15 มีนาคม 2010

งานประชุม OWASP AppSec Conferences

2 มิถุนายน 2010
Froc 2010
Denver, Colorado

3—4 มิถุนายน 2010
OWASP Day Mexico
Aguascalientes, Mexico

21-24 มิถุนายน 2010
AppSec Research 2010
Stockholm, Norway

7—10 กันยายน 2010
AppSec USA 2010
Irvine, California

16-19 พฤศจิกายน 2010
AppSec Brasil 2010
Campinas, Brasil

สมาชิกกรรมการ OWASP

Jeff Williams
Dinis Cruz
Dave Wichers
Tom Brennan
Sebastien Deleersnyder
Eoin Keary
Matt Tesauro

OWASP
The Open Web Application Security Project

โครงการสำรวจการใช้จ่ายในด้านรักษาความปลอดภัย (OWASP Security Spending Project Survey)
Boaz Gelbord

โครงการ The OWASP Security Spending Benchmarks เป็นการมองหาการจัดทำแนวทาง (guidance) และทำให้อุตสาหกรรมให้การยอมรับเบนช์มาร์คของค่าใช้จ่ายของเว็บแอปปลิเคชั่นในทุกๆด้าน. โครงการ OWASP นี้จัดทำรายงานทั่วไปที่ได้จากผลการสำรวจ.

การสำรวจเป็นการได้จากการรวบรวมจากผู้ตอบแบบสอบถาม โดยผู้ตอบเป็นผู้ไม่เปิดเผยและไม่มีข้อมูลส่วนบุคคลใดๆ ข้อมูลนี้รวมเข้าด้วยกันกับการจัดทำรายงานของเราที่สร้างจากการสำรวจข้อมูลดิบไปที่ชุมชน ดังนั้นเวอร์ชั่นใหม่สุดของ OWASP Security Spending Benchmarks Project ได้เปิดให้ใช้จนถึงวันที่ 15 เมษายน นี้. (Songkran's day of Thailand)

https://www.surveymonkey.com/s/TPYZLXK

รหัสลับ (Password): OWASP_Spending

OWASP AppSec USA, Californina 2010 Call for Papers

การประชุมจะเริ่มขึ้นที่ UC Irvine Conference Center ใน Orange County, CA วันที่ 7—10 กันยายน 2010.

การส่ง (Submissions) ประกอบด้วย:

- ชื่อผู้นำเสนอ (Presenter(s) name(s))
- อีเมล์และ/หรือเบอร์โทรศัพท์ของผู้นำเสนอ (Presenter (s) emails and/or phone number(s))
- ชีวะประวัติของผู้นำเสนอ (Presenter(s) bio(s))
- หัวข้อ (Title)
- บทคัดย่อ (Abstract)
- การสนับสนุนใดๆในการวิจัย/เครื่องมือ (Any supporting research/tools (will not be released outside of CFP committee)

วันสุดท้ายในการส่ง คือวันที่ 6 มิถุนายน เวลา 12 PM PST (GMT-8)

Submit proposals to:
http:www.easychair.org/conferences/?conf=appsec2010

เงินทุนสมาชิกโครงการและสมาชิกทั่วไป (Project and Global Committee Funding)

ตัวแบบของสมาชิกได้มีการขยายไปยังสมาชิกทั่วไปและสมาชิกโครงการ. กลุ่มเหล่านี้สามารถหาผู้สนับสนุนของตัวเองเพื่อสร้างแหล่งเงินทุนของตัวเองไปสนับสนุนสมาชิกโครงการหรือสมาชิกทั่วไป.

มีการทำงานนี้อย่างไร:

โครงการและสมาชิกสามารถหาผู้สนับสนุนของตนเองเพื่อสร้างแหล่งเงินทุนของตัวเองไปที่โครงการหรือสมาชิก. มูลนิธิ OWASP จะจัดการและแบ่งปันเงินทุนในทิศทางเดียวกันกับที่ทำในปัจจุบันด้วยข้อบังคับที่ ว่าให้แบ่ง 40/60 สำหรับสมาชิกประเภทองค์กร.

เงินทุนสามารถนำไปใช้ครอบคลุมค่าใช้จ่ายที่เกี่ยวข้องกับโครงการ, แต่ไม่สามารถนำไปจ่ายให้กับสมาชิก OWASP ได้.

ตัวอย่างการนำเงินทุนไปใช้ได้อย่างไร:

ใช้เป็นค่าใช้จ่ายเดินทางของสมาชิกโครงการผู้ซึ่งเดินทางไปปราศัยเกี่ยวกับโครงการ.

ใช้ในการ print เอกสารของโครงการที่นำไปแบ่งปันในการจัดงาน.

ใช้ในการ print แผ่นซีดี (CDs).

เงินทุนไม่สามารถนำไปใช้คืนสมาชิกโครงการสำหรับเวลาที่ใช้ไปในการทำงานบนโครงการ.

ติดต่อ Kate Hartmann เพื่อรวบรวมเงินทุนจากผู้สนับสนุนหรือถ้าท่านมีคำถามเกี่ยวกับการนำโปรแกรมใหม่นี้ไปใช้ได้อย่างไร.

OWASP Podcasts Series

Hosted by Jim Manico

Ep 60 Jeremiah Grossman and Robert Hansen (Google pays for vulns)

Ep 59 AppSec Roundtable with Boaz Gelbord, Ben Tomhave, Dan Cornell, Jeff Williams, Andrew van der Stock and Jim Manico (Aurora+)

Ep 58 Interview with Ron Gula (Web Server Scanning, IDS/IPS)

คุณกำลังมองหางานสำหรับการประยุกต์ใช้ในด้านการรักษาความมั่นคงปลอดภัย ***(AppSec)?*** *สามารถตรวจสอบได้ที่* ***OWASP Job Page***

ถ้าคุณมีงานทางด้าน ***AppSec*** *ที่ต้องการประกาศสมัครงาน?*

ติดต่อ:

Kate Hartmann

เป็นวันของ OWASP ในอิตาลี
Matteo Meucci

วันที่ 5 และ 6 เดือนพฤศจิกายนปีที่ผ่านมา OWASP ได้จัดงาน OWASP สองเหตุการณ์ใหญ่ในโรมและมิลาน ประเทศอิตาลี.

งานแรก เป็นการทำให้เข้าใจในความร่วมมือกับ CONSIP, เป็นบริษัทของ The Italian Ministry of Economy and Finance (MEF), ทำงานร่วมกับ the Italian Public Administrations. ในงานนี้เรียกว่า "The Application Security as trigger for the Italian E-Government." ผู้เข้าร่วมงานได้มาจาก CISOs ของ the Italian Ministries และ Public Administrations ทั้งหมด. บทความที่นำเสนอท่านสามารถหาได้ที่นี่:

http://www.owasp.org/index.php/Italy_OWASP_Day_E-gov_09

OWASP—Italy Day IV ในมิลาน– วันที่สองในมิลานด้วยผู้เข้าร่วมประชุมมากว่าร้อยคน เราได้ใส่บทความ ภาพนิ่งและวีดีโอออนไลน์ที่นี่ here.

OWASP—Italy Day at Security Summit 2010

18 มีนาคม OWASP– อิตาลีจะเสนอ "OWASP Guidelines and tools for Web Applications Security" ที่ Security Summit 2010 ในมิลาน ประเทศอิตาลี. https://www.securitysummit.it/eventi/view/73

อธิบายการโจมตีแบบ Man In The Middle Attack จากบล๊อคของ Michael Coates วันที่ 3/3/2010

"นั่นเป็นช่องโหว่ในการโจมตีแบบ man in the middle attack!ได้"

ท่านอาจจะได้ยินคำนี้มาก่อน แต่ขออนุญาติอธิบายรายละเอียดในเชิงลึกของการโจมตีชนิดนี้ และทำความเข้าใจอย่างแท้จริงว่ามันทำงานกันอย่างไร.

นิยาม

อันดับแรกเป็นการนิยามแบบย่อๆ การโจมตีแบบ man in the middle (MitM) เป็นการโจมตีโดยการแอบเข้าไปเฝ้าดูการติดต่อสื่อสารที่มีแลกเปลี่ยนระหว่างสองบุคคลและเป็นไปได้ที่ถูกแก้ไขโดยมือที่สาม โดยผู้ไม่ได้รับอนุญาติ หรือกลุ่มใดๆ ข้อมูลเพิ่มเติม ส่วนของมือที่สามจะกระทำการโจมตีในขณะนั้น (real time) (เช่น ขโมย logs หรือ ดูข้อมูลจราจรคอมพิวเตอร์ที่ได้มาก่อนหน้านั้นที่เวลาต่อมา เราถือว่าไม่ได้เป็น MitM).

เพราะว่า MitM สามารถถูกกระทำต้านกับโปรโตคอลหรือการติดต่อสื่อสารใดๆ , เราจะกล่าวถึงสิ่งนี้ในความสัมพันธ์ไปที่ข้อมูลจราจรของ HTTP เพียงเล็กน้อยเท่านั้น.

ความต้องการสำหรับการโจมตี

MitM สามารถกระทำได้ในสองวิธีการที่แตกต่างกัน:

1. ผู้โจมตีไปอยู่ภายในการควบคุมของ router ท่ามกลางตำแหน่งปกติของจราจรในการติดต่อสื่อสารระหว่างเหยื่อกับ server ที่เหยื่อติดต่อด้วย.

2.a. ผู้โจมตีถูกวางบนตำแหน่งที่เดียวกันของ broadcast domain (e.g. subnet) เช่นเดียวกับของเหยื่อ.

2.b. ผู้โจมตีถูกวางไว้บนตำแหน่งเดียวกันของ broadcast domain (e.g. subnet) ที่เดียวกันกับอุปกรณ์กำหนดเส้นทางที่ถูกใช้โดยเหยื่อที่ไปกำหนดเส้นทางจราจร.

การโจมตี

สามารถอ่านบทความที่สมบูรณ์ได้ที่ Michael Coates blog

ปล่อยออกมาแล้ว —OWASP ESAPI ver. 1.4.4 สำหรับ JAVA ver. 1.4 และสูงกว่านั้น
Jim Manico

การเปลี่ยนแปลง (Changelog):

http://owasp-esapi-java.googlecode.com/svn/branches/1.4/changelog.txt

สำหรับ links ที่สำคัญอื่นๆ:

ให้ ดาวน์โหลดชุดสมบูรณ์ที่ปล่อยออกมาที่เป็น .zip ได้ที่: http://owasp-esapi-java.googlecode.com/files/ESAPI-1.4.4.zip

ESAPI 1.4.4 Javadoc สามารถพบได้ที่นี่: http://owasp-esapi-java.googlecode.com/svn/trunk_doc/1.4.4/index.html

คำถามในการใช้และการกำหนดค่าต่างๆของ ESAPI? ไปเยี่ยมได้ที่ลิงค์นี้ : https://lists.owasp.org/mailman/listinfo/esapi-user และสามารถเข้าร่วมกลุ่มการส่งข้อความทางเมลล์.

สนใจในการสนับสนุน? เข้าร่วมกลุ่มการส่งข้อความทางเมลล์ที่: https://lists.owasp.org/mailman/listinfo/esapi-dev

OWASP Common Numbering Project
Mike Boberski

เป็นการพัฒนาที่น่าตื่นเต้นมาก , สคีมาตัวเลขใหม่จะเป็นสิ่งธรรมดาในการไขว้กันของ OWASP Guides และ OWASP References ที่ได้มีการพัฒนา ตัวเลขเป็นความพยายามของทีม นำทีมโดย Mike Boberski (ASVS project lead and co-author). โครงการ OWASP Top Ten, Guide, and Reference เป็นการนำและสนับสนุนเช่นเดียวกับระดับผู้นำ OWASP ทำงานเข้าด้วยกันเพื่อพัฒนาตัวเลขที่จะให้ง่ายต่อการแม๊ประหว่าง OWASP Guides กับ References, และจะยินยอมให้เกิดช่วงการส่งผ่านเช่นเดียวกับ Guides และ References ที่ได้ถูกปรับปรุงเพื่อสะท้อนสคีมาตัวเลขใหม่นี้. โครงการนี้ จะติดตามตัวเลขเก่าและเตรียมการสำหรับข้อมูลแม๊ปปิ้งที่ศูนย์กลางเฉพาะกิจ. ท่านสามารถไปที่หน้าโครงการเพื่อศึกษาข้อมูลเพิ่มเติมได้ที่:

http://www.owasp.org/index.php/Common_OWASP_Numbering

OWASP ASVS
Mike Boberski

มีการแปลเสร็จสมบูรณ์เป็นอันดับแรกคือ ภาษาญี่ปุ่น, และ ภาคผนวกของการแนะแนวความคิด ASVS ที่เป็นภาษาญี่ปุ่นกำลังอยู่ในช่วงการพัฒนา. การแปลเป็นภาษาฝรั่งเศส เยอรมัน จีน ฮังการี และภาษามาเลย์ อยู่ในต่อไป. โครงการกำลังมองหาอาสาสมัครในการแปล, ติดต่อ : mike.boberski@owasp.org ถ้าท่านสนใจ.

OWASP Development Guide
Mike Boberski

เป็นการทำงานในช่วงมีการเริ่มทำซ้ำของการแนะแนว (Guide). เวอร์ชั่นถัดไปของการแนะแนวการพัฒนา OWASP (the OWASP Development Guide) จะอยู่ในผลกระทบของการแนะนำรายละเอียดการออกแบบ สำหรับความต้องการของ OWASP ASVS. ทีมของอาสาสมัครมีทั้งหมด 26 คน และมีสัญญาณที่ดีขึ้นในตัวเลขนี้ โครงการนี้ยังคงมองหาอาสาสมัคร.

OWASP Development Guide Project Page

OWASP ESAPI for PHP
Mike Boberski

ยังคงมีการทำงานอย่างต่อเนื่องบนพอร์ต PHP (PHP port) ของ ESAPI. Class ที่เป็นแกนทั้งหมดได้เสร็จสมบูรณ์ หรือไม่ก็อยู่ในช่วงสุดท้ายของการริเริ่มการพัฒนา, รวมทั้งการกำหนดค่าของการรักษาความปลอดภัย (Security Configuration), Validator, Encoder, and Logger. ฐานของกลุ่มผู้ใช้ที่เริ่มนำไปปรับการใช้เพิ่งเกิดขึ้น ต้องการข้อมูลเพิ่มเติม กรุณาไปที่หน้าโครงการ (project page).

สองโครงการใหม่

Paulo Coimbra

OWASP Broken Web Application Project

http://www.owasp.org/intex.php/OWASP_Broken_Web_Applicaitons_Project#tab=project_Details

โครงการนี้ถูกสนับสนุนโดย :

Mandiant.

OWASP Ecosystem Project

เรามุ่งหวังเป็นหุ้นส่วนกันระหว่างเทคโนโลยีแพลตฟอร์มของบริษัทผู้ผลิตกับความก้าวหน้าของ ecosystem มีการเน้นไปที่การรักษาความปลอดภัยของเทคโนโลยีเหล่านั้น The ecosystem จะประกอบด้วยนักวิจัย (ทั้งผู้สร้างและผู้ breakers), เครื่องมือ, ไลบรารี่, แนวทางการแนะแนว, การให้ความตระหนักกับวัสดุ, มาตรฐาน, การศึกษา, การประชุม, ฟอรัม, การส่งข่าว, การประกาศข่าว, และอื่นๆอีกมาก.

http://www.owasp.org/index.php/Security_Ecosystem_Project

***134,000** คนที่ใช้เวลา 1.5 ล้านนาทีที่เว็บไซต์ **OWASP** เดือนกุมภาพันธ์!*

*เงินบริจาคประเทศไฮติ **(Haiti):***

*ยอดเงินบริจาครวม : **$1378.67***

*ส่งไปที่ : **Doctors Without Borders.***

ยอดเงินทั้งหมดไปช่วยและบรรเทาชาวไฮติโดยตรง.

*ขอขอบคุณไปยังสมาชิกประเภทองค์กรของเราผู้ซึ่งให้การสนับสนุนในการต่อสมาชิกต่อมูลนิธิ **OWASP** ในเดือนมกราคม และกุมภาพันธ์.*

มูลนิธิ OWASP

9175 Guilford Road
Suite #300
Columbia, MD 21046

โทรศัพท์: 301-275-9403

โทรสาร: 301-604-8033

อีเมลล์:

Kate.Hartman@owasp.org

เป็นชุมชนการประยุกต์ใช้ด้านการรักษาความปลอดภัยที่ฟรีและเปิดเผย (open)

The Open Web Application Security Project (OWASP) เป็นชุมชนแบบเปิดที่มุ่งเน้นในการทำให้องค์กรได้เข้าใจ ได้พัฒนา ได้รับ ได้ปฏิบัติ และได้บำรุงรักษา ในด้านการประยุกต์ใช้ที่น่าเชื่อถือได้. เครื่องมือ เอกสาร ฟอรัม และบทความต่างๆทั้งหมดของ OWASP ไม่ต้องเสียค่าใช้จ่ายและเปิดให้บุคคลใดๆที่สนใจในการประยุกต์ใช้ในด้านรักษาความปลอดภัยให้ดียิ่งขึ้น. เรา (OWASP) ให้การสนับสนุนแนวทางในการนำเสนอการประยุกต์ใช้ในด้านรักษาความปลอดภัยไม่ว่าจะเป็นบุคคล กระบวนการ และปัญหาของเทคโนโลยี เพราะว่าแนวทางการประยุกต์ใช้ในด้านการรักษาความปลอดภัยที่ให้ประสิทธิผลดีที่สุดนั้นเป็นการรวมการทำให้ดีขึ้นกว่าเดิมในทุกบริเวณเหล่านี้ทั้งหมด. ท่านสามารถพบเราได้ที่ www.owasp.org.

OWASP เป็นหน่วยงานที่แตกต่างจากองค์กรโดยทั่วไป เราเป็นอิสระจากความกดดันทางการค้าใดๆ และยินยอมให้เราเตรียมการการประยุกต์ใช้ในด้านความมั่นคงปลอดภัยโดยไม่มีอคติในด้านการปฏิบัติการ ในด้านข้อมูลที่มีผลต่อต้นทุน.

OWASP ไม่ได้เข้าร่วมกับองค์กรเทคโนโลยีใดๆ ถึงแม้ว่าเราสนับสนุนรายงานการใช้เทคโนโลยีการรักษาความปลอดภัยในเชิงการค้าก็ตาม เช่นเดียวกันกับโครงการซอฟต์แวร์โอเพนซอร์ส, OWASP ผลิตวัสดุหลายประเภทมากมายในการให้ความร่วมมือในทิศทางแบบเปิด.

มูลนิธิ OWASP (The OWASP Foundation) เป็นหน่วยงานที่ไม่หวังผลกำไร ซึ่งทำให้มั่นใจได้ว่าความสำเร็จของโครงการยังคงอยู่อีกนาน.

องค์กรที่ให้การสนับสนุน OWASP (OWASP Organizational Sponsors)

Newsletter Editor: Lorna Alamri Translator: Chukiat Sakjirapapong ติชม แนะนำ ได้ที่ chks60@gmail.com