

# Web Güvenliđi ve Özgür Yazılım

Bünyamin Demir, Mesut Timur, Yusuf Çeri, Bedirhan Urgan

*Web Güvenlik Topluluđu*

*bünyamin@owasp.org, mesut@h-labs.org, yusufceri4@yahoo.com, urgunb@hotmail.com*

## Özet

*İnternet kullanımının hayatımızdaki yeri ile beraber Web uygulamaları/servisleri güvenliđinin önemi de artmaktadır. Web güvenliđi farkındalıđının artmasında anahtar rolü oynayacak en önemli adımlardan biri de “açık sistem” mantıđını benimsemiş toplulukların kurulması ve işleyişidir.*

## 1. Giriş

Son senelerde, Dünya’da ve Türkiye’de artarak devam eden (Web) uygulama güvenliđi önemi, Open Web Application Security Project (OWASP) [1] ve Web Application Security Consortium (WASC) [2] gibi halka açık özgür toplulukların oluşmasını ve kabul görmesini tetiklemiştir. İstatistiklere göre her 10 web sitesinden 9’unda ciddi seviyede bir açıklıđın olmasının yanında siber saldırıların %60’ından fazlasının web teknolojilerine yönelik gerçekleştirilmesi [3], bu toplulukların kısa bir zamanda önem kazanmasında, yaygınlaşmasında ve standardlaşmasında bir katalizör ödevi görmüştür. Bu bağlamda, OWASP-Türkiye’nin [4] işleyişine 2007’nin ortalarından sonra aktif bir şekilde devam etmesi ve bunun yanında Türkçe yayın yapan Web Güvenlik Topluluđu’nun (WGT) [5] yine aynı dönemde çalışmalarına başlaması, ülkemizdeki genelde siber güvenlik özelde ise web güvenliđi bilincine katkı sağlamaktadır.

Topluluđuun başlangıcından bu yana gerçekleştirdiđi aktiviteleri üç ana başlıkta ele almak mümkündür; etkinlikler, dokümantasyon projeleri ve özgür yazılımlar.

## 2. Etkinlikler

WGT’nin kurulduktan sonraki ilk adımı, bilgi güvenliđinin paylaşıldıđı etkinlikler olmuştur. 2007 yılı içerisinde “Web Güvenliđi Günleri” (WGG) adı altında Temmuz’da İstanbul ve Kasım ayı içerisinde

Ankara ve İzmir’de üç ana etkinlik gerçekleştirilmiştir [6]. Bu etkinliklerde yaklaşık 200 katılımcı etkinlikler boyunca web güvenliđi standartları, atak teknikleri, analizleri ve web güvenliđinin hukuk boyutu ile ilgili olarak bilgilendirilmiştir.

Ana etkinliklerin yanısıra ara buluşmalar ve başka etkinliklere katılmak yolu ile konu ile ilgili bireylerin birbirini tanınması ve bilgi paylaşımları sağlanmaya çalışılmıştır.

## 3. Dokümantasyon

Siber güvenliđin genelinde olduđu gibi Web güvenliđinde de en önemli nokta yazılım güvenliđidir. Güvenli yazılım geliştirme standartlarının ve süreçlerinin nadiren uygulandıđı veya hiç uygulanmadıđı özel yapım uygulamalarda güvenlik problemlerinin çıkması kaçınılmazdır. Güvenli yazılım sürecinin en önemli parçalarından biri de geliştiricilerin, kullandıkları teknolojilerde ortaya çıkabilecek güvenlik problemlerinin farkında olmalarıdır. Bu bilinci arttırmanın bir yolu da güvenlik standartlarının açıklandıđı dokümanlardır. OWASP’n dünya çapında tanınmasında ve kabul görmesinde etkili unsurlardan biri ürettiđi kaliteli web ve uygulama güvenliđi dokümanlarıdır. OWASP-Türkiye’nin amaçlarından biri de bu dokümanların Türkçe’ye çevirilmesidir. Bu kapsamda açılmış gönüllü çeviri projesinde, 22 doküman ile beraber toplamda yaklaşık 300 sayfa OWASP dokümanı dilimize kazandırılmıştır [7] ve kazandırılmaya devam etmektedir.

Dokümantasyon kapsamında bahsedilebilecek diđer projeler; ilgililerin hızlı bilgi paylaşımını sağlayabilecekleri e-posta listesi, sadece ülkemizdeki web güvenlik olayları ile ilgili elektronik basında çıkan haberlerin ve gerçekleştirilen saldırı türlerinin bulunabileceđi bir liste projesi ve çođunlukla İngilizce kelimelerden oluşan Web güvenlik terimlerinin Türkçe karşılıklarını içeren interaktif sözlük projesidir [8].

## 4. Yazılım

WGT, etkinlikler ve dokümantasyon projeleri ile beraber yazılım projeleri de üretmektedir. Ülkemizde en ciddi, yaygın ve farkındalığı en fazla olan [9] açıklıklardan SQL Enjeksiyonu ile alakalı olarak yapılan ve aynı zamanda bir OWASP projesi olan “Otomatize Sql Enjektörleri Analizi” bu yazılım/analizlerden biridir. Diğer küçük uygulamaların yanında üretilmekte olan en önemli yazılım projesi son bir iki senedir gittikçe popüler hale gelen Web uygulama güvenlik duvarı ModSecurity [10] ile ilgilidir. Yine aynı zamanda bir OWASP projesi olan “WeBekci”, ModSecurity güvenlik duvarı için hazırlanmış bir yönetim aracıdır [11]. Bu yazılım yardımı ile kurumlar/kullanıcılar, web servislerini ve uygulamalarını açık kaynak kodlu ModSecurity ile korurken, bu kapsamlı ve bir çok açıdan karmaşık yazılımın yönetimini de kolaylıkla yapacaklardır.

## 5. Sonuç

Web güvenliği ve uygulama güvenliği bilincini ülkemizde arttırmak, kurumların daha güvenli yazılımlar geliştirmelerini desteklemek ve yazılım güvenliği araştırma, geliştirmesine önyak olmak OWASP Türkiye ve Web Güvenlik Topluluğu'nun en önemli amaçları arasındadır. Böyle bir girişimin Türkiye'de öncülüğünü yapmanın gururunu duyuyor

ve bu organizasyonun tüm ilgili kurumlara faydalı olmasını umuyoruz.

## 7. Kaynakça

- [1] OWASP, <http://www.owasp.org>
- [2] WASC, <http://www.webappsec.org>
- [3] Web Güvenliği Saldırı İstatistikleri Analizi, <http://www.whitehatsec.com/home/assets/presentations/PPTs/tats032608.pdf>
- [4] OWASP-TR, <http://www.owasp.org/index.php/Turkey>
- [5] WGT, <http://www.webguvenligi.org>
- [6] WGG, [http://www.webguvenligi.org/?page\\_id=85](http://www.webguvenligi.org/?page_id=85)
- [7] WGT çeviri, [http://www.webguvenligi.org/?page\\_id=16](http://www.webguvenligi.org/?page_id=16)
- [8] WGT sözlük, <http://www.webguvenligi.org/sozluk/>
- [9] WGT Web güvenliği farkındalık anketi, <http://www.webguvenligi.org/?p=104>
- [10] ModSecurity, <http://www.modsecurity.org>
- [11] WeBekci, [http://www.webguvenligi.org/?page\\_id=9](http://www.webguvenligi.org/?page_id=9)