PRESS RELEASE Embargoed Until 12:01 AM EDT, March 26, 2007	 **WWW.SANS.ORG**

Questions: Alan Paller at 301-951-0102 x108 or apaller@sans.org	A complete program description, sample questions, test blueprints, and more, are posted at www.sans.org/ssi or www.sans-ssi.org

Coalition of Security Leaders Announces First Secure Coding Assessment and Certification Exams for Programmers

WASHINGTON, DC., March 26 – A coalition of major technology users and vendors, organized by the SANS Institute, today announced the first skills assessment and certification examinations for programming professionals to test their secure coding skills, find the gaps, and, if they choose, gain GIAC Secure Software Programmer (GSSP) status. The six examinations each cover a specific programming language suite: (1) C (2)C++, (3) Java/J2EE, (4) Perl (5)PHP, (6) .NET/ASP, and are designed to enable reliable measurements of technical proficiency and expertise in identifying and correcting the common programming errors that lead to security vulnerabilities. The exams will be administered in August in Washington DC on a pilot basis, and then will roll out worldwide through the remainder of 2007.

"Organized crime groups have turned their attention to computer-based crimes and are increasingly attacking weaknesses in applications, raising the value of secure coding skills. This assessment and certification program will help programmers learn what they don't know, and help organizations identify programmers who have solid security skills," said Alan Paller, director of research at the SANS Institute. "With the right skills, programmers can reduce the risk of losses caused by cyber attacks, and the certification will allow security-aware programmers to stand out in an increasingly competitive marketplace."

The six secure programming examinations provide a focused approach for programming professionals who want to identify the gaps in their secure coding skills and knowledge. They also allow employers of those programmers to differentiate their organizations and help increase their competitive advantage by employing programming professionals who have successfully demonstrated their technical secure programming skills through certification.

A Remarkable Coalition of Leaders Are Shaping This Initiative

MITRE's Steve Christey, editor of the CVE program that monitors all security vulnerabilities, on behalf of the federal government, offers the fundamental justification for this effort.

> "After reviewing more than 7,000 vulnerabilities in 2006 alone, one thing becomes crystal clear. Most of these vulnerabilities could be found very easily, using techniques that require very little expertise. In my CVE work, I regularly interact with vendors who are surprised to hear of vulnerabilities in their products. They react with the classic stages of shock, denial, anger, bargaining, and finally, acceptance.
>
> "This is the sorry state of software today. Most educational institutions have failed to teach the most fundamental skills in making secure products. **There needs to be a revolution.** Secure programming examinations will help everyone draw the line in the sand, to say "No more," and to set minimum expectations for the everyday developer."

OWASP publishes the widely respected Top Ten Web Security Flaws, and OWASP Chairman, Jeff Williams, provides a perceptive perspective on the new exams,

> "Programmers don't wake up one morning and think of SQL injection or cross-site request forgery on their own. Yet you can't secure applications without understanding these attacks and others like them. SANS is doing a great service to the world by creating a way to assess programmers' knowledge in this critical area of security."

Major technology and software manufacturers, government agencies, and financial organizations around the world are partnering with SANS to ensure the exams meet their needs. **Symantec**'s leadership in security makes it a particularly valuable partner in the test development process.

> "Symantec has always been a strong advocate for more focused educational curricula and training on secure programming," said Rob Clyde, vice president of Technology at Symantec. "We are excited about the opportunity to work with SANS and other stakeholders on developing and compiling secure programming assessments and look forward to implementing this program with developers."

Juniper, the networking and security company, has always been out front in building technologies that help networks protect themselves. Here Juniper points out the value of secure coding exams to buyers of software and hardware.

> "Juniper Networks recognizes that its IT network developers are only as effective as their ability to create security solutions that can successfully manage threats and control access," said Hitesh Sheth, vice president of Service Layer Technologies at Juniper Networks. "The Secure Coding Exams help assure Juniper customers that our developers can identify security gaps and that they have the coding skills and expertise to deliver the most resilient security solutions offered in the industry."

Siemens, the global technology giant, provides another good example of enterprise leadership. It was one of the first of eighteen enterprise partners helping to ensure the exams and certifications measure the right things. Each enterprise partner is a very large organization that has already launched its own secure coding initiative but sees value in working in cooperation with other organizations to develop a standard for measuring secure coding mastery.

> "The lack of trustworthy standards and certifications has been a challenge for software buyers and software developers," said Hartmut Raffler, head of Technology Division Information and

> Communication at Siemens Corporate Technology. "Secure programming skills are essential for building software that can be trusted. SANS's willingness to offer this exam as part of a comprehensive secure coding improvement strategy is exciting and will help both buyers and sellers of software."
>
> "As a participant in the development stages of the GIAC Secure Software Programmer certification, we are confident this certification will not only strengthen Siemens' customer offerings but also strengthen the software development industry as a whole," said John Fichtner, head of Siemens Computer Emergency Response Team. "We look forward to continuing to work closely with SANS to enhance and grow the certification."

Major consulting and outsourcing organizations around the world are participating in the initiative to help their customers gain confidence that the people writing applications have adequate security knowledge. **Tata**, the Indian consultancy, for example, has more than 60,000 programmers.

> Mr N. Chandrasekaran, Executive Vice President of Tata Consultancy Services, India's largest technology firm, said, "Participating in this initiative will ensure that our stakeholders always experience high quality deliverables in a secure environment as we continue to pioneer the quality standards for the future."

Even the companies that build software code testing tools and web application testing tools support the need for programmer security training and testing. All five of the leaders in secure code testing and web application security have joined SANS to help make this project successful.

> "It is programmers, not the security team, that we have to rely on to get security right. In order to get the most out of security tools like the ones Fortify makes, programmers need security training and assessment of the results. A test like this can make a big difference," said Brian Chess, Vice President and Chief Scientist of **Fortify Software**.

Comments from the other leading vendors of code testing and web application security tools are in attachment 1.

The world's top vulnerability experts from **TippingPoint** are providing invaluable assistance.

> "Many critical vulnerabilities have been caused by the top three programming flaws: user input sanitization, buffer overflows, and missing integer type checks," said Rohit Dhamankar, senior manager of TippingPoint's DVLabs. People who know how to code securely can avoid nearly all these programming errors; the new SANS Institute exams will help ensure they know how to do that."

Universities and community colleges around the world are also partnering with SANS both as testing sites for administering the certification examinations, and as development team members to ensure the exam questions are as good as they can be, and as centers of excellence in secure software education. **Virginia Tech** in Blacksburg, VA, has played a leadership role from the beginning of this effort. Jung Min Park and Randy Marchany described their reasons as follows:

> "High-profile cyber attacks and system exploits by malicious users have become common, recurring events that increasingly threaten the very fabric of today's digital society. Here at

Virginia Tech, we feel that educating today's CS/CE students on the principles and practices of computer and software security is vital, as those students will become the software engineers and programmers of tomorrow. The secure programming skills assessment program spearheaded by SANS is a step in the right direction that will lead to improved training and education of professional programmers and students."

How the Certification and Assessments Exams Will Be Offered

The examinations will be offered through three mechanisms beginning with a Washington, DC pilot test in the summer and a global rollout later in 2007. Each mechanism uses different questions:

1. Any candidate seeking certification may sit for the certification exams at testing sites around the world (generally at colleges or universities) on specific dates three times a year.
2. Secure Programming Enterprise Partners (companies and government agencies with large numbers of programmers, committed to improving the security skills of those programmers) will have access to enterprise versions of the exams they can use any time for employees or candidates or consultants.
3. Any programmer who wants to take a self assessment version of the exams to know where he or she stands may do so, online at any time, and learn about their level of mastery and gaps in their knowledge.

About the SANS Institute

Founded in 1989, the SANS Institute is the worldwide leader in security training and certifications with more than 70,000 alumni in 53 countries. SANS also operates the Internet Storm Center, the Internet's early warning system.

Attachment 1: Supporting commentary from code testing and web application security vendors
Attachment 2: Key people helping to create the blueprints and examinations

Attachment 1: Supporting commentary from the code testing and web application security vendors

Web application security vendors and code testing tool vendors have a special role in the blueprint and exam development process because of the depth and breadth of their expertise in finding errors that lead to vulnerabilities and in knowing the frequency with which specific errors are actually found in live applications. All the application security leaders (SPI Dynamics, Fortify, Ounce, Watchfire, and Cenzic) partnered with SANS in this initiative and provided extraordinary insights into which problems matter most and into the tasks and rules for the test blueprints. They also are supplying great questions.

Ounce Labs:

"The security industry has always relied on SANS as a source of expert opinion, guidance, and training. We are happy that SANS has looked to Ounce Labs, and our expertise, to assist in the development of the GIAC Secure Software Programmer program." said Ryan Berg, Co-Founder and Chief Scientist of Ounce Labs. "This program will help to strengthen the entire software development industry, and as the secure coding market grows, we look forward to working with SANS to expand and further enhance the certification standards."

Watchfire:

"Application security is today's biggest online threat, and organizations struggling with how to integrate security testing into their SDLC need more than security tools-they also require accessible education. As a contributing application security partner in the development stages of the Secure Coding Skills Assessment and GSSP certification, we are confident this training will help strengthen the software development industry and improve security as a whole," said Michael Weider, CTO, Watchfire. "Secure programming skills are essential for building software that can be trusted. We look forward to continued close work with SANS to enhance and further grow this important certification."

SPI Dynamics:

"In this age of Web 2.0, secure software development is critical. SPI Dynamics has been educating the industry and those involved in the development lifecycle for over five years through our Secure Software Forum initiative including free workshops, executive dinners, customer and key partner webcasts and expert articles to bring attention to the need for secure development practices. In addition, SPI Dynamics has maintained a clear focus on delivering solutions to the development community which integrate secure coding and testing solutions," said Michael Sutton, Security Evangelist for SPI Dynamics. "We are delighted to team with the SANS Institute, who is recognized as a leading educational authority on security, to continue our efforts of evangelizing the need for security as a non-disruptive component of development to our over 950 customers and the broader software industry."

Cenzic:

"Educating and certifying programmers as to best practices in application security is a crucial step in the battle to eliminate web application vulnerabilities," said, Mandeep Khera, Vice President of Marketing at Cenzic. "As the leading provider of application security assessment and risk management solutions, Cenzic is committed to working with a prestigious organization like SANS to bring awareness and solutions to the issue of application security."

Attachment 2: Key People Helping To Create the Blueprints and Examinations

- Randy Marchany, Ruiliang Chen, and Professor Jung Min Park of Virginia Tech.
- Professor Matt Bishop of UC Davis and author of “Computer Security: Art and Science”
- Robert Seacord of CERT/CC and author of “Secure Coding in C and C++”
- Ed Tracy of Booz Allen Hamilton
- Steve Christey of MITRE, and editor of the CVE project
- Ryan Berg and Jack Danahy of Ounce Labs
- Professor James Walden of Northern Kentucky University
- Brian Chess and Eric Cabetas of Fortify Software
- Bryan Sullivan and a large team at SPI Dynamics
- Danny Allen and Karl Snider of Watchfire
- Andrew Van der Stock and Jeff Williams of Aspect Security and OWASP
- Craig Richardson
- Johannes Ullrich of SANS Internet Storm Center and SANS Technology Institute
- Christopher Telfer of Concurrent Technologies
- David Hoelzer of the SANS Institute
- Justin Schuh of Neohapsis and co-author of “The Art of Software Security Assessment”
- Peter Francois of Rockwell
- Amish Shah of Net-Square
- Monty MacDougal of Raytheon
- Dario Forte of DF Labs
- Marc Schoenfeld from Germany
- Johan Peeters, Independent, based in Belgium
- Amit Klein from Israel
- And forty-two others