



T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Çeşitli Hizmetler Alım Teknik Şartnamesi

1. KONU VE TANIMLAR

1.1. Konu

Bu teknik şartname Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından sunulmakta olan bilgi sistemlerinin güvenliğini arttırmaya yönelik, mevcut bilgi güvenliği altyapısının analizi, raporlanması ve iyileştirilmesi çalışmalarını, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği rehberi denetimi hizmet alımları konularını içermektedir.

1.2. Tanımlar ve Kısaltmalar

Dokümantasyon: Bu şartnamede, satın alınacak hizmete ait tüm donanım ve yazılım birimlerin kullanılması, çalıştırılması, bakım için gerekli her türlü el kitabı, her çeşit teknik yayın, kitap, not, çizim, şema, plan, tarife, broşür ve yazılımları ihtiva eder.

Kurum : Süleyman Demirel Üniversitesi

İdare : Süleyman Demirel Üniversitesi İdari ve Mali İşler Daire Başkanlığı

Yüklenici : Hizmetler tablosundan en az birini alan firmayı tanımlar.

T.S.E. : Türk Standartları Enstitüsü

CISSP : Certified Information Systems Security Professional

CISA : Certified Information Systems Auditor

OSCE : Offensive Security Certified Expert

OSCP : Offensive Security Certified Professional

CEH : Certified Ethical Hacker

SIEM : Security Information and Event Management

ISMS : Information Security Management System

ISO : International Standarts Organization(Uluslararası Standart Kurumu)

Zafiyet : Bir sistemde sistemin olası saldırılara karşı dayanma gücünü en aza indirecek hastalıklı/zayıf nokta, açık kapı.

Uyumluluk Testleri: PCI-DSS ya da ISO 27001 standartlarına uygunluğun ölçüldüğü testlerdir.

DDoS Testleri (Distributed Denial of Service): Sistemin, uygulamanın, network ekipmanlarının ya da network hattının kapasitesinin doldurularak hizmet dışı kalması amacıyla yapılan saldırıların kontrollü şekilde simule edilmesi ile yapılan testlerdir.

PCI-DSS (Payment Card Industry Data Security Standard): Kartlı ödeme sistemlerinde veri güvenliğini sağlamak amacıyla, American Express, Mastercard Worldwide, TROY, Visa Inc., JCB International, Discover Financial Services gibi uluslararası ödeme markaları tarafından desteklenen PCI

Kadir SÜMER
Bilişim Personeli

Merye SÜNEŞ
Sürekli İşçi

Mehmet Emin ÜNAL
Sürekli İşçi



0(246) 211 11 45



0(246) 211 11 47



bidb@sdu.edu.tr

SÜLEYMAN ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı, Batı Yerleşkesi, Çünür / ISPARTA

<https://w3.sdu.edu.tr>

<https://bidb.sdu.edu.tr>





T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Çeşitli Hizmetler Alım Teknik Şartnamesi

Güvenlik Standartları Kurulu (PCI Security Standards Council) tarafından oluşturulan PCI-DSS olarak bilinen Ödeme Kartı Sektörü Veri Güvenliği standardıdır.

Penetrasyon (Sızma) Testi: Kontrollü şekilde yapılan 'hacking' saldırı simülasyonudur.

Exploit: Programların zayıflık veya hatalarını kullanan programcılar, sistemlerin zafiyetlerini kullanabilen özel scriptler ya da programlardır.

Test: Uyumluluk testleri ve penetrasyon (sızma) testleri için işbu şartnamede kullanılan genel ifade.

BİGR: Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi

TÜRKAK: Türk Akreditasyon Merkezi

DPO: Data Protection Officer – Veri Koruma Görevlisi

TSE: Türk Standartları Enstitüsü

2. GENEL ŞARTLAR

- 2.1. Yüklenici firmanın elemanları, mesai saatleri dışında çalışacaklarsa, çalışacak kişilerin isimleri ve çalışma süreleri en az 2 gün öncesinde idareye bildirilmelidir.
- 2.2. Yüklenici teklif vermekle aşağıdaki şartları kabul etmiş sayılırlar.
- 2.3. Her bir hizmet alımı maddesi için gerekli şartlar sağlandığı takdirde toplu ya da madde bazlı başvuru yapılabilir.
- 2.4. Yapılacak tüm testlerin zamanlarını ve sürelerini İdare ile birlikte belirleyecektir.
- 2.5. Yapılacak tüm testler İdare ile birlikte koordineli bir şekilde gerçekleştirilecektir. İdareye bilgi verilmeden herhangi bir test çalışması yapılmayacaktır.
- 2.6. HİZMET, Yüklenici Firmanın bordrolu ve şartnamede belirtilen yetkinliklere sahip personeli tarafından sağlanacaktır.
- 2.7. Sızma testini yapacak Yüklenici Firmanın bu sözleşme kapsamında istihdam edeceği personel, konusunda uzman, benzer projelerde bulunmuş, bu konularda en az 2 yıl tecrübe kazanmış olmalıdır.
- 2.8. Sızma testini yapacak Yüklenici Firmanın %100 Yerli ve Türk Sermayesi ile kurulu olması tercih edilmektedir.
- 2.9. Sızma testini yapacak Yüklenici Firmanın gerçekleştirecek olduğu Sızma Testi hizmetinde her bir testin manuel veya otomatik olacağını belirtmeli, test aşamasında kullanıcıdan uygunluğu ile ilgili onay almalıdır.

Kadir SÜMER
Bilişim Personeli

Merve GÜNEŞ
Sürekli İşçi

Mehmet Emin ÜNAL
Sürekli İşçi



0(246) 211 11 45



0(246) 211 11 47



bidb@sdu.edu.tr

SÜLEYMAN ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı, Batı Yerleşkesi, Çünür / ISPARTA

<https://w3.sdu.edu.tr>

<https://bidb.sdu.edu.tr>





T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Çeşitli Hizmetler Alım Teknik Şartnamesi

- 2.10.** Sızma testini yapacak Yüklenici Firmanın bu özelliklere sahip personellerinin sözleşme aşamasında çalıştığını gösteren SGK bildirgelerini, özgeçmişini, sertifikalarını ve diplomalarını sözleşme aşamasında idarenin istemesi halinde sunulacaktır.
- 2.11.** Sızma testini yapacak Yüklenici Firmanın sektörde en az 2 (iki) yıldır faaliyet gösteriyor olmalıdır.
- 2.12.** Sızma testini yapacak Yüklenici Firmanın, sunacağı hizmete benzer olarak Türkiye'de gerçekleştirdiği en az üç (3) adet referans projeyi (işlem hacmi, IP sayısı marka değeri vb. kriterlere göre S.D.Ü. ölçeğinde) sunacaktır. Yüklenici Firma tarafından bu referans projelere ilişkin kontak kişi ve iletişim bilgileri teklif ekinde sunulacaktır.
- 2.13.** Sızma testini yapacak Yüklenici Firma, bu sözleşme kapsamında görevlendirilen teknik personelinden memnun kalınmaması durumunda, İdare'den gelecek değişiklik talebini en az aynı vasıfta başka bir personel istihdam ederek karşılayacaktır.
- 2.14.** Sızma testini yapacak Firmanın güncel ISO27001 sertifikasına sahip olması gerekmektedir.
- 2.15.** Sızma testini yapacak Firmanın güncel T.S.E. tarafından verilmiş olan A veya B düzeyinde "Firma Yetkinlik Seviyesi" bulunmalıdır.
- 2.16.** Sızma testini yapacak Firmanın iş kapsamında kullanacağı personelinin, OSCP, OSCE, CEH, T.S.E. Kıdemli Sızma Testi Uzmanı sertifikalarından en az birine sahip olması gerekmektedir.
- 2.17.** **BİGR** denetimi hizmeti verecek Yüklenicinin yetkinlik sertifikalarını fiyat teklifi ile sunmalıdır. Ortak girişim olması halinde her bir Yüklenici ilgili belgelere sahip olmalı ve bu belgeleri teklif beraberinde sunmalıdır.
- 2.18.** **BİGR** denetimi hizmeti verecek Yüklenicinin son 5 yıl içindeki **BİGR** denetimi Hizmeti konusu ile bağlantılı referanslarını büyüklüklerini sınıflandırarak paylaşacaktır. Referanslarda belirtilen Yüklenici firmaların personel sayıları 1.000 den büyük olmalı ve en az ikisinin kamu kurumu(en az birinin üniversite) olması gerekmektedir.
- 2.19.** **BİGR** denetimi hizmeti verecek Yüklenicinin, mevzuatı gereği kayıtlı olduğu Ticaret ve/veya Sanayi Odası veya Meslek Odası Belgesini sunmalıdır. Ayrıca, teklif vermeye yetkili olduğunu gösteren İmza Beyannamesi veya İmza Sirkülerini paylaşmalıdır.
- 2.20.** Hizmetler tablosunda belirtilen kalemlere kısmi teklif verilebilecektir.

Kadir SUMER
Bilişim Personeli

Merve GÜNEŞ
Süreklili İşçi

Mehmet Emin ÜNAL
Süreklili İşçi



0(246) 211 11 45



0(246) 211 11 47



bidb@sdu.edu.tr

SÜLEYMAN ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı, Batı Yerleşkesi, Çünür / ISPARTA

<https://w3.sdu.edu.tr>

<https://bidb.sdu.edu.tr>





T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Çeşitli Hizmetler Alım Teknik Şartnamesi

2.21. Hizmetler

Sıra No	Ürün Açıklaması	Adet
1	Sızma ve Doğrulama Testi Hizmeti	Hizmet Alımı
2	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi Denetimi Hizmeti	Hizmet Alımı

TEKNİK ŞARTLAR

1. Sızma ve Doğrulama Testi Hizmeti

1.1. Sızma Testinin Gizliliği ve Yüklenicinin Sorumlulukları

1.1.1.İşbu şartname ile tanımlanan tüm yükümlülükleri yerine getirecektir.

1.1.2.Yüklenici yaptığı testler esnasında kuruluş çalışanlarının kişisel bilgilerine ulaşması durumunda, bu bilgileri kuruluş ile paylaşmamalı, sızma testi sonuç raporuna eklememeli ve bir kopyasını kendisine almamalıdır. Sızma test raporunda kullanıcı adı ve parolaları maskelenmelidir.

1.1.3.Sızma testleri esnasında Yüklenici, sadece kuruluşa ait içeriklere erişim sağlanabildiğini göstermeli, bunun dışında kuruluşa ait içeriklerin tamamına erişim sağlayarak tüm içeriği kopyalamamalı ve üçüncü taraflar ile paylaşmamalıdır. Yüklenicinin içeriklere erişim sağlandığını gösterebilmesi için gerekiyorsa örnek olarak birkaç kayıt delil sağlamak amacıyla kopyalayabilir.

1.1.4.İş başlangıcında idare tarafından Yükleniciye verilen bilgi, dokümanlar vb. ve iş sonunda Yüklenici tarafından hazırlanan raporlar, çıktılar, ekran görüntüleri, vb idareye tesliminden sonra Yüklenici tarafından kesinlikle depolanmayacak ve 3. taraflarla paylaşılmayacaktır. İşlerle ilgili tüm bilgiler (network topolojileri, kullanılan protokol bilgileri, güvenlik zafiyetleri, raporlar, vb. aksi yazılı olarak belirtilmedikçe 'GİZLİ' olarak kabul edilecektir.

1.1.5.Raporlar özellikle sunumlarda kullanılmamalı ve örnek mahiyetinde diğer kuruluşlara gösterilmemelidir.

Kadir SUMER
Bilişim Personeli

Merve GÜNEŞ
Sürekliliği

Mehmet Emin ÜNAL
Sürekliliği



0(246) 211 11 45



0(246) 211 11 47



bidb@sdu.edu.tr

SÜLEYMAN ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı, Batı Yerleşkesi, Çünür / ISPARTA

<https://w3.sdu.edu.tr>

<https://bidb.sdu.edu.tr>





T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Çeşitli Hizmetler Alım Teknik Şartnamesi

1.2. Sızma Testi Süreci

Sızma Testi temel olarak keşif, açık bulma, açıklık testi, raporlama, doğrulama aşamalarından oluşmalıdır. Sızma Testi en az aşağıdaki konuları içermelidir:

1.2.1.İletişim Altyapısı ve Aktif Cihazlar Sızma Testleri

- 1.2.1.1. Kurumda kullanılan ağ cihazlarının genel mimarı içindeki yeri incelenecektir.
- 1.2.1.2. Cihazların tespiti
- 1.2.1.3. Tespit edilen cihazların marka, model ve sürüm belirlenmesi
- 1.2.1.4. Ön tanımlı parola ve ayarların kontrolü
- 1.2.1.5. Üretici yamaları ve uygulanması
- 1.2.1.6. VLAN güvenlik kontrollerinin yapılması
- 1.2.1.7. Ele geçirme saldırıları
- 1.2.1.8. Aktif cihaz üzerinde çalışan servisler incelenecektir.
- 1.2.1.9. Mitm(Man in the middle) kontrolleri yapılacaktır.
- 1.2.1.10. Kurum içinde bulunan VOIP hizmetinin testleri.

1.2.2.Dns Servisleri Güvenlik Testleri

- 1.2.2.1. DNS sunucuların topolojik incelenmesi
- 1.2.2.2. DNS Sunucusunun alan yapılandırmasında yer alan kayıtların ortaya çıkartılması
- 1.2.2.3. Sunucu üzerinden alan transferi (zone transfer) yapılmaya çalışılacaktır.
- 1.2.2.4. NXT ve NSEC kaynak kayıtları üzerinden bilgiler elde edilmesi
- 1.2.2.5. Pasif sorgularla bilgi toplanması
- 1.2.2.6. DNS sunucular için ön bellek zehirlemesi kontrolü
- 1.2.2.7. DNS sunucular üzerindeki kaynak kayıt girdileri kontrolü
- 1.2.2.8. DNS sunucuların sürüm bilgisi
- 1.2.2.9. Kurum dışı alan adı sorguları
- 1.2.2.10. Sunucular üzerinde DNS dışında bir servisin çalışıp çalışmadığı
- 1.2.2.11. Güvenlik Duvarında DNS sunucular için izin verilen ayarların kontrolü
- 1.2.2.12. DNS sunucuların zafiyet taraması
- 1.2.2.13. DNS servisini veren yazılımın açıklıkları araştırılması

1.2.3.Etki alanı ve Kullanıcı Bilgisayarları Güvenlik Testleri

- 1.2.3.1. Etki alanında güvenlik politikaları kontrol edilmesi,
- 1.2.3.2. Etki alanındaki yetkili kullanıcıların ayrıcalıkları ve kullanım şekilleri

kontrolleri
Kadir SUMER
Bilişim Personeli

Merve GÜNEŞ
Sürüm

Mehmet Emin ÜNAL
Süreklili İşçi



0(246) 211 11 45



0(246) 211 11 47



bidb@sdu.edu.tr

SÜLEYMAN ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı, Batı Yerleşkesi, Çünür / ISPARTA

<https://w3.sdu.edu.tr>

<https://bidb.sdu.edu.tr>





T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Çeşitli Hizmetler Alım Teknik Şartnamesi

- 1.2.3.3. Yama yönetimi politikaları
- 1.2.3.4. Virüs koruma politikaları
- 1.2.3.5. Hassas bilgi içeren ve yetkisiz erişime olanak sağlayan paylaşım kontrolleri
- 1.2.3.6. Taşınabilir aygıtların kullanımı ile ilgili güvenlik ayarları
- 1.2.3.7. Yerel kullanıcı hesabı ve kullanıcı grupları kontrolleri
- 1.2.3.8. Bilgisayarların fiziksel saldırılara karşı güvenilirliği
- 1.2.3.9. Ağ haritalanması

1.2.4.E-posta Servisleri Güvenlik Testleri

- 1.2.4.1. E-posta sunucularının topolojik konumu
- 1.2.4.2. Virüs tarayıcı ağ geçitlerinin sürüm bilgisi ve açıklarının tespit edilmesi
- 1.2.4.3. Relay zafiyetlerinin tespit edilmesi
- 1.2.4.4. Eposta sunucular üzerinde başka servislerin tespiti
- 1.2.4.5. Eposta sistemi kimlik doğrulama sisteminin denetimi
- 1.2.4.6. Eposta sunucusu üzerinde ilgili servislerin kontrolleri (IMAP, POP3)
- 1.2.4.7. Zafiyet taraması
- 1.2.4.8. İzin verilen eposta boyutu kontrolü
- 1.2.4.9. Eposta liste uygulamalarının zafiyet taramaları

1.2.5.Veritabanı Sistemleri Güvenlik Testleri

- 1.2.5.1. Veritabanı sunucusunun topolojik konumu
- 1.2.5.2. Yamaların kontrolü
- 1.2.5.3. Veritabanı için önemli olan işletim sistemi dosyalarının erişim izinleri
- 1.2.5.4. Veritabanı sunucusunun güvenlik ayarları
- 1.2.5.5. Veritabanı sunucusunun parola politikası, kullanıcı hesapları güvenlik ayarları
- 1.2.5.6. Veritabanı sunucusunda, güvenlik açısından önemli olan paketler, nesneler, roller, tablo ve hakların kontrolü
- 1.2.5.7. Veritabanı sunucusunda, denetleme mekanizmasının kontrolü
- 1.2.5.8. Veritabanı sunucusunun yedekleme ve kurtarma mekanizması
- 1.2.5.9. Veritabanının kurulumu ile birlikte gelen ve kullanıcılar için atanan varsayılan değerlerin kontrolü
- 1.2.5.10. Uzaktan erişimin güvenlik kontrolleri

1.2.6.Web Uygulamaları Güvenlik Testleri

- 1.2.6.1. Veri Kontrolleri

1.2.6.1.1. Girdi denetimi

Kadir ÖMER
Bilişim Personeli

Merve GÜNEŞ
Süreli İşçi

Mehmet Emin ÜNAL
Süreli İşçi



0(246) 211 11 43



0(246) 211 11 47



bidb@sdu.edu.tr

SÜLEYMAN ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı, Batı Yerleşkesi, Çünür / ISPARTA

<https://w3.sdu.edu.tr>

<https://bidb.sdu.edu.tr>





T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Çeşitli Hizmetler Alım Teknik Şartnamesi

- 1.2.6.1.2. Çıktı denetimi
- 1.2.6.1.3. Değiştirilen içeriğin tespiti
- 1.2.6.1.4. HTML etiketlerinin filtrelenmesi
- 1.2.6.1.5. SQL sokuşturma
- 1.2.6.1.6. Sunucu taraflı girdi denetimi
- 1.2.6.1.7. URL yönlendirmeler/Diğer sokuşturma/XSS
- 1.2.6.1.8. HTTP yanıt bölme
- 1.2.6.2. Oturum Yönetimi
 - 1.2.6.2.1. Giriş sonrası oturum bilgisi yenileme, oturum sabitleme
 - 1.2.6.2.2. Çerezlerin içeriği
 - 1.2.6.2.3. Oturum sonlandırma
 - 1.2.6.2.4. Oturum bilgisinin URL içinde taşınması
 - 1.2.6.2.5. Oturum çalma (Session riding)
- 1.2.6.3. CSRF
- 1.2.6.4. Kimlik yönetimi, doğrulama ve iş mantığı
 - 1.2.6.4.1. Yetki artırımı / Yetki dışı işlem /Şifre politikaları
 - 1.2.6.4.2. Bilinen hesap/şifre bileşenlerinin denenmesi
 - 1.2.6.4.3. Basit kimlik doğrulama kullanımı/Kimlik doğrulamanın atlatılması/Çıkış işlevi
 - 1.2.6.4.4. Path traversal
 - 1.2.6.4.5. Bypass authorization
 - 1.2.6.4.6. Privilege escalation
 - 1.2.6.4.7. Uygulama mantığı kontrolleri
- 1.2.6.5. Web Servis Testleri
 - 1.2.6.5.1. Web servislerin tespiti/Web servisi detay tarama/REST
 - 1.2.6.5.2. SOAP
 - 1.2.6.5.3. Ajax
 - 1.2.6.5.4. Bilgi Sızdırma ve Ayar Yönetim
 - 1.2.6.5.5. Yardım sayfaları o SSL kullanımı/HTML comment/Sunucu bilgisi
 - 1.2.6.5.6. Ayrıntılı hata mesajları
 - 1.2.6.5.7. Dosya uzantıları/Yedek dosyalar/Yönetici ara yüzü
 - 1.2.6.5.8. Desteklenen HTTP metotları ve XST açıklığı
 - 1.2.6.5.9. Sitenin SSL sertifikasının geçerlilik testi

Kadir SÜMER
Bilişim Personeli

Merve GÜNEŞ
Süreç Yöneticisi

Mehmet Emin ÜNAL
Sürekli İşçi



0(246) 211 11 43



0(246) 211 11 47



bidb@sdu.edu.tr

SÜLEYMAN DEMİREL ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı, Batı Yerleşkesi, Çünür / ISPARTA

<https://w3.sdu.edu.tr>

<https://bidb.sdu.edu.tr>





T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Çeşitli Hizmetler Alım Teknik Şartnamesi

- 1.2.6.5.10. Metadata kontrolleri
- 1.2.6.6. Yerel Testler
 - 1.2.6.6.1. Web uygulama temelli testler
 - 1.2.6.6.2. XSS ve HTML ekleme (injection)
 - 1.2.6.6.3. Command injection
 - 1.2.6.6.4. CSRF
 - 1.2.6.6.5. SQL injection
 - 1.2.6.6.6. Web Çerezlerinin incelenmesi
- 1.2.6.7. Kimlik Denetimi ve Yetkilendirme
 - 1.2.6.7.1. Kimlik doğrulama atlatma
 - 1.2.6.7.2. OTP ve çok faktörlü kimlik doğrulama
 - 1.2.6.7.3. Yerelde saklanan verilen manipülasyonu
- 1.2.6.8. Dosya Sistemi İncelemesi
 - 1.2.6.8.1. Dosya sistemi izinleri
 - 1.2.6.8.2. Ön-bellekte veri saklama
 - 1.2.6.8.3. Cihaz üzerinde şifrelenmemiş veri saklama
 - 1.2.6.8.4. Kullanıcı adı/parola, cihaz ID, kişisel/hassas veri
 - 1.2.6.8.5. Uygulama yedekleri
 - 1.2.6.8.6. Silinmiş verilerin geri döndürülmesi
- 1.2.6.9. Bellek İncelemesi
 - 1.2.6.9.1. Bellekte tutulan hassas verileri kontrolü
- 1.2.7. Uzak (Remote) Testler
 - 1.2.7.1. Kimlik Denetimi ve Yetkilendirme
 - 1.2.7.1.1. Parola uzunluk ve karmaşıklık gereksinimleri
 - 1.2.7.1.2. Otomatik saldırılar / hesap kitleme
 - 1.2.7.1.3. Tek noktadan kimlik doğrulama (SSO)
 - 1.2.7.1.4. OTP ve iki faktörlü kimlik doğrulama
 - 1.2.7.1.5. Arkadaki sunucu servislerine doğrudan/yetkisiz erişim
 - 1.2.7.1.6. Yatay ve dikey yetki aşırımları
 - 1.2.7.2. Oturum Yönetimi
 - 1.2.7.2.1. Entropi incelemesi
 - 1.2.7.2.2. Cihaz ID bağımlı oturum
 - 1.2.7.2.3. Oturum anahtarlarının yaşam döngüsü ve sonlandırılması

Kadir SÜMER
Bilgi İşlem Daire Başkanı

Merve Çiğdem
Süreklilikçi

Mehmet Emin ÜNAL
Süreklilikçi



0(246) 211 11 47
0(246) 211 11 47
bidb@sdu.edu.tr

SÜLEYMAN ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı, Batı Yerleşkesi, Çünür / ISPARTA

<https://w3.sdu.edu.tr>

<https://bidb.sdu.edu.tr>





T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Çeşitli Hizmetler Alım Teknik Şartnamesi

- 1.2.7.2.4. Yetki aşımı
- 1.2.7.2.5. Oturum anahtarlarının cihaz üzerinde tutulması
- 1.2.7.3. İletim Katmanı Testleri
 - 1.2.7.3.1. Aradaki adam saldırıları
 - 1.2.7.3.2. İzinsiz dinleme
 - 1.2.7.3.3. SSL kontrolleri
- 1.2.7.4. Sunucu tarafı testleri
 - 1.2.7.4.1. SQL injection
 - 1.2.7.4.2. XSS
 - 1.2.7.4.3. Open Redirect
 - 1.2.7.4.4. Tampon bellek taşması
 - 1.2.7.4.5. XML/JSON temelli saldırılar
 - 1.2.7.4.6. İşlenmeyen (unhandled) durumların tespiti
 - 1.2.7.4.7. Kısıtlanmamış dosya yükleme
- 1.2.8. Kablosuz Ağ Güvenlik Testleri
 - 1.2.8.1. Kurum tamamında rogue, merkezi yönetilmeyen gibi erişim noktası tespiti
 - 1.2.8.2. Kurum dâhilinde kullanılan kablosuz altyapının kontrolü
 - 1.2.8.3. Kullanılan PSK'lere kırma denemeleri
 - 1.2.8.4. Kablosuz yanıltma saldırıları
- 1.2.9. Sosyal Mühendislik Testleri
 - 1.2.9.1. Arama motorları, sosyal ağlar ve kurum web siteleri kullanılarak, kurum ve çalışanları hakkında bilgi toplanması
 - 1.2.9.2. Google hacking(Google cache'de kuruma ait dosya, veri tabanı, URL, önemli data olup olmadığı) yapılacaktır.
 - 1.2.9.3. Kurum içinden veya dışından Telefon iletişimi ile hassas bilgilere erişimin denenmesi
 - 1.2.9.4. Epostalar ile kurum içine sızmaya çalışılması

Kadir SUMER
Bilişim Personeli

Merve GÜNEŞ
Süreklili İşçi

Mehmet Emin ÜNAL
Süreklili İşçi



0(246) 211 11 45



0(246) 211 11 47



bidb@sdu.edu.tr

SÜLEYMAN ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı, Batı Yerleşkesi, Çünür / ISPARTA

<https://w3.sdu.edu.tr>

<https://bidb.sdu.edu.tr>





T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Çeşitli Hizmetler Alım Teknik Şartnamesi

1.3. Örnek Kapsam Formu

Kapsam Formu Süleyman Demirel Üniversitesi alt birim, fakülte, daire başkanlıkları, hastanelerini kapsamaktadır.

İnternet Güvenlik Testi	
Toplam Aktif Sunucu Sayısı	~148 adet
Dış Ağ IP Blokları	2 adet /24 olarak belirtilecektir.
Testlerin Uygulama Metodu	White Box
Testlerin Uygulama Zamanı	Mesai İçi ya da Dışı

Yerel Ağ	
Testin Gerçekleştirileceği Yerler	S.D.Ü. Bilgi İşlem D.B.
Aktif Sunucu Sayısı	~140 adet
Toplam Client Sayısı	~3000 adet

Web Uygulama Testleri	
.Net	~21 adet internete açık uygulama testi istenmektedir. Yetkili hesap verilecektir.
Php	2 adet internete açık uygulama testi istenmektedir. Yetkili hesap verilecektir.
Testlerin Uygulama Metodu	Siyah ve Beyaz Kutu
Testlerin Uygulama Zamanı	Mesai İçi ya da Dışı

Mobil Uygulama	
SDU Mobil	Android (x) IOS (x)
	İnternete açıktır
	Test Hesabı Verilecektir
Testlerin Uygulama Metodu	White Box
Testlerin Uygulama Zamanı	Mesai İçi ya da Dışı

Sosyal Mühendislik	
Test Yapılacak Kullanıcı	~3000
Eposta	Tüm kurum yerine kurumdan rasgele ~500 kullanıcıya denenmesi planlanmaktadır.
Telefon	Evet
Fiziksel	Evet
Senaryo Sayısı	Sunulacak senaryolardan 1-2 si seçilerek uygulama denenebilir.

Kadir SÜMER
Bilişim Personeli

Merve GÜNEŞ
Sürekliliği

Mehmet Emin ÜNAL
Sürekliliği



0(246) 211 11 45



0(246) 211 11 47



bidb@sdu.edu.tr

SÜLEYMAN ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı, Batı Yerleşkesi, Çünür / ISPARTA

<https://w3.sdu.edu.tr>

<https://bidb.sdu.edu.tr>





T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Çeşitli Hizmetler Alım Teknik Şartnamesi

Kablosuz Ağ	
SSID Sayısı	2
Lokasyon	S.D.Ü. Bilgi İşlem D.B.
Testlerin Uygulama Metodu	Siyah ve Beyaz Kutu
Testlerin Uygulama Zamanı	Mesai içi

Veri Tabanı	
Veri tabanı sunucu sayısı	5
Testlerin Uygulama Metodu	Siyah ve Beyaz Kutu
Testlerin Uygulama Zamanı	Mesai İçi ya da Dışı

IP Santral (Voip)	
IP Santral	1
Testlerin Uygulama Metodu	Siyah ve Beyaz Kutu
Testlerin Uygulama Zamanı	Mesai İçi ya da Dışı

1.4. Diğer Teknik Hususlar

1.4.1. Sızma testini yapacak Yüklenici; iş bu şartnamede işin kapsamında belirtilen her proje için tanımlanan işleri (bundan sonra tümü “iş” olarak ifade edilecektir) gerçekleştirecek ve iş sonunda Sızma ve Zafiyet Testi raporlarını hazırlayarak Kurum’a sunacaktır.

1.4.2. Test yapılacak sunucu bilgileri Kurum tarafından verilecektir.

1.4.3. Sızma ve zafiyet testi yapılacak olan sunucular için, işin yapılmasında ihtiyaç duyulan bilgi ve dokümanlar (network topolojisi, kullanılan IP bilgileri, proje iç işleyiş bilgileri vb.) Kurum tarafından Yükleniciye verilecektir.

1.4.4. Kurum’un onayı ile ilgili çalışmalar yapılacaktır. Yapılacak olan tüm çalışmalar planlı olacaktır.

1.4.5. İş sonucunda hazırlanacak olan ilgili raporlarda;

- Tespit edilen güvenlik zafiyetleri, ekran çıktıları,
- Bu zafiyetlerin sebep olabileceği zararlar/sonuçları ve zafiyete ilişkin referans bilgileri,
- Güvenlik zafiyetlerini gidermek için yapılması gerekenler, detaylı şekilde açıklanacaktır.

1.4.6. İş sonucunda oluşturulan raporlar, elektronik ortamda Microsoft Word veya Pdf formatında Kurum’a sunulacaktır.

Kadir SUMER
Bilişim

Merve GÜNEŞ
Sistem Yöneticisi

Mehmet Emin ÜNAL
Sürekli İşçi



0(246) 211 11 45

0(246) 211 11 47

bidb@sdu.edu.tr

SÜLEYMAN ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı, Batı Yerleşkesi, Çünür / ISPARTA

<https://w3.sdu.edu.tr>

<https://bidb.sdu.edu.tr>





T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Çeşitli Hizmetler Alım Teknik Şartnamesi

- 1.4.7. İş sonucunda üretilmiş olan raporların tüm telif hakları Kurum'a ait olacaktır.
- 1.4.8. İş kapsamında hazırlanan sızma ve zafiyet testi raporunda projeler için tespit edilen zafiyetler raporlanacaktır.
- 1.4.9. İş kapsamında hazırlanan sızma ve zafiyet testi raporunda tespit edilen güvenlik zafiyetleri kritiklik seviyelerine (kritik, yüksek) göre gruplandırılacak ve sınıflandırmanın nasıl yapıldığı ilgili raporda açıklanacaktır.
- 1.4.10. İş kapsamında hazırlanan sızma ve zafiyet testi raporunda, tespit edilen bir güvenlik zafiyeti, söz konusu zafiyeti bulunduran sistemler bazında gruplandırılmalıdır.
- 1.4.11. İş kapsamında hazırlanan sızma ve zafiyet testi raporunda, tespit edilen her güvenlik zafiyeti için alınması gereken önlem/önlemler Yüklenici tarafından belirlenmeli ve raporlanmalıdır.
- 1.4.12. İş kapsamında yapılacak olan sızma ve zafiyet testlerinde Şirket iç ağının (intranet) ve/veya sistem salonlarının kullanılması gerektiği durumda işi yapacak olan Yüklenici personeli, ilgili lokasyona Kurum izni ile girecektir.
- 1.4.13. İş kapsamında kullanılacak olan bilgisayar, yazılım lisansları ve gerekli donanımlar Yüklenici tarafından temin edilecektir.
- 1.4.14. İş kapsamında kullanılacak olan işletim sistemi yazılımları, tarama yazılımları, uygulama sunucu yazılımları, ...vb yazılımlar ve lisansları Yüklenici tarafından temin edilecektir. Kurum lisanslama ile ilgili herhangi bir yükümlülüğe girmeyecektir. Tüm lisans sorumluluğu Yükleniciye aittir.
- 1.4.15. İş kapsamındaki sistemler üzerinde Yüklenici tarafından yapılacak sızma ve zafiyet testleri, projenin topolojisine göre hem internet hem intranet üzerinden yapılacaktır. Yüklenici bu iş için ilave ücret talep etmeyecektir.
- 1.4.16. İş kapsamında yapılacak olan sızma ve zafiyet testlerinde kullanılması gerekebilecek olan test kullanıcı hesapları ve özel kullanıcı bilgileri (credentials) Kurum tarafından Yüklenici'nin kullanımına verilebilecektir. Söz konusu bilgilerin verilip/verilmeyeceğine Kurum karar verecektir.
- 1.4.17. İş kapsamında hazırlanan raporlar, tespit edilen açıklar kullanılarak gerçekleştirilen bir atak bulunması durumunda ekran görüntülerini ve/veya video çekimlerini içermelidir.
- 1.4.18. Yüklenici zafiyet raporunu sunduktan sonra, 6 ay içerisinde Kurum'un talebi üzerine tespit edilen bulgular üzerinden yeniden değerlendirme testi yapacaktır.

Kadir SÜMER
Bilgi İşlem Dairesi Başkanı

Merve GÜNEŞ
Süreklili İşçi

Mehmet Emre ÜNAL
Süreklili İşçi



0(246) 211 11 45

0(246) 211 11 47

bidb@sdu.edu.tr

SÜLEYMAN ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı, Batı Yerleşkesi, Çünür / ISPARTA

<https://w3.sdu.edu.tr>

<https://bidb.sdu.edu.tr>





T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Çeşitli Hizmetler Alım Teknik Şartnamesi

1.4.19. Tercihen kurumumuzda sızma testi yapacak Yüklenicinin daha farklı detaylar görülmesi amacı ile 2 sene üst üste aynı Yüklenici olmaması beklenmektedir.

1.4.20. Yüklenici, iş ile ilgili olarak elde ettiği her türlü bilgi ile belgelerini özel ve gizli tutacak. Kurum'un önceden yazılı izni olmaksızın kurumumuza ait herhangi bir detayı ifşa etmeyecek veya yayınlamayacaktır. Türk yargı mercilerinin kararları saklı kalmak kaydı ile sözleşmenin amaçları doğrultusunda herhangi bir ifşa veya yayınlama gerekliliği konusunda bir uzlaşmazlık ortaya çıkarsa İdare'nin bu konudaki kararı nihai olacaktır. Gizlilik hükümlülüğü teknik şartnamedeki yükümlülükler herhangi bir nedenle sona ermesinden sonra da devam eder.

2. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi Denetimi Hizmeti

- 2.1.** Yüklenici firma ekibinde, TSE Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Veren Personel ve Firma Belgelendirme Programı kapsamında yetkilendirilen en az bir baş denetçi ve denetçi bulunmak zorundadır. Ekipteki baş denetçi aynı zamanda Denetim Koordinatörü işini yüklenmiş olacaktır. Ekipte birden fazla baş denetçi olması durumunda baş denetçilerden biri Denetim Koordinatörü olarak görevlendirilebilir.
- 2.2.** Yüklenici firma TSE onaylı BİGR Denetim firmaları listesinde yer almalıdır.
- 2.3.** Denetim Sızma Testi sonrası yapılacaktır.
- 2.4.** Yüklenici, denetimi Bilgi ve İletişim Güvenliği Denetim Rehberi'ne harfiyen uyarak yapacağını taahhüt etmiş kabul edilir.
- 2.5.** Denetim işlemleri kurum tarafından ana başlıklar altında bulunan en az iki başlık üzerinden yapılacaktır.
- 2.6.** Yüklenici, kurum ile iletişim sağlayarak süreçleri tamamlayacaktır. Bu süreçte tüm masraflar veya hizmetler (Konaklama, Lojistik vb.) yükleniciye aittir.
- 2.7.** Yüklenici, iş ile ilgili olarak elde ettiği her türlü bilgi ile belgelerini özel ve gizli tutacak. Kurum'un önceden yazılı izni olmaksızın kurumumuza ait herhangi bir detayı ifşa etmeyecek veya yayınlamayacaktır. Türk yargı mercilerinin kararları saklı kalmak kaydı ile sözleşmenin amaçları doğrultusunda herhangi bir ifşa veya yayınlama gerekliliği konusunda bir uzlaşmazlık ortaya çıkarsa İdare'nin bu konudaki kararı nihai olacaktır. Gizlilik hükümlülüğü teknik şartnamedeki yükümlülükler herhangi bir nedenle sona ermesinden sonra da devam eder.

Kadir SÜMER
Bilişim Personeli

Merve GÜNEŞ
Sürekliliği

Mehmet Emin ÜNAL
Sürekliliği

0(246) 211 11 45

0(246) 211 11 47

bidb@sdu.edu.tr

SÜLEYMAN ÜNİVERSİTESİ

Bilgi İşlem Daire Başkanlığı, Batı Yerleşkesi, Çünür / ISPARTA

<https://w3.sdu.edu.tr>

<https://bidb.sdu.edu.tr>

