17 يوليو 2010

OWASP
The Open Web Application Security Project

مؤتمرات أمن التطبيقات

70-10سبتمبر ، 2010 ، إرفين ، كاليفورنيا -- الولايات المتحدة الأمريكية التسجيل مفتوح! http://www.appsecusa.org/

16-17سبتمبر ، 2010 ، ايرلندا دبلن

CFP and CFT OPEN – http://www.owasp.org/index.php/OWASP_IRELAND_2010#Call_for_Papers REGISTRATION OPEN - http://www.owasp.org/index.php/OWASP_IRELAND_2010#Registration

20-21أكتوبر ، 2010 ، روتشستر ، نيويورك -- الولايات المتحدة الأمريكية. CFP OPEN - http://www.rochestersecurity.org/call-for-presentations

20أكتوبر 2010 ، Nurnbeg، ألمانيا

CPF OPEN - http://www.owasp.org/index.php/OWASP_AppSec_Germany_2010_Conference#tab=Call_for_Papers_-_English_Version

20-23أكتوبر ، 2010 ، بكين ، الصين CFP/CFT OPEN - http://www.owasp.org/index.php/

29أكتوبر 2010 ، أوستن ، تكساس -- الولايات المتحدة الأمريكية.

CFP OPEN - http://www.owasp.org/index.php/Lonestar_Application_Security_Conference_2010#tab=Call_for_Papers

08-11نوفمبر ، 2010 ، واشنطن العاصمة -- الولايات المتحدة الأمريكية

CFP/CFT OPEN - http://www.owasp.org/index.php/OWASP_AppSec_DC_2010#tab=CFP

Registration OPEN - http://www.owasp.org/index.php/OWASP_AppSec_DC_2010#tab=Registration

11-12نوفمبر ، 2010 ، لشبونة ، البرتغال

CFP OPEN - http://www.owasp.org/index.php/IBWAS10#tab=Call_for_Papers

16-19نوفمبر ، 2010 ، كامبيناس ، SP ، والبرازيل

CFP and CFT OPEN - http://www.owasp.org/index.php/AppSec_Brasil_2010#tab=Calls

مقابلة مع مات تيزارو و لورنا ألامري:

إن واحدة من أكثر الأمور استثنائية حول OWASP هو أنها تسمح للأشخاص المتحمسين بأن يدخلوا ساحة أمن التطبيقات .

إن مات تيزارو هو مدير مشروع LiveCD، وإن دخوله في عالم الـ OWASP سمح له بتنمية درجته العلمية و وزيادة قاعدة المعرفة لـ OWASP والتوعية حول أمن التطبيقات .

لماذا قررت أن تصنع أول LiveCD؟

لقد قمت بذلك كجزء من منتدى صيف OWASP 2008 ، وصلني ايميل حول SoC من OWASP و عندما قرأت حول هذا المشروع الذي يدمج بين أمن التطبيقات و Linux، أدركت أن هذا سيكون عملي لأن هذين الشيئين هما المفضلين لدي .

ما كان هدفك الأساسي من LiveCD؟ و هل تغير ؟ و كيف تم ذلك ؟

كان الهدف الأساسي من LiveCD هو الحصول على عمل واحد قبل الموعد النهائي لـ SoC.

في الواقع ، كنت أحاول جمع أفضل أدوات أمن التطبيقات معا في حزمة واحدة سهلة الاستخدام ، ولقد احتفظت بالأدوات التي تركز على أمن التطبيقات بدلاً من إنشاء قرص أدوات " قرصنة " عام .

بالتأكيد لقد تغير LiveCD منذ نسخته الأولى في أيلول / سبتمبر 2008. وكان أول تغيير كبير هو إطلاق العديد من المشاريع الفرعية التي انبثقت من LiveCD . وكان أولها النظم الافتراضية من VMware وVirtualBox . كما أطلقنا مشروعا اخر ، ولكنه كان بطيئاً للغاية ، وهو VMware افتراضية على قرص USB.

الحقيقة هي أنه نما إلى أكثر من LiveCD بكثير بعد ذلك. لهذا السبب ، تمت إعادة تسمية الإصدار الأحدث إلى OWASP WTE أو بيئة اختبار الويب . لقد اخذنا النسخة الأساسية من OWASP Live CD و حولناها من SLAX إلى Ubuntu Linux وأنشأنا حزماً متعددة قابلة للتنصيب بشكل مستقل لجميع الأدوات في WTE.

هذا التحسن الكبير سيسمح بطرق متطورة أسهل للحصول على أدوات الاختبار في أيدي المتخصصين في مجال الأمن. مع أحدث الحزم ، يمكنك أن تأخذ عملية تثبيت أوبونتو القياسية ، تربطها قاعدة معطيات WTE ، وتثبيت جميع أدوات العمل في بضع دقائق.

و كيف تطوّر المشروع؟

كما ذكرت أعلاه ، تحولت من مجرد CD إقلاع لمجموعة من الأساليب المختلفة للحصول على الأدوات التي تريدها. حالما ننتهي من التحويل من SLAX إلى Ubuntu Linux ، سيكون لدينا عدد ضخم من أساليب مختلفة لإيصال الـWTEإلى المستخدمين:

- Live CD
- النظم الافتراضية (VMware, VirtualBox, Parallels..)
- إضافة حزم إلى نسخ Ubuntu موجودة مسبقاً.
- WTEعلى قرص USB
- Wubi طريقة إقلاع مزدوجة لـ Windows و Ubuntuبدون إعادة تجزئة القرص.
- نسخ مخصصة مثل نسخة مجموعة أدوات جافا ، أو نسخة تحتوي على أدوات الهجوم وأهدافه (التطبيقات التي تتم مهاجمتها) ، الخ
- فئات جديدة من الأدوات مثل أدوات التحليل الساكن

لقد كنت محظوظاً أيضا أن يكون العديد من الاشخاص قد ساهموا في المشروع. نيشي كومار صمم رسومات الإصدارات. وقد ساهمت براد كوزي ودرو بيب في ساعات طويلة جدا في المشروع كذلك. انهم ايضا يستحقون الذكر للمساعدة في تقديمها.

يجب أن أعترف أنه منذ انتقلت إلى Trustwave's SpiderLab، صرفت وقتا أكثر للاعتياد على المكان الجديد والرائع للعمل و من ثم استكمال المشروع. لقد استمتعت حقا بكفاءة أصدقاءي في SpiderLabs وقضيت المزيد من الوقت للكلام و العمل من أجل الحصول على حزم Debian للـ WTE. و بلا تردد، استمريت في اكتشاف نفسي من خلال العثور على نظم افتراضية من WTE من أجل الحصول على العمل.

ما هو التطبيق الأكثر شعبية في **LiveCD** ؟ وما هو الأكثر إثارة للجدل؟ ما هو المفضل لديك؟

عبر طريق طويل ، فإن معظم ما تم التعليق عليه أو الاستفسار حوله ، واستخدم على الأرجح تطبيقاً في Live CD كان هو الـ WebGoat . أعتقد أن حقيقة أن WebGoatلم يكن سوى تمهيد سريع ، بعيدا عن كونها مهيأة للانطلاق الفعلي كان بمثابة هدية كبيرة لكثير من الناس إما لتعلم أمن التطبيقات أو أولئك المدرسين في الصف.

لست متأكدا من أن هناك تطبيقاً مثيراً للجدل حقا وأضاف -- وربما Metasploitالتي ليست حصراً أداة أمنية لتطبيقWEB. أيضا ، لقد أصبت بشيْ من الحزن بسبب Maltego CE وهي النسخة التجريبية المغلقة المصدر. إن مبيعات Maltegoهو ما يحفظ وجود سقف فوق رأس الشخص الذي كتبها لذلك لن أعيق ذلك في طريقه .

أما بالنسبة لما أفضله شخصياً-- فأنا أكره أن أفرد واحدة فقط . البعض مما استخدمه في معظم الأحيان هو : WebScarab ويبسكاراب ، Burp Suite جناح التجشؤ ، JBroFuzz، Nikto، و DirBuster .هناك أيضا بعض الأمور المفضلة الجديدة التي ستضاف إلى WTE في الإصدار التالي.

ماذا يمكن أن تفعله بشكل مختلف عندما تعرف ما لا تعرفه الآن ، ؟

OWASP Podcasts Series

Hosted by Jim Manico

Ep 72 Interview with Ivan Ristic (WAF)

Ep 73 Jeremiah Grossman and Robert Hansen

شكرا لأعضائنا الشركات الذين جددوا دعمهم لمنظمة OWASPفي حزيران / يونيو وتموز / يوليو

أنا حقا أحببت سلاكس SLAX لصنع قرص مضغوط لايف Live CD. وكان عظيماً في إيفاء هذا الغرض. ومع ذلك ، ففي اللحظة التي تشعبنا فيها إلى VMs ومحاولة تحديث القرص المضغوط لايف ديناميكياً ، لم تكن ملامسةً للحقيقة بشكل مجرد.

لذا ، فإن كنت فاعلاً شيئاً ما أكثر ، فيهمني أن أبدأ مع نسخة من لينكس مع نظام إدارة حزمة سليم. لقد عمل Debian لسنوات على التخلص من المعوقات التي تعرقل إدارة الحزم فلماذا لا نقفز فوق أكتاف هؤلاء العمالقة؟ و هكذا RPM هي أيضاً نظم إدارة حزم جيدة . إذا كنتم من معالجي الـ RPM ، فأحب أن أعمل معكم للحصول على RPMs مبنيّة من حزم deb. من أجل الـ WTE .

ماذا كان التحدي الأكبر الخاص بك لبدء تشغيل المشروع الـ **LiveCD** ؟

وكان أحد التحديات الأولية بالنسبة لي هو المحافظة على نطاق معقول. لقد بدأت أبحث في مختلف أدوات أمن التطبيقات وخرجت بقائمة تضم أكثر من 330 أداة. إن الحصول على هذا الاقتران وبهذا العدد المعقول قد استغرق بعض الوقت. وإن تعلم كيفية إنشاء حزم على النحو الصحيح أيضاً هو صعبَ في البداية ، ولكن بمجرد الحصول عليها ، يمكنك أتمتة تحديث الحزم عند إنشاء إصدارات جديدة من الأدوات بحيث يكون هناك مردود على المدى الطويل.

لماذا تشعر بأن الـ **Live CD** كانت ناجحة؟

وبلغ مجموع آخر مرة احصيت فيها التنزيلات downloads ، و الذي كان في تشرين الثاني / نوفمبر من عام 2009 ، ما يزيد قليلا عن 330،000 من التنزيلات منذ أول إصدار SoC . وهذا عدد هائل من الناس الذين قد عرفوا OWASP وأمن التطبيقات. استمعت أيضاً لعدد من المدربين الذين قد استخدموه في الدورات التدريبية. وكان أحد التطورات الأكثر إثارة للدهشة إدراج القرص المضغوط لايف OWASP في كتاب الكلية التدريسي. في الواقع قبل بضعة أسابيع في AppSec الاتحاد الأوروبي عام 2010 في ستوكهولم ، قام أحد الحضور بالامتنان لي و شكري على إطلاق الإصدار الأخير من WTE فكيف لي أن أشكو أو أتذمر؟

كيف أثرمشروع **LiveCD** على حياتك المهنية؟

أولا ، إن مجرد كونها نشطةً ومشاركةً في وقد OWASP لهو أمرَ هائل. بالنسبة لي ، كان OWASP Live CD وسيلة رائعة للوصول الى والمشاركة مع جمهور الـ OWASP. لأنه وبسبب الـ Live CD و حديثي عن المشروع ، قد ذهبت إلى البرتغال وبولندا والبرازيل وأماكن متعددة داخل الولايات المتحدة. لقد قابلت آلافاً من جمهور الـ OWASP الرائعين حقاً، ووضعت اسمي في مجتمع أمن التطبيقات .

وأعتقد أيضاً أن عملي على القرص المضغوط لايف ومع لجنة المشاريع العالمية ساعدتني لأصبح من أعضاء مجلس مؤسسة الـ OWASP. و إن مساعدتي لأعضاء مجلس الـ OWASP الآخرين في العمل على إتمام مهمة الـ OWASP كانت تجربة رائعة.

على الصعيد العملي ، لقد تم دفعي إلى التدريب عدة مرات بسبب الـ Live CD . ناهيك عن أن وجودي في مشاركة نشطة مع OWASP وكوني من مجلس OWASP هي خلاصة مادّية مفيدة جدا . وأنا على يقين بأن تجربة الـ OWASP بالنسبة لي كانت عاملاً كبيراً في موقعي الحالي مع Trustwave's SpiderLabs .

ما هي الخطوة التالية؟

من أجل الـ WTE ، أود أن ينمو عدد المشتركين بحيث لا أقع في عنق الزجاجة كما وقعت فيه في وقت سابق من هذا العام. أود أيضا أن أوسع الحزم التي هي جزء من الـ WTE حتى تتضمن على أدوات التحليل الساكن ، أدوات الفلاش ، وربما بعض التطبيقات القابلة للاختراق أيضاً.

أما بالنسبة لدوري مع مجلس OWASP، فأنا أعمل بنشاط على البنية التحتية التي تدير العمليات في OWASP .ونأمل بأن يكون في الـ OWASP ما هو جديد ، وبنية تحتية على مستوى المؤسسات للمساعدة في نقل المجتمع إلى مستوى جديد كليا من النجاح.

هل هناك أي شيء آخر كنت ترغب أن تشارك فيه مع المشجعين للمشروع؟

لا استطيع ان اقول ما يكفي لأولئك بأن إيجاد الترخيص من السهل العثور عليه و واحد من التراخيص المفتوحة المصدر الشائعة مثل GPL ، Apache أو BSD . في محاولة لمعرفة ما اذا كان يمكنني تضمين الأدوات بأمان على الـ WTE تبين بأن هناك من الصعوبة أكثر بكثير مما كنت أتوقع. ليس لديك فكرة عن الكم الكبير من المشاريع الت قمت بها من تنزيل download وبحث قبل أن أتمكن من معرفة الرخصة.

إن الشيء الوحيد للمشاركة مع المشجعين للمشروع هو الرجاء بإرسال الملاحظات والاقتراحات والشكاوى أو ما إلى ذلك إلى قائمة البريد أو في منتديات المشروع. إن أفضل طريقة للمشروع ليتحسن هو أن نعرف ، نحن العاملين في المشروع ما هو العمل الناجح وما هو العمل الغير ناجح .

ESAPI Update
Jeff Williams

وقد عرضت NSA إجراء مراجعة عميقة للإجراءات الأمنية لـ ESAPI والاستفادة من النتائج . وبالنسبة لأولئك الذين ليس لديهم الكثير من الخبرة مع NSA ، فإن الدفاع هو الجزء الرئيسي من مهمتهم. في الماضي ، أعربوا عن تأييدهم للمؤتمر الوطني للأمن الحاسوبي ، أنشئوا سلسلة قوس قزح ، ورعوا مشاريع الأعمال الصغيرة ،SSE-CMM. وفي الآونة الأخيرة شاركوا في SCAP و SE-Linux .

إن فريق NSA الداعم لـ OWASP ذو خبرة طويلة في مجال التشفير واستعراضات التطبيقات المحددة مسبقاً ، وسيبدأ عمله في وقت قريب جدا. سيقومون بالتركيز على إصدار جافا ESAPIأولاً ، ويمكنهم دعم إصدارات لغة أخرى عندما يكونون على استعداد لذلك -- ما يعني أن التشفير لديهم يرتقي على الأقل حتى مستوى جافا 0و2. و إن تقديرهم الأولي هو أن هذا الاستعراض سوف يستغرق عدة أشهر ليكتمل .

انا متحمس للغاية ازاء هذا التطور ، وسوف أستمر بإخباركم حول تقدمهم.

OWASPأخبار مشاريع
Paulo Coimbra, OWASPمدير مشروع

مشاريع جديدة

http://www.owasp.org/index.php/Projects/ESAPI_Swingset-

http://www.owasp.org/index.php/Projects/Owasp_Esapi_Ruby

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

المشروع مع الإصدارات الجديدة التي أطلقت مؤخرا

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

المشروع الذي يتطلب مساهمين لإطلاق إصدار جديد

http://www.owasp.org/index.php/Category:OWASP_Testing_Project#tab=Project_About (Testing Guide V 4.0)

المشروع الذي تم إعادة إطلاقه

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

مشروع OWASP ESAPI Swingset له قائد جديد

Cathal Courtney. Please welcome him!

http://www.owasp.org/index.php/ESAPI_Swingset#tab=Project_About

This project has already produced a release, the ESAPI Swingset RC 4, which has been made available right now – please glance at it.

http://www.owasp.org/index.php/Projects/ESAPI_Swingset/Rzeleases/Current

Follow OWASP

OWASP has a Twitter feed

http://twitter.com/statuses/user_timeline/16048357.rss

Can you help OWASP make *every* application developer knowledgeable about the OWASP Top 10? Share this link: OWASP_Top_10_-_2010.pdf

موقع OWASP
Google Analytics

Site visits for May: 233,765
Pageviews: 573,144
Pages/Visit: 2.45
Average Time on Site: 00:02:57
58.3% New Visits
http://conf.oss.my
Content overview:
/index.php/Main_Page 63,070 page views
/index.php/
Category:OWASP_Top_Ten_Project 21,610 page views
/index.php/
Category:OWASP_WebScarab_Project
16,615 page views
/index.php/Category:
OWASP_WebGoat_Project
13,502 page views
/index.php/Category:OWASP_Project
10,915 page views
Top Keywords:
Owasp, webscarb, owasp top 10, webgoat, sql injection.

OWASP O2 Platform
Dinis Cruz

أنا سعيدة أن أعلن أنني نشرت أخيرا الإصدار الرئيسي الأول لبرنامج OWASP O2 (مع المثبت ، وأشرطة الفيديو + وثائق ، وعدد من الإمكانيات المتميزة و المهمة).

هناك ميزة واجهة المستخدم الرسومية الجديدة التي تشكل فارقا كبيرا في العثور على الأكواد المتاحة والأدوات واجهات برمجة التطبيقات الموجودة داخل O2(إذا جربت الإصدارات السابقة فسوف نقدر هذا حقاً). يمكنك أن ترى واجهة المستخدم الرسومية الجديدة والوصول إلى رابط التحميل في هذه الصفحة : http://www.o2platform.com/wiki/O2_Release/v1.1_Beta

الرجاء تجريبها، وتقديم النصائح و الإرشادات معلومات عن : ماذا أعجبك ، ماذا تعمل ، ما لا يعمل ، ما يمكن أن يتحسن ، الخ... (إذا كنت تريد الإبلاغ عن ثغرات أو أخطاء ، الرجاء استخدام واجهة الوب هذه http://code.google.com/p/o2platform/issues/list)

هناك وظائف و إمكانيات و قدرات كافية في هذا الإصدار من O2، تجعلني أخيرا أملك الثقة لجعل هذا الطلب مباشرة بالنسبة لك ، مع العلم انه أيا كان مجال أمن التطبيقات الذي أنت تعمل به، سيكون هناك سيناريو / إمكانية / أداة من O2 شأنها أن تجعلك أكثر إنتاجية.

بما أن واجهة المستخدم الرسومية الجديدة هي حديثة جدا ، فإن معظم وثائق وأشرطة الفيديو المتوفرة تعمل على واجهة المستخدم الرسومية السابقة. ولكن بما أنّي الآن استطيع بسهولة إنشاء صفحات وثائق مفصلة ويكي و / أو أشرطة الفيديو باستخدام O2، فإن خطتي هي للرد على الأسئلة الخاصة بكم بهذه الطريقة (أي مع شريط فيديو أو صفحة ويكي)

OWASP AppSEc ملخص بحث
John Wilander

عقد مؤتمر OWASP AppSec الأوروبي الضخم في ستوكهولم ، 21-24 يونيو. وإن ثلاثة دول هي -- السويد والنرويج والدنمارك -- جنبا إلى جنب مع جامعة ستوكهولم استضافت الحدث ، واستقبلت 275 من الحضور في الدول الاسكندينافية المشمسة .

تم في اليومين الأول والثاني توفير التدريب في مجال التطوير الآمن للبرامج ، واختبارات الاختراق ، وتحليل البرامج الضارة ، و مراجعة البنى التصميمية للبرامج. وخلال عشاء مشترك مساء الاثنين تعلم الضيوف الأمريكان كيفية أكل الهامبرغر بالشوكة والسكين -- الخاصية السويدية :).

وكانت أيام المؤتمر عبارة عن ثلاثة مسارات متوازية من المحادثات والعروض في كل من مجال الصناعة ومجال الأوساط الأكاديمية. وقد قدمت الأساسات حول مستقبل الأمن الممستعرض وتطوير الـ SDL منذ مطلع التسعينات. وتضمن المعرض 12 شركة راعية من قبل الراعي الماسي مايكروسوفت.
في ليلة الاربعاء تم الترحيب بحاضري المؤتمر جنبا إلى جنب مع الأشخاص المهمين الآخرين في قاعة مدينة ستوكهولم مع حفلٍ للعشاء و ترفيه. و كان الحفل الاجتماعي الرائع برعاية جوجل. وتنافسوا على الشمبانيا خلال العشاء في ثلاث فئات -- الثقافة و geekiness، والفنون. إن التحدي الأخير في بناء الـ OWASP المحفزة ما يستوحى من الأنابيب النظيفة المليئة بالكثير من الإبداع. أم كان من النبيذ؟

وقال إن المنظمين يودون أن يشكروا جميع الذين وقفوا وشاركوا في المؤتمر الأول للبحوث OWASP AppSec.
نراكم في العام القادم في دبلن!

هل تبحث عن فرصة عمل AppSec؟

تحقق من صفحة العمل في OWASP

هل لديك مشروعاً عن AppSec تريد أن ترسله ؟

اتصل بـ :

Kate Hartmann

إن مشروع أمن تطبيقات ذو المصدر المفتوح (OWASP)هو مجتمع مفتوح مخصص لتمكين المنظمات من تطوير وامتلاك وتشغيل وصيانة و من أخذ صورة عن التطبيقات التي يمكن الوثوق بها. إن جميع أدوات الـ OWASP، والوثائق ، والمنتديات ، والفصول هي متاحة ومفتوحة لجميع المهتمين في تحسين أمن التطبيقات. ونحن نؤيد بأن يكون هناك أمن للتطبيقات بالنسبة للأشخاص ،والإجرائيات ، والتكنولوجيا ، لأن مسألة النهج الأكثر فعالية لأمن التطبيقات تشمل على تحسينات في جميع هذه المجالات. ويمكن الاطلاع على ذلك من خلال www.owasp.org.

OWASPهو نوع جديد من المنظمات. وإن تحررنا من الضغوط التجارية يتيح لنا تقديم معلومات عملية فعالة و غير متحيزة من حيث التكلفة حول أمن التطبيقات .

لا ينتمي OWASPإلى أي شركة تكنولوجيا ، على الرغم من أننا على علم بالحاجة لدعم استخدام التكنولوجيا التجارية في الأمن . و بشكلٍ مشابه للبرامج المصدر المفتوح في العديد من المشاريع ،فإن OWASPتنتج أنواع كثيرة من المواد بطريقة تعاونية متاحة .

إن مؤسسة OWASPليست كياناً ربحيّاً و يضمن نجاح المشروع على المدى الطويل.

OWASP مـؤسسة
9175Guilford Road
Suite #300
Columbia, MD 21046

Phone: 301-275-9403
Fax: 301-604-8033
E-mail:
Kate.Hartman@owasp.org

مجتمع أمن التطبيقات
المتاح والمفتوح

OWASP Organizational Sponsors

Newsletter Editor: Lorna Alamri, AppSec Research Stockholm photos: Boris Hemkemeier