BİLİSHİM SİBER GÜVENLİK VE YAPAY ZEKÂ

SIZMA TESTİ METODOLOJİSİ

Hazırlayan: Meftun Göktepe

PENETRASYON TESTİ NEDİR?

Kısaca PenTest olarak bilinen Penetrasyon Testi temel olarak bir bilişim sisteminin tüm yapı taşlarının olası siber saldırılara karşı, taranması, analiz edilmesi, sızılması ve sıkılaştırmasını kapsayan ileri mühendislik isteyen özel bir test sürecidir.

Test sırasında uzmanlar tıpkı bir saldırgan gibi hareket eder ve sistemin tüm açıklarını, riskleri ve erişilebilirliği ortaya çıkarırlar. Çok farklı yöntemler ve değişkenler söz konusu olduğundan sızma testinin uzmanlar tarafından gerçekleştirilmesi gerekmektedir.

PENETRASYON TESTİ NEDEN ÖNEMLİDİR

PenTest'in nihai amacı, bir saldırgan gözüyle sistem altyapınızın ne kadar güvende olduğunu ortaya koymak ve açıklık bulunan noktaları kapatmaktır. Bir kuruluşun güvenlik duruşundaki zayıf noktaları tespit etmenin yanı sıra, güvenlik politikasının uygunluğunu ölçmek, personelin güvenlik sorunları konusundaki farkındalığını test etmek ve kuruluşun siber güvenlik prensiplerini uygulama derecesini belirlemektir. Unutulmaması gereken en temel husus, tüm sistemlerin sadırıya karşı hassas olduğudur. Hiçbir sistem 100% güvende değildir. Bu nedenlerden dolayı kuruluşların sistemlerini düzenli olarak

PenTest yaptırması ve işletim sistemi ile uygulamalara zamanında güvenlik yamalarını geçmesi çok önemlidir.

Penetrasyon Testleri temel de üç aşamaya ayrılır

Siyah Kutu: Bu yöntemde pentest gerçekleştirilecek kurumdan herhangi bir bilgi talebinde bulunulmaz, yapılan çalışmalar ile tamamı ile manuel gerçekleştirilen yöntemler sayesinde kurumun internete açık olan veya olmayan ara yüzlerinden sisteme sızılması çalışması gerçekleştirilir. Bu sayede kurumun dışarıdan alabileceği tehditlerin genel analizi ve vektörleri çıkarışmış olur.

Kara Kutu yöntemi, dışarıdan gelen gerçek bir saldırı senaryosuna en yakın test yöntemidir. En büyük amaç hedef sistemde veri tabanına sızmaktır.

Gri Kutu: Gerçekleştirilen bu test sayesinde kurumun içerisinde herhangi bir misafir gibi gelinerek sistemin boşluklarından faydalanıp sistemin tehlike yüzeyi analiz edilir. Bu sayede saldırganın kurumun içerisinden mevcut sisteme geçişi, veri tabanlarına erişimi, uygulamalar üzerinden ki hâkimiyetine kadar pek çok süreç bu test sayesinde ele alınır.

Gri Kutu yöntemi, fiziksel olarak kurum içine girebilen bir hacker tarafından yapılacak saldırının ne oranda başarılı olabileceğini ortaya koyar. En büyük amaç sınırlı bir yetkiyle dahi olsa tüm sistemi ele geçirmektir.

Beyaz Kutu: Güvenlik uzmanı, bu test ile birlikte testin yapıldığı kurumdan standart bir kullanıcıya ait bir tanımlama ister bu sayede uzman standart bir kullanıcı olarak sistem üzerinde haklarını artırıp artırmadığı, veri tabanlarına ve diğer tüm bilişim alt yapısı üzerinde ki hâkimiyeti kontrol edilir. Bu testler esnasında çeşitli araçlar kullanıldığı gibi sistemin saldırganı yakalamaması için gerekli tekniklerinde içinde bulunduğu özel manuel yöntemler kullanılır.

Beyaz Kutu yöntemi, kuruma içten gelecek bir saldırının ne oranda etkili olabileceğini ortaya koyar.

Sızma testlerinde özellikle gri aşamada sistemlerinden en az birine sızamadığımız hiçbir kurum/firma neredeyse olmamıştır.

PENETRASYON TESTİ AŞAMALARI:

Penetrasyon Testi, belli bir sistematik yaklaşım ile icra edilen bir süreçtir. Bilishim Siber Güvenlik ve Yapay Zeka tarafından kullanılan Sızma Testi/Güvenlik Testi bu alanda tüm dünya tarafından kabuledilmiş **OSSTMM (Open Source Security Testing Methodology Manual) v3 Open Source Security Testing Methodology Manual, OWASP (Open Web Application Security Project) Testing Guide 4.0** ve **NIST 800-115 (National Institute of Standards and Technology - Technical Guide to Information Security Testing and Assessment)** metodolojilerini esas almaktadır.

1. **Pasif Bilgi Toplama (İz Sürme):**

Ele alınacak sistemler ve kullanılacak test yöntemleri dahil olmak üzere, testin kapsamını ve hedefler tanımlanır.

Bu aşama, hedef sistem altyapısı ve kapsamı dâhilindeki etki alanı adları, ağ blokları, yönlendiriciler, IP adresleri gibi bilgiler ile çalışan bilgileri, telefon numaraları gibi saldırının başarısına katkı sağlayacak her türlü ayrıntı hakkında bilgi sahibi olunmasını sağlayan adımdır.

Açık kaynaklardan toplanan bu bilgiler birçok defa şaşırtıcı derecede kritik bilgileri içerebilmektedir. Bu maksatla başta hedef kurumun web sitesi ve sosyal medya platformları olmak üzere birçok kaynaktan istifade edilmektedir.

2. Aktif Bilgi Toplama ve Tarama:

Tespit edilen IP aralığı içinden hangi aktif ve pasif cihazların canlı olduğu tespit edilen bu aşamada, birinci aşamada elde edilen bilgilerin de yardımıyla önceliklendirme yapmak mümkündür.

Bu aşamada, tespit edilmiş olan canlı sistemlerde çalışan işletim sistemi, açık portlar ve servisler ile bunların sürüm bilgilerini elde etmek önemlidir.

Ayrıca dinlenebiliyorsa ağ trafiği de takip edilerek sistem altyapısı hakkında mümkün oldukça kritik bilgi toplanmaya çalışılır.

3. Döküm Çıkarma:

Hedef uygulamanın çeşitli izinsiz giriş denemelerine nasıl cevap vereceğini anladıktan sonra bu adımda, canlı olduğu tespit edilen sistemlerle aktif bağlantılar kurulur ve doğrudan sorgulamalar yapılır.

Diğer bir ifadeyle bu aşama; ftp, netcat, telnet gibi servislerin etkin olarak kullanıldığı ve hedef sistemlerle etkileşime geçildiği aşamadır.

4. Sistemi Ele Geçirme

Daha önceki aşamalarda elde edilen tüm bilgilerin tek bir amacı vardır. Hedef sisteme yetkisiz giriş sağlamak, veri tabanını okumak ya da ulaşılmaması gereken bilgilere erişmek.

Bu aşama; hedef sistem üzerinde çalışan işletim sistemi, açık olan portlar ve bu portlarda hizmet veren servisler ile bunların sürümleri ışığında uygulanabilecek sömürü yöntemlerinin denendiği ve içeriye sızılmaya çalışıldığı adımdır.

Özellikle web tabanlı portal ve uygulamalar, hem dışa bakan pencere olmaları, hem çok fazla saldırı vektörü barındırabilme özelliklerinden dolayı özel bir konuma sahiptirler.

Sistemi ele geçirme aşamasında mevcut sömürü yöntemlerini sisteme zarar vermeden, iz bırakmadan, başarılı ve esnek bir şekilde kullanabilmek ciddi bir uzmanlık ve deneyim gerektirmektedir. PenTest'in bu aşaması bu nedenle en önemli ve kritik adımdır.

5. Yetki Yükseltme

Bir sistem, sistemin en zayıf halkası kadar güçlüdür. Bir şekilde başarılan sistem erişimi genelde ilk adımda düşük bir yetki ile gerçekleşmektedir. PenTest uzmanı, bu aşamada, bulunduğu işletim sistemi ya da ortamdaki zafiyetlerden istifadeyle yetkisini yönetici seviyesine çıkarmayı, ardından, kazandığı bu ek

yetkiler ile birlikte ağ ortamında bulunan diğer cihazları ve nihayetinde Etki Alanı Yöneticisi ya da Veri Tabanı Yöneticisi gibi en üst düzey kullanıcı yetkilerini ele geçirmeyi hedefler.

PENETRASYON TESTİ HİZMETİ VE SONRASI:

Penetrasyon testi neticesinde firmamız tarafından hedef sistemlerde tespit edilen güvenlik açıklıkları ve bu zafiyetlerin nasıl istismar edildiği örnek ekran çıktılarıyla birlikte sunulan "Sızma Testi Sonuç Raporu"nda yer alır. Sonuç raporunda ayrıca her bir açıklığın nasıl kapatılacağına dair çözüm önerisi de yer almaktadır.

Bir siber güvenlik firması olarak; yapmakta olduğumuz sızma testlerinin hassasiyeti, bağımsızlığı ve sıhhati açısından özellikle ürün satmıyoruz. Ancak talep edilirse sistemlerin daha güvenli olmasına yönelik güvenli ağ kurulum ve tasarımı danışmanlığı hizmetini ayrıca vermekteyiz.

Referanslar:

1. OSSTMM (Open Source Security Testing Methodology Manual) v3 Open Source Security Testing Methodology Manual
2. OWASP (Open Web Application Security Project) Testing Guide 4.0
3. NIST 800-115 (National lnstitute of Standards and Technology - Technical Guide to Information Security Testing and Assessment)

SIZMA TESTİ TEST KILAVUZU KONTROL LİSTESİ

DoS/DDOS Güvenlik Testleri	Test Adı	Sonuç	Notlar
BST-DOS-001	SYN Flood		
BST-DOS-002	TCP Connection Flood		
BST-DOS-003	ACK/FIN Flood		
BST-DOS-004	UDP Flood		
BST-DOS-005	ICMP Flood		
BST-DOS-006	DNS Flood		
BST-DOS-007	HTTP GET/POST Flood		
BST-DOS-008	SSL/HTTPS Connection Flood		
BST-DOS-009	HTTP Slowloris		
BST-DOS-010	Bant Genişliği Taşırma		
BST-DOS-011	ARP zehirlenmesi		
BST-DOS-012	CDP Spoofing		
BST-DOS-013	DHCP DoS		
BST-DOS-014	SNMP DoS		
BST-DOS-015	Botnet simulasyonu		
BST-DOS-016	Rate Limiting		
BST-DOS-017	Kullanılan Yazılım/Sistemlere Özel DoS/DDoS Testleri		

Ağ Cihazları Güvenlik Testleri	Test Adı	Sonuç	Notlar
BST-NET-001	MAC adresi tabanlı filtreleme tespiti		
BST-NET-002	Port güvenliği, VLAN ve trunk yapısı tespiti		
BST-NET-003	Kimlik doğrulama servislerine (Telnet, SSH, FTP, TFTP, SNMP, HTTP) yönelik ön tanımlı/kaba kuvvet parola testleri		

BST-NET-004	Elde ediler parola hash değerlerinin kırılması		
BST-NET-005	Uzak/yerel erişim kontrolü, kayıt ve kimlik doğrulama mekanizmaları erişim testleri		
BST-NET-006	SNMP üzerinden hassas veri ifşası		
BST -NET-007	SNMP community string testleri		
BST-NET-008	Cihazda çalışan yazılım sürümüne ait çıkmış güvenlik zafiyetlerinin araştırılması ve istismar denemeleri		
BST-NET-009	Ortadaki adam (Man in the middle -MITM) testleri		
BST-NET-010	Ağ cihazları yönetim sistemlerine içeriden/dışarıdan erişim ve istismar		
BST-NET-011	İçerik Filtreleme sistemleri atlatma		
BST-NET-012	Tünelleme ile istismar		

Parola Kırma Testleri	**Test Adı**	**Sonuç**	**Notlar**
BST-PASS-001	Hash/Şifreleme tipinin Belirlenmesi		
BST-PASS-002	LM HASH kullaniminin aktif olup olmadiginin kontrolu		
BST-PASS-003	Bilinen sözlükler kullanarak parola denemeleri		
BST-PASS-004	İnternet üzerinden hash araştırılması		
BST-PASS-005	Kaba kuvvet parola (brute force) testleri		
BST-PASS-006	Parola kırma testleri		
BST-PASS-007	Sözlük listesi oluşturma		

DNS Sunucusu Güvenlik Testleri	**Test Adı**	**Sonuç**	**Notlar**
BST-DNS-001	DNS için ilgili portların (UDP/53, TCP/53) kontrol edilmesi		
BST-DNS-002	DNS sunucu yazılım sürüm bilgilerinin belirlenmesi		
BST-DNS-003	DNS sunucu yazılımında bulunan güvenlik zafiyetlerinin belirlenmesi		
BST-DNS-004	DNS Zone transferine açık olup olmadığının belirlenmesi		
BST-DNS-005	DNS sunucuda kayıtlı alan adlarının belirlenmesi		
BST-DNS-006	Kaynak ve ters kaynak DNS hizmeti (recursive DNS) kayıt girdilerinin belirlenmesi		

BST-DNS-007	DNS sunucunun "." isteklerine cevap verip vermediğinin belirlenmesi		
BST-DNS-008	Alt domain keşfi için kaba kuvvet denemelerinin gerçekleştirilmesi		
BST-DNS-009	Arama motorları kullanarak alt domain keşfi		
BST-DNS-010	DNS ön bellek zehirlenmesi testleri		
BST-DNS-011	DNS cache snooping testleri		
BST-DNS-012	NXT, HINFO ve NSEC kayıtlarından bilgi ifşası kontrolü		
BST-DNS-013	DNS sunucuya yönelik tam kapsamlı Nettarsier/Nessus taraması		
BST-DNS-014	DNSSEC ve EDNS0 desteği olup olmadığının tespiti		

Eposta Servisi Güvenlik Testleri	**Test Adı**	**Sonuç**	**Notlar**
BST-MAIL-001	SMTP versiyon belirleme		
BST-MAIL-002	Eposta sistemine yönelik zafiyetlerin kontrolü		
BST-MAIL-003	Belirli eposta adreslerinin sistemde olup olmadığınırı belirlenmesi		
BST-MAIL-004	MX kaydı olmayan alar adlarından eposta kabul kontrolü		
BST-MAIL-005	Firma içinden geliyormuş gibi eposta gönderim testi		
BST-MAIL-006	MTA eposta geçirme (Open Relay) testleri		
BST-MAIL-007	Çeşitli zararlı yazılım içeren pdf/exe/ofis belgelerinin eposta ile gönderilerek AV atlatma testleri		
BST-MAIL-008	Eposta filtreleme sistemlerini şifreli veri gönderilerek atlatma testleri		
BST-MAIL-009	SPF kaydı olmayan adreslerden eposta kabul etme kontrolü		
BST-MAIL-010	SMTP üzerinden iç ağ ve DMZ IP yapılandırması IP keşif çalışması		
BST-MAIL-011	SMTP kimlik doğrulama testleri		
BST-MAIL-012	EKPN ve VRFY desteği kontrolü, sistem kullanıcısı tespiti		
BST-MAIL-013	POP ve IMAP servislerine yönelik kaba kuvvet denemeleri		
BST-MAIL-014	Eposta harici başka servislerin açık olup olmadığının testleri		
BST-MAIL-015	İşletim sistemine yönelik güvenlik zafiyet taraması		

BST-MAIL-016	Eposta DoS testi amaçlı büyük boyutlu dosyaların gönderilmesi		
BST-MAIL-017	Tek kayna ktarı yüklü sayıda e-posta gönderimi (DoS)		
BST-MAIL-018	Zip bomb gönderilerek Antivirus yazılımının kontrolü (DoS)		
BST-MAIL-019	SMTP ve POP/IMAP Portları için Heartbleed açıklık kortrolü		

İç Ağ Güvenlik Testleri	Test Adı	Sonuç	Notlar
BST-LAN-001	Nmap ile aktif (up) sistemlerin belirlenmesi		
BST-LAN-002	Aktif (up) sistemlerin Nettarsier/Nessus ile taranması		
BST-LAN-003	Nmap ile tüm portların taramanması (Farklı portlarda çalışanı uygulamaların belirlenmesi)		
BST-LAN-004	Yerel ağ uygulama ve servis sürüm bilgilerinin haritasının çıkartılması		
BST-LAN-005	Belirlenen servis sürümlerinde güvenlik zafiyeti ve exploit aranması		
BST-LAN-006	Nmap ile SYN proxy arkasındaki sistemlere port tarama		
BST-LAN-007	Nmap ile kimlik doğrulama gerektirmeyen telnet servislerinin tespiti		
BST-LAN-008	Genele açık dosya paylaşımlarının SMB üzerinden kontrolü		
BST-LAN-009	Genele açık dosya paylaşımlarının NFS üzerinden kontrolü		
BST-LAN-010	Tüm iç ağda Anonim FTP hesaplarının bulunması ve incelenmesi		
BST-LAN-011	Kimlik doğrulama gerektiren top 10 servisin bulunması		
BST-LAN-012	Yerel ağda kullarıları yazılım ve donarımlarını tespiti		
BST-LAN-013	İlgili uygulamalara ait ön tanımlı hesap bilgilerinin denenmesi		
BST-LAN-014	Kimlik doğrulama gerektiren servislere yönelik parola bulma denemeleri		
BST-LAN-015	Ortadaki Adam (Man in The Middle-MITM) Testleri		
BST-LAN-016	MITM-ARP Cache poisoning testleri		
BST-LAN-017	MITM-DHCP Spoofing testleri		
BST-LAN-018	MITM-ICMP Redirect testleri		
BST-LAN-019	Local Admin parolası aynı olan sistemlerin bulunması (Pass The Hash)		

BST-LAN-020	Belirleneri kritik açık port ve servislerin manuel incelenmesi		
BST-LAN-021	Belirlenen SNMP açık sistemlerden bilgi toplarıması		
BST-LAN-022	IP spoofing, MAC spoofing testleri (NAC Testleri)		
BST-LAN-023	NAC çözümü atlatma testleri		
BST-LAN-024	MAC flooding kullanarak DoS testi denemesi		
BST-LAN-025	İç ağdaki web arabirimlerine aitekran görüntüsünün alınması		
BST-LAN-026	LAN-DMIZ, DMZ-LAN, WiFi-LAN arası yetkisiz geçiş testleri		
BST-LAN-027	VLAN Hopping testleri		

Dış Ağ Güvenlik Testleri	**Test Adı**	**Sonuç**	**Notlar**
BST-INTRNT-001	Whois ile IP bloklarının bulunması		
BST-INTRNT-002	Tam kapsamlı Port Tarama		
BST-INTRNT-003	Syrcookle/SynProxy koruma tespiti		
BST-INTRNT-004	Kimlik doğrulama isteyen ağ servislerinin belirlenmesi		
BST-INTRNT-005	Shodan,Bing, Robtex üzerinden bilgi toplama		
BST-INTRNT-006	DNS ve Google aracılığı ile açık sunucu ve cihazların belirlenmesi		
BST-INTRNT-007	Firmaya ait subnetlerin tespiti ve incelenmesi		
BST-INTRNT-008	VPN servislerinin tespiti ve zafiyet denetimi		
BST-INTRNT-009	Aktif IDS/IPS tespiti		
BST-INTRNT-010	Kuruma aitanahtar kelimelerin Pastebin sitesinde arattırılması		

Güvenlik Sistemleri Güvenlik testleri	**Test Adı**	**Sonuç**	**Notlar**
BST-NETSEC-001	Hedef sistem önünde WAF çalışıp çalışmadığını belirleme		
BST-NETSEC-002	Hedef sistem önünde IPS çalışıp çalışmadığını belirleme		
BST-NETSEC-003	Hedef sistem önünde güvenlik duvarı çalışıp çalışmadığını belirleme		

BST-NETSEC-004	Hedef sistem önünde DDoS engelleme sistemi çalışıp çalışmadığını belirleme		
BST-NETSEC-005	IPS/WAF statefull çalışıp çalışmadığının testi (Inline IPS/WAF)		
BST-NETSEC-006	Dışardarı WAF'ı SSL ile atlatma testleri		
BST-NETSEC-007	IPS'i SSL üzerinden atlatma testleri		
BST-NETSEC-008	İçerden Guvenlik duvarı atlatma testleri		
BST-NETSEC-009	İçerden içerik filtreleme, IPS atlatma testleri		
BST-NETSEC-010	İçerden dışarı doğru yapılan testler (Tünelleme)		
BST-NETSEC-011	SSH Tünelleme testleri		
BST-NETSEC-012	DNS Tünelleme testleri		
BST-NETSEC-013	HTTP Tünelleme testleri		
BST-NETSEC-014	Güvenlik duvarının FIN, ACK, PUSH gibi oturum kurulmamış TCP bayraklı paketlere cevap testleri		
BST-NETSEC-015	TTL değerleri kullanarak aradaki cihazların (koruma amaclı L3) belirlenmesi		
BST-NETSEC-016	Rate limiting uygulamasının belirlenmesi		
BST-NETSEC-017	Rate limitirg sonucuna göre istenilen IP adresinin engelletirilmeye çalışılması		
BST-NETSEC-018	SSL inceleme yapılıp yapılmadığının belirlenmesi		
BST-NETSEC-019	Parçalanmış paketlerle IPS/WAF atlatma denemesi		
BST-NETSEC-020	Encoding (Web için) yöntemleriyle atlatma denemesi		
BST-NETSEC-021	DLP testleri		
BST-NETSEC-022	Eposta ağgeçidi testleri		
BST-NETSEC-023	Güvenlik duvarı atlatma testleri		
BST-NETSEC-024	VPN testleri		

VOIP Sistemleri Güvenlik Testleri	Test Adı	Sonuç	Notlar
BST-VOIP-001	VolP sistem keşfi		
BST-VOIP-002	Paket dinlemesi yoluyla ağ üzerinden geçen VoIP paketlerinin yakalanması		
BST-VOIP-003	Kimlik doğrulama bilgilerini ele geçirme		

BST-VOIP-004	Arama sahteciliği (CallerID spoofing) testleri		
BST-VOIP-005	Ortadaki Adam (MITM) testleri		
BST-VOIP-006	VoIP Sistemlere yönelik zafiyetlerin istismarı (Exploitation)		
BST-VOIP-007	VoIP Sistemlere yönelik DoS testleri		

Etki Alanı ve Kullanıcı Bilgisayarları Güvenlik Testleri	**Test Adı**	**Sonuç**	**Notlar**
BST-DOM-001	Kullanıcı bilgisayarlarının açılış ayarlarındaki eksiklilerin tespit edilerek hak yükseltme testleri		
BST-DOM-002	Sistem açılışında BİOS koruması ve disk şifreleme kontrolü		
BST-DOM-003	Yerel yöneticilerin kullanımındaki zafiyetlerin tespit edilerek hak yükseltme testleri		
BST-DOM-004	Güvenlik yama eksikliği kontrolü		
BST-DOM-005	Desteği kaldırılmış eski sistemlerin tespiti ve uzaktan kod çalıştırma/hak yükseltme testleri		
BST-DOM-006	Disk üzerinde ve paylaşım alanlarında hassas veri arama		
BST-DOM-007	Bellek üzerinden parola HASH değerlerinin elde edilmesi		
BST-DOM-008	Bellek üzerinden parola açık değerlerinin elde edilmesi		
BST-DOM-009	Offline olarak disk üzerinden parola hash değerlerinin alınması		
BST-DOM-010	Açılış dosyalarının bulunduğu ortak alanın incelenmesi		
BST-DOM-011	Etki alanındaki şifre politikası ve şifre saklama politikası ve zafiyetlerin tespiti		
BST-DOM-012	Etki alanı ortak parola kullanımı kontrolü		
BST-DOM-013	Eki alanı hesap şifreleri ele geçirme testleri		
BST-DOM-014	Etki alanı yönetici hesaplarının tespiti ve hak yükseltme testleri		
BST-DOM-015	Sisteme psexec üzerinden ajan yazılım yükleme testleri		
BST-DOM-016	Linux kernel hak yükseltme testleri		
BST-DOM-017	SSH üzerinderi brute force denmesi		
BST-DOM-018	Sudo kullanarak root yetkilerine geçiş denemeleri		
BST-DOM-019	777 izinli dosyalarını bulunması		

BST-DOM-020	History dosyalarının araştırılması(.bash/.mysgl)		
BST-DOM-021	Çalışanı proseslerden hassas veri ifşası testi (lsof, ps)		
BST-DOM-022	SSH anahtar dosyalarının izin kontrolü ve ifşası		
BST-DOM-023	Yapılandırma dosyalarında hassas veri arama		

Web Uygulama Güvenlik testleri	Test Adı	Sonuç	Notlar
BST-WEB-001	İlgili domainlere ait whois kayıtlarının incelenmesi		
BST-WEB-002	Ayrı IP adresi üzerindeki web sitelerinin belirlenmesi		
BST-WEB-003	Subdomain tespiti		
BST-WEB-004	Web, uygulama ve veritabanı sunucularının sistem bileşenleri hakkındaki kritik bilgiler (sunucu adı ve sürümü, kullanılan program sürümü vb.) belirleme.		
BST-WEB-005	Uygulamada oluşan hatalar ve uygulama sunucusu ön tanımlı hata mesajlarının detaylı olarak belirlenmesi		
BST-WEB-006	Dosya, dizin listeleme testleri		
BST-WEB-007	Dosya, dizinlerin bulunmasına yönelik kaba kuvvet testleri		
BST-WEB-008	Arama motorları üzerinden bilgi toplama		
BST-WEB-009	Robots.txt dosyası kullanarak hassas dizinlerin belirlenmesi		
BST-WEB-010	Bilinen web yazılımlarına ait imza taraması		
BST-WEB-011	İç ağ IP adres yapısı hakkında bilgi toplama		
BST-WEB-012	SSL/TLS versiyon, algoritma ve sertifika geçerlilik testleri		
BST-WEB-013	SSL zafiyet testleri (Heartbleed vs)		
BST-WEB-014	Hedef uygulamada kullanılan yönetim panelinin belirlenmesi		
BST-WEB-015	Dosya uzantısı yönetimi testleri		
BST-WEB-016	Yedek, kopya, test veya eski sürümlerden kalma sayfa ve uygulamalarını belirlenmesi		
BST-WEB-017	Web arka kapı kontrol testleri		
BST-WEB-018	Sunucu tarafındarı desteklenen metodların ve XST belirlenmesi		

BST-WEB-019	Hassas bilgilerin HTTPS üzerinden aktarımı kortrolü		
BST-WEB-020	Hedef uygulama üzerinde kullanıcı adı belirleme/doğrulama testleri		
BST-WEB-021	Hedef uygulama üzerinde yetkili kullanıcılara yönelik kaba kuvvet parola testleri		
BST-WEB-022	Kimlik doğrulama aşamasını atlatma testleri		
BST-WEB-023	Parola hatırlatma ve parola sıfırlama özelliklerinin testleri		
BST-WEB-024	Browser ön bellek yönetimi ve “Log out” fonksiyonlarının testleri		
BST-WEB-025	CAPTCHA güvenlik testleri		
BST-WEB-026	Captcha atlatma ve replay testleri		
BST-WEB-027	Captcha resim boyutu değiştirerek DoS testi		
BST-WEB-028	Oturum yönetimi zayıflıkları, oturum yönetimi atlatma testleri		
BST-WEB-029	Oturum sabitleme (session fixation) testleri		
BST-WEB-030	Oturum değerleri tahmin saldırıları		
BST-WEB-031	CSRF(Cross site reguest forgeryi testleri		
BST-WEB-032	Parola güncelleme için eski parolanın sorulması kontrolü (CSRF)		
BST-WEB-033	Oturum bilgisi zaman aşımı kontrol testleri		
BST-WEB-034	Oturum bilgisini içeren çerezlerin domain/yol bilgileri sızıntısı		
BST-WEB-035	Hassas formlarda AUTOCOMPLETE ozelligi kontrolu		
BST-WEB-036	Cookie'lere ait Secure ve HttpOnly özelliklerinin kontrolu		
BST-WEB-037	Parola unutma fonksiyonu zayıflık testleri		
BST-WEB-038	Dizin atlatma/gezme (Directory Treversal) testleri		
BST-WEB-039	Yetkilendirme atlatma, yetkilendirme geçiş testleri		
BST-WEB-040	Yetki yükseltme testleri		
BST-WEB-041	Yansıtılan (Reflected) XSS testleri		
BST-WEB-042	Depolanmış (Stored) XSS testleri		
BST-WEB-043	DOM tabanlı XSS testleri		

BST-WEB-044	XSF (Flash XSS) testleri		
BST-WEB-045	SOL enjeksiyonu testler (Error Based)		
BST-WEB-046	SOL enjeksiyonu testler (Boolesan Based)		
BST-WEB-047	SOL enjeksiyonu testler (Blind “Time Based”)		
BST-WEB-048	Local/Remote File Inclusion		
BST-WEB-049	Open Redirection		
BST-WEB-050	LDAP enjeksiyonu testleri		
BST-WEB-051	Xpath enjeksiyonu testleri		
BST-WEB-052	XNL testleri		
BST-WEB-053	Kod enjeksiyonu testleri(Blind/ Normal)		
BST-WEB-054	İşletim sistemi komut enjeksiyonu testleri		
BST-WEB-055	Bellektaşması (buffer overflow) testleri		
BST-WEB-056	HTTP response splitting testleri		
BST-WEB-056	Clickjacking testleri		
BST-WEB-057	SOL wildcard üzerinden DoS testleri Hesap kitleme politikasının testi		
BST-WEB-058	Buffer overflow DoS testleri		
BST-WEB-059	Oturum boyutu arttırma DoS testleri		
BST-WEB-060	HTTP GET Flood DoS testleri		
BST-WEB-061	Slowloris HTTP GET/POST atağının denenmesi		
BST-WEB-062	site:domain.com.tr "SOL syntax"		
BST-WEB-063	site:domain.com.tr inurl:admin inurl:login inurl:vpn		
BST-WEB-064	Firma domainine ait .asp uzantılı web sayfalarının bulunması		
BST-WEB-065	Firma domainine ait .php uzantılı web sayfalarının bulunması		
BST-WEB-066	Firma domainine ait .aspx uzantılı web sayfalarının bulunması		
BST-WEB-067	Firma domainine ait .jsp uzantılı web sayfalarının bulunması		

BST-WEB-068	Firma domainine ait .cgi uzantılı web sayfalarınırı bulunması		
BST-WEB-069	Arama motorlarından “error, warning” gibi ifadelerin arattırılması		
BST-WEB-070	login, yonetim, signup gibi login barındıracak sayfaların bulunması		
BST-WEB-071	Nikto kullanarak statik güvenlik testlerinin yapılması		
BST-WEB-072	Excel, word içerikli dosyalarını belirlenmesi		
BST-WEB-073	Parola, şifre, password gibi kelime gruplarının ilgili domaine özel arattırılması		
BST-WEB-074	İlgili web sayfasına ait girdi alan web sayfalarının bulunması		
BST-WEB-075	Dirbuster, Gobuster, Wfuzz kullanarak alt sayfaların ve dosyaların bulunması		
BST-WEB-076	Hata mekanizmasının test edilerek ek bilgi çıkartılmaya çalışılması		
BST-WEB-077	Kullarıları web sunucu ve platform bilgilerinin bulunması		
BST-WEB-078	Parolaların veritabanında açık olarak tutulup tutulmadığınırı testleri		
BST-WEB-079	Flash dosyaları statik analiz testleri		
BST-WEB-080	Parola resetleme, parola hatırlatma fonksiyonlarının test edilmesi		
BST-WEB-081	AJAX testleri		
BST-WEB-082	WSDL testleri		
BST-WEB-083	XML yapı testleri		
BST-WEB-084	XML enjeksiyon testleri		
BST-WEB-085	XXE enjeksiyon testleri		
BST-WEB-086	SSI enjeksiyonu testleri		
BST-WEB-087	SMTP/IMAP üzerinden komut çalıştırma testleri		
BST-WEB-088	HPP-HTTP Parameter pollution kontrolü		
BST-WEB-089	Kullanılan HTTP metodlarının tespiti		
BST-WEB-090	Eski, arşiv dsyalar üzerinden bilgi ifşası açıklığı		
BST-WEB-091	Hesap kitleme mekanizması testleri		
BST-WEB-092	WAF/IPS tespiti ve keşif testleri		

BST-WEB-093	HTTP Strict Transport Security testi		
BST-WEB-094	Kullanıcı kayıt prosedürlerinin test edilmesi		
BST-WEB-095	Öntanımlı hesap bilgilerinin test edilmesi		
BST-WEB-096	Oturum Sabitleme (Session fixation) güvenlik testleri		
BST-WEB-097	Dosya yükleme fonksiyonlarının testi		

Veritabanı Güvenlik Testleri	Test Adı	Sonuç	Notlar
BST-DB-001	Veritabanı versiyonu, üretici adı vb. bilgi toplama testleri		
BST-DB-002	Ön tarımlı veritabanı kullarıcı hesapları kontrolü		
BST-DB-003	Öntanımlı/zayıf veritabani yönetici/kullanıcı şifrelerinin tespiti		
BST-DB-004	Ele geçirilen veritabanı parola ve hashlerinin kırılması		
BST-DB-005	Diğer sistemlerden sistem kullanıcı yetkileriyle veritabanına erişim testleri		
BST-DB-006	Oracle listener tespiti ve zaafiyetleri		
BST-DB-007	Veritabanı oracle SID tahmini		
BST-DB-008	Veritabanı sürüm tespiti ve zaafiyet analizi		
BST-DB-009	MSQL kimlik doğrulama atlatma testleri		
BST-DB-010	Microsoft SOL üzerinden işletim sistemi ele geçirme		
BST-DB-011	Veritabanı yönetim arabirimleri kimlik doğrulama testleri		

Kablosuz Ağ Güvenlik Testleri	Test Adı	Sonuç	Notlar
BST-WIFI-001	Hedef sisteme ait kablosuz ağların SSID bulunması		
BST-WIFI-002	Gizli durumdaki kablosuz ağların (Hidden SSID) bulunması		
BST-WIFI-003	Kablosuz ağa bağlı sistemlere yönelik bilgi toplama (MAC vs.)		
BST-WIFI-004	Kablosuz ağda kullanılan şifreleme yöntemlerinin belirlenmesi		
BST-WIFI-005	Kablosuz ağa bağlı mobil cihazların bulunması		

BST-WIFI-006	MAC adresinden cihaz tipi belirlenmesi		
BST-WIFI-007	Kullanılan IP adres aralığını belirleme		
BST-WIFI-008	AP cihazına yönetim arabirimine yönelik güvenlik testleri		
BST-WIFI-009	AP cihazı IP adresinin bulunması		
BST-WIFI-010	AP cihazına yönelik kimlik doğrulama (open/shared) testleri		
BST-WIFI-011	Ağa bağlı istemcilerin IP adreslerini ve işletim sistemlerini belirleme		
BST-WIFI-012	MAC adres filtreleme belirleme		
BST-WIFI-013	MAC adres filtreleme özelliğinin atlatma		
BST-WIFI-014	Hotspot atlatma testleri — DNS Tünelleme		
BST-WIFI-015	Ağa bağlı istemcilere yönelik MITM testleri		
BST-WIFI-016	Aga bağlı istemcilerin sistemlerini ele geçirme testleri (fake upgrade)		
BST-WIFI-017	WEP / WPA / WPA2 parola kırma testleri		
BST-WIFI-018	Sahte Access Point kurulumu ve yayını		
BST-WIFI-019	Firmaya ait hotspot ortamının simule edilerek, buraya bağlanan kullanıcılardan bilgi toplanması		
BST-WIFI-020	Ağa bağlı istemcilerden WEP/WPA anahtarı alma testleri		
BST-WIFI-021	Ağa bağlı kablosuz istemcilere De-authentication saldırıları gerçekleştirme		
BST-WIFI-022	Ağa bağlı kablosuz istemcilere de-associate saldırıları gerçekleştirme		
BST-WIFI-023	Access Point'e sahte bağlantı istekleri göndererek bağlantı limitlerinin zorlanması		
BST-WIFI-024	Wireless AP'lerde bulunan bilinen zaafiyetlerin tespiti		
BST-WIFI-025	Nipper kullarak yapılandırma güvenlik testleri		
BST-WIFI-026	SNMP servisi zaafiyetleri kontrolu		

Sosyal Mühendislik Güvenlik Testleri	**Test Adı**	**Sonuç**	**Notlar**
BST-SOSM-001	Çalışanlarına aite-posta adreslerinin bulunması (arama motorları)		

BST-SOSM-002	Google üzerinden çalışanlara aite-posta formatının belirlenmesi		
BST-SOSM-003	LinkedIn üzerinden çalışanlarının e-posta adreslerinin belirlenmesi		
BST-SOSM-004	Arama motorları, sosyal ağlar ve kurum web siteleri kullanılarak çalışanlara ait ad/soyad/görev bilgilerinin elde edilmesi		
BST-SOSM-005	Kurum aları adlarına ait sorumlularını belirlenmesi (registrars)		
BST-SOSM-006	İnternete hizmet veren webmail/VPN servislerin belirlenmesi		
BST-SOSM-007	Kuruma ait alan adlarının parolalarının sıfırlanması testi (whois)		
BST-SOSM-008	Kurumun dışa açık kimlik doğrulama gerektiren hizmetlerinin belirlenmesi		
BST-SOSM-009	Kurumun kullandığı eposta, spam GW sistemlerinin belirlenmesi		
BST-SOSM-010	Kurumun web sitelerine benzer isimde sitelerin belirlenmesi		
BST-SOSM-011	FOCA aracı kullanarak hedef kuruma ait meta bilgilerinin ortaya çıkartılması		
BST-SOSM-012	İnternet uzerindeki servislerde bulunabilecek, firma binasi ve cevresindeki lokasyon bilgisini iceren iceriklerin tespiti (twitter, foursquare vb.)		
BST-SOSM-013	Elde edilen bilgiler kullanılarak sahte içerikli eposta gönderimi. Telefon ile bilgi toplama, sosyal mühendislikten yararlanma testleri		
BST-SOSM-014	Danışma masaları ve yardım merkezlerine yönelik sosyal mühendislik testleri		
BST-SOSM-015	Whois kayıtlarına göre sosyal mühendislik testleri (Nic.tr)		