DERS BİLGİ FORMU

<table>
<tr><td>DERSİN ADI</td><td colspan="4">SİBER GÜVENLİK ATÖLYESİ</td></tr>
<tr><td>DERSİN SINIFI</td><td colspan="4">10. Sınıf</td></tr>
<tr><td>DERSİN SÜRESİ</td><td colspan="4">Haftalık 5 Ders Saati</td></tr>
<tr><td>DERSİN AMACI</td><td colspan="4">Bu derste öğrenciye; bilişim ve siber güvenlik etiği, ağ ve sistem güvenliği, kriptografi, mobil ve web uygulama güvenliği, IoT ve bulut güvenliği, veri tabanı sistemleri güvenliği uygulamaları yapma ile ilgili bilgi ve becerilerin kazandırılması amaçlanmaktadır.</td></tr>
<tr><td>DERSİN ÖĞRENME KAZANIMLARI</td><td colspan="4">1. Siber güvenlik kavramlarını açıklar.
2. Ağ ve sistem güvenliği ilkelerine uyarak ağ cihazlarının güvenlik uygulamalarını yapar.
3. Kriptografi algoritmalarını açıklayarak uygulamalar yapar.
4. Mobil uygulamalar geliştirerek güvenlik denetimlerini yapar.
5. Web uygulamaları geliştirerek güvenlik denetimlerini yapar.
6. IoT mimarisini açıklayarak güvenlik testi uygulamalarını yapar.
7. Bulut bilişim mimarisini açıklayarak güvenlik denetimlerini uygular.
8. Veritabanı yönetim kavramlarını açıklayarak veritabanı güvenliği uygulamalarını yapar.</td></tr>
<tr><td>EĞİTİM-ÖĞRETİM ORTAM VE DONANIMI</td><td colspan="4">Ortam: Bilişim Teknolojileri laboratuvarı,

Donanım: Akıllı tahta/projeksiyon, bilgisayar, yazıcı/tarayıcı, ağ cihazları, sanallaştırılmış bilgisayar</td></tr>
<tr><td>ÖLÇME VE DEĞERLENDİRME</td><td colspan="4">Bu derste; öğrenci performansı belirlemeye yönelik çalışmalar değerlendirilirken gözlem formu, derecelendirme ölçeği ve dereceli puanlama anahtarı gibi ölçme araçlarından uygun olanlar seçilerek kullanılabilir.

Bunun yanında öz değerlendirme ve akran değerlendirme formları kullanılarak öğrencilerin, öğretimin süreç boyutuna katılmaları sağlanabilir.</td></tr>
<tr><td rowspan="8">KAZANIM SAYISI VE SÜRE TABLOSU</td><td>ÖĞRENME BİRİMİ</td><td>KAZANIM SAYISI</td><td>DERS SAATİ</td><td>ORAN (%)</td></tr>
<tr><td>Siber Güvenliğe Giriş</td><td>7</td><td>25</td><td>14</td></tr>
<tr><td>Ağ ve Sistem Güvenliği</td><td>8</td><td>25</td><td>14</td></tr>
<tr><td>Kriptografi</td><td>5</td><td>15</td><td>8</td></tr>
<tr><td>Mobil Uygulama Güvenliği</td><td>4</td><td>30</td><td>17</td></tr>
<tr><td>Web Uygulama Güvenliği</td><td>4</td><td>35</td><td>20</td></tr>
<tr><td>IoT Güvenliği</td><td>4</td><td>15</td><td>8</td></tr>
<tr><td>Bulut Bilişim Güvenliği</td><td>4</td><td>15</td><td>8</td></tr>
</table>

	Veritabanı Sistemleri ve Güvenliği	5	20	11
TOPLAM		43	180	**100**

ÖĞRENME BİRİMİ	KONULAR	ÖĞRENME BİRİMİ KAZANIMLARI ve KAZANIM AÇIKLAMALARI
Siber Güvenliğe Giriş	• Siber güvenlik etik ilkeleri • Siber güvenlik kavramları • Fiziksel güvenlik • Bilgi güvenliği standartları • Dijital arşivleme • Adli bilişim kavramları • Siber güvenlik sertifika programları	**1. Siber güvenlik etik ilkelerini açıklar.** • Bilgi gizliliği ve etik kavramları açıklanır. • Bilgi güvenliği uygulamasıyla ilgili yasal problemler ve telif hakları açıklanır. • Siber güvenlik uzmanlarının ahlaki sorumlulukları açıklanır. **2. Siber güvenlik kavramlarını açıklar.** • Güvenli dijital vatandaşlık özellikleri açıklanır. • Siber zorbalık kavramı açıklanır. • Gizlilik, bütünlük ve erişebilirlik güvenlik unsurları açıklanır. • Siyah Şapkalı, Beyaz şapkalı ve Gri Şapkalı Hacker özellikleri açıklanır. • Siber saldırı türleri açıklanır. • Arka kapı ve kötü amaçlı yazılım özellikleri açıklanır. **3. Fiziksel güvenlik ile ilgili kavramları açıklar.** • Fiziksel güvenliğin önemi açıklanır. • Fiziksel güvenlik önlemleri açıklanır. **4. Bilgi güvenliği standartlarını açıklar.** • Kişisel verilerin korunması kanunu açıklanır. • Bilgi güvenliği yönetimi (ISO/IEC 27001) standardı açıklanır. • Bilgi güvenliği kontrolleri (ISO 27002) standardı açıklanır. • Uluslararası siber güvenlik (ISO/IEC 27032) standardı açıklanır. **5. Dijital arşivlemeyi açıklar.** • Arşivleme açıklanır. • Dijital arşivleme açıklanır. • Dijital arşivleme adımları açıklanır. **6. Adli bilişim ile ilgili kavramları açıklar.** • Adli bilişimde delil kavramı açıklanır. • Adli bilişimde delillerin bulunabileceği ortamlar açıklanır. • Adli bilişimde delil toplama teknikleri açıklanır. • Adli bilişimde delil karartma yöntemleri açıklanır. • Disk imajı alma uygulaması yaptırır. **7. Siber güvenlik sertifika programlarını açıklar.** • Beyaz şapkalı hacker (CEH) sertifika programı açıklanır. • Siber olaylara müdahale ekibi (CIRT) sertifika programı açıklanır. • Ofansif güvenlik (OSCP) sertifika programı açıklanır.

		• Adli bilişim sertifika programı açıklanır.
Ağ ve Sistem Güvenliği	• Ağ güvenliği ilkeleri • Ağ ve sistem güvenliği cihazları • Ağ güvenlik mimarileri • Ağ saldırı türleri • İşletim sistemi güvenlik ilkeleri • Sunucu sistemleri güvenlik ilkeleri • Ağ cihazlarının sıkılaştırılması • Donanım güvenliği ilkeleri	**1. Ağ güvenliği ilkelerini açıklar.** • Ağ güvenliğinin önemi tanımlanır. • Ağ güvenlik planındaki gerekli adımlar tanımlanır. **2. Ağ ve sistem güvenliği cihazlarını açıklar.** • Ağ ve sistem güvenliğine yönelik atakları algılama ve önleme cihazları açıklanır. • Güvenlik duvarı cihazı açıklanır. **3. Ağ güvenlik mimarilerini açıklar.** • Güvenli ağ mimarisi çeşitleri açıklanır. • Güvenlik mimarisinde kullanılan aktif pasif güvenlik sistemleri açıklanır. • Ağda sanal yerel alan ağ (VLAN) kullanımı açıklanır. • Tek güvenlik duvarı ile gerçeklenmiş ağ mimarileri açıklanır. • İki veya daha fazla güvenlik duvarı ile gerçeklenmiş ağ mimarisi açıklanır. • Saldırı tespit ve önleme sistemleri ile gerçeklenmiş ağ mimarileri açıklanır. • Sanal özel ağ cihazları ile gerçeklenmiş ağ mimarileri açıklanır. **4. Ağ saldırı türlerini açıklar.** • Yetkisiz erişim elde etmek için parola kırma teknikleri açıklanır. • DoS ve DDoS ataklarının temel ilkeleri açıklanır. • SQL Injection temel ilkeleri açıklanır. • Man in The Middle ataklarının temel ilkeleri açıklanır. **5. İşletim sistemi güvenlik ilkelerini açıklar.** • İşletim sistemi güvenlik yapılandırmalarını uygulatır. • İşletim sistemi güncelleme ve güvenlik eklentilerini yükletir. **6. Sunucu sistemleri güvenlik ilkelerini açıklar.** • Servis yapılandırmalarını güvenlik ilkelerini uygulayarak yaptırır. • Erişim izinleri ve yetkilendirme ilkeleri açıklanır. • Sunucu rollerini güvenlik ilkelerine göre açıklanır. **7. Ağ cihazlarının sıkılaştırılması ile ilgili kavramları açıklar.**

		• TELNET ve SSH protokolleri açıklanır. • Ağ cihazlarının yapılandırma kontrolleri açıklanır. • Güvenlik duvarı kurallarını yapılandırma kontrollerini yaptırır. • Güvenlik sistemlerinin yapılandırma kontrolünü yaptırır. **8. Donanım güvenliği ilkelerini açıklar.** • Donanımların fiziksel güvenlik ilkeleri açıklanır.
Kriptografi	• Kriptografiye Giriş • Hash Fonksiyonu • Simetrik Kriptografi • Asimetrik Kriptografi • Steganografi	**1. Klasik Kriptografi Sistemlerini açıklar.** • Klasik kriptografi sistemleri açıklanır. • Sezar algoritması açıklanır. • Vigenere şifrelemesi açıklanır. • Yerine koyma şifrelemesi açıklanır. • Hill şifreleme algoritması açıklanır. • Vernam Cipher şifreleme algoritması açıklanır. • LFSR algoritması açıklanır. **2. Özet (Hash) fonksiyonlarını açıklar.** • MD5 hash algoritması açıklanır. • MD5 online ve offline araçlarını kullanarak uygulama yaptırır. • SHA hash algoritması açıklanır. • SHA online ve offline araçlarını kullanarak uygulama yaptırır. **3. Simetrik kriptografiyi açıklar.** • Simetrik kriptografi açıklanır. • Blok şifreleme açıklanır. • DES kripto algoritması açıklanır. • 3DES kripto algoritması açıklanır. • AES kripto algoritması açıklanır. • SEAL kripto algoritması açıklanır. • RC kripto algoritması açıklanır. • Akış (A5/1) şifreleme algoritması açıklanır. **4. Asimetrik kriptografiyi açıklar.** • Asimetrik kriptografi açıklanır. • Çarpanlarına ayırma tekniği açıklanır. • Asallık testi tekniği açıklanır. • Kesikli logaritma tekniği açıklanır. • Diffie-Helman algoritması açıklanır. • ElGamal algoritması açıklanır. • RSA Algoritması açıklanır. • Eliptik Eğri algoritması açıklanır. **5. Steganografi tekniğini açıklar.** • Çevrimiçi / çevrimdışı araçlarla resim içinde metin gizleme uygulaması yaptırır. • Çevrimiçi / çevrimdışı araçlarla resim içinde resim gizleme uygulaması yaptırır.

Mobil Uygulama Güvenliği	• Mobil uygulama kavramları • Mobil uygulama kod editörü • Mobil uygulamalarda güvenlik denetimi • Mobil sistemlerde zararlı yazılım analizi	**1. Mobil uygulama kavramlarını açıklar.** • Mobil uygulama similatör arayüzü açıklanır. • Mobil uygulama kod blok yapısı açıklanır. **2. Mobil uygulama kod editörünü kullanır.** • Kod editörü üzerinde mobil işletim sistemleri simülatörlerini çalıştırır. • Mobil uygulama güvenlik denetimi için ortam oluşturur. • Mobil uygulama kaynak kod denetimi yaptırır. **3. Güvenlik denetimleri için mobil uygulamalardan bilgi toplar.** • Çevrimiçi araçlardan yararlanarak mobil uygulamalardan bilgi toplanır. • Çevrimdışı araçlardan yararlanarak mobil uygulamalardan bilgi toplanır. **4. Mobil sistemlerde zararlı yazılım analiz yöntemlerini kullanır.** • Statik kod analizi tekniklerini uygulatır. • Dinamik kod analizi tekniklerini uygulatır.
Web Uygulama Güvenliği	• Web uygulama kavramları • Web uygulama kod editörü • Web uygulamaları • Uygulama güvenliği	**1. Web uygulama kavramlarını açıklar.** • Web uygulama temel kavramları açıklanır. **2. Web uygulama kod editörünü kullanır.** • .Net Core web editörü arayüzü açıklanır. • PHP web editörü arayüzü açıklanır. **3. Web uygulamaları gerçekleştirir.** • Web servis güvenliği protokollerini uygulanır. • .Net Core tabanlı web uygulaması gerçekleştirir. • Php tabanlı web uygulaması gerçekleştirir. **4. Uygulamaları güvenli hale getirmek için gerekli işlemleri yapar.** • İstemci taraflı girdi denetimini gerçekleştirir. • Sunucu taraflı girdi denetimini gerçekleştirir. • Pozitif girdi denetimi gerçekleştirir. • Çıktı denetimini gerçekleştirir. • XSS denetimini gerçekleştirir. • Kör SQLi (Blind SQLi) uygulaması gerçekleştirir. • Oturum yönetimi temel ilkeleri açıklanır.

IoT Güvenliği	• Nesnelerin İnterneti (IoT) mimarisi • IoT zafiyet ve tehditleri • IoT güvenlik tedbirleri • IoT güvenlik testi	**1. Nesnelerin İnterneti (IoT) mimarisi kavramlarını açıklar.** • Üç katmanlı IoT mimarisi açıklanır. • Beş katmanlı IoT mimarisi açıklanır. • IoT referans mimarisi açıklanır. **2. IoT zafiyetlerini tespit ederek tehditleri açıklar.** • IoT zafiyetleri açıklanır. • IoT zafiyetlerini tespit eder. **3. IoT güvenlik tedbirlerini açıklar.** • IoT yazılım güvenlik tedbirleri açıklanır. • IoT donanım güvenlik tedbirleri açıklanır. **4. IoT güvenlik testini yapar.** • IoT yazılım güvenlik testi gerçekleştirir. • IoT donanım güvenlik testi gerçekleştirir.
Bulut Bilişim Güvenliği	• Bulut mimarisi ve altyapı güvenliği • Bulut güvenliği ve risk yönetimi • Bulut bilişimde veri güvenliği • Kimlik yönetimi denetimi	**1. Bulut mimarisi ve altyapı güvenliğini açıklar.** • Bulut mimarisi açıklanır. • Bulut bilişim altyapı güvenliği ilkeleri açıklanır. **2. Bulut güvenliği ve risk yönetimi işlemlerini gerçekleştirir.** • Bulut güvenliği ile ilgili temel kavramları açıklanır. • Bulut bilişimde risk yönetimi temel kavramları açıklanır. • Bulut güvenliği risklerini azaltıcı önlemler uygulanır. **3. Bulut Bilişimde Veri Güvenliği adımlarını uygular.** • Bulut bilişimde veri güvenliği adımları açıklanır. • Bulut bilişimde veri güvenliğini arttırıcı uygulamaları yaptırır. **4. Bulut Bilişimde Kimlik Yönetimi denetimlerini gerçekleştirir.** • Bulut bilişimde kimlik yönetimi açıklanır. • Bulut bilişimde kimlik yönetimi denetimlerini gerçekleştirmek için gerekli işlemleri yaptırır.
Veritabanı Sistemleri ve Güvenliği	• Veritabanı yönetim sistemleri • Veritabanı yönetim sistemlerin kurulumu • Veritabanı yönetim sistemlerinin kullanımı • Sql, nosql uygulamaları • Veritabanı güvenliği	**1. Veritabanı Yönetim Sistemlerini açıklar.** • Veritabanı kavramı açıklanır. • Veritabanı yönetim sistemleri tanımlanır. **2. Veritabanı Yönetim Sistemlerini kurar.** • Veritabanı yönetimi sistemlerinin kurulumunu yaptırır. **3. Veritabanı Yönetim Sistemlerini kullanır.** • Veritabanı yönetim sistemi arayüzü açıklanır. • Veritabanı yönetim sistemi yapılandırmalarını gerçekleştirir.

		• Veritabanı yönetim sistemi arayüzünü kullanarak tablolar oluşturur. • Veritabanı yönetim sistemi arayüzünü kullanarak tablolar arası ilişkileri oluşturur. **4. SQL, NoSQL uygulamalarını kullanır.** • SQL kavramları açıklanır. • NoSQL kavramı açıklanır. • SQL ve NoSQL arasındaki farklar açıklanır. • Veritabanı yönetim sistemi kullanılarak SQL uygulaması yaptırılır. • Veritabanı yönetim sistemi kullanılarak NoSQL uygulaması yaptırılır. **5. Veritabanı Güvenliğini sağlar.** • Veritabanı güvenliği temel ilkeleri açıklanır. • Güvenli veritabanı için gerekli yapılandırmaları gerçekleştirir.
UYGULAMA FAALİYETLERİ/TEMRİNLER		
Uygulama faaliyeti/temrinler; ders kazanımına uygun olarak okulun fiziki kapasitesi ve donatımı, öğrenci sayısı göz önünde bulundurularak en fazla uygulama faaliyeti/temrini yaptıracak şekilde meslek, alan zümre öğretmenler kurulu tarafından seçilir. Meslek, alan zümre öğretmenleri tarafından aşağıda yer alan temrinlerden farklı temrinlerin uygulanmasına karar verilebilir**.**		
Siber Güvenliğe Giriş	**1.** Siber güvenlik uzmanının sorumluluklarını özetleyen bir sunum hazırlamak **2.** Siber saldırı türleri ile ilgili bir sunum hazırlamak **3.** Ağ cihazlarının fiziksel güvenliğini sağlama uygulaması yapmak **4.** IoT cihazlarının fiziksel güvenliğini sağlama uygulaması yapmak **5.** Bilgi güvenliği standartları ile ilgili bir poster hazırlama uygulaması yapmak **6.** Bilgisayar adli analizi hazırlık aşamaları ile ilgili sunum hazırlamak **7.** Adli bilişim için disk imajı alma uygulaması yapmak	
Ağ ve Sistem Güvenliği	**1.** VLAN oluşturma uygulaması yapmak **2.** Tek güvenlik duvarı kullanılarak ağ kurulumu yapmak **3.** İki veya daha fazla güvenlik duvarı kullanılarak ağ kurulumu yapmak **4.** IPS ve IDS kullanılarak ağ kurulumu yapmak **5.** DMZ ağı uygulaması yapmak **6.** Dos ve DDoS ataklarını simüle eden uygulamaları kullanmak **7.** İşletim sistemi güvenlik yapılandırmalarını uygulamak. **8.** İşletim sistemi güncelleme ve güvenlik eklentilerini yüklemek **9.** Servis yapılandırmalarını güvenlik ilkelerini uygulamak **10.** Sunucu kullanıcı yetkilendirme ilkeleri uygulaması yapmak **11.** Ağ cihazlarının ve sistemlerinin yapılandırma uygulaması yapmak	
Kriptografi	**1.** Sezar algoritması ile uygulama yapmak. **2.** Vigenere şifrelemesi uygulaması yapmak. **3.** Yerine koyma şifrelemesi uygulaması yapmak. **4.** Hash fonksiyonları ile uygulama yapmak. **5.** Simetrik kriptografi uygulamaları yapmak. **6.** Asimetrik kriptografi uygulamaları yapmak. **7.** Steganografi tekniğini kullanarak uygulamalar yapmak.	

Mobil Uygulama Güvenliği	**1.** Mobil uygulama geliştirme simülatörü kurulum uygulaması yapmak **2.** Simülatör üzerinde temel seviyede kod geliştirme uygulaması yapmak **3.** Mobil uygulama kaynak kod denetimi uygulaması yapmak **4.** Çevrim içi ve çevrim dışı araçlar kullanılarak mobil uygulamalardan veri toplama uygulaması yapmak **5.** Statik ve Dinamik kod inceleme teknikleri kullanımı uygulaması yapmak
Web Uygulama Güvenliği	**1.** .Net Core web editörü kurulum uygulaması yapmak **2.** PHP web editörü kurulum uygulaması yapmak **3.** .Net Core uygulaması geliştirmek **4.** PHP uygulaması geliştirmek **5.** İstemci ve sunucu taraflı girdi denetimleri için, HTTP (post, get, put metotları), URL, URN, DOM (Domain Object Model), SOP (Same Origin Policy), HTML5, WebSocket, WebGL, WebCL, SSL/TLS) uygulamaları geliştirmek **6.** Güvenli kimlik doğrulama ve yetkilendirme için SOAP, SAML, WS-I uygulamaları geliştirmek **7.** Oturum çalma uygulaması yapmak **8.** Oturum bilgisinin tahmin edilmesi uygulaması yapmak **9.** Oturum sabitleme uygulaması yapmak **10.** Oturumda hak yükseltme uygulaması yapmak, **11.** Oturumda yetkisiz işlem yapılması uygulaması yapmak **12.** XSS denetimi uygulaması yapmak **13.** Kör SQLi (Blind SQLi) uygulaması yapmak
IoT Güvenliği	**1.** IoT cihazlara web arayüzden ulaşma uygulaması yapmak **2.** IoT cihazlara güvenlik yapılandırma uygulaması yapmak **3.** IoT iletişimde güvenli iletişim protokollerini (MQTT, XMPP, AMQP, DDS) kullanma uygulaması yapma **4.** IoT yazılım zafiyetlerini tespit etmek için test araçları kullanmak **5.** IoT donanım zafiyetlerini tespit etmek için test araçları kullanmak
Bulut Bilişim Güvenliği	**1.** Bulut bilişimde veri sızıntılarına neden olan insan hataları veya dikkatsizliğine sebep olan durumlar için sunum yapmak **2.** Bulut bilişimde kimlik ve erişim yönetimi (IAM) uygulaması yapmak **3.** Bulut bilişim sistemlerini izleme, uyarı ve raporlama uygulaması yapmak **4.** Bulut bilişimde veri güvenliği için şifreleme uygulaması yapmak **5.** Bulut bilişimde veri güvenliği için yük dengeleyicisi (load balancer) uygulaması yapmak **6.** Bulut bilişimde veri güvenliği için yük devretme sistemi (failover system) uygulaması yapmak
Veritabanı Sistemleri ve Güvenliği	**1.** Veritabanı yönetim sistemi kurulumu yapmak **2.** Veritabanı yönetim sistemi arayüzü ile veritabanı oluşturma, tablo oluşturma uygulaması yapmak **3.** Veritabanında tablolar arası ilişki kurma uygulaması yapmak **4.** Veritabanında SQL sorgu komutları yazmak **5.** Veritabanında NoSQL sorgu komutları yazmak **6.** Veritabanı normalizasyon uygulaması yapmak **7.** Veritabanı güvenli erişim uygualaması yapmak **8.** SQL/NoSQL yerleştirme saldırılarını önleme uygulaması yapmak **9.** DoS/DDoS saldırısı önleme uygulaması yapmak **10.** Arabellek taşması uygulaması yapmak **11.** SQL kimlik bilgilerine deneme yanılma saldırısı uygulaması yapmak

DERSİN UYGULANMASINA İLİŞKİN AÇIKLAMALAR
1. Bu derste, verilen görevi yapma değer, tutum ve davranışları ön plana çıkaran etkinliklere yer verilmelidir. 2. Her öğrencinin uygulama yapması için ortam oluşturulmalıdır. 3. Uygulama faaliyetlerinde İş sağlığı ve güvenliğine ilişkin risk ve tehlike oluşturacak her türlü duruma karşı tedbirler alınmalıdır. 4. Bu dersin işlenişi sırasında yasalara uyma, çevre temizliği, emeğe saygı, özgüven, kendini ifade edebilme, emanete sahip çıkma, hedef belirleme, işbirliği, vb. değer, tutum ve davranışları ön plana çıkaran etkinliklere yer verilmelidir. 5. Bu etkinliklerde beyin fırtınası, grup tartışması, düz anlatım, soru cevap, örnek olay incelemesi gibi yöntem ve teknikler kullanılabilir. 6. Uygulama faaliyetleri ve temrinler örnek olup, örnekler çoğaltılmalıdır.