0. Foreword by Eoin Keary (Önsöz: Eoin Keary)

Güvensiz yazılım sorunu belki de zamanımızın en önemli teknik zorluğudur. İş, sosyal ağ vb. sağlayan web uygulamalarının dramatik yükselişi, yalnızca İnternet, Web Uygulamaları ve Verilerimizi yazmak ve güvence altına almak için sağlam bir yaklaşım oluşturmak için gereksinimleri artırmıştır.

Open Web Uygulama Güvenliği Projesi'nde (OWASSP®), dünyayı güvensiz yazılımın norm değil, anomali olduğu bir yer haline getirmeye çalışıyoruz. OWASP Test Kılavuzu, bu ciddi sorunu çözmede önemli bir role sahiptir. Güvenlik sorunları için yazılımı test etmeye yaklaşımımızın mühendislik ve bilim ilkelerine dayanması hayati önem taşımaktadır. Web uygulamalarını test etmek için tutarlı, tekrarlanabilir ve tanımlanmış bir yaklaşıma ihtiyacımız var. Mühendislik ve teknoloji açısından bazı minimal standartlara sahip olmayan bir dünya kaos içinde bir dünyadır.

Üzerinde güvenlik testi yapmadan güvenli bir uygulama oluşturamayacağınızı söylemeye gerek yok. Test, güvenli bir sistem oluşturmak için daha geniş bir yaklaşımın parçasıdır. Birçok yazılım geliştirme kuruluşu, standart yazılım geliştirme sürecinin bir parçası olarak güvenlik testini içermez. Daha da kötüsü, birçok güvenlik satıcısının farklı kalite ve titizlik dereceleriyle test yapmasıdır.

Güvenlik testi, kendi başına, bir uygulamanın ne kadar güvenli olduğunun özellikle iyi bir ölçütüdür, çünkü bir saldırganın bir uygulama molası verebileceği sonsuz sayıda yol vardır ve hepsini test etmek mümkün değildir. Bir saldırganın böyle bir kısıtlamaya sahip olmadığı yerleri test etmek ve savunmak için sadece sınırlı bir zamanımız olduğu için kendimizi güvende tutamayız.

Code Review Guide, Development Guide ve OWASP ZAP gibi araçlar gibi diğer OWASP projeleriyle birlikte, bu güvenli uygulamaların oluşturulması ve sürdürülmesi için harika bir
başlangıçtır. Bu Test Kılavuzu, çalışan uygulamanızın güvenliğini nasıl doğrulayacağınızı gösterecektir. Bu kılavuzları uygulama güvenliği girişimlerinizin bir parçası olarak kullanmanızı şiddetle tavsiye ederim.

Neden OWASP?

Bunun gibi bir rehber oluşturmak, dünyadaki yüzlerce insanın uzmanlığını gerektiren büyük bir girişimdir. Güvenlik kusurlarını test etmenin birçok farklı yolu vardır ve bu kılavuz, önde gelen uzmanların bu testi hızlı, doğru ve verimli bir şekilde nasıl gerçekleştireceği konusunda fikir birliğini yakalar. OWASP, benzer güvenlikli insanlara birlikte çalışma ve bir güvenlik sorununa önde gelen bir uygulama yaklaşımı oluşturma yeteneği verir.

Bu kılavuzun tamamen özgür ve açık bir şekilde sunulmasının önemi, vakfın misyonu için önemlidir. Herkese ortak güvenlik sorunlarını test etmek için kullanılan teknikleri anlama yeteneği verir. Güvenlik, sadece birkaçının uygulayabileceği bir siyah sanat veya kapalı bir sır olmamalıdır. Güvenlik uygulayıcılarına değil, aynı zamanda QA, Geliştiriciler ve Teknik Yöneticilere de özel olarak açık olmalıdır. Bu kılavuzu oluşturma projesi, bu uzmanlığı ihtiyacı olan insanların - siz, ben ve yazılım oluşturmada yer alan herkesin elinde tutar.

Bu kılavuz, geliştiricilerin ve yazılım testçilerinin eline geçmelidir. Dünyada genel sorunda herhangi bir önemli kesinti yapmak için neredeyse yeterli uygulama güvenliği uzmanı yoktur. Uygulama güvenliği için ilk sorumluluk, kodu yazdıkları için geliştiricilerin omuzlarına düşmelidir. Geliştiricilerin, bunu test etmiyorlarsa veya savunmasızlık getiren böcek türlerini göz önünde bulundurmadıkları takdirde güvenli kod üretmemeleri sürpriz olmamalı.

Bu bilgileri güncel tutmak bu kılavuz projesinin kritik bir yönüdür. Wiki yaklaşımını benimseyerek, OWASP topluluğu hızlı hareket eden uygulama güvenlik tehdidi manzarasına ayak uydurmak için bu kılavuzdaki bilgileri geliştirebilir ve genişletebilir.

Bu Kılavuz, üyelerimizin ve proje gönüllülerinin bu konuda sahip olduğu tutku ve enerjinin büyük bir kanıtıdır. Dünyayı bir seferde bir kod satırının değiştirmeye yardımcı olacaktır.

Terzilik ve Öncelikli

Bu kılavuzu organizasyonunuzda benimseymelisiniz. Kuruluşunuzun teknolojilerini, süreçlerine ve organizasyonel yapısına uyacak şekilde bilgileri uyarlamanız gerekebilir.

Genel olarak, bu kılavuzu kullanabilecek kuruluşlarda birkaç farklı rol vardır:

- Geliştiriciler bu kılavuzu güvenli kod ürettiklerinden emin olmak için kullanmalıdır. Bu testler normal kod ve birim test prosedürlerinin bir parçası olmalıdır.
- Yazılım testçileri ve QA, uygulamalara uyguladıkları test vakalarını genişletmek için bu kılavuzu kullanmalıdır. Bu güvenlik açıklarını erken yakalamak, daha sonra önemli zaman ve çaba sağlar.
- Güvenlik uzmanları, bu kılavuzu bir uygulamada hiçbir güvenlik deliğinin kaçırılmadığını doğrulamanın bir yolu olarak diğer tekniklerle birlikte kullanmalıdır.
- Proje Yöneticileri, bu kılavuzun var olmasının nedenini ve güvenlik sorunlarının kod ve tasarımdaki hatalar yoluyla ortaya çıktığını düşünmelidir.

Güvenlik testi yaparken hatırlanması gereken en önemli şey sürekli olarak yeniden önceliklendirmektir. Bir uygulamanın başarısız olabileceği sonsuz sayıda olası yol vardır ve kuruluşlar her zaman sınırlı test süresine ve kaynaklarına sahiptir. Zaman ve kaynakların akıllıca harcandığından emin olun. İşiniz için gerçek bir risk olan güvenlik deliklerine odaklanmaya çalışın. Uygulama ve kullanım durumları açısından riski bağlamsallaştırmaya çalışın.

Bu kılavuz en iyi farklı güvenlik deliği türlerini bulmak için kullanabileceğiniz bir dizi teknik olarak görülür. Ancak tüm teknikler eşit derecede önemli değildir. Kılavuzu bir kontrol listesi olarak kullanmaktan kaçınmaya çalışın, yeni güvenlik açıkları her zaman tezahür eder ve hiçbir rehber “test edilecek şeylerin” kapsamlı bir listesi olamaz, ancak başlamak için harika bir yer.

Otomatik Araçların Rolü

Otomatik güvenlik analizi ve test araçları satan bir dizi şirket var. Bu araçların sınırlamalarını hatırlayın, böylece onları iyi oldukları şey için kullanabilirsiniz. Michael Howard'ın Seattle'daki 2006 OWASP AppSec Konferansı'nda belirttiği gibi, "Araçlar yazılımı güvenli hale getirmez! Sürecin ölçeklendirilmesine yardımcı oluyorlar ve politikanın uygulanmasına yardımcı oluyorlar.”

En önemlisi, bu araçlar jeneriktir - yani özel kodunuz için değil, genel olarak uygulamalar için tasarlanmıştır. Bu, bazı jenerik problemler bulabilseler de, çoğu kusuru tespit etmelerine izin vermek için uygulamanız hakkında yeterli bilgiye sahip olmadıkları anlamına gelir. Deneyimlerime göre, en ciddi güvenlik sorunları

jenerik olmayan, ancak iş mantığınızda ve özel uygulama tasarımınızda derinden iç içe geçmiş olanlardır.

Bu araçlar da çok yararlı olabilir, çünkü birçok potansiyel sorun bulurlar. Aletleri çalıştırmak çok zaman almazken, potansiyel sorunların her birinin araştırılması ve doğrulaması zaman alır. Amaç en ciddi kusurları mümkün olduğunca çabuk bulmak ve ortadan kaldırmaksa, zamanınızın en iyi şekilde otomatik araçlarla mı yoksa bu kılavuzda açıklanan tekniklerle mi harcandığını düşünün. Yine de, bu araçlar kesinlikle dengeli bir uygulama güvenlik programının parçasıdır. Akıllıca kullanıldığında, daha güvenli kod üretmek için genel süreçlerinizi destekleyebilirler.

Eylem Çağrısı

Yazılımı oluşturuyorsanız, tasarlar veya test ediyorsanız, bu belgedeki güvenlik testi rehberliğine aşina olmanızı şiddetle tavsiye ederim. Uygulamaların bugün karşılaştığı en yaygın sorunları test etmek için harika bir yol haritasıdır, ancak kapsamlı değildir. Hatalar bulursanız lütfen tartışma sayfasına bir not ekleyin veya değişimi kendiniz yapın. Bu kılavuzu kullanan binlerce kişiye yardım edeceksiniz.

Lütfen bize bireysel veya kurumsal bir üye olarak katılmayı düşünün, böylece bu test kılavuzu ve OWASP'deki diğer tüm harika projeler gibi malzemeler üretmeye devam edebiliriz.

Bu kılavuza tüm geçmişe ve gelecekteki katkıda bulunanlara teşekkür ederiz, çalışmanız dünya çapında uygulamaları daha güvenli hale getirmeye yardımcı olacaktır.

- Eoin Keary, OWASP Yönetim Kurulu Üyesi, 19 Nisan 2013 Open Web Uygulama Güvenliği Projesi ve OWASP, OWASP Foundation, Inc.'in tescilli ticari markalarıdır.