently Achieve Your Career Goals
- Goals Change as Your Careers Progress
  - Plan Allows You to Easy Modify Goals & Efficiently Take Advantage of Past Experience to Get There

# Overarching Principle

## How?

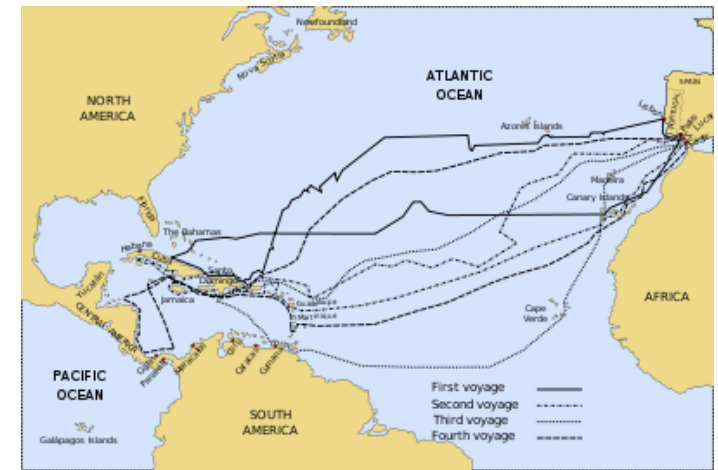
- Pick a Goal
- Decide Steps for How to Achieve Goal
- Periodically Reevaluate Against that Plan
- Replan, replan, replan, ...
  - More Efficient Path
  - Goals Changing





# Overarching Principle Tips

- Goal
  - Think of As Destination
  - Steps Help Strategically Navigate to Goal
- Don't Get Too Detailed - Stick to 1/3/5 Stages
  - Dream Goal Way Out (~ 10, 15, or 20 years later)
- Doesn't Have to Be Perfect
  - Goal WILL Change
  - Steps WILL Change
  - “Perfection is the Enemy of Good Enough”



Just Come Up with Something ... Anything ... and Adjust As You Go Along

# Concepts

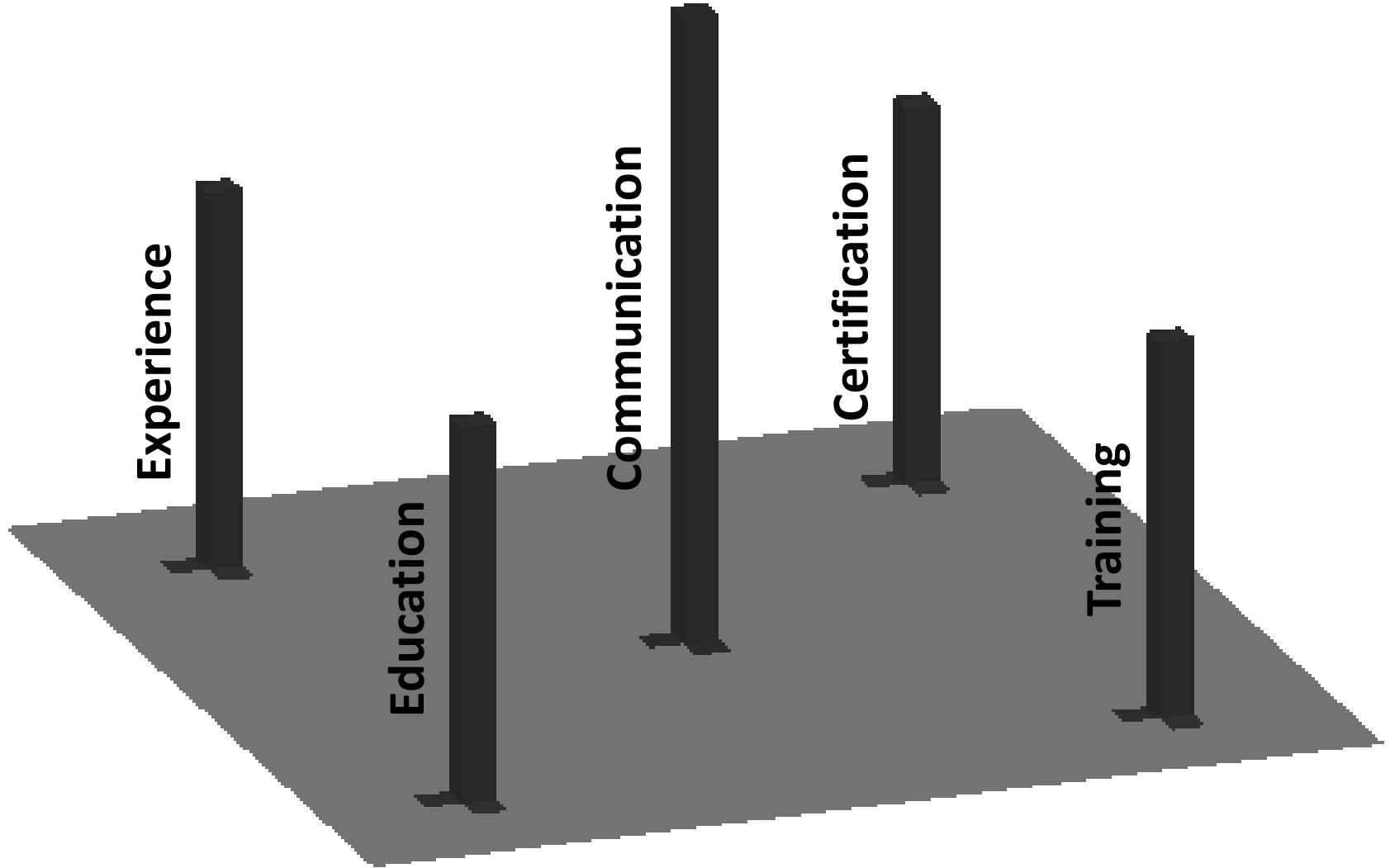
- Poles
  - Education
  - Experience
  - Certification
  - Training
  - Communication

- Goals
  - Keep Poles Balanced
  - Augment Underdeveloped Ones to “Minimum”
  - Further Develop Ones You Excel At



**More Corporate Focused**

# Concepts

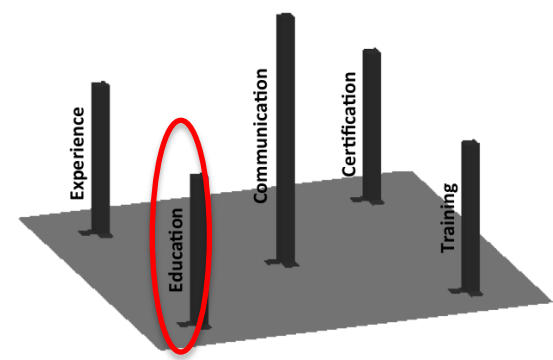


# Concepts



**More Outreach Focused**

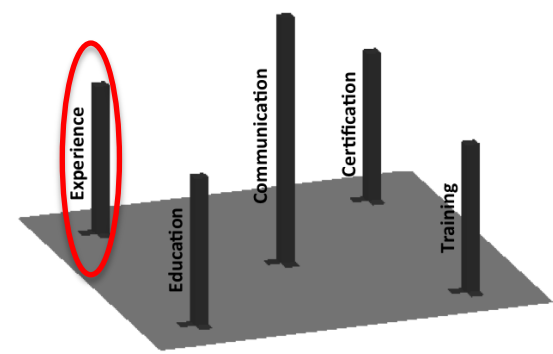
# Concepts Education



- Wikipedia
  - “Derived from a technical term in Ancient Greek philosophy. The word *theoria*, θεωρία, meant "a looking at, viewing, beholding", and referring to **contemplation or speculation, as opposed to action**.
- No Implementation Details
  - Usually More Theory Related
  - Just Overall Concepts
- Examples
  - Darwin's Theory of Evolution
  - Einstein's General Relativity Theory
  - CS: Sorting Algorithms, Search Trees, Linked Lists, Heaps, Stacks

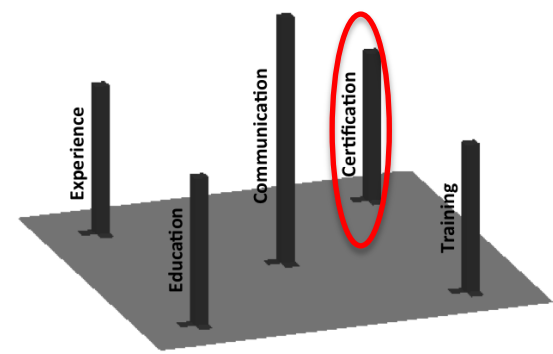
# Concepts

## Experience



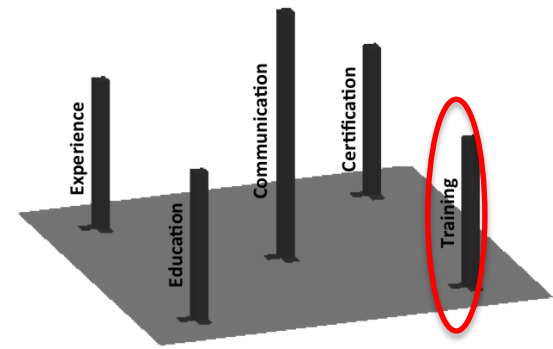
- Wikipedia
  - Comprises knowledge of or skill of some thing or some event **gained through involvement** in or exposure to that thing or event.
- Related More to Real-World Hands-On Learning
  - Implementation Details
- Examples
  - 5 Years of Programming in PHP for Company

# Concepts Certification



- Wikipedia
  - A **designation earned** by a person to assure **qualification** to perform a job or task
- Examples
  - Security+
  - GWEB
  - CSSLP
  - OSWE

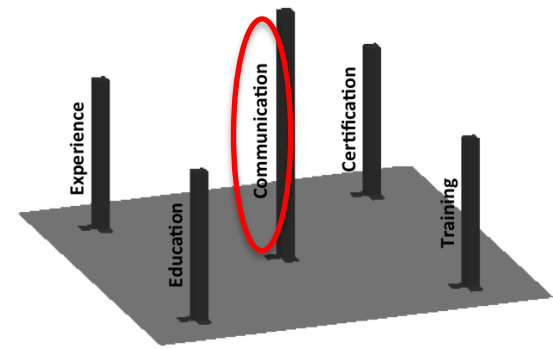
# Concepts Training



- Wikipedia
  - Refers to the acquisition of knowledge, skills, and competencies as a **result of the teaching of vocational or practical skills** and knowledge that relate to specific useful competencies.
- Examples
  - Taking PHP Course from Training Company



# Concepts Communication



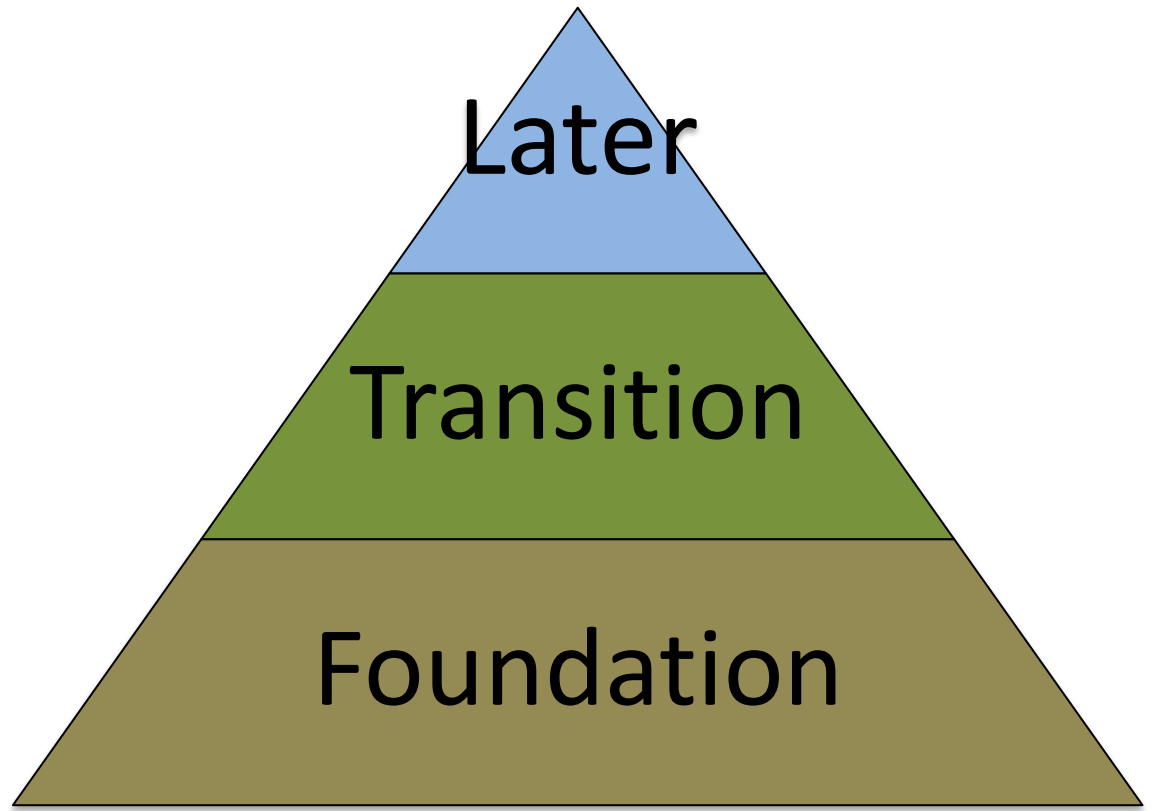
- Wikipedia
  - The activity of **conveying information**.  
Communication has been derived from the Latin word "communis", meaning to share.
- Written & Oral
- Examples
  - Whitepaper
  - Blog Post
  - Presentation

# Concepts

# Catalysts

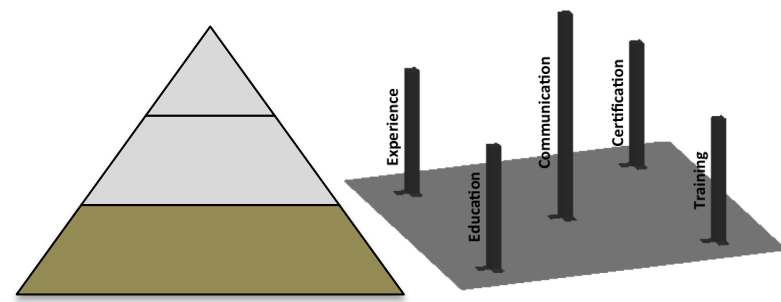
- Wikipedia
  - A **substance that increases the rate** of a chemical reaction without itself undergoing any permanent chemical change.
- Things that Help You Reach Your Goals Faster
- Primary Methods (do overlap some)
  - Blogging
  - Social Networking
  - Online Community-ing
  - Networking
  - Mentoring
- Examples
  - CitySec Meetups
  - Hallway Track at Conferences
  - Community Participation





## **CAREER STAGES**

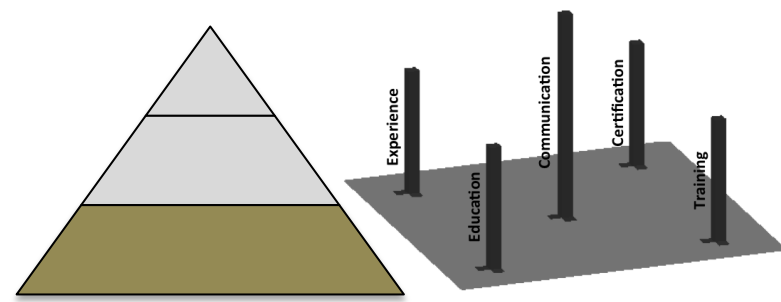
# Foundation



- No Security Yet ... Establish Foundation First
- "Learn industry first so you can secure it later."

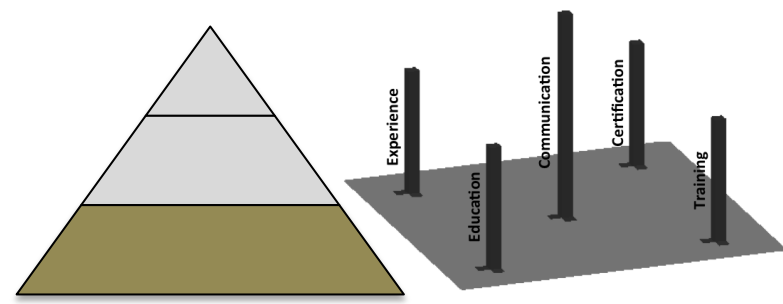


# Foundation Tent Poles



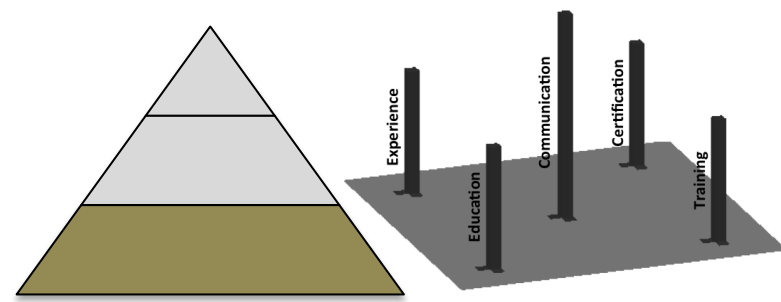
- Education
  - Traditional CS Undergrad
    - Mainly Theory
    - Some Hands-On
  - Other Engineering/Technical Degrees Fine
  - Head to Local Library & Learn Theory Yourself
- Experience
  - Real-World Web Development Work
  - The More Years the Better But Maybe 3 at Minimum
  - Depth & Width Play Into (Specialist v. Generalist)

# Foundation Tent Poles



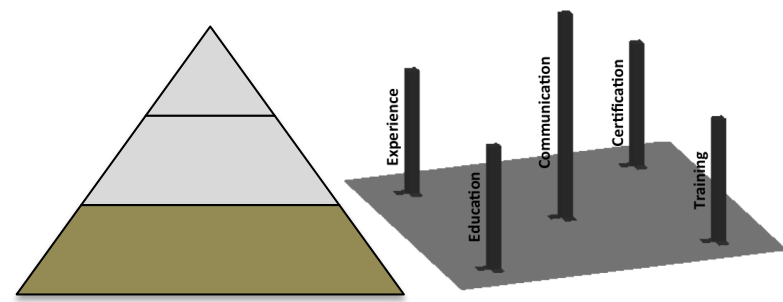
- Certification
  - Web Application Developer Certifications
  - What Are the Big Ones?
- Training
  - Continuous Training in Web Development
  - If Company Won't Pay, Do It Yourself (5% Rule)

# Foundation Tent Poles



- Communication
  - Technical Writing Course in Undergrad
  - Electives to Take English 101 Course
  - Be Go-To Person for Developer Documentation
  - Offer to Write Whitepapers
  - Teach Others In Your Company

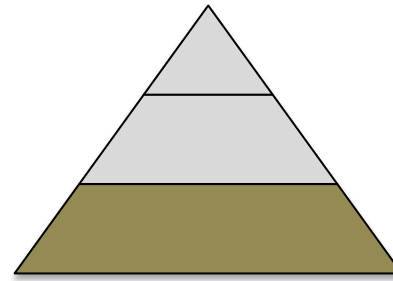
# Foundation Tent Poles



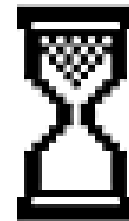
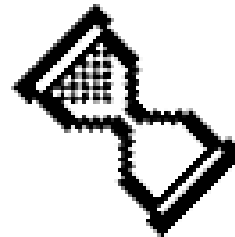
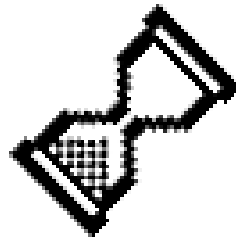
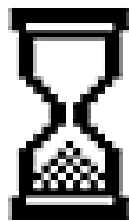
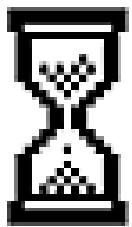
- Overall
  - Focus on Web Application Developer Industry ...  
Not Security ... Good to Sprinkle Some In Though
  - If Schools Doing Right
    - Security Embedded into Classes
    - Electives that Offer Basic Security Concepts
  - Study On Own
  - Starting in Middle
    - Backfill as Needed



# Foundation Catalysts

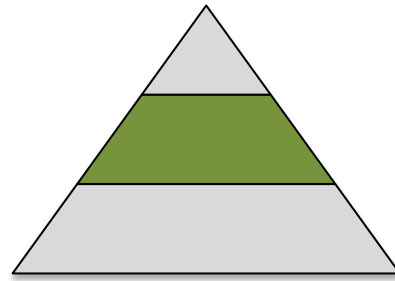


- Blogging
  - Regularly Publish Web Developer Articles
  - Give Lessons Learned or New Ideas Back to Web Developer Community
- Social Networking
  - Twitter, Facebook, LinkedIn, etc.
  - Create “Web Dev” Focuses Accounts Now & Start to Build Out by Sharing Interesting Things
- Online Community-ing
  - Join Online Developer Groups (e.g., forums, email lists, etc.)
  - Take Part In Discussions (i.e., learn from everyone & give back when you can)
- Networking
  - Attend Local Web Developer Meetups
  - Volunteer to Take Part In/Organize Something as Part of an Event
- Mentoring
  - Find Someone Skilled In Web Development & Ask for Mentoring
  - Formal/Informal/Whatever



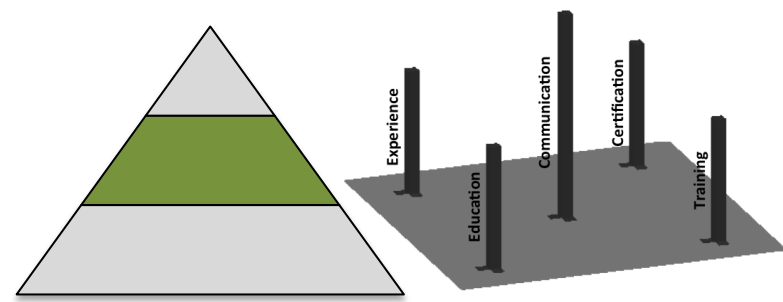
**3 YEARS LATER**

# Transition



- At this Point Have 3 Years Total Experience in Web Development
- Good Understanding of This Area
- Start to Establish Security Foundation

# Transition Tent Poles



- Education

- IA/Cyber Masters or Graduate Certificate Program

- Mainly Theory
    - Some Hands-On

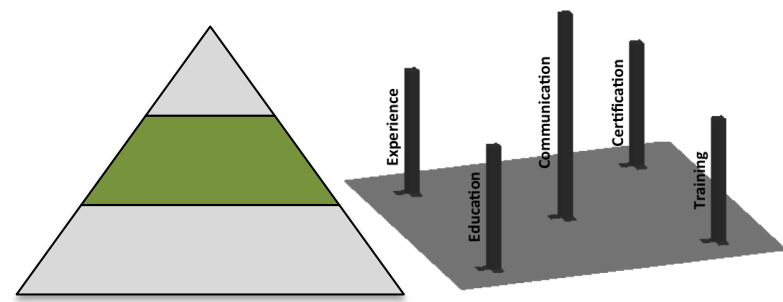
- Head to Local Library & Learn Theory Yourself

- Experience

- Real-World Work Doing Web Application Security

- Depth & Width Conundrum

# Transition Tent Poles



- Certification

- Web Application Security Certifications

- What Are the Big Ones?

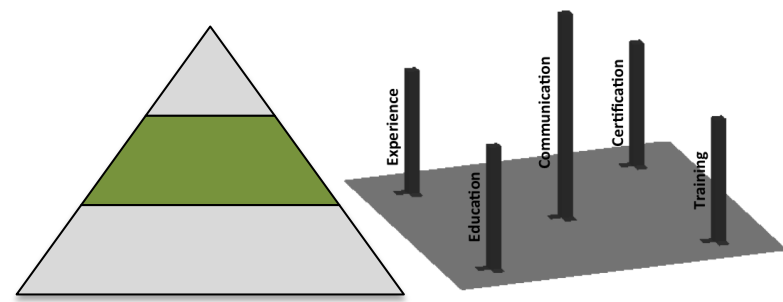
- Security+ & one of GWEB, CSSLP, or OSWE?

- Training

- Continuous Training in Web Application Security

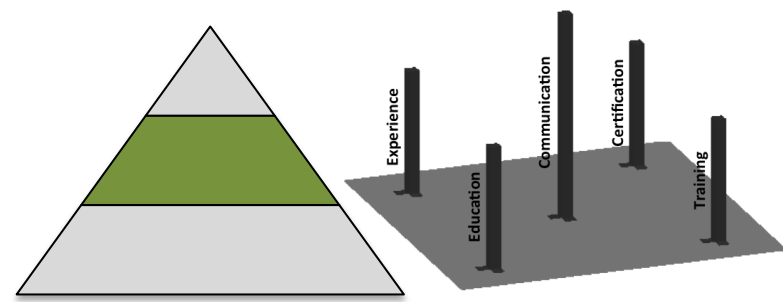
- 5% Rule

# Transition Tent Poles



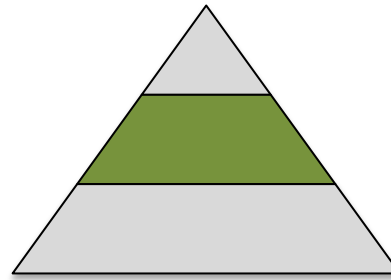
- Communication
  - Be Go-To Person for Web Security Documentation
    - Company Processes or Best Practices
    - Assessment Reports
  - Offer to Write Whitepapers
  - Teach Others in Your Company

# Transition Tent Poles



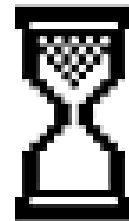
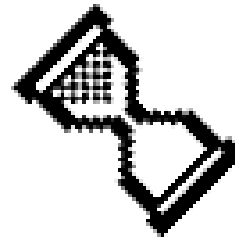
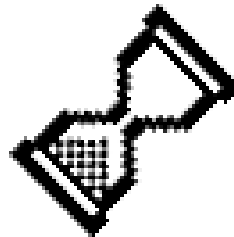
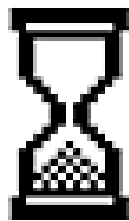
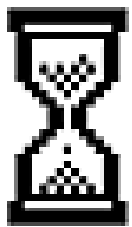
- Overall
  - Focus on Security Industry ... Not Web Development ... Still Want to Sprinkle Some In Though
  - Study On Own
  - Starting in Middle
    - Backfill as Needed

# Transition Catalysts



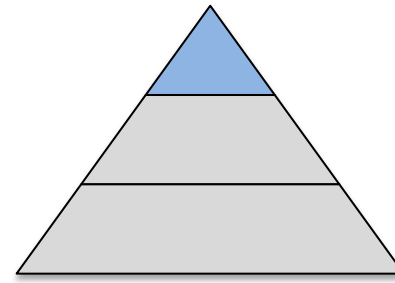
- Blogging
  - Regularly Publish Web Security Articles
  - Give Lessons Learned or New Ideas Back to Web Security Community
- Social Networking
  - Twitter, Facebook, LinkedIn, etc.
  - Transition Accounts to Focus More on Security
- Online Community-ing
  - Join Online Web Security Groups
  - Take Part In Discussions
- Networking
  - Attend Local Web Security Meetups (OWASP)
  - Volunteer to Take Part In/Organize Something as Part of an Event
- Mentoring
  - Find Someone Skilled In Web Application Security & Ask for Mentoring ([infosecmentors.org](http://infosecmentors.org))
  - Formal/Information/Whatever





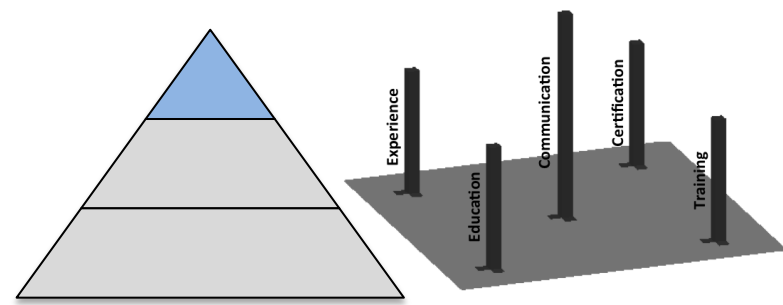
**2 YEARS LATER**

# Later



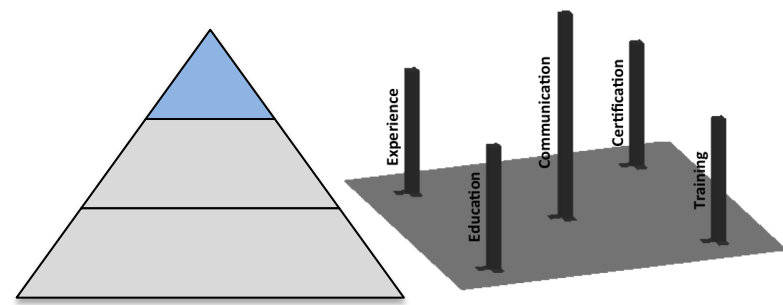
- At this Point Have 5 Years Total Experience with 3 in Development & 2 in Security
- Depth v Width v Height
  - Specialist, Generalist, Leadership
  - No Right Solution
  - Experiment & Do What You Enjoy
- Assume Depth
  - Continue Specializing in Gaining More Web Security Experiences

# Later Tent Poles



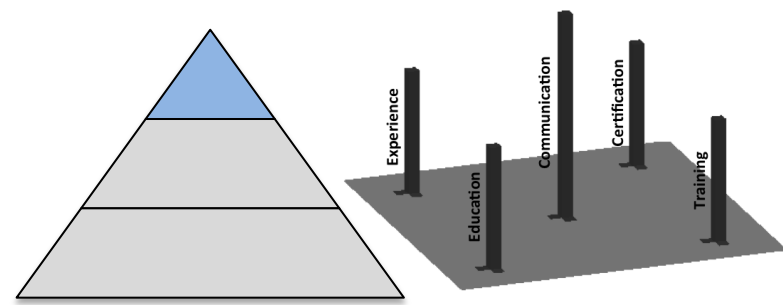
- Education
  - In-Depth Exploration of Concepts Learned from Research or Innovations
  - PhD, Second Masters, Another Graduate Certificate?
- Experiences
  - More Real-World Work Doing Web Application Security
  - Leadership Roles Where So Can Focus On Higher-Level Tasks & Delegate Mundane Activities
- Certification
  - Maintain Existing Security Certifications
  - Obtain One Advanced Web Security Certification

# Later Tent Poles



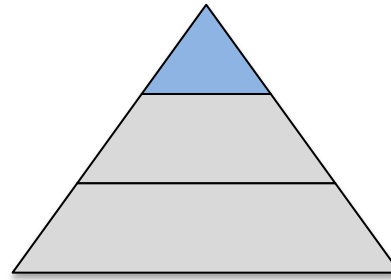
- Training
  - More Continuous Training in Web Application Security
  - 5% Rule
- Communication
  - Editor for Web Security Documentation
  - Idea Generator/Editor for Whitepapers
  - Continue Teaching Others in Your Company

# Later Tent Poles

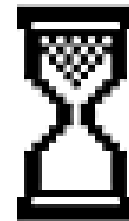
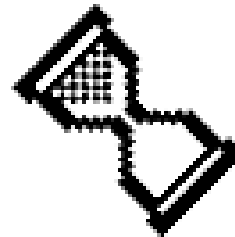
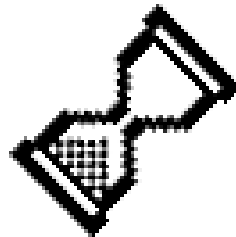
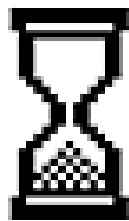
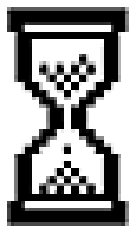


- Overall
  - Focus on Security Industry ... Maybe Getting into Some Technical Leadership
  - Study On Own
  - Starting in Middle
    - Backfill as Needed

# Later Catalysts

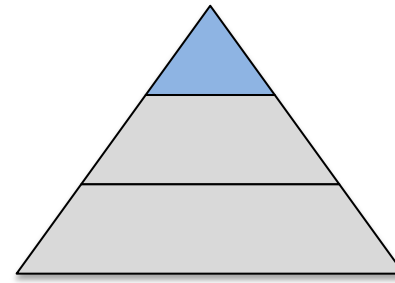


- Blogging
  - Regularly Publish Web Security Articles with Some Published in More Mainstream Pubs
  - Give More Lessons Learned or New Ideas Back to Web Security Community
- Social Networking
  - Twitter, Facebook, LinkedIn, etc.
  - Continue Focusing on Security & Also Include Engagement & Influence
- Online Community-ing
  - Continue Participation in Online Web Security Groups
  - Take Part In & Lead Discussions
- Networking
  - Lead Local Web Security Meetups (OWASP)
  - Focus More on Organizing Talks, Events, etc.
- Mentoring
  - Continue Various Security Mentoring Relationships
  - Find Mentees & Mentor Them ([infosecmentors.org](http://infosecmentors.org))



**3 YEARS LATER**

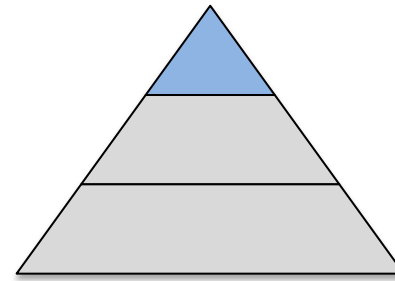
# More Later



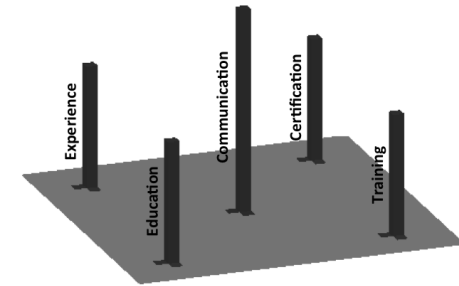
- At this Point Have 8 Years Total Experience with 3 in Development & 5 in Security
- Depth v Width v Height
  - Specialist, Generalist, Leadership
  - No Right Solution
  - Experiment & Do What You Enjoy
- Assume Leadership
  - Continue Start Taking on More Strategic Responsibilities



# More Later



- Tent Poles - Pretty Much Some ... Keep Balanced
  - Education: Continue Course Focusing More on Exploration
  - Experience: Less Tactical & More Strategic
  - Certification: Just Maintain If Needed
  - Training: Continue 5% Rule
  - Communication: More of Idea Generator & Final Review
- Catalysts
  - Blogging: Focus More on Main Stream Pubs
  - Social Networking: Continue Course
  - Online Community-ing: Focus on Leadership Roles
  - Networking: Continue Course
  - Mentoring: Focus on Mentoring Others



# CHEATSHEET

# Conclusion

- Multiple Tent Poles to Manage Your Career
  - Education, Experience, Certification, Training, & Communication
  - More Corporate Focused
  - Keep Poles Balanced
  - Augment Underdeveloped Ones to “Minimum” & Further Develop Ones You Excel At
- Catalysts
  - Blogging, Social Networking, Online Community-ing, Networking Mentoring
  - More Outreach Focused
  - Extra Activities to Accelerate Career
- Career States (one possibility)
  - Don't Jump Right into Security ... Learn to Be Good Web Developer First
  - Migrate into Web Application Security
  - Transition into More Technical Security Leadership Roles
  - Move into Strategic Type Security Positions
- Cheatsheet

# Contact Info

- Twitter      @greecs
- Website      NovalInfosecPortal.com
- Contact      <http://bit.ly/nispcontact>





Questions?