Web Uygulama Guvenlik Duvarı Tercih Rehberi

Web uygulama güvenlik duvarınızı seçmeden önce bu yazıyı okumanız önemle tavsiye olunur

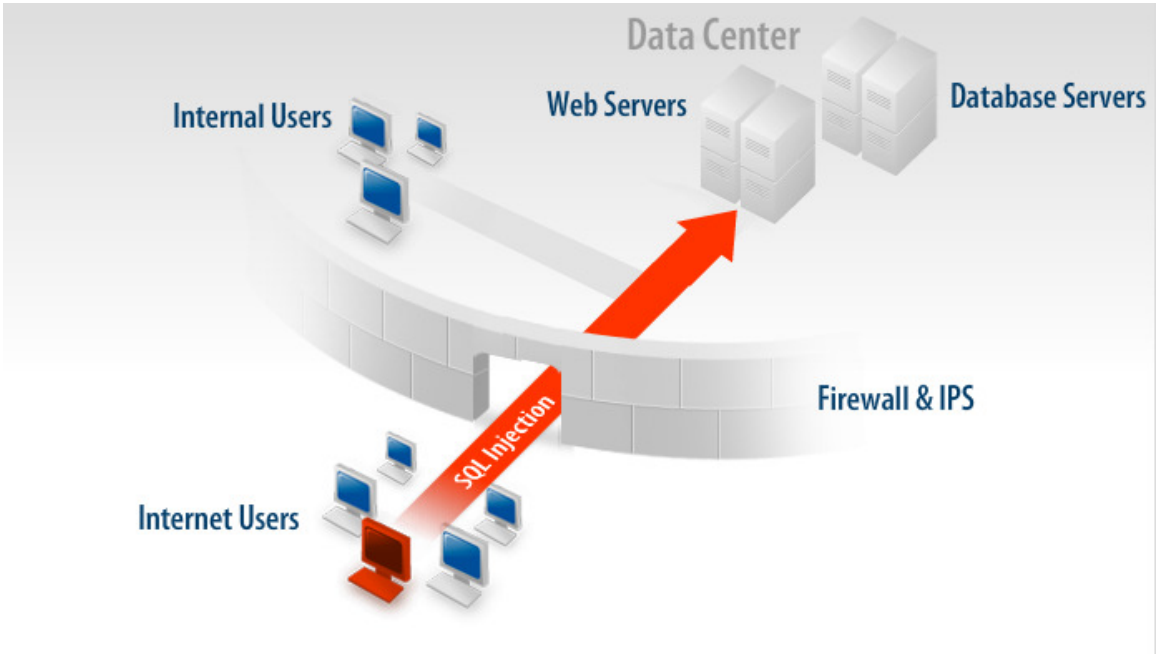
Web Uygulama Güvenlik Duvarı nedir?

Günümüzde hemen hemen internete açık her şirket güvenlik duvarı kullanmaktadır. Kimileri bunu güvenlik amaçlı kimileri de getirdiği ek özellikler için tercih ederler. Klasik güvenlik duvarları ip adresi, port numarası, bağlantı durumu gibi bir paketi OSI katmanında 4. seviyeye kadar inceleyerek karar verirler. Bazı güvenlik duvarları yedinci katmana kadar çıkarak belirli protokoller için inceleme imkânı sunsa da günümüz için bunlar istisna sayılacak kadar azdır.

Yakın gelecekte artık port kavramı yerine uygulama kavramına göre kurallar yazılan güvenlik duvarlarının çıkması kaçınılmaz gözüküyor. Yani 80. porta izin ver yerine http protokolüne izin ver ya da 25. portu yasakla yerine smtp protokolünü yasakla şeklinde kural yazağımız günler çok uzak değil.

Geleceği bırakıp günümüz gerçeklerine dönecek olursak klasik güvenlik duvarları artık yeterli olmamaktadır. Bunun sebebi eskiden yapılan ataklar genelde network seviyesinde olur, network servislerini hedef alırdı

.



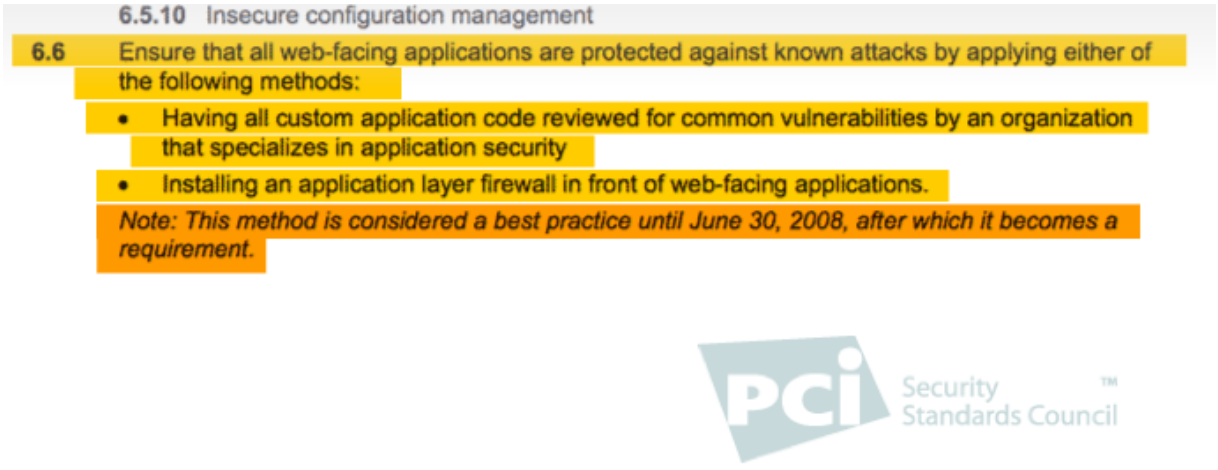
Şimdi ise gereksiz servisler güvenlik duvarları tarafından kapatılarak, açık olanlar için de güvenliğini kanıtlanmış, sıkılaştırılmış servisler ve IPS sistemleri kullanarak eski tip açıklıklardan büyük oranda kurtulunduğu söylenebilir.
Uygulamaların hızlı bir şekilde web üzerine kayması ile birlikte klasik firewallar için sadece açık port manasına gelen 80 ve 443 portları daha bir önem kazandı. Belirli güvenlik anlayışına sahip çoğu şirket gereksiz servisleri firewallar aracılığı ile kapatıyor fakat internete açılan kapıları olan web sunucular zorunlu olarak açık kalıyor. Hal böyle olunca saldırılar da bu portlar ve üzerinde çalışan uygulamara yöneldi. Web üzerinden sunulan servislerin çeşitliliği ve bu konuda oturmuş bir standart olmaması geliştirilen uygulamarın güvenlik yönünden yeteri olgunluğa erişememesine sebep oluyor.

Kullanılan uygulamaları tekrar basitleştiremeyeceğimize göre bunlar için önlem almakta fayda var. Web Uygulama Guvenlik duvarı -yazıda WAF(Web Application Firewall) olarak bahsedilecektir- olarak adlandırılan sistemler karmaşıklaşan web trafiği üzerinde detaylı inceleme yaparak anormal trafiği engellemeye yarayan teknoloji olarak karşımıza çıkıyor. Kısacası HTTP/HTTPS/SOAP/XML-RPC/Web Servisleri üzerinde detaylı paket incelemesi yaparak zararlı istekleri bloklamak için kullanılan bir araç diyebiliriz.

WAF sistemlerinin kullanımı bazı güvenlik standartları tarafından da tavsiye edilmekte. Bunların başında duruma göre WAF kullanımını zorunlu tutan PCI Veri Güvenliği standartı geliyor.

WAF kullanımı PCI DSS (6.6)'a göre zorunlu tutuluyor. Ya da kod analizi, kaynak kod incelemesi uzun vadede daha efektif bir çözüm sunsa da kısa vadede WAF çözümü daha uygun gözüküyor.

Diğer yandan kaynak kod incelemesi sadece incelenen koddaki açıklıkları bulur ve düzeltilmesi için çözümler sunarken WAF ile bu açıklıklar kapatılır.



6.5.10 Insecure configuration management

6.6 Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:

- Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security
- Installing an application layer firewall in front of web-facing applications.

Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.

PCI Security Standards Council

30 Haziran 2008 sonrası PCI uyumlu olma zorunluluğu bulunan tüm firmalar ya kod denetimi ya da WAF sistemini devreye almak zorunda.

WAF için temel kavramlar/ Güvenlik Modelleri

Positive security model(Beyaz liste modeli): İzin verilen belirli işlemler hariç her şeyin engellenmesi yaklaşımı. Sadece izin verilen objelerin belirlenmesi ve geri kalanların engellenmesini öngörür. Bu modeli kullanan ürünlerde sistemi tam devreye almadan positive modeli disable etmekte fayda var, yoksa model doğası gereği izin verilmeyen tüm her şeyi engelleyecektir.

Negative security model (Kara liste modeli): Yasaklanmış belirli işlemler hariç her şeye izin verilmesidir. Sadece yasaklanan objelerin belirlenmesi ve bunların dışındakilere izin verilmesini öngörür ve nadir durumlarda kullanılan bir yaklaşımdır.

learning-based firewall: Gelen ve giden istekleri inceleyerek web sayfalarının haritasını çıkarmaya çalışır. Burada web adminlerin katkısı WAF cihazına yönlendirilir ve öğrendikleri onaylanır ya da reddedilir. Bu işlem sonrasında artık web sayfasına yapılacak yeni tip ataklar kolaylıkla önlenecektir ya da sizin haberiniz dışında çalıştırılan web siteleri ortaya çıkacaktır.

Basit bir örnek verecek olursak, öğrenme sonrası http://www.example.com/~user/ dizini yasaklandıysa sonradan bu dizin altından okunmaya çalışılacak. bash_history dosyası herhangi bir incelemeye uğramadan engellenecektir ya da aynı sunucu üzerinde sizin haberiniz olmadan çalıştırılan www.xyz.com web sitesi farkedilerek engellenecektir. . Learning-based özelliği olmayan ürünlerde WAF arkasında koruma altına alınmak istenen tüm siteler tanımlanması gerekir.

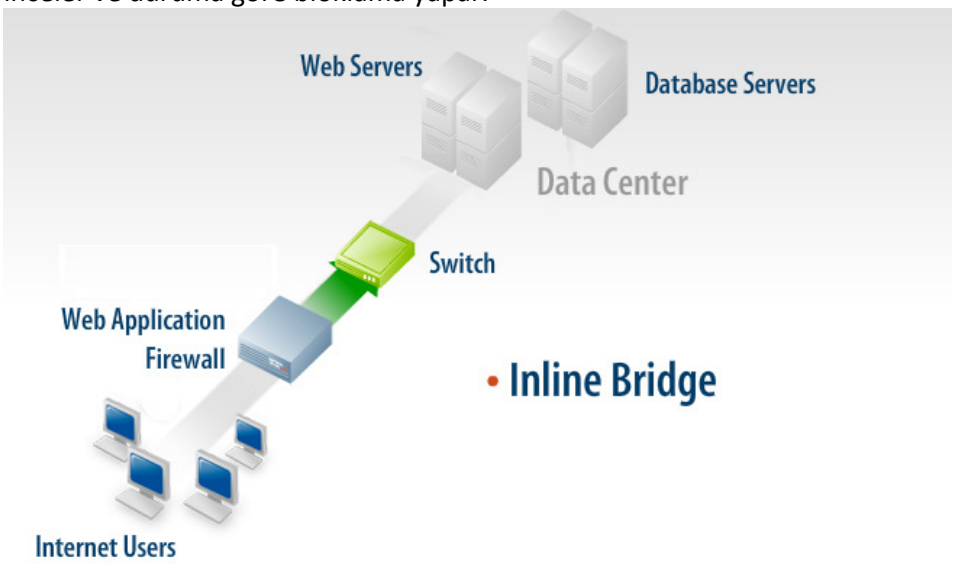
Çalışma yapısı

Yerleşim senaryoları

WAF için temelde dört yerleşim senaryosu vardır. Bunlar teknik olarak inline bridge, Offline(passive), integrated ve reverse proxy olarak adlandırılabilir. Yerleşim modeline göre ürün tercihi yapılmalıdır.

Bridge Yerleşim Modeli

Bu yöntemde WAF cihazının web sunucuların önüne bridge modda yerleştirilerek trafiği üzerinden geçirmesi ve incelemesi sağlanır... Bu yöntemin kullanılması durumunda ağ cihazlarında, web sunucularda ya da dns sunucularda herhangi bir değişiklik yapılması gerekmez.
Network tabanlı IPS benzeri bulunduğu konum üzerinden geçen tüm trafiği inline olarak alır, inceler ve duruma göre bloklama yapar.

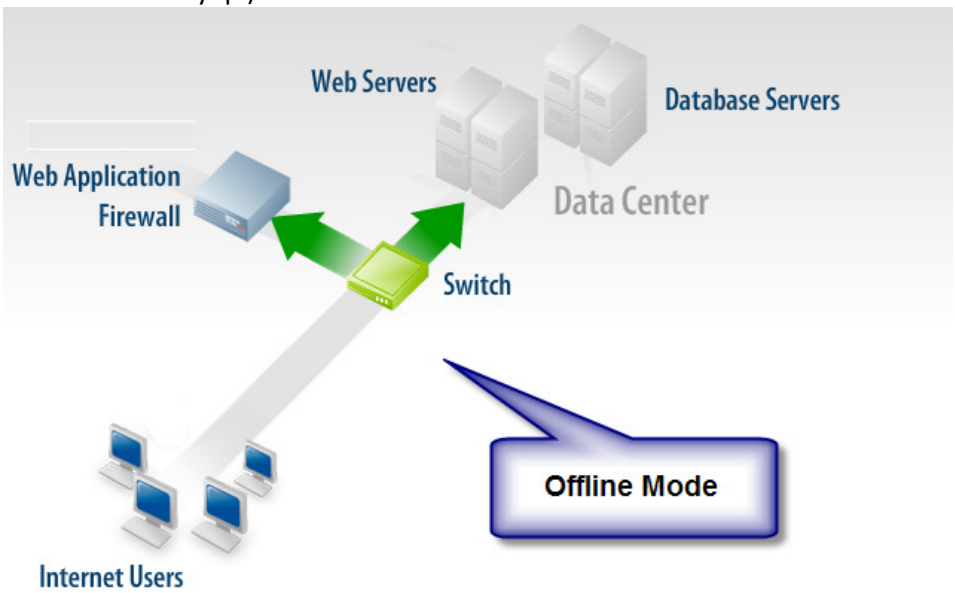


Tek dezavantajı sistemde yaşanacak bir arıza sonrası web trafiğinin kesilmesi olasılığıdır. Bu da ilgili cihazın fail-open(cihazda yaşanacak bir problem sonrası trafiğin akmaya devam etmesi) özellikde olması ile aşılabilir.

Offline(passive) Yerleşim Modeli

Bu yerleşim modelinde WAF Intrusion Detection System benzeri çalışır. WAF cihazı web sunucuların olduğu switch mirrorlarak ya da hub aracılığı ile bağlanır ve pasif olarak web sunuculara giden trafiğin bir kopyasını alır. Alınan kopya trafik üzerinde detaylı paket analizi yapılarak zararlı istekler için cevap üretilir, bu cevaplar TCP RST paketleridir. (Aktif yanıt IDS

sistemlerindeki yapı).



Burada aktif yanıt IDS sistemlerindekine benzer sorun ortaya çıkar. Saldırganın gönderdiği isteğin cevabı WAF tarafından gönderilecek TCP RST paketlerinden önce ulaşabilir ya da saldırgan http kullanarak geriye yönelik udp bağlantısı açmaya çalıştığında WAF cihazı işlevsiz kalabilir. Bu modelin kullanımında iyi karar verilmelidir ve TCP RST paketlerinin cevap paketlerinden önce hedefe ulaşması için yerleşimi iyice düşünülmelidir.

Bununla birlikte canlı trafiği üzerinden geçirmediği için sistem ek bir yük getirmez, sistem için "point of failure" konumunda olmaz ve Web sunucu, DNS sunucu üzerinde ek ayar gerektirmez.

Bütünleşik Yerleşim Modeli

Bu model türü en basit WAF yerleşimidir ve tamamen çalışan işletim sistemine, web sunucusuna bağlıdır. Mesela Microsoft IIS için kullanabileceğiniz xyz ürününü Linux üzerinde ya da Windows üzerinde Apache için kullanamazsınız, benzer şekilde Apache için Kullanılan modsecurity yazılımını IIS için kullanamazsınız. Bütünleşik WAF yazılımları yerine göre avantajlı olabilmektedir.
Özellikle koruyacağınız sistemlerin sayısı fazla değilse bu tip bir yazılım tercih edilebilir.

Reverse Proxy Yerleşim Modeli

Reverse Proxy yerleşim modeli bildiğimiz Proxy mantığı ile çalışır. Web sayfasına ulaşmaya çalışan tüm istemciler web sunucu yerine reverse Proxy modundaki WAF sistemine ulaşır,

WAF isteği aldıktan ve gerekli incelemelerden geçirdikten sonra arkadaki web sunucuya iletir veya doğrudan isteği bloklar.

Bu model, diğerlerine göre ortamda en fazla değişiklik gerektiren modeldir. Sağlıklı çalışacak bir yapı için dns, web sunucu ve network ayarlarında değişiklik gerektirir. WAF tarafından korunmaya alınacak tüm web sayfalarının A kayıtları WAF cihazına ulaşacak şekilde değiştirilmelidir ki dns üzerinde yapılacak değişikliklerin aktif olma süresini en az 12 saat düşünürsek bu zaman dilimi içerisinde web sayfasına ulaşımda problemler yaşanabilir.

Ek olarak web sunucuya gelen her istek ve dönen her cevap WAF sistemi üzerinden geçeceği için yine diğer yerleşim yöntemlerine oranla gecikme oranı (latency) daha yüksektir. Gecikme oranı caching, l7 compression vs gibi ek özellikler kullanılarak düşürülebilir. Bununla birlikte tüm paketler WAF üzerinden onaylı geçtiğinden dolayı http istek ve cevapları üzerinde daha sıkı kontroller yapma imkânı sağlar.

Aşağıdaki karşılaştırma tablosu bu dört farfklı yerleşim modeli için hangi özelliklerin hangi modelde kullanılabileceğini gösteriyor.

	Network architecture changes	Web server configuration changes	Site/ application changes	Network point of failure	Web server impact	Network separation	SSL	Changes client IP address	Blocking	Content rewriting	Performance enhancement (compression, caching, TCP multiplexing, ...)	Traffic management (routing, load balancing, ...)
Out of line	No	No	No	No	None	No	Passive decryption	No	TCP resets; 3rd party and application integration	No	No	No
Reverse proxy	Yes	Yes (1)	In some cases (2)	No, but requires HA configuration	None	Yes	Termination	Yes (1)	Intermediation w/buffering; 3rd party and application integration	Yes	Yes	Yes
Embedded	No	Yes - requires installation of the module into web server	No	No	Competes for server resources; can affect server on malfunction	No	Not applicable	No	Intermediation w/buffering; 3rd party and application integration	Yes	No	No
Transparent reverse proxy (layer 7)	No	No	In some cases (2)	No, when fitted with a fail-open card	None	Yes for HTTP, device must work as fw for other traffic	Termination	No	Intermediation w/buffering; 3rd party and application integration	Yes	Yes	No

Alacağınız ürünü görün, inceleyin ve karar verin

İhtiyaçları Belirleme

Alacağınız üründe kararınızı etkileyecek en önemli husus ihtiyaçlarınızdır. İhtiyaçlarınızı belirlemeden yapacağınız bir alım ilerde işe yaramayan cihazlar müzesine kaldırılmaya mahkûmdur. İhtiyaçları netleştirme konusunda geniş bir çalışma yaparak kurulacak sistemin hangi özellikleri barındıracağı, hangi tip sistem ve uygulamaları koruyacağı, cihazın/yazılımın yerleşim planı vs belirlenmelidir.

Mesela sistemlerinizin ihtiyaç duyabileceği SSL hızlandırma, caching, load balancing, fail-open gibi özellikler ve WAF'ı nerede konumlandırmak istediğiniz alacağınız ürünü tümden değiştirebilir. Zira piyasada tüm seçenekleri üzerinde barındıran ürün yok. Bununla birlikte ürünün sağladığı yapılandırma yönetimi, loglama, raporlama, sorun giderme özellikleri ve fiyat durumu da kararlarınızı etkileyecektir.

Karar öncesi ürün testleri

Nasıl test ederim?

İncelediğiniz ürün aşağıdaki atak türlerinin başarı ile yakalayıp engelleyebilmeli.

Buffer Overflow Exploit, Forceful Browsing, parameter tampering, Cookie/Session Poisoning, Form/Hidden Field Manipulation, Cross-Site Scripting (XSS), SQL Injection, Command Injection, Sensitive Information Leaks, Server Misconfiguration, Well-known Platform Vulnerabilities

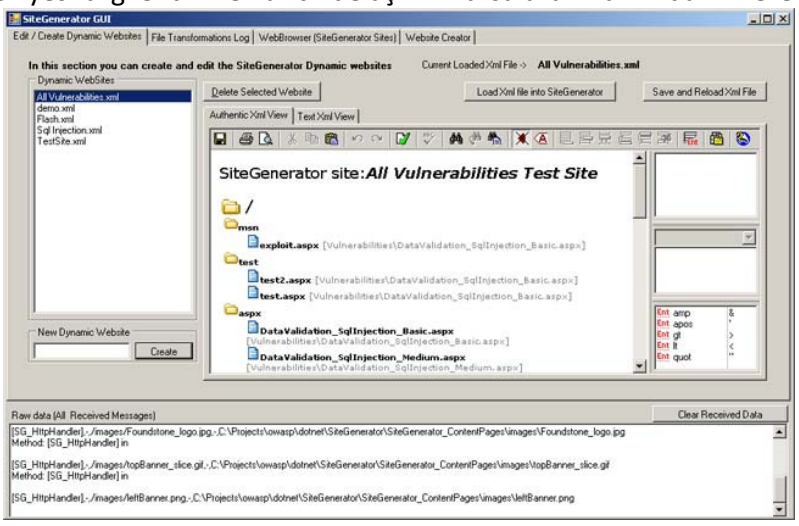
Performans testleri

curl-loader, siege, ab gibi araçlarla istemci simulasyonu yapılarak test edilir.

zayıflık testleri

Yapılacak en basit test sağlam bir web güvenlik tarayıcısı ile daha önce belirlediğimiz, çeşitli güvenlik zayıflıkları içeren web sayfasını taramak ve rapor oluşturmak. Sonra aynı taramayı araya WAF cihazı koyarak yapmak ve her iki raporu karşılaştırmak.

Bu test size en kısa yoldan test edeceğiniz WAF ürünü hakkında bilgi verecektir. Eğer delta raporda seviyesi bilgilendirme haricinde açıklık varsa ürün hakkında iki kere düşünmenizde fayda var.



Web Uygulama Güvenlik duvarı için test ortamı oluşturma

hangi araçları kullanarka nasıl yaparım
bir iki tane vulnerable site bulunabilir, eski phpnuke ve wordpress sürümleri iyi fikir.

False positive konusu çok önemli, koruma yaparken web sitenize giden normal istekleri de yasaklıyor olabilirsiniz.

Loglama konusu da önemli ve loglarda ne kadar detaylı bilgi verdiği. Bir url li blokluyorsa hangi kuraldan, hangi sebepten dolayı

blokladığını net gösterebiliyor olmalı.

Performans konusu: inline ya da reverse proxy olarak yerleştirilen ürünlerdeki en büyük çekince performans problemi ve single

point of failure olmasıdır.

++Alım konusunda incelenecek raporlar

Web uygulama güvenlik duvarı konseptinin başlancı 2000 yılı civarı olmasına rağmen ticari ürünlerin çıkması ve yaygınlaşması

2005–2006 yıllarına denk gelir. Ürünler yeni olduğu için tatmin edecek derecede teknik rapor yok. Yine de ICSA Labs'in raporu bu konuda incelenmesi gerekir.

++Hangi ürünler var piyasada

ticari, acik kaynak kodlu. Ürünün iyiliği konusunda Turkiye'de destek veren firma da önemlidir. Yerel desteği olmayan bir ürünü

kullanmak genelede problemli olmaktadır.

++Modsecurity ile Koruma

modsecurity Apache ile birlikte çalışan(Apache modülü) bütünleşik bir web uygulama güvenlik duvarıdır. Fakat Apache'nin mod_proxy

modülü ile birlikte gateway seviyesinde uygulama güvenlik duvarı vazifesi de görebilir.

Sonuç

WAF sistemleri defense in depth yaklaşımı için önemli bir katmandır fakat tek başına kesinlikle yeterli olmayacaktır. Bugünler için yeterli gözükse de gerek atakların tiplerinin devamlı değişmesi ve karmaşıklaşması gerek de uygulamalar üzerinde yapılan mantıksal hataların devam etmesi WAF kullanımının yanında kod denetimi ve güvenlik testlerini kaçınılmaz kılmaktadır. Buna en iyi örnek WAF ürünlerinin çağrılan sayfalardaki yorm satırlarına(html comments) dokunmaması. Oysa bazen öyle uygulamalarla karşılaşıyoruz ki geliştirici admin parolasını yorum olarak koda eklemiş...