GİRİŞ

Zamanımızın büyük bölümünü güvensiz yazılımlara meydan okuyarak geçiririz. Bilişim teknolojilerinde neler yaratabileceğimizin ve yapabileceğimizin limiti ve anahtari artik güvenliktir. Bizler OWASP olarak dünyada güvensiz ve uygunsuz yazılımları düzeltmeye çalışıyoruz ve OWASP Testing Guide puzzlein çok önemli bir parçasıdır.

Güvenlik testleri yapmadan, kesinlikle güvenli bir yazilim gelistirdiğinizi iddaa edemezsiniz. Çok fazla sayıdaki yazlim geliştirici firma / firmalar güvenlik testlerini yapmamaktadir ve güvenlik testleri için bir standart belirlememiştir.

Kendi başınıza güvenlik testi yapmak özellikle yazilimlarin güvenligini test etmek önerilmez, çünkü saldırganın limitsiz sayıda saldırı tekniği olduğunu ve yazilima zarar verebileceğini biliyoruz ve bütün teknikleri test etmek mümkün değil.

NEDEN OWASP?

Bir guide hazırlar ve büyük sorumluluk alır, on yıldır dunyada yüzlerce insane tarafından temsil edilir. Güvenlik hatalarini test etmek için cok fazla seçenek vardır ve bu guide içindekiler uzmanlara hızlı, kesin ve verimli bir şekilde uygulamalari orta ölçekli olarak test etmede liderlik eder.

Bu guidein açık kaynak kodlu olarak herkes tarafından kullanıma açık olmasını anlamak imkansızdır. Güvenlik karanlık bir sanat değildir sadece pratik / alışkanlıktır. Bir çok güvenlik kılavuzu sadece insanları problemler hakkında endişelendirmek ile yetinir, yeterli açıklama yapılmadan, teşhis edilmeden, ve güvenlik sorunlarını çözmeden kullanima sunulur. Bu proje ile birlikde artık güvenlik ile ilgilenenler uzmanlarca hazırlanmış bu kılavuzla problemlerine çözüm bulabilecek (sacmaladim).

*Bu kılavuz developerler ve software denetmenleri tarafından hazirlanmistir. Dünya üzerinde yeteri kadar güvenlik uzmanı bulunmamakta ve sorunlara geniş kapsamlı açıklama yoktur. Uygulama Güvenliğinde ilk sorumluluk ve destek developerlardan gelmelidir. Bu bir supriz olmadı, developerlar eğer ki test etmiyorlarsa güvenli kod yazamazlar.

Bu bilgiyi unutmayin çünkü bu kılavız projesinin kritik noktalarindan birisidir(*). Wiki açıklaması:

OWASP Topluluğu gelişen ve genişliyen bir topluluktur, adim adim hizli sekilde uygulama guvenligi zaafiyetlerini bulur.

ÖZELLEŞTİRMEK VE ÖNCELİKLENDİRMEK

Organizasyon / Kurum / Kuruluşunuza bu kılavuzu kabul ettirin. Bilgileri organizasyon / kurum / kuruluşunuz için teknolojiler, işlemler ve organizasyon / kurum / kuruluş yapısına gore yeniden şekillendirmeniz gerekir. Eğer standart teknolojileri kullanıyorsanız, ilgili teknolojilerin kullanıma ve oluşuma uygun olduğundan emin olunuz.

- Developerlar güvenli yazılım gelistirdiklerinden emin olmak icin bu kılavuzu kullanmalıdır. Bu testler normal kodların ve takım kodların bir prosedürüdür.
- Software denetmenleri bu kılavuzu mevcut bilgilerini gelistirmek ve denetledikleri uygulamalarda uygulamak için kullanabilirler. Uygulamalardaki güvenlik zaaflarını bulmak, değerlendirmek için daha sonra efor sarf edebilirler.
- Güvenlik Uzmanları bu kılavuzu diğer teknikler ile birlikde kombine bir sekilde kullanarak uygulamada herhangi birşeyi gözden kaçırıp kaçırmadıklarına emin olmak adına kullanabilir.

Hatırlamanız gereken en önemli şey bir uygulamayi periyodik olarak kontrol etmektir. Sınırsız sayıda uygulamayı başarısız yapabilecek şeyler olduğunu ve her zaman zamanınızın bunları bulmak için kısıtlı olduğunu unutmayın ve zamanınızı akıllıca kullandığınızdan emin olun. Guvenlik ile ilgili bölüme odaklanmaya çalışın, bu bir saldırgan tarafından keşedilebilir ve bu ciddi prestij kayiplarına ve problemlerin başlangıcına sebep olabilir.

Bu kılavuz en iyi teknikleri görüntülemişdir, burada farklı güvenlik alanlarının cesitli tiplerini bulmanız mümkün. Ama bütün teknikler eşit şekilde önemli değildir.

OTOMATIK DENETİM ARAÇLARININ ROLÜ

Kurum / Kuruluşların sattığı otomatik denetim ve analiz malzemeleri. Asistan olduklari ve güçlendirdikleri sürece önemlidirler ama hatırlamanız gereken sey onların limitleri olduğu bu yüzden ne için işinize yardimci oluyorlarsa onun için iyidirler.

En önemlisi, bu araçlar geneldir yani sizin kodunuza uyarlanmamışlardır ama uygulamalar için yaygın şekilde kullanılırlar. Bunun anlamı bu araçlar sadece genel problemleri bulmanıza yardımcı olur, en tehlikeli guvenlik zaaflari genel olanlar değil genel olmayan / herkes tarafından bilinmeyendir. Şirket mantığı ve genel uygulama tasarımlarında deeply intertwined?

Potansiyel zaafiyetleri bulmaya başladıkları zamandan itibaren bu araçlar baştan çıkarıcı olmuşlardır. Program çalışma zamanından itibaren pek fazla zaman harcamaz, her bir potansiyel zaafı araştırır ve doğrular. Eğer açık bulamamış ve elemişse ciddi hatalar hala mumkundur, zamanınızı otomatik araçlar için harcamak, kendi tekniklerinizi kullanmak bu kılavuzda açıklanmıştır. Bu araçlar kesinlikle doğru zamanlı uygulama güvenlik programlarıdır. Akıllıca kullanıldığında, size her konuda destek olur ve guvenli kod yazmanıza yardım eder.

HAREKETE GEÇMEK İÇİN ÇAĞRI

Eğer bir yazılım geliştiriyorsanız, kesinlikle bu kılavız icinde bilindik guvenlik denetim kılavuzunu bulacaksınız. Eğer bir hata ya da sorun ile karşılaşırsanız lutfen not bırakın ya / ya da kendiniz düzeltin. Siz bu kılavuzu kullanan diğer arkadaşlarımıza yardım etmiş olacaksınız. Lutfen OWASP'in bir uyesi olup olmayacaginizida değerlendirin katılmak için http://www.webguvenligi.org ya da http://www.owasp.org adresini ziyaret edebilirsiniz. Bize katılabilir projelerde yer alabilirsiniz.

Bu kılavuzun yapimina yardım eden herkese teşekkür ederim, sizler tum dünyadaki uygulamaları daha güvenli hale getirmemize yardım ediyorsunuz.

Jeff Williams, OWASP Chair, December 15, 2006

1. FRONTISPIECE

WELCOME TO THE OWASP TESTING GUIDE 2.0

“Açık ve İşbirliğini bilen: OWASP’”

Matteo Meucci

OWASP yazarlara, eleştirmenlere ve editörlerine bu zor işi bugün getirdikleri bu nokaya getirdikleri için çok teşekkür eder.

Eğer yorum yapmak ya da öneride bulunmak isterseniz lütfen Testing Guide mail havuzuna katilin

- http://lists.owasp.org/mailman/listinfo/owasp-testing
- http://lists.owasp.org/mailman/listinfo/owasp-testing

COPYRIGHT AND LICENSE

REVISION HISTORY

Testing Guide çalışmalarına 2003 yılında Dan Cuthber ile başlandı. 2005 yılında Eoin Keary’nin elinden geçerek wikiye transfer edildi. Matteo Meucci OWASP Testing Guide’ın OWASP Testing Guide Autumn of Code projesine öncülük etmesine karar verdi.

- "OWASP Testing Guide", Version 2.0 - December 25, 2006
- "OWASP Web Application Penetration Checklist", Version 1.1 - July 14, 2004
- "The OWASP Testing Guide", Version 1.0 - December 2004

EDITORS

Matteo Meucci: OWASP Testing Guide "Autumn of Code" 2006 Lead.

Eoin Keary: OWASP Testing Guide Lead.

AUTHORS - YAZARLAR

- Vicente Aguilera
- Mauro Bregolin
- Tom Brennan
- Gary Burns
- Luca Carettoni
- Dan Cornell
- Mark Curphey
- Daniel Cuthbert
- Sebastien Deleersnyder
- Stephen DeVries
- Stefano Di Paola
- David Endler
- Giorgio Fedon
- Javier Fernández-Sanguino
- Glyn Geoghegan
- Stan Guzik
- Madhura Halasgikar
- Eoin Keary
- David Litchfield
- Andrea Lombardini
- Ralph M. Los
- Claudio Merloni
- Matteo Meucci
- Marco Morana
- Laura Nunez
- Gunter Ollmann
- Antonio Parata
- Carlo Pelliccioni
- Harinath Pudipeddi
- Alberto Revelli
- Mark Roxberry
- Tom Ryan
- Anush Shetty
- Larry Shields
- Dafydd Studdard
- Andrew van der Stock
- Ariel Waissbein
- Jeff Williams

REVIEWERS – YORUMCULAR / KONTROL EDENLER GOZDEN GECİRENLER

- Vicente Aguilera
- Mauro Bregolin
- Daniel Cuthbert
- Paul Davies
- Stefano Di Paola
- Simona Forti
- Matteo G.P. Flora
- Eoin Keary
- James Kist
- Syed Mohamed A
- Matteo Meucci
- Alberto Revelli
- Mark Roxberry
- Antonio Parata

TRADEMARKS - MARKALAR

- Java, Java Web Server, and JSP are registered trademarks of Sun Microsystems, Inc.
- Merriam-Webster is a trademark of Merriam-Webster, Inc.
- Microsoft is a registered trademark of Microsoft Corporation.
- Octave is a service mark of Carnegie Mellon University.
- VeriSign and Thawte are registered trademarks of VeriSign, Inc.
- Visa is a registered trademark of VISA USA.
- OWASP is a registered trademark of the OWASP Foundation

Bütün diğer kurumlar isimleri altinda kendi kişisel markalarının sahipleri olabilirler.

ABOUT THE OPEN WEB APPLICATION SECURITY PROJECT

OVERVIEW

The Open Web Application Security Project (OWASP) herkesin katılabileceği açık bir topluluktur, çeşitli organizasyonlar düzenler, satın alma işlemleri yapar ve uygulamalarin guvenlilir olup olmadığını kontrol eder. Bütün OWASP araçları, dökümanları, forumları ve bölümleri güvenlik ile ilgilenen herhangi birisi tarafindan kullanima açık ve ücretsizdir. Hepsini ve daha fazlasını öğrenmek için lütfen http://www.OWASP.org adresini ziyaret edin.

OWASP yeni bir oluşumdur. Tarafsiz ve özgür bir topluluk olarak tarafsiz, pratik, mali sonuç hakkinda uygulama / yazılım güvenliği sunar. OWASP herhangi bir teknonoji / bilişim kurumu ile ortak değildir, ticari güvenlik teknolojileri ile ilgili gelişimlerden haberdar eder. Benzer bir çok açık kaynak yazılımlar ile karşılaşabilirsiniz. OWASP çok fazla sayıda material üretir ve işbirliği yapar. OWASP çıkar elde etmeye çalışmaz bu yuzden projelerin başarılı olacağına inanır. Daha fazla bilgi için:

- OWASP ile iletişime gecmek için Contact
- Nasıl katkıda bulunacağınızı ve / veya ekibe dahil olacağınızı öğrenmek için Contributions
- OWASP'in web sitesinde tanıtım / reklam calışması yapmayı düşünürseniz Advertising
- OWASP projeleri ve nasıl yönetildiği hakkında How OWASP Works
- OWASP brand hakkında OWASP brand usage rules

STRUCTURE

OWASP oluşumunun tek amacı para kazanmak değildir bu OWASPin altyapısını gösterir. OWASP oluşumu ekibine serverlarını, bandwidthini, projeleri kolaylaştırmak için sunar ve bölümleri ile tüm dünyada OWASP Uygulama Güvenliği Seminerleri verir ve yönetir.

LICENSING

Bütün materyaller açık kaynak kod lisanslidir, eğer OWASPin bir üyesiyseniz OWASPin ticari lisanslarinida kullanabilir, düzenleyebilir, dağıtabilirsiniz. OWASP'in bütün materyalleri tek bir lisans ile sizin olusumunuzun bir parçasi olabilir.

Lisanslar hakkında daha fazla bilgi almak isterseniz **OWASP Licenses** sayfasını ziyaret edebilirsiniz.

PARTICIPATION AND MEMBERSHIP – KATILIM VE ÜYELİK

İsteyen herkes bizim forumlarımız, projelerimiz, bölümlerimiz ve seminerlerimize katilabilir. OWASP uygulama güvenliği hakkında birşeyler öğrenmek için çok fantastik bir yerdir ve ününüze ün katar.

Eğer OWASP uygulamalarını ve materyallerini kullanılabilir buluyorsanız lutfen ekibin bir parçası olup olmayacağınızı değerlendirin. OWASP'ın elde ettiği tüm gelir direk olarak OWASP projelerini desteklemekde kullanılır.

Üyelik hakkında daha fazla bilgi almak isterseniz **Membership** sayfasını ziyaret edebilirsiniz.

PROJECTS

OWASP çok yönlü uygulama / yazılım güvenliği üzerine geliştirdigi projeler ile herkese yetmektedir. Biz kılavuzlar, kontrol listeleri ve daha fazla materyal ile kurum / kuruluş ve oluşumların daha güvenli uygulama ve yazılım geliştirmesine yardım ediyoruz.

Daha fazla bilgi almak isterseniz **OWASP Project** sayfasini ziyaret edebilirsiniz.

OWASP PRIVACY POLICY

OWASP'in görevi kurum / kuruluşlara ve oluşumlara uygulama / yazılım güvenliği hakkına yardımcı olmaktır, bizden herhangi bir kişisel bilgilerinizi korumamızı talep edebilirsiniz biz tüm kullanıcılarımızın kişisel bilgilerini toplamaktayız.

Genellikle kullanıcılarımızdan siteyi ziyaret etmeleri esnasında herhangi bir kişisel bilgi talep etmemekteyiz. Kullanıcılarımızın ip adreslerini toplamaktayız, *e-posta adreslerinizi degil, bu bilgiler website istatistiklerimize yardımcı olmaktadır.

Kullanıcılarımızdan herhangi bir OWASP ürününü indirdiklerinde isim ve eposta adresi talep etmekteyiz. Bu bilgiler açıklanmaz ve 3. şahıs / kurumlar ile paylaşılmaz. Bu bilgileri toplamaktaki amacımız:

- Düzeltilen hatalar / yeni sürümler hakkında iletişim kurabilmek
- OWASP Materyalleri hakkında öneri / tavsiye ve geribildirim alabilmek

- OWASP ve AppSec seminer / konferansları hakkında sizleri bilgilendirmek ve davet etmek

OWASP kullanıcılarının bir listesini ve kişisel bilgilerinin bulunduğu bir bölüme sahiptir. Sadece gönüllülerin bulundugu bu listede yer almak istemeyen üyeler listeden çıkarılır.

Kurum / Kuruluş ve Oluşumların fax ile göndermis olduğu tüm bilgiler fiziksel olarak güvendedir. Gizlilik ve Kullanım Şartları ile ilgili sormak istedikleriniz varsa ya / ya da konu ile ilgili başka bir sorunuz varsa lutfen bizimle owasp@owasp.org adresini kullanarak iletişim kurun.

2. INTRODUCTION

OWASP Testing Projesi yillardir gelismektedir. Biz kişilere web uygulamalarının ne, neden, ne zaman ve nasil test edildiği konusunda yardım etmek istiyoruz ve sadece basit bir kontrol listesi vermiyoruz. Biz tipki diğerlerinin yaptığı gibi kendi uygulama kontrol kütüphanemizi geliştirmek istiyoruz. Diğerlerinden farkli olarak Uygulama Kontrol Projesini yazıyoruz.

Bu ortak çalışma ve kişisel içeriklerden farkli olarak onlara meydan okumakta, kim tüm içerik ve kütüphaneleri buraya yayınlar, kendi ortam ve kültürünce çalışarak. Bu yazılım / uygulamalardaki ve gömülü (embedded) test mantığına meydan okumakta ve yeni bir tarz katmakda. Birçok endüstri uzmani yazılım ve uygulamalardaki guvenliğe yardımcı olmak için calışmaktadır ve web uygulamalarını OWASP Testing Parts 1. ve 2. bu organizasyon ve yetkililerine en etkili şekilde en kısa sürede yazılım ve uygulamalarını test etme imkanı sunmaktadır aynı zamanda hazırlanmıs olan kılavuz ve checklistlerde bu organizasyon / kurum / oluşumlar tarafından desteklenmekde ve kullanılmaktadır. OWASP yükselen kalitesi ile ve anlayışı değiştirme şansına, deneyimi geliştirme ve orta ölçekli uzmandır. Kısaca “en küçük ortak birim”.

The Economics of Insecure Software

*Güvensiz yazılımların dünya ekonomisine maliyeti ölçülemez. Haziran 2002de, Amerika Ulusal Standartlar Enstütüsü (*US National Institute of Standards (NIST)) Amerika ekonomisinde güvensiz yazılımlar ve yetersiz güvenlik denetimlerinden bahsetmiştir. *. (2002, June 28). Retrieved May 4, 2004, from http://www.nist.gov/public_affairs/releases/n02-10.htm)*

Güvenlik zaaflarında, birçok insan temel uyarıları ya / ya daha derin teknik bilgileri anlayabilir. Ne yazık ki, bir çok insan olayın parasal boyutunu ve bunun şirketlere maliyet / sonuçlarını düşünmez. Biz inaniyoruzki bu söylediklerimiz gerçekleşmeden, CIO’lar bütçe ayırmadıkları sürece, uygulama ve yazılımlar güvenli şekilde gelişemeyecek. Ross Anderson’un sayfasında güvenliğin ekonomik boyutu hakkında daha fazla açıklama bulabilirsiniz.

Bu kılavuz kurum ve kişilerin geliştirecekleri uygulama / yazılımları test ettirmesi gerektigi konusunda yüreklendirecektir. Şirketlere masrafı, güvensiz yazılımın yarattigi etkiyi açıkta gösterecek, kurumları riski yönetmeye yönlendirecektir. Güvensiz yazılımların sonuçları pek acı olmasada web uygulamaları ve yazılımları için milyonlarca kullanıcıyı ilgilendirmekde ve büyük önem taşımaktadır. Artık, müşteriler World Wide Web (Internet)i kullanarak ürün satın almakta bu müşterilerin ihtiyacı olan şey web uygulamalarındaki olası atakları minumuma indirmektir. Asagıda Web uygulamalarını test ederken bilmeniz gereken şeyler yer almakta:

- Ne test edeceğinizi anlama yeteneği.
- Denetim Prensipleri ve İlkeleri
- Denetim teknikleri açıklanmıştır
- OWASP Denetim mekanizması açıklanmıştır

2. bölümde yazılım geliştirme ve denetiminin nasıl yapılacağı hakkında çeşitli teknikler bulacaksiniz. Örnek vermek gerekirse Bölüm 2 spesifik güvenlik zaaflarina yer vermekte SQL Injection vs.

Scope of this Document – Dökümanın Konusu
Bu döküman kurum ve kuluşuşlara web uygulamalarının denetimi için; denetim programları, denetim aşamaları, doğrulamalar ve kendi denetim programlarını yapılandırmaları konusunda yardım etmek amacıyla yazılmıştır. Kuruluşların kendi uygulamalarını geliştirmesi için gerekli elementleri görüntülemesi ve ayrıntılı bir program geliştirmesi için çeşitli

görüntüler sunar. Bu kılavız belkide mevcut pratikler ve geniş anlatımları sektörin en iyi pratik bilgleri ile bir referans ve metodoloji olarak kullanılabilir. Bu kılavız kurum / kuruluş ve oluşumlara kendilerini sektörün ciddi calışanları ile kıyaslama, yazılımları iyileştirme konusunda anlama ve bunun hesap denetimini anlamaları için çok önemlidir. Bu döküman teknik detaylar, nasıl yazılım test edilir ve tipik güvenlik oluşumlarının kütüphanelerini ile aynı değildir. Teknik detaylar ve bir yazılım nasıl test edilir, pen testin bir parçasıdır. Biz Denetim kelimesinden ne anlariz? web uygulamarının gelisimi sirasinda, bir çok şey test edilmeye ihtiyaç duyar. Merriam-Webster Sözlüğü Test/Denetim kelimesini şöyle açıklamıştır:

- Denetle ya da kanıtla
- Denetime uğra
- Denetim için zaman ayir ve boş zamanlarında kontrol et

Bu dökümanın amacı, denetim ve işleyişini karşılaştırmak ve bazı kriterleri yeniden belirlemektir. Güvenlik sektöründe, kişiller sıklıkla mental kriterleri denetler ve hiçbir denetimi belirtmez ya / ya da tanımlamaz. Bu sebepten dolayı diğerleri ve daha bir çok insan güvenliğe denetimine karanlık bir sanat olarak bakar. Bu döküman bu bakış açısını ve görünüşünü değiştirmeyi hedefler, daha kolay bir sekilde derin bilgilerden ayirarak kişilerin bilgi edinmesini kolaylaştırır.

The Software Development Life Cycle Process

Güvenlik hatalarının önüne geçmenin en iyi yolu uygulama ve aplikasyonları the Software Development Life Cycle (SDLC)'ı güvenliğe dahil etmektir. Eğet hala uygulamalarınızda SDLC kullanmiyorsaniz, birtane almanın zamanı geldi! Aşağıdaki şemada SDLC modelini ve hataları düzeltmeye katkısını açık bir şekilde görebilirsiniz.

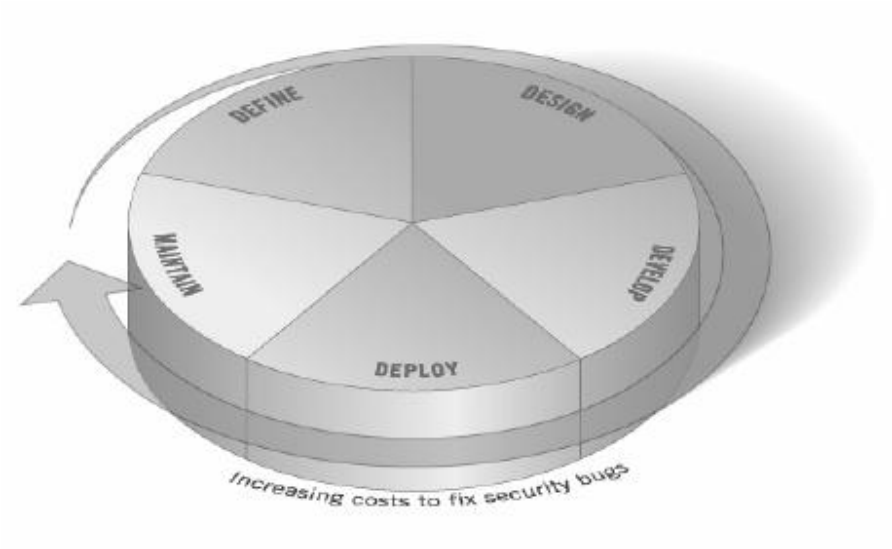

Figure 1: Generic SDLC Model

Kurumlar SDLCyi gözden geçirmeli ve güvenliğin önemli bir parçası olduğuna emin olmalıdır. SDLC'ler uygulamalara dahil edildiğinde controller ve gelişlim sürecinin daha güvenilir ve daha hizli olmasini sağlar.

The Scope of What To Test

Uygulama Geliştirmeyi kişi,işlem ve teknoloji olarak kombine düşünmek işleri biraz daha kolaylaştırabilir. Bütün bu faktörler yaratılması mantıklı olur ve bu faktörler test edilmiltir. Bugün insanlar geliştirdikleri teknolojileri kendi başına test etmektedir, ve bir çok insane uygulamalarını test etmeden yayınlar (örnek: kodlama yapılır ve calışmakta olan bir uygulamaya yüklenir). Genellikle bu çok anlamsız ve gelişimi olumsuz etkliyen bir faktördür. Bir denetim programında bulunan componentler için:

* Yeteri kadar bilgili olduğuna emin olmalı ve kişileri garanti altına almalı

* Gizlilik Politikası ve standartlarını bildiğinden ve kullandığından emin olmalı, ilgili sorumlulukları yerine getirdiğinden emin olmalı, sadece teknik işlemleri gerçekleştirmeli, yönetim ve kullanıma hazır zaafları göstermemelidir.

Denis Verdon, , Head of Information Security at Fidelity National Financial (http://www.fnf.com) NewYork'daki 2004 OWASP AppSec konferansında uygulama güvenligi hakkında guzel bir açıklama yapmıştır. "Arabaları aplikasyonlar ve uygulamar gibi düşünecek olursak, güvenlik testleri çarpışmayı engellemek üzere yapılır. Tekerlekler test edilmez ya / ya da acil durumda ne yapılacağı test edilmez, frenleri test edilmez, çarpışmaya karşı dayanıklılığı test edilmez."

Feedback and Comments – Geri Bildirim ve Yorumlar

OWASP projeleri, geribildirim ve yorumlarınızı dinlemeye hazır ve açıktır. Biz özellikle işimizin etkileyici ve kullanılabilir olduğunun farkındayız.

Dökümanın Aslı : OWASP TESTING GUIDE v2

Çeviri : Taygun Alban – taygun.alban@gmail.com