29.12.2022
Ödev No: 7

BM359 – İNTERNET PROGRAMLAMA

Web Güvenliği

Ümmü Nur GÜLMEZ
Bilgisayar Mühendisliği Bölümü – 191180762

Özet

Web güvenliği, bir web sitesinin veya web uygulamasının güvenliğini sağlamaya yönelik önlemlerdir. Web güvenliği, genellikle bir web sitesine veya web uygulamasına yönelik saldırıları önlemek için yapılır. Bu tür saldırılar arasında SQL injection, cross-site scripting (XSS) ve cross-site request forgery (CSRF) gibi saldırılar bulunur. Web güvenliği, bir web sitesinin veya web uygulamasının güvenliğini sağlamak için güncel tutulma, güvenlik duvarı ve güvenlik testleri gibi yöntemler kullanılır. Bu sayede, bir web sitesi veya web uygulaması güvenliği tehdit eden saldırılardan korunur ve web sitesi veya uygulamanın performansı bozulmadan çalışır. Web güvenliği, bir web sitesinin veya web uygulamasının güvenliğini sağlamak için önemlidir ve bu sayede bir web sitesi veya web uygulaması kullanıcıların güvenliğini de sağlar. Zararlı yazılımlar, bir bilgisayar veya ağı tehdit eden yazılımlardır. Zararlı yazılımlar, genellikle bir bilgisayar veya ağın performansını bozar ve güvenliğini tehdit eder. Bu tür yazılımlar arasında virüsler, Trojanlar, ransomware, adware ve diğer zararlı araçlar bulunur. Zararlı yazılımlar, genellikle bir bilgisayara veya ağa yönelik saldırılar için kullanılır ve bu sayede bilgisayar veya ağın güvenliği tehdit edilir. Web güvenliği tehditleri, bir web sitesine veya web uygulamasına yönelik saldırıları ifade eder. Web güvenliği tehditlerini önlemek için çeşitli önlemler alınabilmektedir. Bunlara örnek olarak internet protokolü güvenliği, ağ katmanı güvenliği ve çok faktörlü kimlik uygulama verilebilir.

Web Güvenliği Nedir?

Web güvenliği, internet üzerinde yapılan etkinliklerin güvenliğini sağlamak amacıyla kullanılan önlemler ve yöntemlerdir. Bu önlemler ve yöntemler, internet üzerinde kişisel bilgilerinizin gizliliğini ve güvenliğini koruma, bilgiye erişimin kontrolü, cihazlarınızın ve ağlarınızın güvenliğini sağlama, internet üzerinde yapılan işlemlerin doğruluğunu ve bütünlüğünü koruma gibi amaçları vardır. Web güvenliği, özellikle internet üzerinde ödeme işlemleri yapılırken, alışveriş yapılırken ve kişisel bilgilerinizi paylaştığınız durumlarda önemlidir. Bu nedenle, internet üzerinde gezinirken ve online işlemler yaparken güvenliğinizi sağlamaya yönelik önlemler almanız önerilir. Web güvenliği önlemleri arasında şifreleme, güvenlik duvarı kullanımı, güncel güvenlik yazılımlarının kullanılması, phishing saldırılarına karşı dikkatli olmak gibi önlemler yer alır. Ayrıca, internet üzerinde gezinirken dikkatli olunması ve güvenilir kaynaklardan bilgi edinilmesi de web güvenliği açısından önemlidir.

Zararlı Yazılımlar Nedir?

Zararlı yazılımlar, bilgisayar ve diğer cihazların güvenliğini tehdit eden yazılımlardır. Bu yazılımların birçok türü vardır ve genellikle kötü niyetli olarak tasarlanmışlardır. Aşağıda zararlı yazılımların bazı örnekleri bulunmaktadır:

1. **Virüsler:** Virüsler, bilgisayarınızın dosyalarını değiştirerek veya bilgisayarınızın işlevselliğini bozarak zarar verirler. Virüsler genellikle e-posta ekleri veya indirilen dosyalar gibi güvenilmeyen kaynaklardan yüklenirler ve bilgisayarınızın işlevselliğini bozarak veya çalışmamasına neden olarak zarar verirler.
2. **Wormlar**: Wormlar, bilgisayar ağları üzerinden kendi kendine yayılan ve yüksek miktarda trafik üreten zararlı yazılımlardır. Wormlar bilgisayarınızın performansını düşürerek ve ağın işlevselliğini bozararak zarar verirler.
3. **Trojanlar:** Trojanlar, güvenilir görünümlü uygulamalar veya dosyalar içinde gizlenmiş zararlı yazılımlardır. Trojanlar kötü niyetli olarak tasarlanmışlardır ve genellikle bilgisayarınızın güvenliğini tehdit ederler. Trojanlar, bilgisayarınızın güvenliğini tehdit ederek veya bilgisayarınızın performansını düşürerek zarar verirler.
4. **Ransomware**: Ransomware, bilgisayarınızdaki verilerin kilidini açmak için para talep eden zararlı yazılımlardır. Ransomware, genellikle e-posta ekleri veya indirilen dosyalar gibi güvenilmeyen kaynaklardan yüklenir ve bilgisayarınızdaki verilerin kilidini açmak için para talep eder.

Şekil 1 – Zararlı Yazılım Örnekleri

Web Tehditi Güvenliği Çeşitleri Nelerdir?

- **Hizmet Reddi Saldırıları:** Hizmet reddi saldırıları (DoS attack), bir web sitesi veya bir ağın performansını bozarak veya tamamen çalışmamasını sağlayan saldırılardır. Bu tür saldırılar, ağa aşırı miktarda istek göndererek veya ağın çalışmasını engelleyecek şekilde bir ağ trafiği üreterek yapılır. Bu sayede, hedef ağın veya web sitesinin kullanılması engellenir ve hizmet reddedilir. DoS saldırıları, genellikle kötü niyetli olarak tasarlanmışlardır ve ağın performansını bozarak veya tamamen çalışmamasını sağlayarak zarar verirler. Bu tür saldırılar, genellikle kuruluşların çalışmasını engelleyerek veya ticari faaliyetlerini etkileyerek zarar verirler.
- **E-dolandırıcılık**: E-dolandırıcılık, internet üzerinden yapılan dolandırıcılık faaliyetleridir. E-dolandırıcılar, genellikle insanların kişisel bilgilerini ve finansal bilgilerini çalarak veya yanıltarak para kazanmayı amaçlarlar. Bu tür dolandırıcılık faaliyetleri, genellikle e-posta, sosyal medya veya diğer internet platformları üzerinden gerçekleştirilir. E-dolandırıcılar, insanların güvenini kazanmak için yalan ve yanıltıcı bilgiler kullanırlar ve insanları para göndermeye veya kişisel bilgilerini vermeye ikna etmeye çalışırlar. E-dolandırıcılık türleri arasında, sahte ürün satışı, sahte kazanç fırsatları, sahte hizmetler ve sahte lotteri çekilişleri gibi faaliyetler bulunur.

- **<u>Uygulama Güvenlik Açıkları:</u>** Uygulama güvenlik açıkları, bir uygulamanın güvenliğini tehdit eden ve uygulamanın performansını bozan hatalardır. Bu hatalar, genellikle uygulamanın yazılımında bulunur ve uygulamanın güvenliğini tehdit ederek veya uygulamanın performansını bozararak zarar verirler. Uygulama güvenlik açıkları türleri arasında şu örnekler verilebilir:

❖ **SQL injection**: Bu tür bir güvenlik açığı, veritabanına yönelik bir saldırıdır ve veritabanına zararlı sorgular gönderilerek veritabanının işlevselliğini bozar.

❖ **Cross-site scripting (XSS**): Bu tür bir güvenlik açığı, bir web sitesine zararlı JavaScript kodları gönderilerek web sitesinin güvenliğini tehdit eder.

❖ **Cross-site request forgery (CSRF):** Bu tür bir güvenlik açığı, bir kullanıcının oturum açmış olduğu bir web sitesine yönelik bir saldırıdır ve kullanıcının bilgisi olmadan web sitesine zararlı istekler gönderilerek web sitesinin güvenliğini tehdit eder.

Web Tehditlerine Karşı Alınabilecek Önlemler Nelerdir?

Ağ Katmanı Güvenliği: Ağ katmanı güvenliği, bir ağın güvenliğini sağlamaya yönelik önlemlerdir. Ağ katmanı güvenliği, genellikle bir ağın fiziksel veya sanal ağ cihazlarının güvenliğini sağlar. Bu cihazlar arasında router, switch, firewall gibi cihazlar bulunur. Ağ katmanı güvenliği, bir ağın performansını bozan ve güvenliğini tehdit eden saldırıları önlemek için yapılır. Bu tür saldırılar arasında, DoS saldırıları, virüsler, Trojanlar ve diğer zararlı yazılımlar gibi saldırılar bulunur. Ağ katmanı güvenliği, genellikle ağ cihazlarının yapılandırılması ve güncel tutulması ile sağlanır. Bu sayede, ağ cihazları güvenlik açıklarından korunur ve ağın performansı bozulmadan çalışır. Ayrıca, ağ cihazlarının yapılandırılması sayesinde ağ trafiği filtre edilerek güvenlik önlemleri alınır.

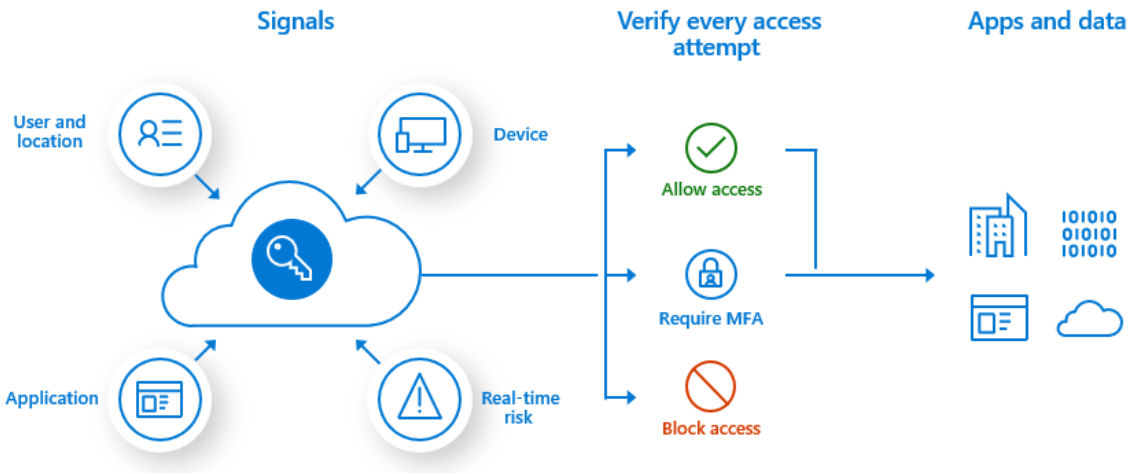
İnternet Protokolü Güvenliği (IPsec): İnternet Protokolü Güvenliği (IPsec), bir ağ üzerindeki verilerin güvenliğini sağlamaya yönelik bir protokoldür. IPsec, bir ağ üzerinde iletişim kurulurken verilerin şifrelenmesini ve güvenliğini sağlar. Bu sayede, ağ üzerinde iletişim kurulurken verilerin güvenliği korunur ve verilerin gizliliği sağlanır. IPsec, bir ağ üzerinde iletişim kurulurken verilerin güvenliğini sağlamak için iki ana yöntem kullanır:

- **Veri İletim Güvenliği (ESP):** Bu yöntem, bir ağ üzerinde iletişim kurulurken verilerin şifrelenmesini sağlar. Bu sayede, verilerin güvenliği korunur ve verilerin gizliliği sağlanır.

- **İletişim Güvenliği Protokolü (AH):** Bu yöntem, bir ağ üzerinde iletişim kurulurken verilerin değiştirilmesini önler. Bu sayede, verilerin güvenliği korunur ve verilerin doğruluğu sağlanır.

IPsec, genellikle bir ağ üzerinde iletişim kurulurken verilerin güvenliğini sağlamak için kullanılır ve ağ cihazları arasında iletişim kurulurken verilerin güvenliğini sağlar. IPsec, ayrıca bir ağ üzerinde iletişim kurulurken verilerin gizliliğini de sağlar ve verilerin güvenliği için güçlü şifreleme algoritmaları kullanır.

Çok Faktörlü Kimlik Doğrulama: Çok faktörlü kimlik doğrulama (multi-factor authentication, MFA), bir kullanıcının kimliğini doğrulamaya yönelik bir güvenlik yöntemidir. MFA, bir kullanıcının kimliğini doğrulamak için birden fazla faktör kullanır ve bu faktörler arasında parola, cep telefonu veya biyometrik veriler gibi faktörler bulunur. MFA, bir kullanıcının kimliğini doğrulamak için birden fazla faktör kullanır ve bu sayede kimlik doğrulama işlemi daha güvenlidir. MFA sayesinde, bir kullanıcının kimliğini doğrulamak için sadece bir parola kullanılmaz ve bu sayede kullanıcının kimliği daha güvenli bir şekilde doğrulanır. MFA, genellikle bir kullanıcının hesabına erişim için kullanılır ve bir kullanıcının hesabına erişim için gerekli olan birden fazla faktörün doğrulanması gerekir. MFA sayesinde, bir kullanıcının hesabına erişim için gerekli olan birden fazla faktörün doğrulanması sayesinde hesabın güvenliği artar ve hesaba yönelik saldırılar önlenir.



Şekil 2 – Çok Faktörlü Kimlik Doğrulama

İnternet Güvenlik Ürünleri Nelerdir?

İnternet güvenlik ürünleri, bir bilgisayar veya ağın güvenliğini sağlamaya yönelik ürünlerdir. İnternet güvenlik ürünleri, genellikle bir bilgisayar veya ağın güvenliğini tehdit eden saldırılardan korunmak için kullanılır. Bu tür saldırılar arasında, virüsler, Trojanlar, zararlı yazılımlar ve diğer zararlı araçlar bulunur.

İnternet güvenlik ürünleri türleri arasında şu örnekler verilebilir:

- **Antivirüs yazılımı:** Bu tür bir ürün, bir bilgisayarda bulunan veya indirilen virüsleri tespit etmek ve önlemek için kullanılır. Antivirüs yazılımı, genellikle bir bilgisayarın güncel tutulması ve güncel bir antivirüs yazılımı kullanılması ile sağlanır.
- **Firewall:** Bu tür bir ürün, bir ağın güvenliğini sağlamaya yönelik bir üründür. Firewall, bir ağın güvenliğini sağlamak için ağ trafiğini filtre eder ve ağın güvenliğini tehdit eden saldırıları önler.
- **Güvenlik duvarı:** Bu tür bir ürün, bir ağın güvenliğini sağlamaya yönelik bir üründür ve ağın güvenliğini sağlamak için ağ trafiğini filtre eder. Güvenlik duvarı, ağın güvenliğini tehdit eden saldırıları önler ve ağın performansını bozan saldırıları filtreler.
- **Güvenlik yönetim sistemi**: Bu tür bir ürün, bir ağın güvenliğini yönetmek için kullanılır. Güvenlik yönetim sistemi, bir ağın güvenliğini sağlamak için ağ cihazlarını yönetir ve ağın güvenliğini tehdit eden saldırıları tespit eder.

Sonuç

Web güvenliği, bir web sitesinin veya web uygulamasının güvenliğini sağlamaya yönelik önlemlerdir. Web güvenliği, genellikle bir web sitesine veya web uygulamasına yönelik saldırıları önlemek için yapılır ve bu tür saldırılar arasında SQL injection, cross-site scripting (XSS) ve cross-site request forgery (CSRF) gibi saldırılar bulunur. Web güvenliği, bir web sitesinin veya web uygulamasının güvenliğini sağlamak için güncel tutulma, güvenlik duvarı ve güvenlik testleri gibi yöntemler kullanılır. Bu sayede, bir web sitesi veya web uygulaması güvenliği tehdit eden saldırılardan korunur ve web sitesi veya uygulamanın performansı bozulmadan çalışır.

Kaynakça

1- https://siberdagitim.com/Web-Sitesi-Guvenligi-nedir-a3#:~:text=Web%20sitesi%20g%C3%BCvenli%C4%9Fi%20%2C%20web%20sitelerini,k%C3%B6t%C3%BC%20ama%C3%A7l%C4%B1%20yaz%C4%B1l%C4%B1mlara%20kar%C5%9F%C4%B1%20taran%C4%B1r.
2- https://tr.wikipedia.org/wiki/%C4%B0nternet_g%C3%BCvenli%C4%9Fi
3- https://ikwebtasarim.com/blog/detay/web-sitesi-guvenligi-nedir-ve-nasil-saglanir
4- https://www.cybermagonline.com/daha-guvenli-web-uygulamalari-icin-10-altin-kural
5- https://www.beyaz.net/tr/guvenlik/makaleler/web_uygulama_guvenligi.html
6- https://serdizayn.com.tr/Blog/Web-Sitesi-Guvenligi-Nedir-Guvenlik-Aciklari-Nelerdir
7- https://www.mcafee.com/tr-tr/antivirus/malware.html
8- https://www.bilisimle.com/zararli-yazilimlar-cesitleri-ve-korunma-yontemleri-nelerdir/