PRIVIAHUB FREYA-CLIENT-WHITE MAKİNESİ

SIZMA TESTİ SONUÇ RAPORU

PRIVIA SECURITY SİBER GÜVENLİK VE DANIŞMANLIK HİZMETLERİ

Küçükbakkalköy Mah. Albay Sokak LDAP Plaza No:22

Ataşehir / İstanbul

Tel: +90 216 416 51 94

Tel: +90 312 557 16 17

info@priviasecurity.com

08.08.2020-12.08.2020

Bu belge '**PRIVIAHUB FREYA-CLIENT-WHITE**' makinesine ait gizli bilgiler içermektedir ve yetkili kişiler haricinde okunması yasaktır.Bu belge elinize yetkisiz bir şekilde ulaştıysa lütfen info@priviasecurity.com adresine bildiriniz.

Rapor Detayları

Rapor Başlığı : PriviaHub Freya-Client-White Sızma Testi Sonuç Raporu

Versiyon : 1.0

Yazan : Şeyma Yaldız

Test Ekibi : Şeyma Yaldız

Kontrol Eden : Şeyma Yaldız

Onaylayan : Şeyma Yaldız

Rapor Sınıfı : Gizli

Müşteri Kurum Yetkilisi

Yetkili Adı ve Soyadı: XXX

Ünvanı : XXX

Kurum Adı : PriviaHub

Rapor Denetimi

Versiyon : V1.0

Tarih : 12.08.2020

Yazar : Şeyma Yaldız

Tanım : Final

Yasal Sorumluluklar

Söz konusu raporun içeriği gizli olup, taraflar arasında yazılı mutabakat olmadan üçüncü kişilere basılı olarak (hardcopy) ya da elektronik ortamda (softcopy) paylaşılamaz, yayınlanamaz ve çoğaltılamaz.

İÇİNDEKİLER

1.GİRİŞ

Bu rapor, Privia Security Şirketi tarafından "PriviaHub Freya-Client-White" sistemi üzerindeki güvenlik açıklarını ortaya çıkartmak amacı ile 08.08.2020 - 12.08.2020 tarihleri arasında gerçekleştirilen güvenlik ve sızma testlerinin detaylı sonuçlarını içermektedir.

Pentest çalışması kapsamında "PriviaHub" altyapısı ve sunucularının çalışmasını olumsuz yönde etkileyecek araçlar ve yöntemler kullanılmamış izinsiz ve yetkisiz bir şekilde hizmetin aksamasına neden olabilecek herhangi bir işlem gerçekleştirilmemiştir.

Rapor,kapsam,yönetici özeti,öneriler ve kategorik olarak tespit edilen güvenlik açıklıklarına ait detayları ve referansları içermektedir.

Sızma testi raporunda kullanılan yabancı ve teknik terimlere ait sözlük rapor sonunda EK-1 olarak sunulmuştur.

Raporda sadece açıklık barındıran uygulamalar ve bu uygulamalardaki düşük,orta,yüksek,kritik ve acil seviye güvenlik zafiyetleri detaylı incelenmiş yanlış alarm(false positive) olabilecek başlıklar elenerek gerekli görülenler rapora eklenmiştir.

2.KAPSAM

Sızma testinde ana amaçlardan biri tüm zafiyetlerin değerlendirilerek sisteme sızılmaya çalışılmasıdır.Bu amaç doğrultusunda gerçekleştirilecek sızma testlerinde kapsam pentest çalışmasının en önemli adımını oluşturmaktır.

Gerçekleştirilen denetimlerde "PriviaHub" yetkilileri tarafından bildirilen ve aşağıda belirtilen sistemlere yönelik sızma testleri gerçekleştirilmiştir.

Test Başlığı	Detaylar
İç Ağ IP	192.168.1.178
E-posta Sunucuları	xxxx
Dns Sunucuları	xxxx
Web Uygulamaları	http://192.168.1.178

Testler süresince kullanılan dış IP adresleri:

XXXXXXXXX

3.YÖNETİCİ ÖZETİ

Bu rapor, Privia Security Şirketi tarafından PriviaHub FREYA-CLIENT-WHITE makinesi üzerindeki güvenlik açıklarını ortaya çıkartmak amacı ile 08.08.2020 - 12.08.2020 tarihleri arasında gerçekleştirilen sızma testleri (penetration test) ve güvenlik testleri çalışmalarının sonuçlarını içermektedir. Testler, raporun devamında detayları verilen web uygulama,etki alanı/sunucu-istemci sistemler, e-posta servisi, DNS servisi, veritabanı sistemleri ve DoS/DDoS kapsamında gerçekleştirilmiştir. Çalışmalar süresince dış/iç siber saldırgan gözüyle sistemler tüm detaylarıyla incelenmiş ve kurum yetkilisinin onayı dahilinde çıkan açıklıklar istismar edilerek sızma denemeleri gerçekleştirilmiştir. Çalışmalar sonucunda 2 düşük, , 4 orta olmak üzere toplamda 6 farklı güvenlik açıklığı tespit edilmiştir. Bir açıklığın birden fazla sistemde bulunması açıklık sayısını etkilememektedir. Açıklıklara ait yüzdeler ve grafikler takip eden sayfalarda verilmiştir.Sistemlere sızma denemelerinde tüm sistemleri ele geçirebilecek yetkiye sahip "root" haklarına erişilmiştir. Testler sonucu en büyük güvenlik eksikliği, çalışan sistemin güvenlik standartlarına ve prosedürlerine uygun olarak kurulmaması ve kurulumdan sonra gereken güvenlik sıkılaştırmalarının yapılmaması veya eksik yapılmasından kaynaklandığı belirlenmiştir. Bu sebeple her bir işletim sistemi, ağ cihazı ve diğer cihazlar için bir kurulum prosedürünün hazırlanması, bütün kurulumların yazılı prosedürlere uygun olarak yapılması ve ürün ortamına alınmadan önce mutlaka güvenlik taramasından geçirilmesi önerilmektedir. Raporda her bir açıklığın hangi sistemlerde bulunduğu, açıklıklar ile ilgili alınması gereken önlemler detaylı olarak açıklanmıştır.Sistem adına başarısız sonuçlanan testlerin sebebi olan güvenlik açıklıklarının kapatılması için gerekli çalışmalar yapılmalıdır. Açıklıkların kapatılmasında izlenecek sırayı belirlerken teknik raporda belirtilen açıklık önem dereceleri öncelikli rol oynamalıdır. Bu çalışmada Privia Security'yi tercih ettiğiniz için teşekkür ederiz.

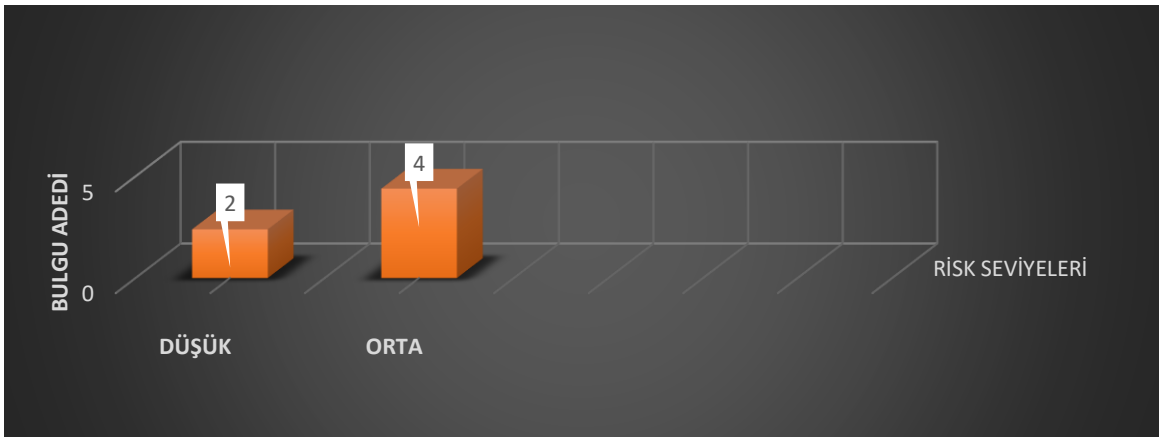
- **RİSK SEVİYELERİNE GÖRE GÜVENLİK AÇIKLIKLARININ DAĞILIMI**

---------KAPSAM----------	----------RİSK SEVİYESİ----------					
	ACİL	KRİTİK	YÜKSEK	ORTA	DÜŞÜK	TOPLAM
Web Uygulamaları				3		3
Sunucu İstemci Sistemleri				1	2	3
Toplam				4	2	6

- **BULUNAN GÜVENLİK ZAFİYETLERİNİN ÖZET TABLOSU**

Bulgu Adı	**Önem Derecesi**	**Bulgu Kategorisi**
Gezilebilir Web Dizinleri	Orta	Web
Çoklu Siteler Arası Script Çalıştırma(XSS)	Orta	Web
Clickjacking	Orta	Web
Zayıf SSH Algoritması	Orta	Sistem
Zayıf SSH MAC Algoritması	Düşük	Sistem
SSH Sunucu CBC Şifreleme	Düşük	Sistem

- **RİSK SEVİYELERİNE GÖRE GÜVENLİK AÇIKLIKLARININ DAĞILIMI**



4.GENEL SIZMA TESTİ METODOLOJİSİ

Günümüzde bilgi güvenliğini sağlamak için iki farklı yaklaşım sunulmaktadır. Bunlardan ilki savunmacı yaklaşım(defensive) diğeri de proaktif yaklaşım (offensive)olarak bilinir. Bunlardan daha yaygın olarak kabul göreni proaktif yaklaşımdır. Pentest –sızma testleri– ve vulnerability assessment –zayıflık tarama- konusu proaktif güvenliğin en önemli bileşenlerinden biridir. Pentest(sızma testleri) ve Vulnerability assessment(zayıflık tarama) birbirine benzeyen fakat farklı kavramlardır. Zayıflık tarama, hedef sistemdeki güvenlik açıklıklarının çeşitli yazılımlar kullanarak bulunması ve raporlanması işlemidir. Pentest çalışmalarında amaç sadece güvenlik açıklıklarını belirlemek değil, bu açıklıklar kullanılarak hedef sistemler üzerinde gerçekleştirilebilecek ek işlemlerin (sisteme sızma, veritabanı bilgilerine erişme) belirlenmesidir. Zayıflık tarama daha çok otomatize araçlar kullanılarak gerçekleştirilir ve kısa sürer. Pentest çalışmaları zayıflık tarama adımını da kapsayan ileri seviye tecrübe gerektiren bir süreçtir ve zayıflık tarama çalışmalarına göre çok daha uzun sürer.

"Security Assessment Framework" hazırlanırken konu hakkındaki uluslararası standartlar incelenmiş ve azami ölçüde faydalanılmıştır. Aşağıda bu belgenin hazırlanmasında kaynak olarak kullanılan dökümanların isimleri yer almaktadır.

• OWASP Testing Guide v3

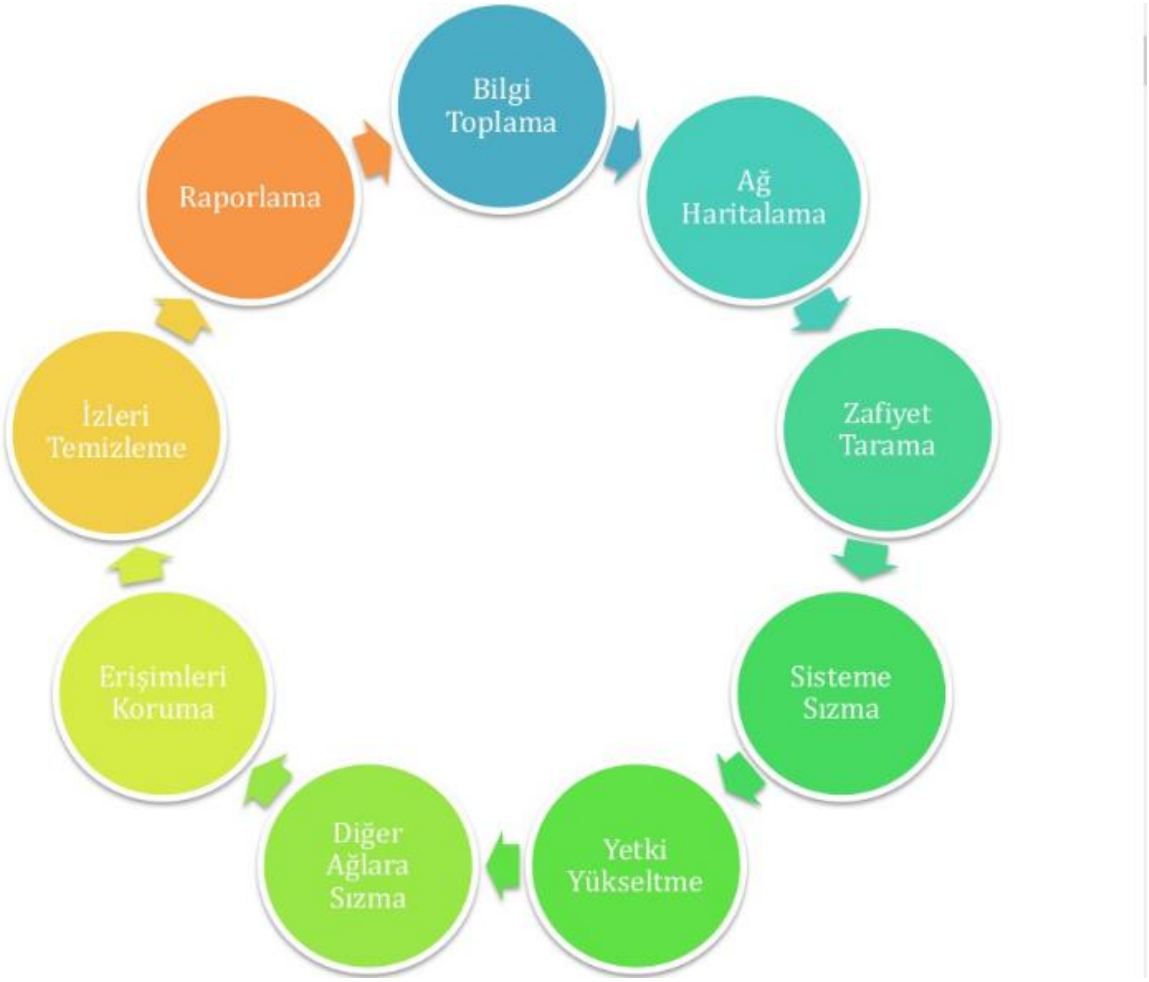
• OSSTM

• ISSAF

• NIST

Gerçekleştirilen testler uluslararası standart ve yönetmeliklere(HIPPA, Sarbanes-Oxley, Payment Card Industry (PCI), ISO 27001) tam uyumludur.

Sızma testlerinde ISSAF tarafından geliştirilen metodoloji temel alınmıştır. Metodolojimiz üç ana bölümde dokuz alt bölümden oluşmaktadır.



1.1.[BİLGİ TOPLAMA]

Amaç, hedef sistem hakkında olabildiğince detaylı bilgi toplamaktır. Bu bilgiler firma hakkında olabileceği gibi firma çalışanları hakkında da olabilir. Bunun için internet siteleri haber grupları e-posta listeleri, gazete haberleri vb., hedef sisteme gönderilecek çeşitli paketlerin analizi yardımcı olacaktır.

Bilgi toplama ilk ve en önemli adımlardan biridir. Zira yapılacak test bir zaman işidir ve ne kadar sağlıklı bilgi olursa o kadar kısa sürede sistemle ilgili detay çalışmalara geçilebilir. Bilgi toplama da aktif ve pasif olmak üzere ikiye ayrılır. Google, Pipl, Shodan, LinkedIn, Facebook gibi genele açık kaynaklar taranabileceği gibi hedefe özel çeşitli yazılımlar kullanılarak DNS, WEB, MAIL sistemlerine yönelik detaylı araştırmalar gerçekleştirilir. Bu konuda en iyi örneklerden biri hedef firmada çalışanlarından birine ait e-posta ve parolasının internete sızmış parola veritabanlarından birinden bulunması ve buradan VPN yapılarak tüm ağın ele geçirilmesi senaryosudur.

1.2. [AĞ HARİTALAMA]

Amaç hedef sistemin ağ yapısının detaylı belirlenmesidir. Açık sistemler ve üzerindeki açık portlar, servisler ve servislerin hangi yazılımın hangi sürümü olduğu bilgileri, ağ girişlerinde bulunan VPN, Firewall, IPS cihazlarının belirlenmesi, sunucu sistemler çalışan işletim sistemlerinin ve versiyonlarının belirlenmesi ve tüm bu bileşenler belirlendikten sonra hedef sisteme ait ağ haritasının çıkartılması ağ haritalama adımlarında yapılmaktadır. Ağ haritalama bir aktif bilgi toplama yöntemidir. Ağ haritalama esnasında hedef sistemde IPS, WAF ve benzeri savunma sistemlerinin olup olmadığı da belirlenmeli ve gerçekleştirilecek sızma testleri buna göre güncellenmelidir.

1.3. [ZAFİYET/ZAYIFLIK TARAMA SÜRECİ]

Bu sürecin amacı belirlenen hedef sistemlerdeki açıklıkların ortaya çıkarılmasıdır. Bunun için sunucu servislerdeki bannerler ilk aşamada kullanılabilir. Ek olarak birden fazla zayıflık tarama aracı ile bu sistemler ayrı ayrı taranarak oluşabilecek false positive oranı düşürülmeye çalışılır. Bu aşamada hedef sisteme zarar vermeycek taramalar gerçekleştirilir. Zayıflık tarama sonuçları mutlaka uzman gözler tarafından tekrar tekrar incelenmeli, olduğu gibi rapora yazılmamalıdır. Otomatize zafiyet tarama araçlar öntanımlı ayarlarıyla farklı portlarda çalışan servisleri tam olarak belirleyememktedir.

2.1 [PENETRASYON(SIZMA) SÜRECİ]

Belirlenen açıklıklar için POC kodları/araçları belirlenerek denelemeler başlatılır. Açıklık için uygun araç yoksa ve imkan varsa ve test için yeteri kadar zaman verilmişse sıfırdan yazılır. Genellikle bu tip araçların yazımı için Python, Ruby gibi betik dilleri tercih edilir. Bu adımda dikkat edilmesi gereken en önemli husus çalıştırılacak exploitlerden önce mutlaka yazılı onay alınması ve mümkünse lab ortamlarında önceden denenmesidir.

2.2 [ERİŞİM ELDE ETME VE HAK YÜKSELTME]

Sızma sürecinde amaç sisteme bir şekilde giriş hakkı elde etmektir. Bu süreçten sonra sistemdeki kullanıcının haklarının arttırılması hedeflenmelidir. Linux sistemlerde çekirdek (kernel) versiyonunun incelenerek priv. escelation zafiyetlerinin belirlenmesi ve varsa kullanılarak root haklarına erişilmesi en klasik hak yükseltme adımlarından biridir. Sistemdeki kullanıcıların ve haklarının belirlenmesi, parolasız kullanıcı hesaplarının belirlenmesi, parolaya sahip hesapların uygun araçlarla parolalarının bulunması bu adımın önemli bileşenlerindendir. Hak Yükseltme Amaç, ele geçirilen herhangi bir sistem hesabı ile tam yetkili bir kullanıcı moduna geçişttir.(root, administrator, system vs). Bunun için çeşitli exploitler denenebilir. Bu sürecin bir sonraki adıma katkısı da vardır. Bazı sistemlere sadece bazı yetkili makinelerden ulaşılabiliyor olabilir. Bunun için rhost, ssh dosyaları ve mümkünse history'den eski komutlara bakılarak nerelere ulaşılabiliyor detaylı belirlemek gerekir.

2.3. [DETAYLI ARAŞTIRMA]

Erişim yapılan sistemlerden şifreli kullanıcı bilgilerinin alınarak daha hızlı bir ortamda denenmesi. Sızılan sistemde sniffer çalıştırılabiliyorsa ana sisteme erişim yapan diğer kullanıcı/sistem bilgilerinin elde edilmesi. Sistemde bulunan çevresel değişkenler ve çeşitli network bilgilerinin kaydedilerek sonraki süreçlerde kullanılması.

3.1. [ERİŞİMLERİN KORUNMASI]

Sisteme girildiğinin başkaları tarafından belirlenmemesi için bazı önlemlerin alınmasında fayda vardır. Bunlar giriş loglarının silinmesi, çalıştırılan ek proseslerin saklı olması , dışarıya erişim açılacaksa gizli kanalların kullanılması(covert channel), backdoor, rootkit yerleştirilmesi vs.

3.2. [İZLERİN SİLİNMESİ]

Hedef sistemlere bırakılmış arka kapılar, test amaçlı scriptler, sızma testleri için eklenmiş tüm veriler not alınmalı ve test bitiminde silinmelidir.

3.3 [RAPORLAMA]

Raporlar bir testin müşteri açısından en önemli kısmıdır. Raporlar ne kadar açık ve detaylı/bilgilendirici olursa müşterinin riski değerlendirmesi ve açıklıkları gidermesi de o kadar kolay olur. Testler esnasında çıkan kritik güvenlik açıklıklarının belgelenerek sözlü olarak anında bildirilmesi test yapan takımın görevlerindendir. Bildirimin ardından açıklığın hızlıca giderilmei için çözüm önerilerinin de birlikte sunulması gerekir. Ayrıca raporların teknik, yönetim ve özet olmak üzere üç farklı şekilde hazırlanmasında fayda vardır. Teknik raporda hangi uygulama/araçların kullanıldığı, testin yapıldığı tarihler ve çalışma zamanı, bulunan açıklıkların detayları ve açıklıkların en hızlı ve kolay yoldan giderilmesini amaçlayan tavsiyeler bulunmalıdır.

5.TANIMLAR

Testlerin gerçekleştirildiği,

- Erişim Noktası : VPN ile sistemin iç ağına bağlanılmıştır.
- Kullanıcı Profili : PriviaHub sitesine kayıtlı kullanıcı hesabı ile sisteme bağlanılmıştır.

6.GERÇEKLEŞTİRİLEN GÜVENLİK TESTLERİ VE SONUÇLARI

Aşağıda gerçekleştirilen testler ve testlere ait çıktılara yer verilmiştir.

6.1.Web Uygulama Güvenlik Testleri

Web uygulamasına yönelik yapılan güvenlik testi işlemleri internet üzerinden vpn kullanılarak gerçekleştirilmiştir.Sunucular üzerinde çalışan servislerin ve işletim sisteminin bilinen açıklıklarının araştırılmasının yanında, sistemdeki uygulamalara has güvenlik açıklıkları da araştırılmıştır.

OWASP Test rehberinde sınıflandırılan test adımları sırasıyla uygulanmıştır.

1. Giriş ve Amaçlar

1.1. Kontrol Listesinin Test Edilmesi

2. Bilgi Toplama

2.1. Spiders, Robots and Crawlers (OWASP-IG-001)

2.2. Arama Motoruyla Keşif (OWASP-IG-002)

2.3. Uygulamaya Giriş Noktalarının Belirlenmesi (OWASP-IG-003)

2.4. Web Uygulaması Parmak İzinin Test Edilmesi(OWASP-IG-004)

2.5. Uygulama Keşfi (OWASP-IG-005)

2.6. Hata Kodlarının Analizi (OWASP-IG-006)

3. Yapılandırma Yönetim Testleri

3.1. SSL/TLS Testleri (SSL Versiyon, Algoritma, Anahtar Uzunluğu, Dijital Sertifika Geçerliliği) (OWASP-CM-001)

3.2. DB Listener Testi (OWASP-CM-002)

3.3. Altyapı Yapılandırma Yönetimi Testi (OWASP-CM-003)

3.4. Uygulama Yapılandırma Yönetimi Testi (OWASP-CM-004)

3.5. Dosya Uzantısı Yönetimi Testleri(OWASP-CM-005)

3.6. Yedek,Kopyaa,Test veya Eski Sürümlerden Kalma Sayfa Ve Uygulamaların Belirlenmesi(OWASP-CM-006)

3.7. Altyapı ve Uygulama Yönetici Arayüzleri(OWASP-CM-007)

3.8. Http metodları ve XST Testleri (OWASP-CM-008)

4. Kimlik Doğrulama Testleri

4.1. Hassas Bilgilerin şifreli/şifresiz Kanallardan Aktarımı (OWASP-AT-001)

4.2. Hedef Uygulama Üzerinde Kullanıcı Adı Belirleme/Doğrulama Çalışmaları(OWASP-AT-002)

4.3. Tahmin Edilebilir Kullanıcı Hesaplarının Test Edilmesi(OWASP-AT-003)

4.4. Hedef Uygulama Üzerinde Yetkili Kullanıcılara Yönelik Brute Force Parola Denemeleri (OWASP-AT-004)

4.5. Kimlik Doğrulama Aşamasını Atlatma Denemeleri (OWASP-AT-005)

4.6. Parola Hatırlatma ve Parola Sıfırlama Özelliklerinin Testleri (OWASP-AT-006)

4.7. Browser Önbellek Yönetimi ve 'Log out' Fonksiyonlarının Testleri (OWASP-AT-007)

4.8. CAPTCHA Güvenlik Testleri (OWASP-AT-008)

4.9. Çok Adımlı Hesap Doğrulama Testleri (OWASP-AT-009)

4.10.Race Conditions Testleri(OWASP-AT-010)

5. Oturum Yönetimi Testleri

5.1. Oturum Yönetimi Zayıflıkları, Oturum Yönetimi Bypass Testleri (OWASP-SM-001)

5.2. Detaylı Cookie Güvenlik Testleri (OWASP-SM-002)

5.3. Oturum Sabitleme Testleri (OWASP-SM-003)

5.4. Oturum Değerleri Tespit Saldırırları (OWASP-SM-004)

5.5. CSRF Testleri (OWASP-SM-005)

6.Yetkilendirme Testleri

6.1. Dizin Atlatma/Gezme Testleri (OWASP-AZ-001)

6.2. Yetkilendirme Atlatma Testleri (OWASP-AZ-002)

6.3. Yetki Yükseltimi Testleri (OWASP-AZ-003)

7. Mantığı Denetim Testleri(OWASP-BL-001)

7.1 Uygulamanın İşleyişinin Belirlenmesinden Sonra Uygulamanın İşleyişine Yönelik Teknik Olmayan Atakların Denenmesi

8.Veri Doğrulama Testleri

8.1. Yansıtılan XSS Testleri (OWASP-DV-001)

8.2. Depolanmış XSS Testleri (OWASP-DV-002)

8.3. DOM Tabanlı XSS Testleri (OWASP-DV-003)

8.4. XSF (Flash XSS) Testleri(OWASP-DV-004)

8.5. SQL Enjeksiyonu Testleri (OWASP-DV-005)

8.6. LDAP Enjeksiyonu Testleri (OWASP-DV-006)

8.7. ORM Enjeksiyonu Testleri (OWASP-DV-007)

8.8. XML Enjeksiyonu Testleri (OWASP-DV-008)

8.9. SSI Enjeksiyonu Testleri (OWASP-DV-009)

8.10. XPath Enjeksiyonu Testleri (OWASP-DV-010)

8.11. IMAP/SMTP Enjeksiyonu Testleri (OWASP-DV-011)

8.12. Kod Enjeksiyonu Testleri(OWASP-DV-012)

8.13. Komut Enjeksiyonu (OWASP-DV-013)

8.14. Bellek Taşması (Buffer overflow) Testleri (OWASP-DV-014)

8.15. Testing for incubated vulnerabilities (OWASP-DV-015)

8.16. HTTP Response Splitting Testleri (OWASP-DV-016)

9. Hizmet Dışı Bırakma Testleri

9.1. SQL Wildcard Üzerinden Dos Testleri (OWASP-DS-001)

9.2. Hesap Kitleme Politikasının Testi (OWASP-DS-002)

9.3. Buffer Overflow Dos Testleri (OWASP-DS-003)

9.4. Oturum Boyutu Arttırma Dos Testleri (OWASP-DS-004)

9.5. Bir Döngü Sayacı Olarak Kullanıcı Girişi Testleri (OWASP-DS-005)

9.6. Kullanıcı Tarafından Sağlanan Verileri Diske Yazma Testi (OWASP-DS-006)

9.7. Kaynakların Serbest Bırakılmasında DoS Başarısızlığı Testi (OWASP-DS-007)

9.8. Oturumda Çok Fazla Veri Saklamayı Test Etme (OWASP-DS-008)

4.10. Web Servisi Testleri

10.1. Web Servisi Bilgi Toplama(OWASP-WS-001)

10.2. WSDL Testleri (OWASP-WS-002)

10.3.XML Yapı Testleri (OWASP-WS-003)

10.4. XML Content-level Testleri (OWASP-WS-004)

10.5. HTTP GET parametreleri/REST Testleri (OWASP-WS-005)

10.6. Naughty SOAP Ekleri(OWASP-WS-006)

10.7. Replay Testleri (OWASP-WS-007)

11. AJAX Testleri

11.1. AJAX Zafiyetleri (OWASP-AJ-001)

12.Web Uygulama Güvenlik Sistemlerinin Testleri

12.1. Web Uygulama Güvenlik Duvarı Testleri

12.2. Network IPS Keşif Testleri

12.3. IPS/Web Uygulama Güvenlik Duvarı Testleri

6.1.1. Tespit Edilen Açıklıklar

6.1.1.1. Yansıtılan XSS testleri

Önem Derecesi : Orta

Açıklığın Etkisi : Yetkisiz Erişim, Bilgi İfşası

Erişim Noktası : Yerel Ağ

Kullanıcı Profili : Site Kullanıcısı

Bulgu Kategorisi : Web

Bulgu Sebebi : Uygulama Geliştirmede 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 browserini 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 veritabanında 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 payload'un, dönen sunucu cevabı içerisinde encode edilmeden döndürülmesi durumunda açığa çıkmaktadır. Bu durumda isteği yapan istemci tarafında enjekte edilen kod parçaçığı eylemini gerçekleştirecektir. Bu açıklık türü istismar edilerek client tarafında html, javascript, action script benzeri kod parçaçıkları sayfaya enjekte edilebilir. Kulanıcı kandırma veya cookie hırsızlığı gerçekleştirilebilir.

Açıklığı Barındıran Sistemler:

- **http://192.168.1.178/js/jquery.min.js**

Çözüm Önerileri:

- Halihazırda yüklü olan JQUERY 1.4.1 sürümü, 3.5.0 ve daha fazlasına yükseltilmelidir.

Referanslar:

- http://www.owasp.org/index.php/XSS
- http://www.cgisecurity.com/articles/xss-faq.shtml
- http://ha.ckers.org/xss.html

6.1.1.2. Gezilebilir Web Dizinleri

Önem Derecesi : Orta

Açıklığın Etkisi : Yetkisiz Erişim, Bilgi İfşası

Erişim Noktası : Yerel Ağ

Kullanıcı Profili : Site Kullanıcısı

Bulgu Kategorisi : Web

Bulgu Sebebi : Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması :

Dizin geçişi (dosya yolu geçişi olarak da bilinir), kötü niyetli kişilerin, bir uygulamayı çalıştıran sunucuda rastgele dosyaları okumasına olanak tanıyan bir web güvenlik açığıdır. Bu, uygulama kodunu ve verilerini, arka uç sistemleri için kimlik bilgilerini ve hassas işletim sistemi dosyalarını içerebilir. Bazı durumlarda, bir saldırgan sunucudaki rastgele dosyalara yazarak uygulama verilerini veya davranışını değiştirmelerine ve nihayetinde sunucunun tam kontrolünü ele geçirmelerine olanak sağlar.

Açıklığı Barındıran Sistemler:

- http://192.168.1.178/img/
- http://192.168.1.178/js/

Çözüm Önerileri:

Göz atılabilir dizinlerin gizli bilgileri sızdırmadığından veya hassas kaynaklara erişim sağlamadığından emin olunmalı.Erişim kısıtlamaları kullanılmalı, dizin indeksleme devre dışı bırakılmalıdır.

Referanslar:

- https://portswigger.net/

6.1.1.3. Clickjacking

Önem Derecesi : Orta

Açıklığın Etkisi : Yetkisiz Erişim, Bilgi İfşası

Erişim Noktası : Yerel Ağ

Kullanıcı Profili : Site Kullanıcısı

Bulgu Kategorisi : Web

Bulgu Sebebi : Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması :

Clickjacking, kötü niyetli kişilerin, kullanıcının bilgisayarını manipüle etmesine izin vermek için uygulamalarda ve web sayfalarında bulunan güvenlik açıklarından yararlanır.Örneğin, clickjack edilmiş bir sayfa, kullanıcıyı gizli bir bağlantıya tıklayarak istenmeyen eylemler gerçekleştirmesi için kandırır. Böyle bir sayfada kötü niyetli kişiler, şeffaf bir katmanda üzerine başka bir sayfa yükler. Şüphelenmeyen kullanıcılar, aslında görünmez sayfada eylemler gerçekleştirirken görünür düğmelere tıkladıklarını düşünürler. Gizli sayfa gerçek bir sayfa olabilir; bu nedenle kötü niyetli kişiler, kullanıcıları asla amaçlamadıkları eylemleri gerçekleştirmeleri için kandırabilir. Bu tür eylemleri daha sonra kötü niyetli kişiler için izlemenin bir yolu yoktur, çünkü kullanıcıların kimliği gizli sayfada gerçekten doğrulanmış olacaktır

Çözüm Önerisi :

X-Frame-Options veya Content-Security-Policy ('frame-ancestors' ile) HTTP başlığı sayfanın yanıtıyla birlikte döndürülmelidir.

Bu, frame veya iframe HTML etiketleri kullanılırken sayfanın içeriğinin başka bir site tarafından oluşturulmasını engeller.

Referanslar :

- https://en.wikipedia.org/

6.2. Sunucu İstemci Sistemleri Güvenlik Testleri

6.2.1. Tespit Edilen Açıklıklar

6.2.1.1.Zayıf SSH MAC Algoritması

Önem Derecesi : Düşük

Açıklığın Etkisi : Yetkisiz Erişim, Bilgi İfşası

Erişim Noktası : Yerel Ağ

Kullanıcı Profili : Site Kullanıcısı

Bulgu Kategorisi : Sistem

Bulgu Sebebi : Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması :

Güvenli Kabuk (SSH), verilerin alışverişine izin vermek için ağa bağlı iki cihaz arasında güvenli bir kanal oluşturan bir ağ protokolüdür. SSH sunucusu, Cipher Block Chaining (CBC) şifrelemesini destekleyecek şekilde yapılandırılmıştır. SSH, CBC modu şifrelemesini kullanarak bu güvenli kanalı oluşturabilir. Bu mod, her bloğun bir sonraki bloğun şifrelemesini değiştirmek için kullanılmasını sağlayacak şekilde çalışan bir blok şifresine bir geri bildirim mekanizması ekler.

Fakat bu şifreleme güvenlik açığı içermektedir. Bu güvenlik açığından yararlanan saldırılar, SSH oturumunun kaybedilmesine yol açacar.Kötü niyetli kişiler şifreli metinden şifresiz metin mesajını elde edebilir.

Çözüm Önerisi:

Bu güvenlik açığını azaltmak için SSH, CBC modu yerine CTR modunu kullanacak şekilde ayarlanabilir.

Referanslar:

- https://www.tenable.com/
- https://www.kb.cert.org/

6.2.1.2 Zayıf SSH Algoritması

Önem Derecesi : Orta

Açıklığın Etkisi : Yetkisiz Erişim, Bilgi İfşası

Erişim Noktası : Yerel Ağ

Kullanıcı Profili : Site Kullanıcısı

Bulgu Kategorisi : Sistem

Bulgu Sebebi : Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması :

Uzak SSH sunucusu, zayıf şifreleme algoritmalarına izin verecek şekilde yapılandırılır.SSH mesajlarında, kötü niyetli kişilerin şifreli bir metin bloğundan düz metin elde etmesine olanak verebilecek CBC modunu kullanan bir güvenlik açığı bulundurur.Bu açıklıkta yer alan "Arcfour" şifresi, 128-bit anahtarlara sahip bir şifredir, zayıf anahtar sorunlarına neden olur, gizlilik koruması sağlamadığı için artık kullanılması tavsiye edilmez.

Çözüm Önerisi:

Zayıf şifreleme kaldırılmalıdır.

Referanslar:

- https://www.tenable.com/

6.2.1.3. SSH Server CBC Mode Şifreleme

Önem Derecesi : Düşük

Açıklığın Etkisi : Yetkisiz Erişim, Bilgi İfşası

Erişim Noktası : Yerel Ağ

Kullanıcı Profili : Site Kullanıcısı

Bulgu Kategorisi : Sistem

Bulgu Sebebi : Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması :

SSH sunucusu, Cipher Block Chaining (CBC) şifrelemesini destekleyecek şekilde yapılandırılmıştır. Bu, kötü niyetli kişilerin şifreli metin mesajını şifresiz şekilde elde etmesine izin verebilir.

Çözüm Önerisi:

Bu güvenlik açığını azaltmak için SSH, CBC modu yerine CTR modunu kullanacak şekilde ayarlanabilir.

Referanslar :

- https://www.tenable.com

EK – 1 : Raporda Geçen Teknik Terimler ve Kısaltmalar

.....

.....

EK – 2 : Güvenlik Testleri Esnasında Kullanılan Araçlar

- **NMAP**
- **METASPLOIT FRAMEWORK**
- **NESSUS**
- **BURP SUİTE**
- **MSFVENOM**

EK – 3 : REFERANSLAR

- **https://www.bgasecurity.com/makale/ornek-sizma-testleri-sonuc-raporu/**