|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Satınalan Birim** | Bilgi İşlem Daire Başkanlığı | | |
| **Talep Eden Birim** | BİLGİ İŞLEM DAİRE BAŞKANLIĞI | | |
| **Talep Eden Birim**  **Sorumlusu** |  | |  |
| **Dosya Numarası** | 2023-13 | | |
| **Satınalma Usulü** | Piyasa fiyat araştırması | | |
| **Satınalma Memuru** | Zafer CAN | **Tel** : 0224 294 28 23-24 | |
| **Fax**: 0224 294 05 01 | |
| **E-mail**:  zafercan@uludag.edu.tr | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Sıra No** | **Mal/Hizmet Cinsi** | **Mal/Hizmet Özellikleri** | **Miktarı** |
| **Donanım** | | | |
| **1-** | **Bursa Uludağ Üniversitesi Sızma Testi Hizmet Alımı** | **Teknik Şartname** | **1** |
| **2-** |  |  |  |
| **3-** |  |  |  |
| **4-** |  |  |  |
| **5-** |  |  |  |
| **6-** |  |  |  |
| **7-** |  |  |  |
| **8-** |  |  |  |
| **9-** |  |  |  |

Üniversitemiz Bilgi İşlem Daire Başkanlığı Kurum bünyesinde yer alan BURSA ULUDAĞ ÜNİVERSİTESİ **Bursa Uludağ Üniversitesi Sızma Testi Hizmet** satın alımı işi için teklifler 20/10/2023 tarih ve saat 17:00 ye kadar U.Ü. Rektörlüğü Bilgi İşlem Daire Başkanlığına elden teslim edileceği gibi posta yoluyla da gönderilebilir. (Not: Fax ile gönderilen teklifler geçerli sayılmayacaktır.)

1. Teklif mektubu imzalı ve kaşeli olmalıdır.
2. Teklifin hangi tarihe kadar geçerli olduğu belirtilmelidir.
3. Sipariş sonrasında mal/hizmetin kaç günde teslim edileceği belirtilmelidir.
4. Teklif mektubuna dosya numarası yazılmalıdır.
5. Kısmi teklif verilmeyecektir.
6. Mal/Hizmetle ilgili her türlü giderler (Montaj, nakliye, sigorta, vergi, vb.) tedarikçiye aittir.
7. Teklifler **KDV hariç** olarak **TL** cinsinden verilmelidir. (TL cinsinden verilmeyen teklifler değerlendirmeye alınmayacaktır.)
8. Mal/Hizmet ile ilgili Garanti verilmelidir. (4077 sayılı Tüketici Korunması hakkında kanun ve ilgili mevzuat gereği)
9. Teklifler sıra numaralarına göre verilecektir.
10. Sipariş edilen mal/hizmetin teklifte belirtilen tarihe kadar teslim edilmesi , belirtilen tarihten sonra teslim edilmek istenilmesi halinde idare tarafından mal/hizmetin kabulü yapılmayacaktır.
11. **Aşağıda idare tarafından standart hale getirilen teklif mektubu eksiksiz doldurulup gönderilmesi ve teknik şartnamenin kaşeli imzalı olması halinde geçerli sayılacaktır.**

**Adres: Uludağ Üniversitesi Rektörlüğü – Bilgi İşlem Daire Başkanlığı Görükle Kampusü 16059 Nilüfer / BURSA**

**Tel : (0224) 294 05 00 Fax : (0224) 294 05 01**

**TEKLİF MEKTUBU**

**ULUDAĞ ÜNİVERSİTESİ REKTÖRLÜĞÜ**

**BİLGİ İŞLEM DAİRE BAŞKANLIĞINA**

**Tarih: …./…./2023**

|  |  |
| --- | --- |
| **Teklif Vermeye Yetkili Kişinin;** | |
| **Adı ve Soyadı** |  |
| **Firma Adı** |  |
| **Açık Tebligat Adresi** |  |
| **Vergi Dairesi ve Vergi Numarası** |  |
| **Telefon ve Fax Numarası** |  |
| **Elektronik Posta Adresi** |  |

|  |  |
| --- | --- |
| **Teklife İlişkin Kurum Dosya Numarası:** | |
| **Sıra No** | **Mal/Hizmet Cinsi** | **Miktarı** | **Birim Fiyatı** | **Toplam** |
| **1-** |  |  |  |  |
| **2-** |  |  |  |  |
| **3-** |  |  |  |  |
| **4-** |  |  |  |  |
| **5-** |  |  |  |  |
| **6-** |  |  |  |  |
| **KDV’siz Genel Toplam (TL)** | |  |

**1-** Yukarıda belirtilen **( …… Kalem )** mal/hizmet alımına ait teklifimizi **KDV** **hariç** ……………….. **TL** bedel karşılığında vermeyi kabul ve taahhüt ediyorum/ediyoruz.

**2-**Teklifimiz **…./…./2023**  tarihine kadar geçerlidir.

**3-**Söz konusu mal/hizmet idarece tarafımıza sipariş verilmesinden sonra **……………. takvim günü içerisinde** teslim edilecektir.

**4-** 4077 Sayılı Tüketici Koruması hakkında kanun ve ilgili mevzuat hükümlerini kabul ediyor, mal/hizmet için ……. (gün/ay/yıl) garanti taahhüt ediyorum.

**5-** Teklifimizin kabul edilmesi halinde sipariş yazısının, yukarıda yer alan; 🟋

**🞎** Elektronik posta adresime veya faks numarama tebligat yapılmasını kabul ediyorum.

**🞎** Elektronik posta adresime veya faks numarama tebligat yapılmasını kabul etmiyorum.

🟋**Teklif veren istekli kabul ettiği seçeneği yazacaktır.**

**Teklif Vermeye Yetkili Kişinin;**

**Adı ve Soyadı:**

**İmzası:**

**Firma Kaşe**

**Bursa Uludağ Üniversitesi Sızma Testi Hizmet Alım Şartnamesi**

1. **Amaç :**

Gerçek bir saldırganın kullandığı yöntemlerin ve bakış açısının kullanılması ve bu sayede

Rutin kontrollerde tespit edilemeyen güvenlik zafiyetlerinin belirlenmesi ve teknoloji bağımsız çözümler tavsiye edilmesi hedeflenmektedir.

1. **Tanımlar ve Kısaltmalar**

İDARE: Bu şartnamede, İşin sahibi Bursa Uludağ Üniversitesi’dir.

FİRMA: Taahhüt işini yüklenecek firma

YÜKLENİCİ: Taahhüt işini yüklenen firma

İSTEKLİ: Teklif veren firma

PROJE: İşbu ihale çerçevesinde gerçekleştirilecek tüm faaliyetler

CEH : Certified Ethical Hacker

TSE : Türk Standartları Enstitüsü

1. **Kapsam :**

İdarenin belirteceği bir adet uygulama için yapılması gereken testlerin kapsamı aşağıda belirtilmiştir.

* + 1. Web Uygulamaları
    2. Kaynak Kod Tarama

1. **Genel Şartlar**
   1. Teknik Güvenlik Denetimleri Kurum tarafından yürütülen iş süreçleri, uygulamalar ve fiziksel olarak merkez binası ile sınırlı olacaktır.
   2. Yüklenici, bu teknik şartname kapsamındaki projenin eksiksiz olarak tamamlanmasından sorumlu olacaktır.
   3. Sızma testi sonucunda tespit edilen açıklıkların Kurum tarafından kapatılmasının ardından Yüklenici kontrol denetimi yapacaktır.
   4. Projede görev alacak tüm uzmanlar Türkiye Cumhuriyeti vatandaşı olacak ve hizmet tümüyle Türkiye Cumhuriyeti sınırları içerisinde verilecektir.
   5. Test ve inceleme hizmetlerini yürütecek personel/personeller güncel olan CEH, ECSA/LPT, OSCP, TSE Beyaz Şapkalı Hacker sertifikalarından en az birine sahip olacak ve personel/personeller Yüklenicinin çalışanı olacaktır.
   6. Penetrasyon testini sağlayacak Yüklenici TSE Onaylı Pentest firması unvanına sahip olacaktır.
   7. Yüklenici yapılacak tüm testlerin zamanlarını ve sürelerini Kurum ile birlikte belirleyecektir.
   8. Yüklenici yapılacak tüm testler Kurum ile birlikte koordineli bir şekilde gerçekleştirilecektir. Kurum yetkililerine bilgi verilmeden herhangi bir denetim çalışması yapılmayacaktır.
   9. Yükleniciden daha önce yaptığı testlerle ilgili örnek raporlar istenebilecektir.
   10. Testler belirli ip adreslerinden yapılacak ve bu ip adresleri Kurum’a bildirilecektir.
   11. Yüklenici test için kullandıkları standartları Kurum’a bildirecektir.
   12. Yüklenici tarafından Kurum’a verilecek raporlar okunabilir ve anlaşılır olacaktır.
   13. Yüklenici proje kapsamında hazırlayacağı ve Kurum'a sunacağı bütün dokümanları Türkçe olarak hazırlayacaktır.
   14. Yüklenici projeyi belirtilen zaman planına uygun şekilde tamamlayacak, zaman planında gecikme olmaması için gerekli önlemleri alacaktır.
   15. Yüklenici proje kapsamında en az bir proje yöneticisi atayacaktır.
   16. Proje yöneticisi proje boyunca Kurum ile sürekli ilişki içerisinde olarak, gerekli koordinasyonu sağlayacaktır.
   17. İçeride yapılacak testlerde kullanılacak (dizüstü bilgisayar, masaüstü bilgisayar vb.) cihazlar Yüklenici tarafından temin edilecektir.
   18. Yapılacak tüm sızma testleri , çalışmakta olan sistemleri kesintiye uğratmayacak şekilde gerçekleştirilecektir.
   19. Projenin başlangıcında Yüklenici ile Kurumun arasında şartname dışında gizlilik sözleşmesi imzalanacaktır.
   20. Yüklenici analizin sonuçlarına ilişkin proje bazlı raporlar hazırlayacakve idareye sunacaktır.
   21. Firma, aşağıda maddelenmiş olan hizmetleri eksiksiz bir şekilde vermeyi taahhüt etmelidir.
       1. Kaynak Kod Testi
       2. Web Uygulaması Testi
2. **Web Uygulamaları**
   1. Sunucular üzerinde çalışan servislerin ya da işletim sistemlerinin bilinen açıklıklarının araştırılmasının yanında, sistemdeki uygulamalara has güvenlik açıklıkları da araştırılmalı ve asgari olarak aşağıda listelenen açıklık ve zafiyetlerin varlığına ilişkin testler gerçekleştirilmelidir.
      1. Veri Denetimi
      2. Yetersiz Girdi Denetimi
      3. Yetersiz Çıktı Denetimi
      4. XSS Enjeksiyonu (XSS Injection)
      5. SQL Enjeksiyonu (SQL Injection)
      6. Diğer Enjeksiyonlar (XPATH, LDAP v.b.)
      7. HTTP Yanıt Bölme (HTTP ResponseSplitting)
      8. Kontrolsüz URL Yönlendirmeleri
   2. Oturum Yönetimi
      1. Oturum Sabitleme (SessionFixation)
      2. Çerez Etiketlerinin Kullanılmaması
      3. Yetersiz Oturum Sonlandırma Fonksiyonu
      4. Oturum Bilgisinin URL İçinde Taşınması
      5. Siteler Arası istek Sahteciliği (Cross-Site RequestForgery, CSRF)
   3. Kimlik Doğrulama ve Yetkilendirme
      1. Yetki Arttırımı, Yetkilendirmenin Atlatılması
      2. Eksik Hesap/Parola Yönetimi ve Yetersiz Parola Politikası
      3. Kimlik Doğrulamanın Atlatılması
      4. Tersine yol ( PathTraversal)
      5. Uygulama Mantığı Hatları ( Application LogicFlaw, Business LogicFlaw)
   4. Bilgi Sızdırma ve Ayar Yönetimi
      1. Minimum Bilgi Prensibine Aykırı Yardım Sayfaları, HTML Yorumları, Hata Mesajları, Hata Sayfaları ve Durumlar
      2. Veri İletiminde SSL Kullanılmaması
      3. Zayıf veya Geçersiz SSL Sertifikası Kullanılması
      4. Sunucu Bilgisinin Kısıtlanmaması
      5. Kullanılan Teknoloji Bilgisinin Kısıtlanmaması
      6. Yedeklenmiş ve Unutulmuş Dosyaların Varlığı
      7. Yönetici Ara yüzüne Erişim
      8. Hizmet Dışı Bırakma
      9. Kaba Kuvvet Saldırısına Açık Ekranlarda Risk Azaltıcı Metotlar kullanılmaması
3. **Kaynak Kod Tarama :**
   * 1. Build: Projenin başarıyla derlenmesi.
     2. Translate: Fortify kodlarının, tarama aracının anlayacağı dile çevrilmesi.
     3. Scan: Projenin taranması ve olası güvenlik açıklarının belirlenmesi.
4. **İşin Süresi :**
   * 1. Yüklenici, Sözleşmenin İmzalanmasından sonra 10 Aralık 2023 tarihinden önce bu şartnamede konu olan tüm süreçleri tamamlayacaktır.