

งานประชุม OWASP
AppSec
Conferences

Froc 2010
Denver, Colorado

OWASP Day Mexico

Aguascalientes, Mexico

AppSec Research
2010

AppSec USA 2010
Irvine, California

AppSec Brasil 2010
Campinas, Brasil

OWASP

Matt Tesauro



OWASP

The Open Web Application Security Project

Boaz Gelbord

Spending Benchmarks Project ได้เปิดให้ใช้งานถึง
วันที่ 15 เมษายน นี้. (Songkran's day of Thailand)

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

การสำรวจเป็นการ ได้จากการรวบรวมจากผู้ตอบแบบสอบถาม โดย ผู้ตอบเป็นผู้ไม่เปิดเผยและไม่มีข้อมูลส่วนบุคคลใดๆ ข้อมูลนี้รวมเข้าด้วยกันกับการจัดที่รายงานของเราที่สร้างจากการสำรวจข้อมูลลับไปทั้งหมด ดังนั้นเวอร์ชันใหม่สุดของ OWASP Security

รหัสลับ (Password): OWASP_Spending

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

การส่ง (Submissions) ประกอบด้วย:

- ชื่อผู้นำเสนอ (Presenter(s) name(s))
- อีเมลและ/หรือเบอร์โทรศัพท์ของผู้นำเสนอ (Presenter(s) emails and/or phone number(s))
- ชีวประวัติของผู้นำเสนอ (Presenter(s) bio(s))

- หัวข้อ (Title)
- บทคัดย่อ (Abstract)
- การสนับสนุนใดๆ ในการวิจัย/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>

ตัวแบบของสมาชิกได้รับการขยายไปยังสมาชิกทั่วไปและสมาชิก
โครงการ. กลุ่มเหล่านี้สามารถหาผู้สนับสนุนของตัวเองเพื่อสร้างแหล่ง
เงินทุนของตัวเองไปสนับสนุนสมาชิกโครงการหรือสมาชิกทั่วไป.

ใช้ในการ **print** เอกสารของโครงการที่นำไปแบ่งปันในการจัดงาน.

ใช้ในการ print แผ่นซีดี (CDs).

โครงการและสมาชิกสามารถหาผู้สนับสนุนของตนเองเพื่อสร้างแหล่ง
เงินทุนของตัวเองไปที่โครงการหรือสมาชิก. มูลนิธิ OWASP จะ
จัดการและแบ่งปันเงินทุนในทิศทางเดียวกันกับที่ทำงานปัจจุบันด้วย
ข้อบังคับที่ 40/60 สำหรับสมาชิกประเภทองค์กร.

เงินทุนไม่สามารถนำไปใช้คืนสมาชิกโครงการสำหรับเวลาที่ใช้ไปในการทำงานบนโครงการ.

ติดต่อ [Kate Hartmann](#) เพื่อรวบรวมเงินทุนจากผู้สนับสนุน
หรือถ้าท่านมีคำถามเกี่ยวกับการนำโปรแกรมใหม่นี้ไปใช้ได้อย่างไร.

เงินทุนสามารถนำไปใช้ครอบคลุมค่าใช้จ่ายที่เกี่ยวข้องกับโครงการ, แต่ไม่สามารถนำไปจ่ายให้กับสมาชิก OWASP ได้.

ตัวอย่างการนำเงินทอนไปใช้ได้อย่างไร:

ใช้เป็นค่าใช้จ่ายเดินทางของสมาชิกโครงการผู้ซึ่งเดินทางไปปราชัย
เกี่ยวกับโครงการ.



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)

คุณกำลังมองหางานสำหรับการประยุกต์ใช้
ในด้านการรักษาความปลอดภัย

(AppSec)? สามารถตรวจสอบ

ได้ที่ [OWASP Job Page](#)

ถ้าคุณมีงานทางด้าน

AppSec ที่ต้องการประกาศ
สมัครงาน?

ติดต่อ:

[Kate Hartmann](#)

OWASP

Matteo Meucci

วันที่ 5 และ 6 เดือนพฤศจิกายนปีที่ผ่านมา OWASP ได้จัดงาน
OWASP สองเหตุการณ์ใหญ่ในโรมและมิลาน ประเทศอิตาลี.

งานแรก เป็นการทำให้เข้าใจความร่วมมือกับ CONSIP, เป็นบริษัท
ของ 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. บทความที่น่าสนใจที่ท่านสามารถหาได้ดังนี้:

<http://www.owasp.org/index.php/>

Man In The Middle Attack

Michael Coates 3/3/2010

"นั่นเป็นช่องโหว่ในการโจมตีแบบ man in the middle
attack!"

ท่านอาจจะได้ยินคำนี้มาก่อน แต่ขออนุญาตอธิบายรายละเอียดในเชิงลึก
ของการโจมตีชนิดนี้ และทำความเข้าใจอย่างแท้จริงว่ามันทำงานกัน
อย่างไร.

นิยาม

อันดับแรกเป็นการนิยามแบบย่อๆ การโจมตีแบบ man in the
middle (MitM) เป็นการโจมตีโดยการแอบเข้าไปเฝ้าดูการ
ติดต่อสื่อสารที่มีแลกเปลี่ยนระหว่างสองบุคคลและเป็นไปได้ที่ถูกแก้ไข
โดยมือที่สาม โดยผู้ไม่ได้รับอนุญาต หรือกลุ่มใดๆ ข้อมูลเพิ่มเติม ส่วน
ของมือที่สามจะกระทำการโจมตีในขณะนั้น (real time) (เช่น
ขโมย logs หรือ ดูข้อมูลจราจรคอมพิวเตอร์ที่ได้มาก่อนหน้านั้นที่
เวลาต่อมาเราถือว่าไม่ได้เป็น MitM).

เพราะว่า MitM สามารถถูกกระทำด้านกับโปรโตคอลหรือการ
ติดต่อสื่อสารใดๆ , เราจะกล่าวถึงสิ่งนี้ในความสัมพันธ์ไปที่ข้อมูล
จราจรของ HTTP เพียงเล็กน้อยเท่านั้น.

OWASP ESAPI ver. 1.4.4 JAVA ver. 1.4
Jim Manico

การเปลี่ยนแปลง (Changelog):

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

สำหรับ links ที่สำคัญอื่นๆ:

ให้ดาวน์โหลดชุดสมบูรณ์ที่ปล่อยออกมาที่เป็น .zip ได้ที่:
<http://owasp-esapi-java.googlecode.com/files/ESAPI-1.4.4.zip>

หน้า 2

[Italy OWASP Day E-gov 09](#)

OWASP—Italy Day IV ในมิลาน— วันที่สองในมิลานด้วยผู้เข้าร่วม
ประชุมมากกว่าร้อยคน เราได้สัปดาห์ความ ภาพนิ่งและวิดีโอออนไลน์ที่ [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>

ความต้องการสำหรับการโจมตี

MitM สามารถกระทำได้ในสองวิธีการที่แตกต่างกัน:

1. ผู้โจมตีไปอยู่ภายในการควบคุมของ router ท่ามกลางตำแหน่ง
ปกติของจราจรในการติดต่อสื่อสารระหว่างเครือข่าย server ที่
เชื่อมต่อด้วย.

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

2.b. ผู้โจมตีถูกวางไว้บนตำแหน่งที่เดียวกันของ broadcast domain (e.g. subnet) ที่เดียวกันกับอุปกรณ์กำหนดเส้นทางที่ถูก
ใช้โดยเครือข่ายที่กำหนดเส้นทางจราจร.

การโจมตี

สามารถอ่านบทความที่สมบูรณ์ได้ที่ [Michael Coates blog](#)

ESAPI 1.4.4 Javadoc สามารถพบได้ที่: <http://owasp-esapi-java.googlecode.com/svn/trunk/doc/1.4.4/index.html>

คำถามในการใช้และการกำหนดค่าต่างๆของ ESAPI? ไปเยี่ยมได้ที่ลิงค์
นี้: <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

เป็นการพัฒนาที่น่าตื่นตาตื่นใจมาก, สถิติตัวเลขใหม่จะเป็นสิ่งธรรมดาในการใช้กันของ 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 ทำงานเข้าด้วยกันเพื่อพัฒนาตัวเลขที่จะให้ช่วยต่อการเปรียบเทียบระหว่าง OWASP Guides กับ References, และจะยินยอมให้เกิดช่วงการส่งผ่านเช่นเดียวกับ Guides และ Ref-

OWASP ASVS

Mike Boberski

มีการแปลเสร็จสมบูรณ์เป็นอันดับแรกคือ ภาษาญี่ปุ่น, และ ภาคผนวกของการแนะนำความคิด ASVS ที่เป็นภาษาญี่ปุ่นกำลังอยู่ในช่วงการพัฒนา. การแปลเป็นภาษาฝรั่งเศส เยอรมัน จีน อังกฤษ และภาษาแม่ อยู่ต่อไป. โครงการกำลังมองหาอาสาสมัครในการแปล,

OWASP Development Guide

Mike Boberski

เป็นการทำงานในช่วงมีการเริ่มทำซ้ำของการแนะนำ (Guide). เวอร์ชันถัดไปของการแนะนำการพัฒนา OWASP (the OWASP Development Guide) จะอยู่ในผลกระทบของการแนะนำรายละเอียดการออกแบบ สำหรับความต้องการของ

OWASP ESAPI for PHP

Mike Boberski

ยังคงมีการทำงานอย่างต่อเนื่องบนพอร์ต PHP (PHP port) ของ ESAPI. Class ที่เป็นแกนทั้งหมดได้เสร็จสมบูรณ์หรือไม่ก็อยู่ในช่วงสุดท้ายของการริเริ่มการพัฒนา, รวมทั้งการกำหนดค่าของการรักษาความปลอดภัย (Security Configuration),

สองโครงการใหม่

Paulo Coimbra

OWASP Broken Web Application Project

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

โครงการนี้ถูกสนับสนุนโดย :

Mandiant.

OWASP Ecosystem Project

เรามุ่งหวังเป็นส่วนกันระหว่างเทคโนโลยีแพลตฟอร์มของ

references ที่ได้ถูกปรับปรุงเพื่อสะท้อนสถิติตัวเลขใหม่นี้. โครงการนี้ จะติดตามตัวเลขเก่าและเตรียมการสำหรับข้อมูลแม้ปีงบประมาณกลางเฉพาะกิจ. ท่านสามารถไปที่หน้าโครงการเพื่อศึกษาข้อมูลเพิ่มเติมได้ที่:

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

ติดต่อ : mike.boberski@owasp.org ถ้าท่านสนใจ.

OWASP ASVS. ทีมของอาสาสมัครมีทั้งหมด 26 คน และมีสัญญาณที่ดีขึ้นในตัวเลขนี้ โครงการนี้ยังจมองหาอาสาสมัคร.

[OWASP Development Guide Project Page](#)

Validator, Encoder, and Logger. ฐานของกลุ่มผู้ใช้ที่เริ่มนำไปปรับการใช้เพิ่งเกิดขึ้น ต้องการข้อมูลเพิ่มเติม กรุณาไปที่หน้าโครงการ ([project page](#)).

บริษัทผู้ผลิตกับความก้าวหน้าของ ecosystem มีการเน้นไปที่การรักษาความปลอดภัยของเทคโนโลยีเหล่านั้น The ecosystem จะประกอบด้วยนักวิจัย (ทั้งผู้สร้างและผู้breakers), เครื่องมือ, ไลบรารี, แนวทางการแนะนำ, การให้ความตระหนักกับวัสดุ, มาตรฐาน, การศึกษา, การประชุม, ฟอรัม, การส่งข่าว, การประกาศข่าว, และอื่นๆอีกมาก.

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

หน้า 3

134,000 คนที่ใช้เวลา 1.5

ล้านนาที่เว็บไซต์

OWASP นเดือนกุมภาพันธ์!

เงินบริจาคประเทศไฮติ

(Haiti):

ยอดเงินบริจาครวม :

\$1378.67

ส่งไปที่ : Doctors

Without Borders.

ยอดเงินทั้งหมดไปช่วยและ

บรรเทาชาวไฮติโดยตรง.

ขอขอบคุณไปยังสมาชิกประเภทองค์กร
ของเราผู้ซึ่งให้การสนับสนุนในการต่อ
สมาชิกต่อมูลนิธิ OWASP ใน
เดือนมกราคม และกุมภาพันธ์.

Booz | Allen | Hamilton



INFOVISION

protiviti®
Independent Risk Consulting

มูลนิธิ OWASP

9175 Guilford Road
Suite #300
Columbia, MD 21046

โทรศัพท์: 301-275-9403

โทรสาร: 301-604-8033

อีเมล:

Kate.Hartman@owasp.org

เป็นชุมชนการประยุกต์ใช้ด้านการ

รักษาความปลอดภัยที่ฟรีและเปิดเผย

(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 เพราะว่าแนวทาง การประยุกต์ใช้ในด้านการรักษาความปลอดภัยที่ให้ประสิทธิผลดีที่สุดนั้นเป็นการรวมการทำให้ดีขึ้นกว่าเดิมในทุกบริเวณเหล่านั้นทั้งหมด. ท่านสามารถพบเราได้ที่ www.owasp.org.

OWASP เป็นหน่วยงานที่แตกต่างจากองค์กรโดยทั่วไป เราเป็นอิสระจากความกดดันทางการค้าใดๆ และยินยอมให้เราเตรียมการการประยุกต์ใช้ในด้านความมั่นคงปลอดภัยโดยไม่มียอด ในด้านการปฏิบัติการ ในด้านข้อมูลที่มีผลต่อต้นทุน.

OWASP ไม่ได้เข้าร่วมกับองค์กรเทคโนโลยีใดๆ ถึงแม้ว่าเราสนับสนุนรายการการใช้เทคโนโลยีการรักษาความปลอดภัยในเชิงการค้าก็ตาม เช่นเดียวกันกับโครงการซอฟต์แวร์โอเพนซอร์ส, OWASP ผลิตภัณฑ์หลายประเภทมากมายในการให้ความร่วมมือในทิศทางแบบเปิด.

มูลนิธิ OWASP (The [OWASP Foundation](http://www.owasp.org)) เป็นหน่วยงานที่ไม่หวังผลกำไร ซึ่งทำให้มั่นใจได้ว่าความสำเร็จของโครงการยังคงอยู่ถาวร.

OWASP (OWASP Organizational Sponsors)

