TECHCAREER

SİBER GÜVENLİK EĞİTİMİ

SIZMA TESTİ RAPORU
BİTİRME PROJESİ

GİZEM AKTAŞ

İÇİNDEKİLER **SAYFA**

1.1.Sızma Testi Aşamaları Nelerdir?.....1

1.1.1.Kapsam Belirlenmesi.....1

1.1.2.Bilgi Toplama.....1

1.1.3.Güvenlik Açığı Tespiti.....1

1.1.4.Bilgilerin Analizi ve Planlama.....1

1.1.5.Sömürü Aşaması.....1

1.1.6.Yetki Yükseltme/Sömürü Sonrası Aşama.....1

1.1.7.Temizlik.....2

1.1.8.Raporlama.....2

1.2.Test Çeşitleri.....2

1.2.1.Ağ Güvenlik Testleri.....2

1.2.1.1.İnternet Güvenlik Testleri.....2

1.2.1.2.Yerel Ağ Güvenlik Testleri.....2

1.2.1.3.Kablosuz Ağ Güvenlik Testleri.....2

1.2.1.4.EKS Güvenlik Testleri.....2

1.2.2.Uygulama Güvenlik Testleri.....3

1.2.2.1.Web Uygulama Güvenlik Testleri.....4

1.2.2.2.Web Servis/API (Application Programming Interface) Güvenlik Testleri.....4

1.2.2.3.Mobil Uygulama Güvenlik Testleri.....4

1.2.2.4.Kaynak Kod Analizi.....4

1.2.3.Sistem Özelinde Güvenlik Testleri.....4

1.2.3.1.Veritabanı Sistemleri Güvenlik Testleri.....5

1.2.3.2.ATM/KIOSK Sistemleri Güvenlik Testleri.....5

1.2.3.3.Nesnelerin İnterneti (IoT) ve Gömülü Sistemler Güvenlik Testleri.....5

1.2.3.4.VOICE OVER IP (VOIP) Güvenlik Testleri.....6

1.2.4.Yük / DDoS Testleri.....6

1.2.4.1.Dağıtık Hizmet Dışı Bırakma Testleri.....6

1.2.4.2.Web Uygulama Yük Testleri.....6

1.2.5.Sosyal Mühendislik Testleri.....6

2.Web Uygulama Güvenlik Testi.....6

2.1.Tespit Edilen Açıklar.....7

2.1.1.Yansıtılan Siteler Arası Script Çalıştırma/XSS (Reflected XSS)….....7

2.1.2.Depolanan Siteler Arası Script Çalıştırma (DOM XSS).....9

2.1.3.Blind SQL Injection Zafiyeti (OWASP-DV-005).....11

2.1.4.LFI (Local File Inclusion) Yerel Dosya Dahil Etme Açıklığı.....13

1.Genel Tanımlar

Sızma Testi Nedir?

Sızma testi (pentest) kurum zafiyetlerini tespit etmek ve bu zafiyetlere karşı gerekli güvenlik önlemlerini almayı sağlamak için sızma testi uzmanları tarafından sunulan bir güvenlik hizmetidir. Siber güvenlik uzmanı bir red team üyesi olup OSCP, TSE ve CEH gibi sertifikalara sahip kişidir. Pentest çalışması ile hedefe belirtilen kapsam dahilinde veya tamamen uzmanın kendisinin tespit edeceği kapsam dahilinde çeşitli güvenlik testleri gerçekleştirilir. Pentest uzmanı saldırganların uygulayacağı tüm saldırı vektörlerini hedef sisteme karşı uygulayarak potansiyel güvenlik risklerini ve zafiyetlerini tespit edip raporlar. Sunulan bu hizmete ise sızma testi hizmeti denilmektedir.

Sızma Testi Nasıl Yapılır?

Kurumların bilişim altyapısın içerisinde barındırdığı tüm sistemler, alanında uzman kişiler tarafından saldırganın kullanabileceği araç ve yöntemleri kullanarak sızılması ve elde edilen zafiyet sonuçlarının raporlanmasıdır.

Sızma Testi Süreçleri Nasıl Yürütülür?

Testin yapılacağı hedef sistemler müşteri tarafından belirlenir ve test edilecek sistemler hakkında testi yapan kuruma bilgi verilir. Gerekli sözleşmeler imzalandıktan sonra müşteri onayı ile testin yapılacağı IP adresi müşteri ile paylaşılır, böylelikle kuruma farklı IP adresinden gelen saldırıların test olup olmadığı anlaşılması sağlanır. Teste başlanılır, kritik bulgular test esnasında müşteri ile paylaşılırken, düşük seviyeli bulgular/zafiyetler test sonunda kritik bulgularla beraber raporlanır ve test sonlanır.

1.1.Sızma Testi Aşamaları Nelerdir?

1.1.1.Kapsam Belirlenmesi

Müşteri, testin yapılmasını istediği hedefi/kapsamı belirler. Testin yaklaşım türüne göre (Black Box, White Box, Gray Box) testi yapacak olan firma ile bilgiler paylaşılır.

1.1.2.Bilgi Toplama

Kapsam/Hedef hakkında pasif (sistem ile doğrudan etkileşime geçmeden) ve aktif (sistem ile doğrudan etkileşime geçerek) bilgi toplama işlemi gerçekleştirilir. Bunlara; kullanılan teknoloji, uygulama ve versiyon bilgisi, fonksiyonlar gibi bilgiler örnek gösterilebilir.

1.1.3.Güvenlik Açığı Tespiti

Toplanan bilgiler ışığında var olan güvenlik açıklıklarının belirlendiği aşamadır. Otomatize araçlar kullanılarak taranan sistemler, tarama sonrasında/esnasında uzmanlar tarafından manuel olarak test edilir. Bilgi toplama aşamasında tespit edilen servis ve versiyon bilgisi araştırılarak var olan bir güvenlik açığı olup olmadığı kontrol edilir.

1.1.4.Bilgilerin Analizi ve Planlama

Tespit edilen güvenlik açıklıklarının sömürülmesi için gerekli araştırmalar yapılarak sömürü kodları, zararlı yazılımlar gibi ofansif araçlar hazırlanır.

1.1.5.Sömürü Aşaması

Tespit edilen zafiyetler saldırgan bakış açısı ile sömürülmeye çalışılır ve zafiyetin sistem üzerindeki etkileri incelenir. Saldırgan, sisteme yetkisiz giriş yapabiliyor mu? Servisi durdurabiliyor mu? Gibi sorulara cevap aranır.

1.1.6.Yetki Yükseltme/Sömürü Sonrası Aşama

Saldırgan sisteme erişim elde ettikten sonraki aşamada halihazırdaki yetkilerini yükseltebilecek mi? Yetkisi olmayan dosyaları görebilecek mi? Veya sızılan sistem/ler kullanılarak nasıl ilerlenebilir? Ne gibi kritik dosyalara erişim sağlanabilir? Gibi sorulara yanıt aranır. Saldırganın sömürü sonrası yapacağı teknik/taktik/prosedürler simüle edilmeye çalışılır.

1.1.7.Temizlik

Test edilen sistemlerde yapılan değişiklikler geri alınır. Test için oluşturulan/yüklenen dosyalar sistemden temizlenir.

1.1.8.Raporlama

Yukarıdaki adımların özeti çıkarılır. Var olan veya ileride oluşabilecek potansiyel riskler, alınması gereken önlemler gibi bilgiler raporlanır.

1.2.Test Çeşitleri

1.2.1.Ağ Güvenlik Testleri

Ağ güvenlik testleri genel olarak kurumların network altyapılarının ve varlıklarının testlerini kapsamaktadır. Bu varlıklar testin türüne göre internet, yerel ağ veya kablosuz ağ olarak 3 alt başlığa bölünebilmektedir. Bu testler gerçekleştirilirken global güvenlik standartları ve PwC deneyimi ile birleştirilmiş bir yaklaşım metodoloji izlenir.

1.2.1.1.İnternet Güvenlik Testleri

İnternet güvenlik testleri, İnternet üzerinden erişilebilir varlıkların güvenliklerinin incelenmesini kapsamaktadır. Bir saldırgan bakış açısı ile internet üzerinden erişilebilecek varlıklar üzerinde incelemeler yapılır ve kurum aleyhine oluşabilecek durumlar tespit edilmeye çalışılır.

Test bitiminde bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir, bulgu özelinde yorumlamalar yapılıp kuruma öneriler sunulmakta ve internet üzerindeki varlıkların güvenliklerinin artırılması hedeflenmektedir.

1.2.1.2.Yerel Ağ Güvenlik Testleri

Yerel ağ sızma testlerinde amaç kurum iç ağında bulunabilecek saldırı vektörlerinin tespiti ve ardından öneriler ile kurum güvenlik postürünü geliştirmektir. Genellikle kurum çalışanı profili ile yapılan testlerde kurum içerisinden kötü niyetli bir kişinin yapabilecekleri simüle edilmeye çalışılır. Testler sırasında kurumun isteğine göre çeşitli yetkiler ile test yapılabilmektedir. Bunların yanında istenirse cihazlardaki konfigürasyon kontrolleri gibi konularda destek sağlanabilmektedir.

Test sonucunda bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir, bulgu özelinde yorumlamalar yapılıp kuruma öneriler sunulmakta ve kurumun yerel ağında bulunan varlıkların güvenliklerinin artırılması hedeflenmektedir.

1.2.1.3.Kablosuz Ağ Güvenlik Testleri

Kablosuz ağ güvenlik testlerinde kurumun kablosuz networküne gelebilecek saldırı vektörleri tespit edilir ve bu vektörler ile başarı elde edilip edilmediği test edilir. Bunun yanı sıra kurum kablosuz ağlarının parola politikaları gibi detaylar global güvenlik standartlarına uygun olarak incelenir.

Test sonucunda bulunan zafiyetler/açıklıklar/eksiklikler uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir ve bulgu özelinde yorumlamalar yapılıp kuruma detaylı öneriler sunulmaktadır.

1.2.1.4.EKS Güvenlik Testleri

Kurum EKS ağındaki bileşenlere yönelik pasif zafiyet taraması gerçekleştirilir. Keşfedilen zafiyetlerin doğrulanması ve bu zafiyetlerin sömürülebilmesi sonucu olası etkilerin değerlendirilmesi yapılır. Bu zafiyetler aynı zamanda sömürü testlerinde vektörlerin belirlenmesi için kullanılmaktadır.

Aktif tarama yapılması belli şartlara bağlanır ve ancak kuruluşun bu şartları sağlaması durumunda aktif zafiyet taraması gerçekleştirilir.

Kurum EKS ağı üzerinde yapılan zafiyet taramaları beklenmedik sonuçlar verebilir. Canlı sistemler üzerinde yapılacak zafiyet taraması sırasında uygulamalara paketler gönderilip canlı sistemde beklenmedik fonksiyonel bozukluklara sebebiyet verilebilir. Bu sebeplerden ötürü üretim veya otomasyon tarafında yapılacak testler risk teşkil etmektedir. Bu bakımdan, test yaptıracak kurumların bir testbed (deney düzeneği) ortamı hazırlaması ve bu ortamda EKS'de kullanılan bileşenlerin sahip olduğu versiyonlarla birlikte hazırlanması canlı ortamda mevcut olan zafiyetlerin belirlenmesi açısından faydalı olmaktadır. Hazırlanacak test ortamı, üretim ortamında bulunan EKS bileşenlerinin (SCADA Sunucusu, PLC, RTU, SCADA Historian Database, haberleşme protokolleri, vb.) işletim sistemi, yazılım, donanım versiyonlarının aynı olacağı şekilde tasarlanmalıdır.

Denetlenecek kurumun belirtilen koşullarda bir test ortamı bulunmuyorsa üretim ortamında zafiyet taraması pasif zafiyet taraması şeklinde gerçekleştirilir.

Belirtilen koşullarda test ortamı bulunuyorsa aktif bir şekilde zafiyet taraması gerçekleştirilebilmektedir.

Kullanılacak yöntemde ilk adım test edilecek farklı tipteki sistemlerin belirlenmesidir. Örneğin; bir EKS ağında, gerçek-zamanlı sunucular, farklı birkaç işletim sistemi üzerinde çalışan HMI, veritabanları, PLC cihazları gibi farklı sunucu ve iş istasyonları bulunabilir. Sunucu ve iş istasyonları haricinde yönlendiriciler, anahtarlar, haberleşme sunucuları ve güvenlik duvarları da bulunabilir. Belirtilen bu sistemlerin (yönlendiriciler, anahtarlar, haberleşme sunucuları ve güvenlik duvarları) tarama sırasında zarar görmesi çok olası değildir.

EKS üzerinde zafiyet taraması sırasında dikkat edilmesi gerekenler aşağıdaki gibi listelenmiştir (İlgili konular canlı sistem üzerinde yapılan taramalara ilişkin önerilerdir):

Taranan cihazın fonksiyonel yapısının bozulmayacağından ve bir cihazın kaybının operasyonları etkilemeyeceğinden emin olunmalı.

Sistem yöneticisinin testte yer alması sağlanmalı.

Pratik olarak hızlı bir şekilde yeniden kurtarma planı yapılmalı. Genellikle bu sadece yeniden başlatma işlemidir, ancak sistemin kurtarılması ya da yeniden kurulması için bir plan mevcut olmalıdır. Eğer varlık sahibinin böyle bir planı yoksa bu da bir zafiyet olarak değerlendirilmelidir.

Başka bir durum ise, kritik sistemin yedekliliğinin olmadığı durumlarda yapılacak olan tarama işleminin sınırlandırılmasıdır.

Testler sırasında EKS ağında mevcut bilinen işletim sistemlerine, uygulamalara ve gömülü sistemlere yönelik sömürü testleri yapılabilir. Bununla birlikte istenildiği takdirde EKS ağında zararlı yazılım analizi yapılabilir ve bulunan kablosuz ağ bileşenleri de test edilebilmektedir. Keşfedilen zafiyetler incelendikten sonra sistemde uzmanlarımız tarafından bir değişiklik yapılmışsa (kullanıcı ekleme, dosya yükleme vb.) bu değişiklikler testin son aşaması olarak yetkili gözetimi altında geri alınmaktadır.

Test bitiminde bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir ve bulgu özelinde yorumlamalar yapılıp kuruma öneriler sunulmaktadır.

1.2.2.Uygulama Güvenlik Testleri

Uygulama güvenlik testleri ağ güvenlik testleri tarafından farklılaşmakta ve daha özelleşmiş bir hal almaktadır. Genel olarak uygulama mimarileri, kullanılan diller özelinde oluşabilecek zafiyetler, fonksiyonalite ile birlikte ortaya çıkabilecek iş mantığı hataları gibi otomatize araçların tam olarak tespit edemeyeceği saldırı vektörleri dahil olmaktadır. PwC olarak uygulamalar özelinde sızma testlerini web, mobil, web service/API güvenlik testleri ve kaynak kod analizi olarak 4 alt başlıkta ele almaktayız.

1.2.2.1.Web Uygulama Güvenlik Testleri

Web uygulama sızma testleri, kullanılan ve geliştirilen uygulamaların güvenilirliğinin test edilmesi ve bir saldırgan bakış açısı ile incelenmesi anlamına gelmektedir. Uygulamanın çalışma mantığı anlaşılıp kimi zaman dil bağımsız kimi zaman dil özelinde açıklıklar tespit edilmeye çalışılır. Bu çalışma yapılırken OWASP gibi global metodolojilerden ve PwC deneyiminden esinlenilir. Çalışma kapsamı ve yetki türleri firma isteğine göre belirlenir; örneğin web uygulama kimi çalışmalarda uzmanlar tarafından haritalandırılırken kimi zaman detaylı bilgilendirmeler ile devam edilebilmektedir. PwC Siber Güvenlik ekibi müşteri isteğine göre çalışmayı şekillendirmektedir.

Test sonunda bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir ve bulgu özelinde yorumlamalar yapılıp kuruma öneriler sunulmaktadır.

1.2.2.2.Web Servis/API (Application Programming Interface) Güvenlik Testleri

Web Servis / API güvenlik testi, web uygulama güvenlik testleri gibi çeşitli yetkilendirmeler ve bilgi seviyeleri ile kurumun isteği doğrultusunda ilerlemektedir. Temel amaç firmanın geliştirdiği servislerin/API'nin kimi konfigürasyon eksikliklerinde destek olmak, bilinen veya uzmanlarca keşfedilebilecek zafiyetler ile ilgili problemlerin bir saldırgan gözü ile incelenip tespit edilmesidir.

Test sonrasında bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir ve bulgu özelinde yorumlamalar yapılıp kuruma öneriler sunulmaktadır.

1.2.2.3.Mobil Uygulama Güvenlik Testleri

Mobil uygulama testlerinin amacı, kurum tarafından kullanılan mobil uygulamalar üzerinden kuruma ve mobil uygulamayı kullanan kullanıcılara yönelik tehditleri tespit etmektir. Bu kapsamda, kapsam dahilindeki mobil uygulamalara verilen test kullanıcılarıyla birlikte veya oturumsuz bir şekilde OWASP TOP 10, BDDK, PCI DSS gibi metodolojiler ve regülasyonların istekleri baz alınarak güvenlik testi gerçekleştirilmektedir.

Test sonrasında bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir ve bulgu özelinde yorumlamalar yapılıp kuruma ve uygulamaya özel öneriler sunulmaktadır.

1.2.2.4.Kaynak Kod Analizi

Kaynak kod analizinde izlenen test yönteminde, bir statik kaynak kod analiz aracı ile birlikte, kodun ağaç yapısı içerisinde ki akışının belirlenmesi, üzerinde bulunabilecek zafiyetlerin ayrıştırılması, kodun kalitesinin değerlendirilmesi ve kaynak yönetimini içeren bulgu maddelerinin otomatik olarak belirlenmesi amaçlanmaktadır. Bu süreç zarfında çıkan bulgular elle yapılan kontrollerle doğrulukları ispatlanarak testler tamamlanmaktadır.

Statik tarama aşamasında kaynak kod üzerinde bulunan konfigürasyon hataları ve bilinen güvenlik zafiyetleri tespit edilir. Dizin içeriği listeleme, dizin atlatma, kaynak kod kalite değerlendirmesi, web sunucu hata denetim mekanizmasının kontrol edilmesi gibi işlemler yapılmaktadır.

Test bitiminde bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir ve bulgu özelinde yorumlamalar yapılıp kuruma öneriler sunulmaktadır.

1.2.3.Sistem Özelinde Güvenlik Testleri

Siber güvenlik konusunu sızma testleri, kırmızı takım operasyonları gibi çalışmalarla desteklesek de sistemlerin özelinde de derinlemesine çalışmalar güvenliği artırmakta fayda sağlayacaktır.

Genel sızma testlerinin yanında özellikle güvenlik testine tabii tutulması gereken bir alt sistem varsa bu güvenlik testlerini "Sistem Özelinde Güvenlik Testleri Olarak" tanımlamaktayız.

1.2.3.1.Veritabanı Sistemleri Güvenlik Testleri

Veritabanı sistemleri sızma testlerinde güvenlik açısından kritik olan konfigürasyon ayarları, veritabanı sunucusunda denetleme mekanizmasının varlığı, yedekleme ve kurtarma mekanizmasının varlığı incelenmektedir. Bu incelemelerin ardından sistemde fonksiyonelliği bozmayacak olan güncel sistem ve güvenlik yamalarının uygulanıp uygulanmadığı, veritabanı için önemli olan işletim sistemi dosyalarının erişim izinleri, sunucuya uzaktan erişiminin güvenlik düzeyi gibi çeşitli durumlar incelenmektedir.

Test bitiminde bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir ve bulgu özelinde yorumlamalar yapılıp kuruma öneriler sunulmaktadır.

1.2.3.2.ATM/KIOSK Sistemleri Güvenlik Testleri

ATM/KIOSK sistemleri güvenlik testlerinde sistemlerin genel mimari içindeki konumu, uç noktalar ile merkez arası haberleşme yapısı incelenmektedir. Bu incelemelerin ardından kurum ağı içinden taramalar yapılarak ATM/KIOSK sistemlerinin bulunduğu ağlara erişilip erişilmediği, cihazlara fiziksel olarak müdahale edilip edilemeyeceği, işletim sistemi ve çalışan servislere yönelik bir zafiyet bulunup bulunmadığı araştırılır. Kritik bir zafiyet bulunursa, onay alındıktan sonra zafiyet sömürülerek cihazlara sızılmaya çalışılması gibi çeşitli yöntemlerle cihazlarin güvenlik postürleri incelenmektedir.

Test bitiminde bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir ve bulgu özelinde yorumlamalar yapılıp kuruma öneriler sunulmaktadır.

1.2.3.3.Nesnelerin İnterneti (IoT) ve Gömülü Sistemler Güvenlik Testleri

Zafiyet tarama ve sızma testi gibi faaliyetler kurum/kuruluş bünyesinde, ön tanımlı kapsam dahilindeki zafiyetleri ve açıklıkları tespit etmek için yapılmaktadır. Bu faaliyetler genellikle kurum/kuruluşun maruz kalabileceği iç ve dış tehditler çok fazla analiz edilmeden yapıldığından dolayı yapılan çalışmalar sınırlı bir alanı kapsar ve sadece bu kapsam içerisindeki zafiyetler belirlenebilir. Ancak gerçek saldırganların motivasyonu sızma testi yapan uzmanlardan farklılık göstermektedir. Bu nedenle sızma testleri sonucu ortaya çıkan zafiyetler kapatılsa dahi saldırganlar başarılı olabilmektedir.

Bu nedenle kurum/kuruluşun kullandığı donanımların maruz kalabileceği iç ve dış tehditler tespit edilmeli ve bu tehditlere yönelik gerçekçi ve kontrollü testler düzenlenmelidir. Bu sayede gerçek saldırganların kullandıkları araç, teknik ve taktikler kullanılan donanımlara yönelik simüle edilmiş olacaktır. Bu sayede gerçek bir saldırıyı beklemek yerine gerçekçi bir saldırıyı tatbik ederek insan/süreç/teknoloji ve fiziksel güvenlik bazındaki zafiyetler tespit edilebilecektir.

Nesnelerin İnterneti (IoT) Güvenlik Testleri Hizmeti hedef odaklıdır ve kurum/kuruluşun sahip olduğu cihazlara yönelik tehditlerin modellenmesine ve olan- olabilecek saldırıları ortaya koyup çözümler üretmeyi hedeflemektedir.

Nesnelerin İnterneti güvenlik testleri hizmeti; geliştirici ekibin güvenlik yeterliliklerinin tespit edilmesi, donanımın güvenlik yeterliliklerinin ölçülmesi, kurum/kuruluştaki insan/süreç/teknoloji kaynaklı zafiyetlerin tespit edilmesi konularının hepsini veya bir kısmını amaçlayabilmektedir.

Nesnelerin interneti ve gömülü sistem bileşenlerinin güvenlik testleri test edilirken izlenen adımlar hedefin belirlenmesi, hedef ile ilişkili bileşenlerin tespiti, araçların ve yöntemlerin hazırlanması ve testin gerçekleştirilmesi şeklindedir.

Hedef belirlenmesi aşamasında test yapılacak IoT sistemi bileşenleri kurum ile gerçekleştirilen görüşmeler sonucunda belirlenir.

Hedef ile ilişkili bileşenlerin tespiti aşamasında test edilecek IoT cihazlara ait saldırı yüzeyi detaylı bir şekilde çıkarılmaktadır.

Araçların ve yöntemlerin hazırlanması aşamasında her obje için kullanılacak olan donanım, yazılım ve yöntemler netleştirilir ve bir yol haritası çizilmiş olur.

Testin gerçekleştirilmesi adımında iste bir önceki aşamada belirlenen bileşenlere yönelik testler gerçekleştirilir.

Keşfedilen zafiyetler incelendikten sonra sistemde uzmanlarımız tarafından bir değişiklik yapılmışsa (kullanıcı ekleme, dosya yükleme vb.) bu değişiklikler testin son aşaması olarak yetkili gözetimi altında geri alınmaktadır.

Test bitiminde bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir ve bulgu özelinde yorumlamalar yapılıp kuruma öneriler sunulmaktadır.

1.2.3.4.VOICE OVER IP (VOIP) Güvenlik Testleri

Zafiyet tarama ve sızma testi gibi faaliyetler kurum/kuruluş bünyesinde, ön tanımlı kapsam dahilindeki zafiyetleri ve açıklıkları tespit etmek için yapılmaktadır. Bu faaliyetler genellikle kurum/kuruluşun maruz kalabileceği iç ve dış tehditler çok fazla analiz edilmeden yapıldığından dolayı yapılan çalışmalar sınırlı bir alanı kapsar ve sadece bu kapsam içerisindeki zafiyetler belirlenebilir. Ancak gerçek saldırganların motivasyonu sızma testi yapan uzmanlardan farklılık göstermektedir. Bu nedenle sızma testleri sonucu ortaya çıkan zafiyetler kapatılsa dahi saldırganlar başarılı olabilmektedir.

Bu nedenle kurum/kuruluşun kullandığı donanımların maruz kalabileceği iç ve dış tehditler tespit edilmeli ve bu tehditlere yönelik gerçekçi ve kontrollü testler düzenlenmelidir. Bu sayede gerçek saldırganların kullandıkları araç, teknik ve taktikler kullanılan donanımlara yönelik simüle edilmiş olacaktır. Bu sayede gerçek bir saldırıyı beklemek yerine gerçekçi bir saldırıyı tatbik ederek insan/süreç/teknoloji ve fiziksel güvenlik bazındaki zafiyetler tespit edilebilecektir.

PwC İnternet Güvenliği VOIP Güvenlik Testi'nde, firmanın kullandığı VOIP sisteminin detaylı analizi yapılarak VOIP sistemi üzerinden işlenebilecek sahtekarlıkların ve zafiyetlerin test edilmesi amaçlanmaktadır. VOIP altyapınızdaki tüm zafiyetler tespit edilerek raporlanır ve açıklıkların kapatılması için öneriler sunulur.

VOIP bileşenleri testleri hedefin belirlenmesi, hedef ile ilişkili bileşenlerin tespiti, araç ve yöntemlerin hazırlanması, son olarak da testin gerçekleştirilmesi aşamalarından oluşmaktadır.

Keşfedilen zafiyetler incelendikten sonra sistemde uzmanlarımız tarafından bir değişiklik yapılmışsa (kullanıcı ekleme, dosya yükleme vb.) bu değişiklikler testin son aşaması olarak yetkili gözetimi altında geri alınmaktadır.

Test bitiminde bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir ve bulgu özelinde yorumlamalar yapılıp kuruma öneriler sunulmaktadır.

1.2.4.Yük / DDoS Testleri

1.2.4.1.Dağıtık Hizmet Dışı Bırakma Testleri

DDoS saldırısı, sistemlerin bant genişliği, işlemci ve bellek gibi kaynaklarının tüketerek, kullanıcılar tarafından erişilemez duruma getirmek amacıyla yapılan saldırılardır. DDoS saldırıları, son yıllarda en çok kullanılan siber savaş aracı olarak tanımlanmakta ve kesin olarak çözümü bulunamayan tehditlerin başında gelmektedir. DDoS, alternatif diğer saldırı türlerine göre daha kolay gerçekleştirilebildiği için siber saldırganlar tarafından kurum ve kuruluşların, hatta ülkelerin internet altyapılarını ve sunulan hizmetleri işlevsiz hale getirmek için sıklıkla tercih ettiği yöntemlerin başında yer almaktadır. HTTP DDoS, TCP DDoS, ICMP DDoS, UDP DDoS gibi temel kategorilere ayrılmaktadır.

DDoS testleri kapsamındaki hizmetlerimizi her defasında aynı yüksek kalite standardında gerçekleştirebilmek amacıyla oluşturduğumuz yöntemleri takip ediyoruz.

Test sonuçlarını istatistiksel olarak ifade etmek ve hatalı sonuçları en aza indirmek amacıyla, DDoS testleri sırasında farklı lokasyonlarda bulunan izleme (monitoring) araçlarıyla hedef sunucu ve uygulamaların cevap verme süreleri, hizmet dışı kalma süreleri gibi ölçümler yapılmaktadır. Aynı zamanda, testler için kullanılan makinelerde de hedefe gönderilen paket sayısı, tüketilen bant genişliği miktarı gibi ölçümler yapılarak atak yoğunluğu tespit edilmektedir.

Test bitiminde bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir ve bulgu özelinde yorumlamalar yapılıp kuruma öneriler sunulmaktadır.

1.2.4.2.Web Uygulama Yük Testleri

Yük testi, sistemdeki darboğazları(bottle-neck) bulmak amacıyla gerçek kullanıcıları simüle edebilecek bir araç ile taklit ederek bir uygulamayı test etme sürecidir. Yük testinde, donanım ve yazılım açısından ölçeklenebilirlik, kullanılabilirlik ve performans niteliklerini test edilir. Bu süreç içerisinde yükün geçtiği tüm bileşenlerin ve kaynakların (CPU kullanımı, bellek kullanımı, önbellek tutarlılığı, güç tüketimi ve ağın bant genişliği gibi) monitör edilmesi ve izlenmesi gerekmektedir. Bu monitör işlemlerinin bir kısmı PwC Güvenlik Test Hizmetleri ekibi tarafından gerçekleştirilebilse bile, kapsamlı bir sonuca varabilmek adına yük testi gerçekleştiren kurumun da sistemler üzerinde incelemeler yapması önemlidir.

Yük testi gerçekleştirilirken, hedef uygulama üzerinde bulunan fonksiyonlar, bir kullanıcı gibi kullanılır ve bu süreç kayıt altına alınır. Sonrasında, elde edilen botlar üzerinde farklı HTTP oturumları açılarak bu kullanıcıların gerçekleştirdiği HTTP istekleri taklit edilir ve seçilen senaryolar web uygulaması üzerinde uygulanır. Bu aşama esnasında test edilen uygulamanın yalnızca HTTP cevap süresi PwC Güvenlik Test Hizmetleri ekibi tarafından monitör edilebildiği için, diğer kaynakların da sistem üzerinde incelenmesi, darboğazın gerçekleştiği noktayı bulmak adına testin önemli bir parçası olarak değerlendirilir.

Test bitiminde bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir ve bulgu özelinde yorumlamalar yapılıp kuruma öneriler sunulmaktadır.

1.2.5.Sosyal Mühendislik Testleri

Sosyal Mühendislik, insanların zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışma veya istenilen şeyleri yaptırma işlemlerinin bütünüdür.

PwC Cyber kurumun ihtiyaçlarına ve isteklerine göre çeşitli senaryolar ile kurum çalışanlarının bu tür saldırılara karşı farkındalığını test etmektedir. Yapılan çalışma kurumun istediği zamanlarda veya rastgele bir zamanda yapılabilmekte, çalışma türüne göre (siyah kutu/beyaz kutu) kapsam değişebilmektedir.

Sosyal mühendislik testleri esnasında çalışanların kişisel bilgilerine ulaşılması durumunda bu bilgiler kuruluş ile paylaşılmaz, sızma testi raporuna eklenmez ve bir kopyası alınmaz.

Test bitiminde bulunan zafiyetler/açıklıklar uzmanlarımız tarafından detaylandırılıp rapor haline dönüştürülmektedir ve bulgu özelinde yorumlamalar yapılıp kuruma öneriler sunulmaktadır, sosyal mühendislik özelinde gerekirse farkındalık eğitimleri düzenlenebilmektedir.

2.Web Uygulama Güvenlik Testi

2.1.Tespit Edilen Açıklar

2.1.1.Yansıtılan Siteler Arası Script Çalıştırma/XSS (Reflected XSS) (OWASP-DV-001)	
Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu Açıklaması:

Siteler arası script çalıştırma zafiyeti olarak bilinen XSS, kötü niyetli kişilerin bu site üzerinden diğer kullanıcılara istemci tarafında çalışmak üzere kod (genellikle JavaScript ve html) gönderip kötü amaçlarla çalıştırmalarına imkân tanımaktadır.

XSS zafiyetleri uygulamalarda dışarıdan alınan bilgiler için yeterli girdi ve çıktı denetimi yapılmadığı durumlarda ortaya çıkar ve art niyetli bir kullanıcı istediği gibi javascript kodu çalıştırarak hedef aldığı kişilere ait oturum bilgilerini çalabilir, hedef aldığı kişilerin browserını istediği gibi yönlendirebilir. Ele geçirdiği kurban browseri kullanılarak iç ağda port tarama, ortamda ses kaydı ve görüntü kaydı gerçekleştirebilir.

Reflected (yansıtılmış) XSS açıklığı en sık karşılaşılan XSS açıklığı türüdür. İlgili açıklık türünde, hedef sisteme gönderilen kod parçaçığı(payload) kalıcı olarak veri tabanında tutulmamaktadır.

Bu sebeple ilgili açıklığın istismarı için, öncesinde kullanıcı tarafında bir bağlantı ziyaret ettirme şeklinde bir sosyal mühendislik saldırısı gerçekleştirilmelidir. Reflected XSS açıklığı HTTP GET ve POST taleplerinin her ikisinde iletilen parametrelerde de bulunabilir. Reflected XSS açıklığı, temelde hedef sisteme gönderilen payloadın, dönen sunucu cevabı içerisinde encode edilmeden döndürülmesi durumunda açığa çıkmaktadır. Bu durumda isteği yapan istemci tarafında enjekte edilen kod parçacığı eylemini gerçekleştirecektir. Bu açıklık türü istismar edilerek client tarafında html, javascript, action script benzeri kod parçacıkları sayfaya enjekte edilebilir. Kullanıcı kandırma veya cookie hırsızlığı gerçekleştirilebilir. Uygulamanın arama kısmında Yansıtılan Siteler Arası Script çalıştırılabileceği görülmüştür. Aşağıdaki tabloda admin kullanıcısıyla yapılan işlemlerin hangi url adresinde ve hangi parametrelerde olduğu detaylı bir şekilde ifade edilmiştir.

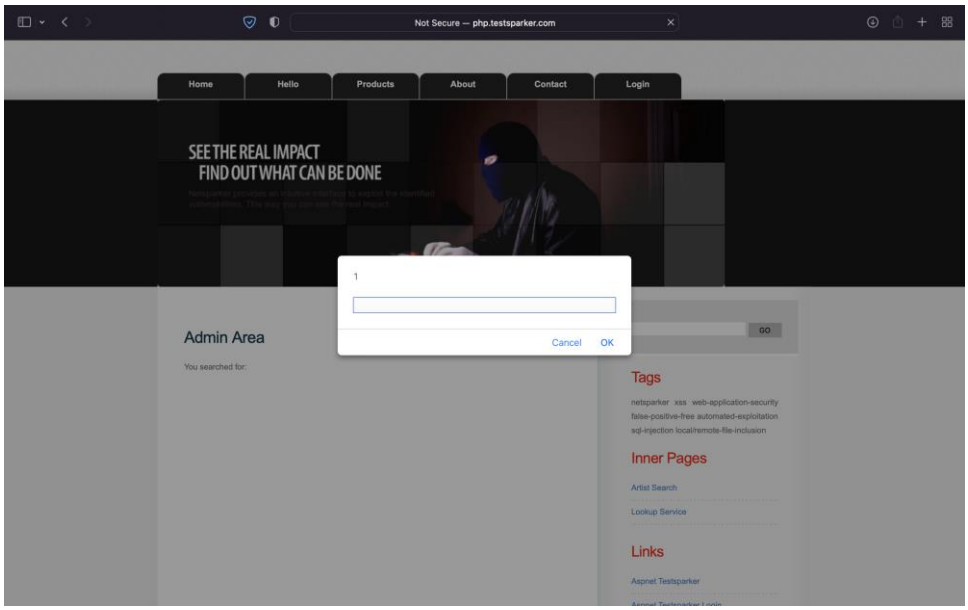
Bulgu 1:

URL	http://php.testsparker.com/auth/internal.php
HTTP Talep Türü	POST
Payload	<img onerror="prompt(1)" src="1.jpg">

Hedefe gönderilen POST isteği;
POST /auth/xss.php HTTP/1.1 Host: php.testsparker.com Content-Length: 64 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 Origin: http://php.testsparker.com Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8 Sec-GPC: 1 Accept-Language: tr-TR,tr;q=0.9 Referer: http://php.testsparker.com/auth/internal.php Accept-Encoding: gzip, deflate Cookie: PHPSESSID=7042348d138c49624693eb07a37cae61 Connection: close search=%3Cimg+onerror%3D%22prompt%281%29%22+src%3D%221.jpg%22%3E

Bu verilen bilgiler doğrultusunda uygulamanın arama kısmında belirtilen payload çalıştırıldığı zaman XSS çalışacaktır ve aşağıdaki gibi bir görüntü ile karşılaşılacaktır.

İstismar Ekran Görüntüsü



Şekil 1: Payload başarılı bir şekilde çalışmıştır.

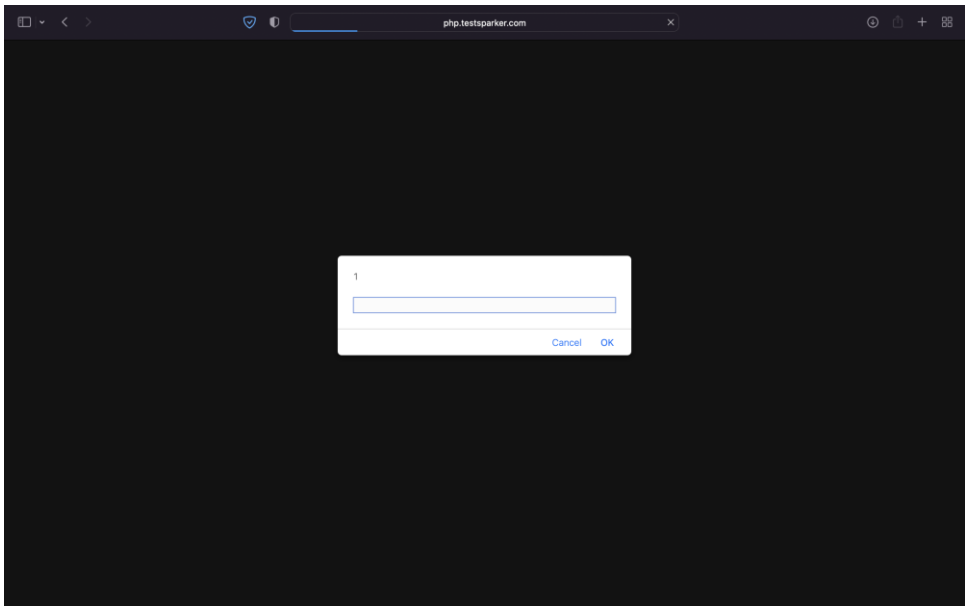
Bulgu 2:

URL	http://php.testsparker.com/auth/internal.php
HTTP Talep Türü	GET
Payload	<img onerror="prompt(1)" src="1.jpg">

Hedefe gönderilen GET isteği;
GET /artist.php?id=%3Cimg+onerror%3D%22prompt%281%29%22+src%3D%221.jpg%22%3E+ HTTP/1.1 Host: php.testsparker.com User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: close Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp Cookie: PHPSESSID=cbe7e9b19d1791264a5bbdf384bf7da8 Upgrade-Insecure-Requests: 1

Bu verilen bilgiler doğrultusunda uygulamanın arama kısmında belirtilen payload çalıştırıldığı zaman XSS çalışacaktır ve aşağıdaki gibi bir görüntü ile karşılaşılacaktır.

İstismar Ekran Görüntüsü



Şekil 1: Payload başarılı bir şekilde çalışmıştır.

Açığı Barındıran Sistemler:

http://php.testsparker.com/auth/internal.php

http://php.testsparker.com/auth/xss.php

Çözüm Önerileri:

Uygulama kodlarının gözden geçirilerek parametreler ve http başlığındaki diğer alanlar vasıtası ile yollanan her türlü bilginin kullanılmadan önce zararlı karakterlerden filtrelenmesi önerilmektedir. Uygulamalardaki bütün girdi ve çıktı noktalarından gelen değişkenler kontrole tabi tutulmalı ve bu girdilerdeki bütün meta karakterler filtrelenmelidir.

Detaylı XSS önleme yöntemleri için aşağıda belirtilen referanslar incelenebilir.

Referanslar:

- https://owasp.org/www-community/attacks/xss/
- http://www.cgisecurity.com/articles/xss-faq.shtml
- http://ha.ckers.org/xss.html
- http://www.bindshell.net/tools/beef
- https://www.bgasecurity.com/

2.1.2.Depolanan Siteler Arası Script Çalıştırma (DOM XSS)	
Önem Derecesi	Kritik
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Web
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

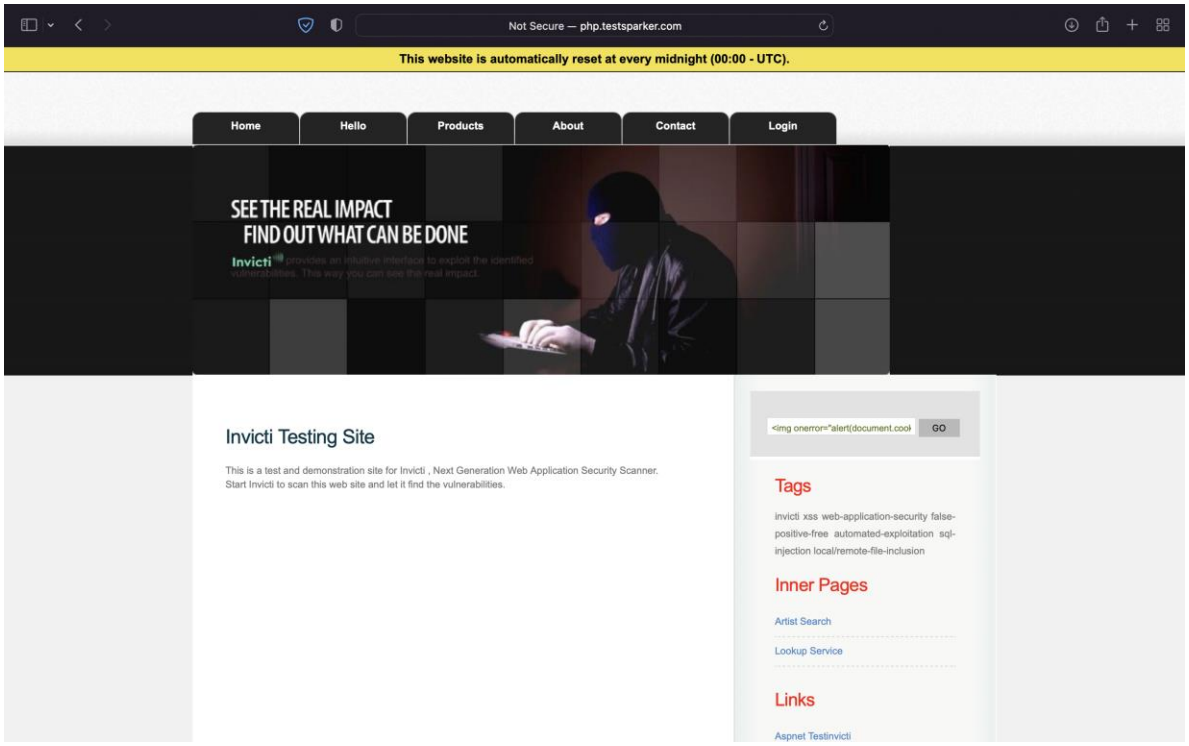
Bulgu Açıklaması:

Siteler arası script çalıştırma zafiyeti olarak bilinen XSS, kötü niyetli kişilerin bu site üzerinden diğer kullanıcılara istemci tarafında çalışmak üzere kod (genellikle JavaScript ve html) gönderip kötü amaçlarla çalıştırmalarına imkân tanımaktadır.

XSS zafiyetleri uygulamalarda dışarıdan alınan bilgiler için yeterli girdi ve çıktı denetimi yapılmadığı durumlarda ortaya çıkar ve art niyetli bir kullanıcı istediği gibi javascript kodu çalıştırarak hedef aldığı kişilere ait oturum bilgilerini çalabilir, hedef aldığı kişilerin browserını istediği gibi yönlendirebilir.

URL	http://php.testsparker.com/auth/internal.php
HTTP Talep Türü	POST
Payload	<img onerror="alert(document.cookie)" src="1.jpg">

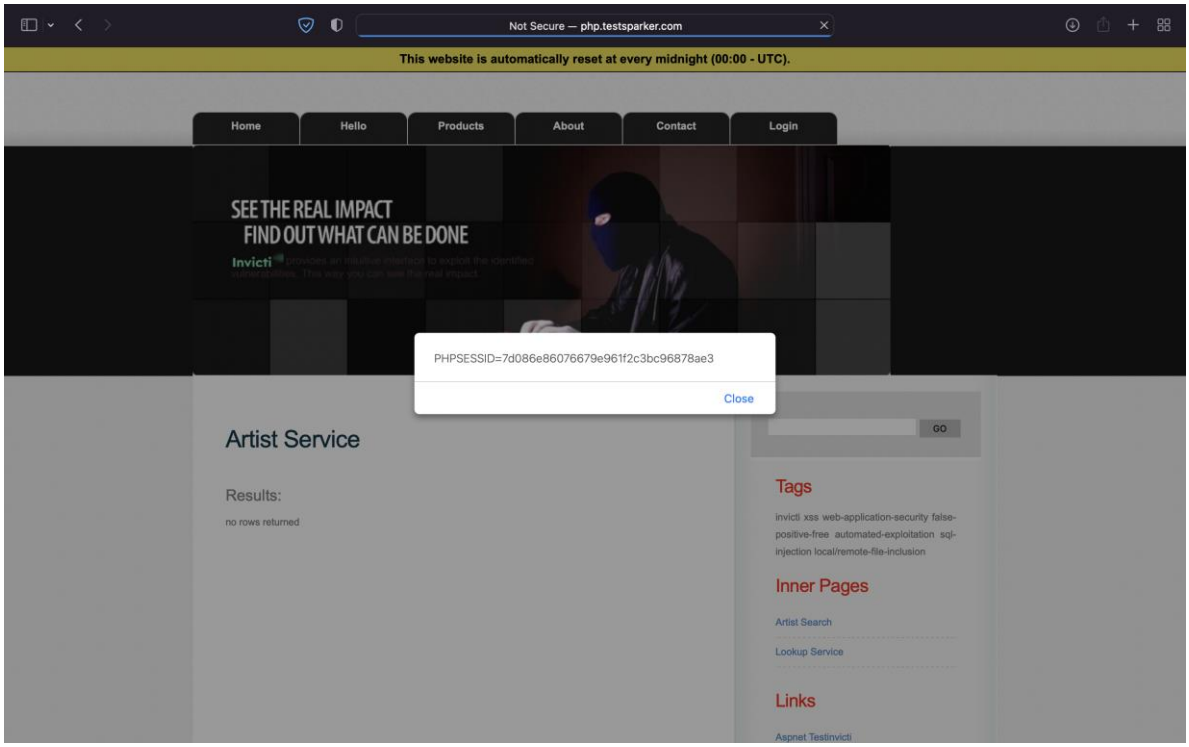
Aşağıdaki ekran görüntüsünde açıklığın bulunduğu alan görünmektedir. Belirtilen payload ilgili yere yazılıp gönderildiği zaman görüntünün altında bulunan tablodaki gibi bir POST isteği gidecektir.



Şekil 2:XSS payloadının yazılacağı yer

Hedefe gönderilen POST isteği;
POST /auth/xss.php HTTP/1.1 Host: php.testsparker.com User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 78 Origin: http://php.testsparker.com Connection: close Referer: http://php.testsparker.com/auth/internal.php Cookie: PHPSESSID=cbe7e9b19d1791264a5bbdf384bf7da8 Upgrade-Insecure-Requests: 1 search=%3Cimg+onerror%3D%22alert%28document.cookie%29%22+src%3D%221.jpg%22%3E+

Bu parametreler doğrultusunda gönderilen XSS çalıştığı zaman aşağıdaki gibi bir ekran görüntüsü olacaktır.



Şekil 3: XSS'in çalıştığı an.

Açığı Barındıran Sistemler:

http://php.testsparker.com/auth/internal.php

Çözüm Önerileri:

Uygulama kodlarının gözden geçirilerek parametreler ve http başlığındaki diğer alanlar vasıtası ile yollanan her türlü bilginin kullanılmadan önce zararlı karakterlerden filtrelenmesi önerilmektedir. Uygulamalardaki bütün girdi ve çıktı noktalarından gelen değişkenler kontrole tabi tutulmalı ve bu girdilerdeki bütün meta karakterler filtrelenmelidir.

Detaylı XSS önleme yöntemleri için aşağıda belirtilen referanslar incelenebilir.

Referanslar:

- https://owasp.org/www-community/attacks/xss/
- http://www.cgisecurity.com/articles/xss-faq.shtml
- http://ha.ckers.org/xss.html
- http://www.bindshell.net/tools/beef
- https://www.bgasecurity.com/

2.1.3.Blind SQL Injection Zafiyeti (OWASP-DV-005)	
Önem Derecesi	Acil
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı

Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

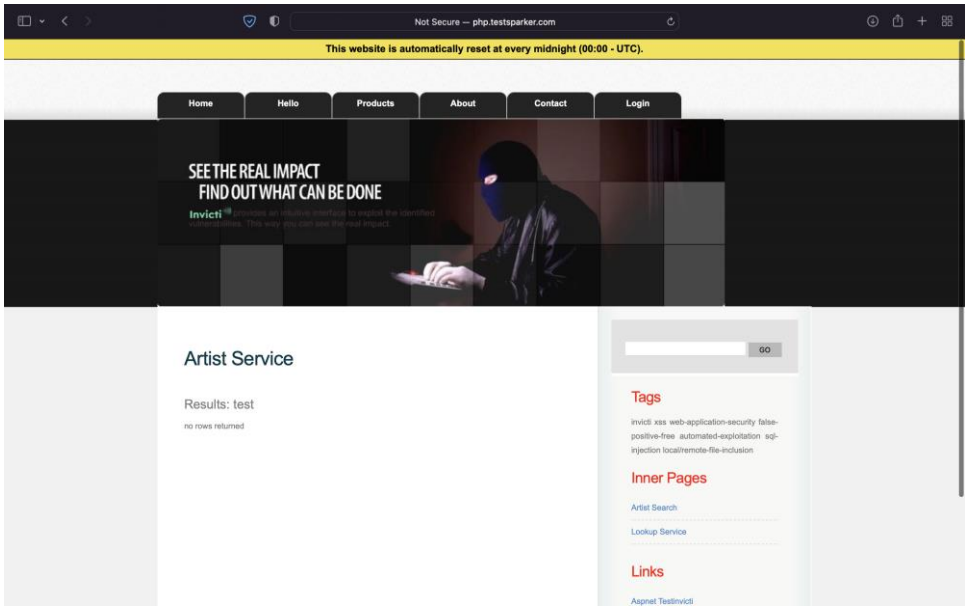
Bulgu Açıklaması:

SQL Injection zafiyeti, uygulama parametreleri aracılığı ile yollanan bilgilerin düzgün kontrol edilmemesi sebebi ile arka planda çalışan veri tabanına yollanan sorgulara, saldırganın sorgularını eklemesine imkân tanıyan bir güvenlik açığıdır.

Hata Tabanlı SQL Injection saldırıları, uygulamanın veri tabanına gönderdiği sorgularda herhangi bir yazım hatası syntax error olması durumunda veya sorgunun veri tabanında çalışması sonucu dönen verilerin, ekrana çıktı olarak verilmesi temeline dayanır.

URL	http://php.testsparker.com/artist.php?id=test
HTTP Talep Türü	GET
Parametre	id=
Payload	1 OR 1

Aşağıdaki ekran görüntüsünde açıklığın bulunduğu alan görünmektedir. Belirtilen payload ilgili yere yazılıp gönderildiği zaman görüntünün altında bulunan tablodaki gibi bir GET isteği gidecektir.

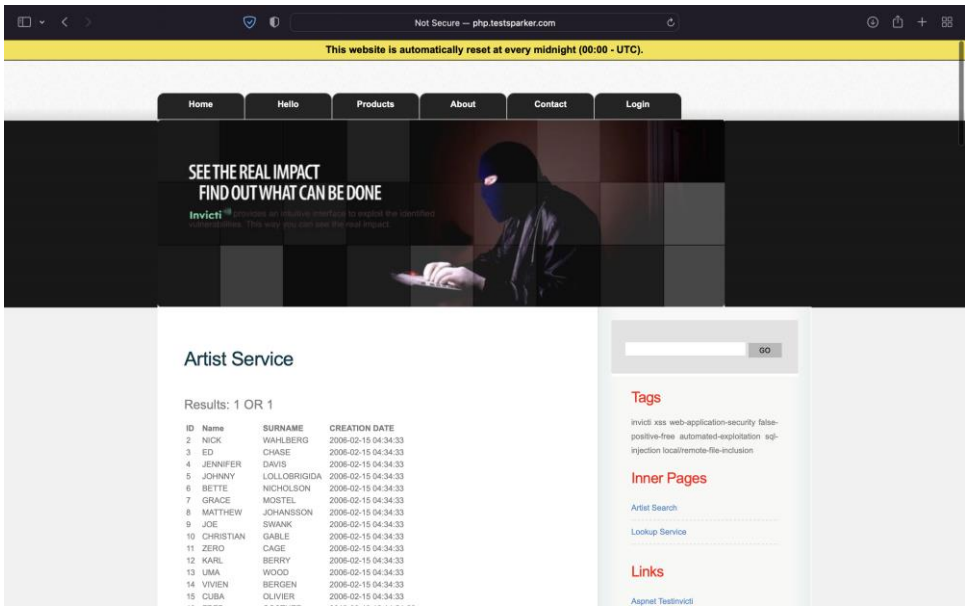


Şekil 2: Çalışmadan önce

Hedefe gönderilen GET isteği;
GET /artist.php?id=1%20OR%201 HTTP/1.1 Host: php.testsparker.com User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: close Cookie: PHPSESSID=cbe7e9b19d1791264a5bbdf384bf7da8

Upgrade-Insecure-Requests: 1

Bu parametreler doğrultusunda gönderilen XSS çalıştığı zaman aşağıdaki gibi bir ekran görüntüsü olacaktır.



Şekil 3: Çalıştığı an.

Açığı Barındıran Sistemler:

http://php.testsparker.com/artist.php?id=test

Çözüm Önerileri:

Uygulama kodlarının gözden geçirilerek parametreler ve http başlığındaki diğer alanlar vasıtası ile yollanan her türlü bilginin kullanılmadan önce zararlı karakterlerden filtrelenmesi önerilmektedir. Uygulamalardaki bütün girdi ve çıktı noktalarından gelen değişkenler kontrole tabi tutulmalı ve bu girdilerdeki bütün meta karakterler filtrelenmelidir.

Detaylı XSS önleme yöntemleri için aşağıda belirtilen referanslar incelenebilir.

Referanslar:

- https://owasp.org/www-community/Injection_Flaws
- http://www.unixwiz.net/techtips/sql-injection.html
- http://www.ngssoftware.com/papers/more_advanced_sql_injection.pdf
- http://www.nextgenss.com/papers/advanced_sql_injection.pd
- https://www.bgasecurity.com/
- http://www.securiteam.com/securityreviews/5DP0N1P76E.html

2.1.4.LFI (Local File Inclusion) Yerel Dosya Dahil Etme Açıklığı	
Önem Derecesi	Kritik

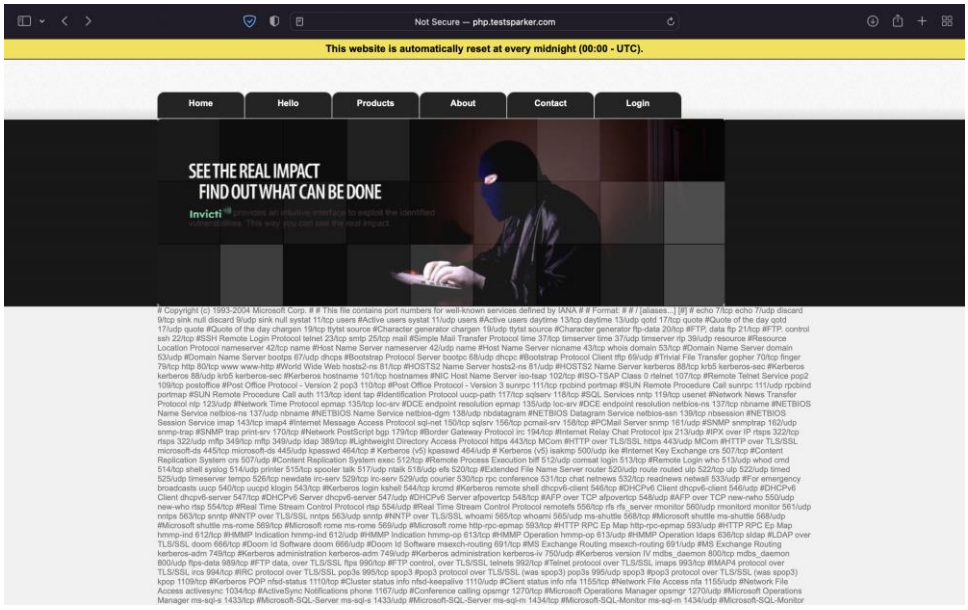
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu Açıklaması:

BGA pentest ekibi tarafından internet üzerinden hedefe yönelik olarak gerçekleştirilen sızma testlerinde, web uygulaması üzerinde Local File Inclusion olarak bilinen yerel dosya dahil etme açıklığı olduğu belirlenmiştir. İlgili açıklık istismar edilerek, hedef sistemde dizin yolu bilinen dosyaların içeriği okunabilir. Saldırganlar bu yolu izleyerek veri tabanı bağlantı dosyalarını okuyabilir, veri tabanını ele geçirebilir, ajan uygulamalar aracılığı ile işletim sistemini ele geçirebilirler.

URL	http://php.testsparker.com/process.php?file=Generics/index.nsp
HTTP Talep Türü	GET
Parametre	sayfa
Payload	c%3A%5CWindows%5CSystem32%5Cdrivers%5Cetc%5Cservices%00.nsp

Yukarıdaki tabloda belirtilen bilgiler doğrultusunda browser üzerinden uygulama çalıştırıldığı zaman yetkisiz yerlere erişim sağlandığı görülmüştür. Aşağıdaki ekran görüntüsünde açıklık istismar edilmiş ve yetkisi olmamasına rağmen C:\Windows\System\drivers\etc\service dosyasının içeriği görüntülenmiş.



Şekil 3: Çalıştığı an.

Yukarıda verilen hedef web uygulamasındaki LFI açıklığı istismar edilerek C:\Windows\System\drivers\etc\service dosyası altındaki bilgiler okunmuştur.

Açığı Barındıran Sistemler:

http://php.testsparker.com/process.php?file=Generics/index.nsp

Çözüm Önerileri:

Dışarıdan input olarak alınan dosyaların mutlaka kontrol edilmesi önerilmektedir. Whitelist veya blacklist kullanılarak okunacak veya okunamayacak dosyaların belirtilmesi önerilmektedir. Bu tür saldırılara karşı önlem olarak web application firewall benzeri uygulamaların kullanılması tavsiye edilmektedir.

Referanslar:

- https://www.bgasecurity.com/
- https://en.wikipedia.org/wiki/File_inclusion_vulnerability
- http://hakipedia.com/index.php/Local_File_Inclusion