Welcome

Welcome to SnowFROC 2012, the fourth Front Range OWASP Application Security Conference!

After successful FROC's in June of 2008, March of 2009, and 2010 we are back in Denver, Colorado USA on **Thursday the 22nd of March**!

This year we again present a full day, multi-track event, which will provide valuable information for managers and executives as well as developers and engineers. **ALSO**, on Friday March 23rd several instructors from OWASP will be conducting day-long deep-dives!

In 2010, we attracted a packed venue with our great AppSec speakers, and we hope to achieve the same again in 2012.

Registration

Registration for SnowFROC is now open!

$20 covers breakfast, lunch, and a WORLD-CLASS AppSec conference!

Click http://snowfroc2012.eventbrite.com/ to register now for SnowFROC!

Agenda and Presentations: 22 March 2012

The agenda follows the successful OWASP conference multi track format, with opening keynotes and presentations in the main room, split tracks in the middle of the day, and closing panel discussions back in the main room.

March 22nd, 2012	
07:45-08:30	Registration and Continental Breakfast in the Adirondack Room
08:30-08:45	Welcome to SnowFROC 2012 Conference *OWASP Denver and OWASP Boulder Chapter Leaders*
08:45-09:10	**State of OWASP** *Matt Tesauro*
09:10-10:10	**Keynote:** *John Pirc, Co-Author of "Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats"*
10:10-	Break - Expo

10:30		
	Tech Track - Zenith Room 640	**Management Track - Senate Chamber**
10:30-11:15	OWASP Passfault *Cameron Morris*	Managing IT Risk in a Cloud Environment *Karl Steinkamp*
11:15-12:00	State of Web Security: Monitored Attacks *Robert Rowley*	PCI vs Risk Management *Doug Landoll*
12:00-13:00	Lunch - Expo	
13:00-13:50	Panel Discussion - Favorite tools and techniques - pen-testing, static analysis, code reviews *Panelists*	Securing Data from the Web Tier *Mike Fleck*
13:50-14:40	Gray, the new black: Gray box vulnerability testing *Adam Hills*	Web Session Intelligence *LAZ*
14:40-15:00	BREAK	
15:00-15:50	"The Mobile Top 10" *Mike Zussman*	A Scalable Secure Development Program *Rajiv Sharma*
15:50-16:30	End of Conference Panel Discussion: Topic: *The Crystal Ball and the 2-headed Calf - What's on the Horizon and Why Does It Seem So Unnatural?* Moderator: Steve Kosten or Andy Lewis Panelists: Laz, Matt Tesauro, John Pirc, Tanner Coltrin, Steve Kosten, others	
16:30-17:30	Wrap up, vendor raffles!	

On March 23rd three day-long deep-dives will be taught at the Auraria Campus classrooms. Classes start at 8. Topics, instructors, and registration links are below:

Click https://www.owasp.org/index.php/Denver,_Colorado to register for OWASP Deep Dives in Denver! OWASP training on Friday March 23, 2012 at Auraria campus classrooms

Course	Instructor	Description	Cost	Registration
8:00 AM - 5:00 PM FROC 2012 CN CN 212 SamuraiWTF: Integrating Manual Testing Techniques and Automated Testing Tools	Justin Searle	**Course Abstract:** One of the best skills a penetration tester can learn is not how to use a lot of penetration testing tools such as those on the SamuraiWTF DVD, but rather how to successfully integrate their manual testing techniques with all of those penetration testing tools. This one-day course focuses on this skill through two instructor-lead penetration tests followed by a capture-the-flag like student challenge. This course also introduces you to several of SamuraiWTF's testing tools such as Zed Attack Proxy (ZAP), w3af, and the latest Firefox extensions for penetration testing. This course is designed for persons new to penetration testing and for those persons with basic to intermediate experience with web application penetration testing. Please come prepared with VMware player, workstation, or fusion pre-installed.	$675 until 3/9 then $745	REGISTER NOW
8:00 AM - 5:00 PM FROC 2012 CN CN 213 Defense against the Dark Arts: ESAPI	Chris Schmidt	It has been said that software engineering is 10% engineering and 90% art. Given the same set of technical specifications, two engineers will have drastically different methods of addressing those specifications. This is the beauty of innovation and forward thinking, and while it is this type of creative problem solving that has kept the technical industry lurching forward in large strides	$675 until 3/9 then $745	REGISTER NOW

		– it is also the boon of application security. Enter the Enterprise Security API – a central repository for engineers to solve security concerns in application code. I have said many times that it should not be the responsibility of the engineers cranking out code every day to design security controls. It is difficult to remain on the bleeding edge of Application Security and Software Engineering at the same time and even more difficult to bring these two disciplines together into a cohesive, reusable component that addresses the threats specific to an organization. This course will illustrate the importance of having an Enterprise Security API and how to effectively design, build and deploy a solution that addresses the Threat Model of the single application or enterprise application portfolio. Topics Include (but are not necessarily limited to) ESAPI Architecture; Security Controls Overview; OWASP Reference Implementations; Designing Custom Controls; Integrating with existing Applications; Starting Fresh; Enterprise Security Configuration; Error Handling, Logging and Intrusion Detection/Prevention; Authentication and Authorization; Validation and Encoding		
8:00 AM - 5:00 PM FROC 2012 CN CN 214 Threat Modeling: From the "cloud" on down	Matt Tesauro	Everyone knows that catching software vulnerabilities early is the best way to create secure software with the least cost (and drama). However, how do you do this in the Agile, Cloud-based application environment that we face today? This training walks you trough an overview of threat modeling techniques and tools with an eye on pragmatic solutions to real world problems. Using the topics covered	$675 until 3/9 then $745	REGISTER NOW

		in this class, you will learn how to determine and describe an applications attack surface, understand the probability of an attack while gaining insight into its impact. Whether you're looking to find design flaws early, eliminate low-hanging vulnerabilities or improve and optimize testing, the discussion and hands-on portions of this class provide real-world examples of application security. The hands-on portion draws lessons from actual software such as those powering web-scale, cloud software stacks allowing you to gain practical experience working through tough software problems.		