



สำหรับนำไปใช้ได้ทันที:

เผยแพร่ OWASP TOP 10 สำหรับปี 2010

ท่านจะช่วยให้เราส่งไปถึงนักพัฒนาเว็บทุกคนในโลกนี้ได้หรือไม่?

โคลัมเบีย, เอ็มดี 4/19/2010

ตั้งแต่ปี 2003 นักวิจัยการประยุกต์ด้านความปลอดภัยและผู้เชี่ยวชาญจากทุกมุมโลกที่ Open Web Application Security Project (OWASP) มีความระมัดระวังการจับตามองสถานะของความปลอดภัยการประยุกต์ใช้บนเว็บและผลิตภัณฑ์เอกสารในการให้ความตระหนักเพื่อเป็นความรู้และความน่าเชื่อถือโดยองค์กรที่เป็นที่รู้จักกันทั่วโลก ประกอบด้วย PCI, DOD, FTC และอื่นๆที่ไม่ได้กล่าวถึง

ปัจจุบัน OWASP ได้มีการเสนอรายงานการปรับปรุงการติดตามความเสี่ยงสูงสุด 10 ประการที่สัมพันธ์กับการประยุกต์ใช้บนเว็บในระดับองค์กร รายงาน 22 หน้าสี่สหายงานนี้ถูกรวบรวมด้วยตัวอย่างและรายละเอียดที่อธิบายความเสี่ยงเหล่านี้ไปที่นักพัฒนาซอฟต์แวร์ ผู้จัดการ และใครก็ได้ที่สนใจในอนาคตของความปลอดภัยเว็บ ทุกๆสิ่งที่ OWASP ฟรีและเปิดให้กับทุกคน และท่านสามารถดาวน์โหลดรายงานสูงสุด 10 ประการของ OWASP (OWASP Top 10) ล่าสุดสำหรับฟรีที่:

http://www.owasp.org/index.php/Top_10

เดฟ วิทเซอร์ (Dave Wichers) สมาชิกกรรมการ OWASP และ ผู้อำนวยการฝ่ายปฏิบัติงานของบริษัท Aspect Security มีการจัดการโครงการตั้งแต่เริ่มต้น “ปีนี้เรามีการปรับปรุง Top 10 ใหม่ไปสร้างให้ความกระฉ่างเพื่อที่เราสามารถกล่าวเรื่องความเสี่ยง ไม่ใช่เฉพาะช่องโหว่ ความพยายามในการจัดลำดับช่องโหว่โดยปราศจากบริบทเป็นการกระทำที่ไม่มีเหตุผล ท่านไม่สามารถตัดสินใจทางธุรกิจที่เหมาะสมได้โดยปราศจากความเข้าใจในภัยคุกคามและผลกระทบทางธุรกิจ “ การเน้นไปที่ความเสี่ยงใหม่เป็นการมุ่งในการนำองค์กรไปทำความเข้าใจและการจัดการความปลอดภัยการประยุกต์ใช้งานที่แน่นอนมากขึ้นขององค์กรเหล่านั้น

เวลาได้มาถึงแล้วในการสร้างความตระหนักความปลอดภัยของการประยุกต์ใช้งาน โดยหลุดพ้นจากชุมชนความปลอดภัยและตรงไปที่ประชาชน ผู้ซึ่งจำเป็นต้องรู้มากที่สุด ในปีนี้ เป้าหมายที่เราสนใจเป็นการนำ **OWASP Top 10** ไปสู่มือของนักพัฒนาเว็บทุกคนบนโลกนี้ - แต่เราต้องการความช่วยเหลือจากท่าน ถ้าใครก็ได้ที่อ่านบทความนี้ ว่า ท่านยินดีที่จะเป็นหนึ่งในตัวอย่างบางสิ่งของการเข้าไปช่วยป้องกันอินเทอร์เน็ตในอนาคตหรือไม่ ถ้าท่านรู้บุคคลผู้ซึ่งเขียนโปรแกรมสำหรับเว็บ ท่านสามารถฟอร์เวิร์ดบทความ OWASP Top 10 และถามพวกเขาอย่างสุภาพได้หรือไม่

.....

ท่านคุ้นเคยกับความเสี่ยงทั้งหมดใน OWASP Top 10?

ท่านจะสร้างคำยินยอมวันนี้ไปป้องกันโปรแกรมของท่านเพื่อต้านกับ OWASP Top 10?

สำหรับเวลาที่ยาวนาน มืองค์กรมมากมายมีการยอมรับในการสำรวจหรือทดสอบการเจาะระบบในการประกันการประยุกต์ใช้งานบนเว็บทั้งภายในและภายนอก วิธีการนี้มีค่าใช้จ่ายมากขึ้นไปและไม่ได้เตรียมการมากพอในทิศทางของความครอบคลุม เหมือนกับความปลอดภัยชนิดอื่นๆ ที่ความปลอดภัยโปรแกรมประยุกต์ต้องการ โปรแกรมการจัดการความเสี่ยงซึ่งจัดเตรียมการไว้กับของ portfolio และการควบคุมกลยุทธ์ในการพัฒนาความปลอดภัยให้ดียิ่งขึ้น ถ้าองค์กรของท่านพร้อมแก้ปัญหาความปลอดภัยโปรแกรมประยุกต์ มีหนังสือฟรีเป็นโหล มีเครื่องมือ มีโครงการ มีฟอร์มส์ มีรายชื่ออีเมลล์ และอื่นๆอีกมากที่ OWASP ท่านสามารถเข้าร่วมเป็นหนึ่งใน 180 กลุ่มทั่วโลกหรือเข้าร่วมการประชุมวิชาการ AppSec ที่ไม่แพงและเป็นที่ยอมรับในด้านคุณภาพที่สูง

The OWASP Top 10 สำหรับ 2010 ได้แก่ :

- A1: Injection**
- A2: Cross-Site Scripting (XSS)**
- A3: Broken Authentication and Session Management**
- A4: Insecure Direct Object References**
- A5: Cross-Site Request Forgery (CSRF)**
- A6: Security Misconfiguration**
- A7: Insecure Cryptographic Storage**
- A8: Failure to Restrict URL Access**
- A9: Insufficient Transport Layer Protection**
- A10: Unvalidated Redirects and Forwards**

การปรับปรุงในปี 2010 อยู่บนพื้นฐานมาจากแหล่งสารสนเทศช่องโหว่ของโปรแกรมประยุกต์บนเว็บที่มีมากกว่ารุ่นก่อนหน้านี้ เมื่อมีการกำหนด Top 10 ใหม่ เป็นการนำเสนอสารสนเทศนี้กระชับมากกว่า มีความสนใจมากกว่า และตรงกลุ่มเป้าหมายมากกว่า และรวมถึงการอ้างอิงที่น่าเชื่อถือไปที่แหล่งเปิดใหม่ๆมากมายซึ่งสามารถช่วยชี้ไปแต่ละประเด็น โดยเฉพาะโครงการใหม่ของ OWASP ได้แก่ [Enterprise Security API \(ESAPI\)](#) และ [Application Security Verification Standard \(ASVS\)](#)

เกี่ยวกับ OWASP

โครงการ OWASP (The Open Web Application Security Project) เป็นชุมชนเปิดและฟรีให้กับทั่วโลกที่เน้นการปรับปรุงความปลอดภัยของโปรแกรมประยุกต์ให้ดียิ่งขึ้น เป้าหมายของเราคือการสร้างความปลอดภัยโปรแกรมประยุกต์ที่จับต้องได้ ดังนั้นบุคลากรและองค์กรสามารถสร้างรูปแบบการตัดสินใจเกี่ยวกับความเสี่ยงด้านความปลอดภัยโปรแกรมประยุกต์ได้อย่างแท้จริง สมาชิกทุกคนฟรีในการเข้าร่วมใน OWASP และ [วัสดุของเราทั้งหมด](#) นำไปใช้ได้ภายใต้ลิขสิทธิ์ซอฟต์แวร์ที่ฟรีและเปิด มูลนิธิ OWASP เป็นองค์กรไม่หวังผลกำไรหมายเลข 501c3 ทำให้มั่นใจได้ว่าความพร้อมในการนำไปใช้งานได้อย่างต่อเนื่องและได้รับการสนับสนุนสำหรับงานของเราจากสมาชิกของเราได้แก่: [ปัจเจกบุคคล](#), [ผู้สนับสนุนจากองค์กร](#) & [ผู้สนับสนุนจากมหาวิทยาลัย](#)

สัมภาษณ์ : เจฟ วิลเลียม – ประธาน OWASP และผู้ก่อตั้งโครงการ Top 10 (jeff.williams@owasp.org)

สัมภาษณ์ : เดฟ วิชเชอร์ – สมาชิกกรรมการ OWASP และหัวหน้าโครงการ Top 10 (dave.wichers@owasp.org)

ติดต่อ : ลอร์นา อลามรี – สมาชิกสำหรับการติดต่อสมาชิก (lorna.alamri@owasp.org)

ชื่อองค์กร : Open Web Application Security Project (OWASP)

ที่อยู่ของเว็บไซต์ : <http://www.owasp.org>

ผู้แปล : ชูเกียรติ สักดิ์จิรพาพงษ์ (Chukiat Sakjirapapong) (chks60@gmail.com)

###