# WEB SECURITY RUDIMENTS

## ( SUMMARY )

Nowadays web is being an important part of life. Its usage areas are increasing day by day. As web sites are increasing attacks to web sites are increased too. It's not because web application's count is getting higher, it's because applications are not developed security in mind which makes attackers job easier. Because of these, web application's security becomes an important subject today.

There are some applications that people get knowledge about security subjects. One of the most common used sources is MSDN documents but it gives a wide research area for its users and gives detailed information about each web security subject. But MSDN does not give chance to try some attacks or test them. Also there is a project developed by OWASP named GoatProject but there is not enough information in this project.

Purpose of this project is to help people for learning web security. Furthermore, chance to try securing and insecure solutions will be given to the users. By the way users could get educational information about web security, also test attacks, see the results and learn usages of protection methods.

In the project general security management principles, tips for implementing better protections are introduced. Furthermore attacks, how they are made, how to protect applications from these attacks are told and tools for trying these attacks, protection advices are included. The subjects which are searched and implemented are: digital certificates, different security tokens, code access security, role based security, denial of service attacks, importance of permissions, allocating memory on disk for anonymous users, SQL injection attacks, shell code injection attacks, script injection attacks, input validity and buffer overrun attacks.

# WEB GÜVENLİK TEMELLERİ

## ( ÖZET )

Günümüzde web hayatın vazgeçilmez bir parçası olmuştur, kullanım amaçları ve alanları hızla artmaktadır. Web sitelerinin artması aynı zamanda web sitesi saldırılarına da ortam hazırlamıştır. Elbette bu saldırıların artmasının ve sıkça başarılı olarak sonuçlanmasının altında web sitelerinin artmasından ziyade web uygulamalarının ve sistemlerinin güvenliğine yeterince önem verilmemesi yatmaktadır. Web siteleri hızlı bir şekilde hazırlanıp sunulmaktadır. Özellikle forum, hazır web portal yazılımları; dinamik içerik sağlamak için veritabanı desteği sağlayan uygulama kodları (php, asp, jsp, cgi … vb) web sitesinin en zayıf halkalarını oluşturmaktadır. Bu sitelerin hazırlanırken hiçbir güvenlik kontrolünün yapılmadığını, kodlarda kullanıcıdan girdi alınan kısımlarda, alınan verinin hiç kontrol edilmediğini gözlenmektedir. Özetle güvenlik, planlama, geliştirme ve hatta test aşamalarında göz ardı edilmekte, bu da bir çok kullanıcının dikkatsiz geliştirilmiş uygulamalardan zarar görmesine neden olmaktadır.

Bu olumsuz gidişat nedeniyle web uygulamalarının güvenliği son zamanlarda önem kazanan bir konu haline gelmiştir fakat ne yazık ki web güvenliği konusunda eğitici uygulamaların sayısı oldukça azdır. Web güvenliği konusunda internet ortamında bilgi ednilebilecek kaynaklardan biri MSDN'de yer alan dökümanlardır fakat kullanıcıya test etme, sonuçları gözlemleme gibi fırsatlar verilmemekte ve güvenlik başlığı altında tüm konuları toplamamktadır. Bununla birlikte verilen bilgiler Microsoft ürünleri odaklıdır. Diğer bir ürün ise OWASP tarafından geliştirilen GoatProject'tir. Bu projede kullanıcıya test imkânı verilirken, yeterli bilgi verilmemiş ve az sayıda sorun ele alınmıştır. Bu eksikliği

tamamlamak amacıyla bu projede önemli web uygulamaları güvenliği konuları incelenmiş ve eğitici bir web uygulaması hazırlanmıştır.

Projenin amacı web sitesinin kullanıcılarının web güvenliğinin önemini kavramasını sağlamak, sıkça görülen ataklar konusunda haberdar etmek, bu hususlarda gerekli bilgiyi sağlamak, bununla birlikte kullanıcıya bu ataklar ve sonuçlarını görebileceği bir ortam hazırlamaktır. Proje böylece web uygulamasının güvenliği konusunda yeterli bilincin oluşturulması hedeflenmektedir.

Projede dijital sertifika, kod güvenliği, rol tabanlı programlama, kullanıcıya diskte yer ayırma, “session” yönetimi, “Denial of Service” atakları, “script injection”, “shell code injection”, “sql injection”, “buffer overrun”, “input validity”, “reply attacks”, “form validity” gibi çok önemli ve güncel ataklar ve güvenlik yöntemleri ele alınmıştır. Proje kapsamında öncelikle bu atakların ne oldukları, ne şekilde saldırganlar tarafından kullanıldığı, nasıl olumsuz sonuçlar doğurdukları ve de en önemlisi ne şekilde önlem alınacağı konusunda detaylı incelemeler yapılmıştır. Bu incelemeler bir web sitesi yardımı ile kullanıcılara sunulmuştur. Bunun yanında projelerde web güvenliğine ilişkin plan yapılmasının önemini ve ne şekilde plan yapılabileceği konusunda öneriler sunan ve güvenlik konusunda bazı ipuçlarının yer aldığı sayfalarda bulunmaktadır.

Kullanıcı web sitesini ziyaret ettiğinde bir çok atak ile ilgili bilgi edinebilecek, bununla birlikte bazı konuların kullanımı, kodun efektifliği hakkında bilgi sahibi olmak için hazırlanan deneme alanlarını kullanabilecektir.

Kullanıcının site üzerinde gerçekleştirebileceği temel işlemler şöyle sıralanabilir:

- Bir projede güvenlik planlama hususunda bilgi edinebilir.
- İpuçları yardımı ile geliştirdiği bir projeyi güvenlik açsından daha efektif hale getirebilir.

- Digital sertifikalar konusunda bilgi edinebilir, web servisleri ile bağlantı sırasında SOAP paketlerinin güvenli ve güvenli olmayan durumlar oluştuğunda ne şekilde iletildiğini görebilir. Bununla birlikte değişik güvenlik jetonları hakkında bilgi sahibi olabilir, değişik jetonlar kullanılması durumunda oluşturulan SOAP paketi içeriklerini görebilir. Dijital sertifikaların kullanılmaması yahut yanlış kullanılması durumunda ortaya çıkabilecek güvenlik açıkları ve bunların nasıl gerçekleştirileceği konusunda bilgi sahibi olabilir.
- Rol tabanlı yazılımın hakkında bilgi edinebilir ve önemini web sitesinde verilen alanı kullanarak kavrayabilir. Erişimin sınırlandırılmasının ne şekilde güvenliğe katkısının olduğunu görebilir.
- Kod erişim güvenliği unsurlarının kullanılarak, bazı kritik noktalarda ne şekilde önlem alınması gerektiğini görebilir.
- Kullanıcıya verilen izinlerin hassasiyeti nedeni ile kullanıcıya diskten ne şekilde yer ayrılacağı konusunda tavsiyeleri ve bu kullanımın ne şekilde gerçekleştiğini görebilir.
- Dinamik yapılı sitelerin işledikleri kodların işleniş şekillerinin ve üretilen sonuçların önemliliği hakkında fikir sahibi olabilir.
- Veritabanı güvenliği, oturum güvenliği, form güvenliği gibi kritik konularda bilgi sahibi olabilir.
- Katmanlı yapının ne anlama geldiği ve neden önemli olduğunu anlayabilir.

- Kodun karmaşıklığının önemi ve yazılan uygulamanın minimum alan, zaman ve kaynak almasının önemini, aksi halde oluşacak istenmeyen durumları öğrenebilir ve test edebilir.

Bu hizmetlerin verilebilmesi için geliştirme sürecinde öncelikle birbirinden farklı güvenlik unsurlarını inceleyen parçalar belirlenmiştir. Geliştirme sırasında bu parçalar tek tek ele alınmıştır. Her biri için veri tabanı, sınıflar oluşturulmuştur. Ardından öğretici olacak şekilde her parça için güvenli ve güvensiz çözümleri içeren geliştirilmeler yapılmıştır. Bu geliştirilmelerin uygun şekilde yansıtılması için ara yüz oluşturulmuştur. Tüm parçaların ayrı ayrı tamamlanmasından sonra, genel taslak hazırlanmış ve parçalar tek bir web sitesinde toplanmıştır.

Projenin geliştirilmesi sırasında en önemli sorunlardan biri, geliştirilen projede izin verilen güvensiz yöntem denemelerinin sınırlandırılması ve oluşturulan web sitesinin kendisinin güvenli olmasının sağlanmasıdır. Bunun için kullanıcıya sınırsız izin verilmemiş, belirli kısıtlamalar getirilmiştir. Kullanıcı güvensiz yöntemleri belirli bir çerçeve içerisinde denemektedir fakat güvensiz yöntemdeki açığı görüp, anlayabileceği gerekli bilgi, açıklama kendisine verilmektedir.

Sonuç olarak proje kapsamında web uygulamalarının güvenliği ile ilgili bir çok konu, bilhassa sıkça görülen ve önemli ataklar incelenmiştir. Web uygulamalarının güvenliğine ilişkin dokümantasyon hazırlanmış, atakları önlemek için çözüm yöntemleri geliştirilmiştir. Bu yöntemler ve araştırmalar hakkında kısa bilgi ise site ziyaretçileri ile paylaşılmak üzere web sitesine eklenmiştir. Her konu başlığının altında ilgilenilen açık için kullanıcının

anlayabileceği, deneme yapabileceği, güvenli ve güvensiz yöntemleri içeren bir uygulama, test etme alanı web sitesi ziyaretçilerini hizmetine sunulmuştur.

# INDEX