You're invited to attend the 1st ever MN OWASP Conference on October 21st. We're very excited out the line up of internationally known speakers we were able to bring together for this one day of Application Security talks. The local MN OWASP chapter is hosting this event which we've brought to you at a nominal fee of $25.00 per person which includes lunch. Seating is limited and we expect this event to sell out. On site registration the day of the event is not expected to be available so please register prior to the event to guarantee your seat at this event.

To Register:
http://guest.cvent.com/i.aspx?4W,M3,c2618ba0-022d-434e-a053-39fcc4120313

Event Page:
https://www.owasp.org/index.php/OWASP_Minneapolis_St_Paul_2008_Conference

Tentative Agenda

8:00-9:00	Registration / Check-In

9:00-9:30	**Kuai Hinojosa** OWASP MN President Conference Introduction
9:30-10:30	**Jeff Williams** CEO, Aspect Security OWASP founder; Chair, OWASP Foundation Application security is getting more complicated every day with increasing connectivity, more mixing of code and data, more parsers, more interpreters, more assets, and more functionality available. We have to take steps now to simplify the problem. So if you're tired of securing one application at a time, and wrestling with the same vulnerabilities again and again, is establishing your organization's ESAPI is one of the best things you can do? **Bio**: I'm Jeff Williams, I work as CEO of Aspect Security and I serve as the volunteer Chair of the OWASP Foundation. I've worked on a number of projects at OWASP, including creating the OWASP Top 10, WebGoat, Stinger, Secure Software Contract Annex, Honeycomb Project and the Enterprise Security API. You can find more about my background here: http://myappsecurity.blogspot.com/2007/03/reflection-on-jeff-williams.html.

10:30-11:00	**Arshan Dabirsiaghi** Director of Research, Aspect Security Many of the challenges we face in application security could be solved at an architectural layer without trying to accomplish the impossible task of fixing millions of websites with billions of lines of code behind them. The OWASP Intrinsic Security Working Group is a new OWASP effort focused on addressing root causes of application security problems and fixing them where it's easiest. Sometimes that means pushing a browser to include a feature, or asking a language framework to provide a new API, or helping standard-makers come up with useable security protections. Our goal with the OWASP ISWG is to leverage the collective security know-how of OWASP into practical advice and suggestions for all those technologies that our applications lean on in one way or another. We've got the modest goal of fixing the Internet - what could be more valuable? **Bio**: Arshan Dabirsiaghi is the Director of Research at Aspect Security. Arshan has over seven of years of professional experience writing code, four years of professionally auditing code, and many years of hobbying in both. At Aspect Security, Arshan performs the normal array of security assurance work, including code reviews, architecture reviews and penetration testing. He spends the balance of his work time teaching classes all over the world and doing research into next generation web application attacks and defenses. Arshan earned his Master's degree in Computer Science from Towson University with a focus on Information Security. He has delivered tutorials at Blackhat and OWASP conferences and has been a featured speaker at a number of security and artificial intelligence conferences. Arshan is also the author of the OWASP AntiSamy project and the founder of the OWASP Intrinsic Security Working Group.
11:00-12:30	Lunch

12:30-13:30	**Anil Kumar Revuru** Microsoft Microsoft Connected Information Security Framework (CISF) and Tools: The Connected Information Security Group, part of Microsoft internal Information Security organization are working on a technology framework and set of applications to support corporate information security management programs. The Microsoft corporate Information Security Organization (and a few 'early adopter' customers) will be dog-fooding early prototypes in late 2008/early 2009. This presentation provides a short overview of the problem space and current thinking on our approach to solving it. **Bio**: Anil Kumar Revuru currently works for Microsoft as a Security Technologist where he is responsible for architecting security tools. In his previous life at Microsoft, Anil was conducting security design reviews, threat modeling, and application and source-code assessments. Previously as a Security Consultant for a security services vendor, he helped Fortune 100 clients evaluate the security of their software products and applications. He has authored security tools and has presented courses internally at Microsoft. Anil holds a Diploma in Mechanical Engineering from JNTU Hyderabad. Anil displayed expert proficiency in the substantive and technical areas of design and development, He also made significant contribution to the security development of products at V-Empower Inc. After joining in Microsoft, he worked towards finding security weaknesses and providing necessary countermeasures to application teams. He excelled in his abilities by developing security tools such as Microsoft Threat Analysis and Modeling Tool used for application threat modeling
1:30-2:30	**Brian Chess** Fortify Software Creating secure code requires more than just good intentions. Programmers need to know how to make their code safe in an almost infinite number of scenarios and configurations. Static source code analysis gives users the ability to review their work with a fine tooth comb and uncover the kinds of errors that lead directly to vulnerabilities. This talk frames the software security problem and shows how static analysis is part of the solution. Highlights include: • The most common security short-cuts and why they lead to security failures • Why programmers are in the best position to get security right • Where to look for security problems • How static analysis helps • The critical attributes and algorithms that make or break a static analysis tool We will look at how static analysis works, how to integrate it into the software development processes, and how to make the most of it during security code review. **Bio**: Dr. Chess's research focuses on methods for creating secure systems. He received his Ph.D. from the University of California at Santa Cruz, where he applied his background in integrated circuit test and verification to the problem of identifying security errors in software. In addition to authoring numerous patents and technical papers, Dr. Chess has more than ten years of experience in the commercial software arena, having led development efforts at Hewlett Packard and NetLedge

2:30-3:00	Break

3:00-4:00	**Elliot Glazer**
	DTCC
	Information Security Architecture Layers and Key Processes:
	• Information Security Architecture is driven by an Information Security Strategy and Principles. It is also critical the architecture support the Business Strategy:
	  ◦ Security Functional Architecture: the layout of key functions in security to be accomplished, which drives security requirements.
	  ◦ Security Technical Architecture: the solutions and standards to implement key functions, usually an overlay on top of the Functional Architecture. This is generally a definition of components, intended to be leveraged for reuse by organization, business, line of business or across the enterprise.
	  ◦ Security Reference Architecture: the implementation of Technical Architecture components into a strategy, platform, or particular complex solution set, to be used as a model for other, like needs. This is usually a set of components organized together.
	  ◦ Security Technology Lifecycle – the process of phasing in and out, technology and process solutions that improve the security environment. Six phases ranging from researching new solutions to exiting old and failing solutions are defined.
	  ◦ Security Program Implementation Planning – the process of identifying high level scheduling based on priority and available resources, for solutions defined in the Technical Architecture. Priority is generally established based on risk. The program also

	helps in the planning cycles for budgeting, as it will try to take a multiyear view. **Bio**: Elliott has over 25 years of information technology experience and has worked in the security field for over 10 years. He is currently Director of Security Architecture for the Depository Trust and Clearing Corporation (DTCC), where he has created a number of innovative solutions in the areas of security monitoring and security architecture. He also provides consulting to the organization on critical security issues. Prior to this, Mr. Glazer was Vice President for Security Solutions at American Express, leading many large and small solutions for the Internet, Security, Privacy, and Customer Servicing. Previous to this, Elliott held leadership positions at Citigroup, Sprint International, and BT Dialcom in software development and operations. He has led architecture, development, and operations organizations including an enterprise architecture group, Internet software development, and distrbitured operations among others.
4:00-5:00	**Corey Benninger** Intrepidus Group Exploring the how poor application security mixed with a phishing is leading to a costly cocktail of disaster. This talk will go over real world examples of phishing attacks that have taken advantage of cross site scripting flaws, SQL injection vulnerabilities, session fixation attacks, and others web application flaws. Learn what phishers are doing to take their attacks to the next level by chaining multiple vulnerabilities together. The presentation will also share resources that help to track phishing trends and research. **Bio**: Corey is a Principal Consultant with the Intrepidus Group, specializing in web and mobile application security. He has performed code reviews and conducted application penetration tests for numerous Fortune 500 clients. Prior to joining Intrepidus Group's professional services team, Corey served as a Senior Consultant and Trainer at Foundstone. Corey is a polished public speaker and has been invited to speak at leading conferences like Black Hat, OWASP AppSec, NYCBSDCon, Secure Development World and Infragard. In addition, his expert opinion has been published in industry publications like eWeek. He has also published several whitepapers on cutting edge security issues, like vulnerabilities in AJAX, and the security implications of web browser data caching. He is the co-founder and leader of the OWASP Mobile Security Project, a consortium of mobile security developers and experts. Corey has an undergraduate degree from Boston University. He is a Certified Information Systems Security Professional (CISSP).

5:00-5:15	**Richard Stallman** Richard Matthew Stallman is a software developer and software freedom activist. In 1983 he announced the project to develop the GNU operating system, a Unix-like operating system meant to be entirely free software, and has been the project's leader ever since. With that announcement Stallman also launched the Free Software Movement. In October 1985 he started the Free Software Foundation. The GNU/Linux system, which is a variant of GNU that also uses the kernel Linux developed by Linus Torvalds, are used in tens or hundreds of millions of computers, and are now preinstalled in computers available in retail stores. However, the distributors of these systems often disregard the ideas of freedom which make free software important. That is why, since the mid-1990s, Stallman has spent most of his time in political advocacy for free software, and spreading the ethical ideas of the movement, as well as campaigning against both software patents and dangerous extension of copyright laws. Before that, Stallman developed a number of widely used software components of the GNU system, including the original Emacs, the GNU Compiler Collection, the GNU symbolic debugger (gdb), GNU Emacs, and various other programs for the GNU operating system. Stallman pioneered the concept of copyleft, and is the main author of the GNU General Public License, the most widely used free software license. Stallman gives speeches frequently about free software and related topics. Common speech titles include "The GNU Operating System and the Free Software movement", "The Dangers of Software Patents", and "Copyright and Community in the Age of the Computer Networks". A fourth common topic consists of explaining the changes in version 3 of the GNU General Public License, which was released in June 2007.

For more information: https://www.owasp.org/index.php/OWASP_Minneapolis_St_Paul_2008_Conference

The conference is being held at the University of Minnesota on the St. Paul Campus in the Student Center, at the Auditorium and Ballroom.
http://www1.umn.edu/twincities/maps/StCen/StCen-map.html

Kuai Hinojosa
President Minnesota Chapter - OWASP

For More information contact:

Lorna Alamri VP Minnesota Chapter - OWASP
Dir: 651-259-1001
Cell: 651-338-0243
Fax: 651-631-2544