ModSecurity İle Web Güvenliği Ve OWASP

Bunyamin Demir
OWASP-Turkey Chapter Lead
OWASP-WeBekci Project
bunyamin@owasp.org

OWASP
May 6th, 2007

Copyright 2007 © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

The OWASP Foundation
http://www.owasp.org

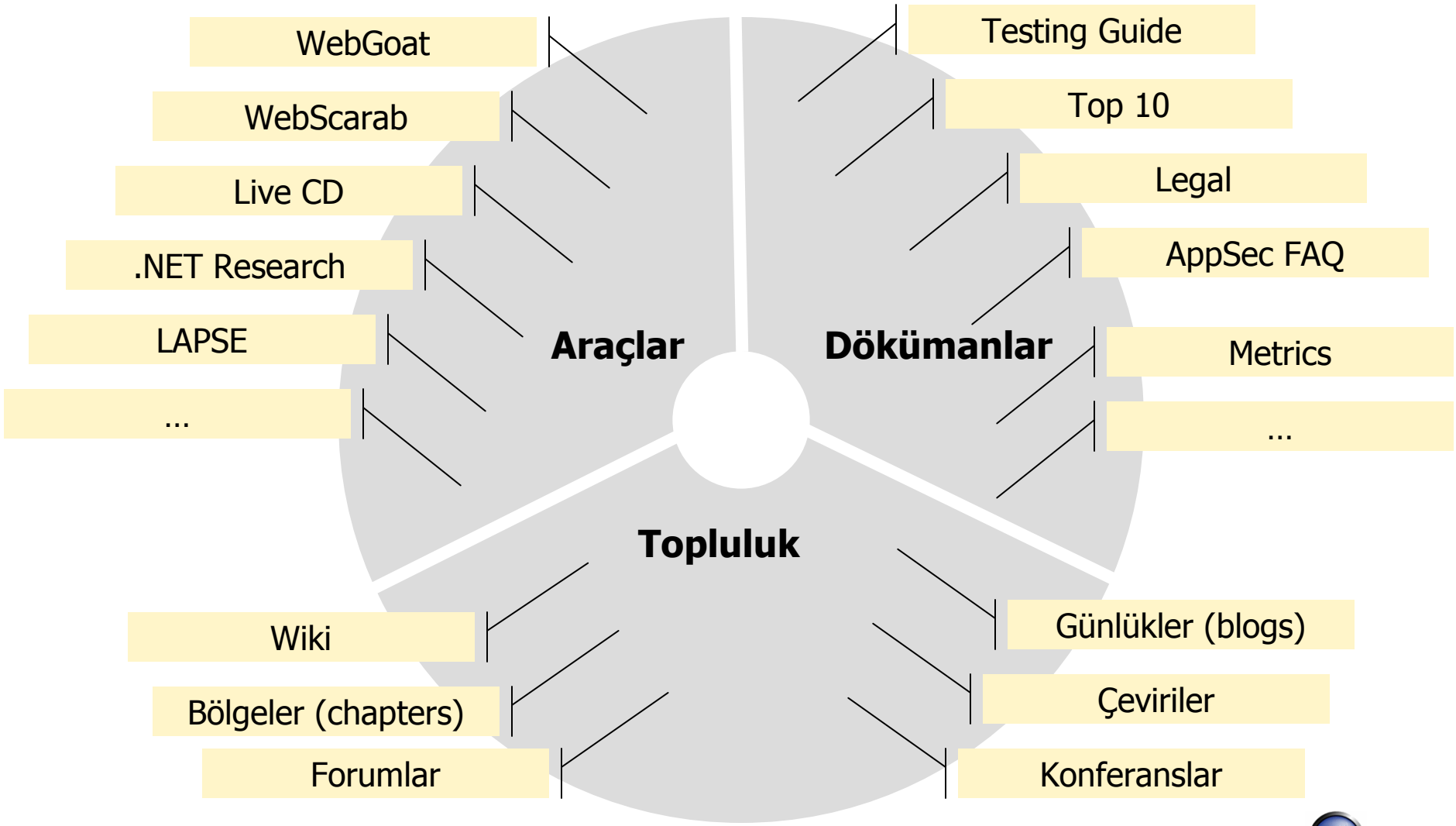
İçerik

- OWASP
  - OWASP Topluluğunun Yapısı
  - OWASP Testing Guide
  - OWASP Top 10
  - OWASP Projeleri
- ModSecurity
  - Web Application Firewall`ın (WAF) Önemi ve Neden İhtiyaç Duyarız?
  - WAF İle Korunma Stratejileri
  - Gömülü WAF`ların Avantajları
  - ModSecurity Kurulum ve Kullanım Modelleri
  - ModSecurity Kurallarının Uygulama Fazları
  - ModSecurity Konfigürasyon Parametreleri, Kural Dili, ve Etkiler
  - Log Analizi ve Hata Ayıklama
  - Core Rules, Cool Rules ve OWASP-WeBekci Projesi

OWASP Vakfı ve Yapısı

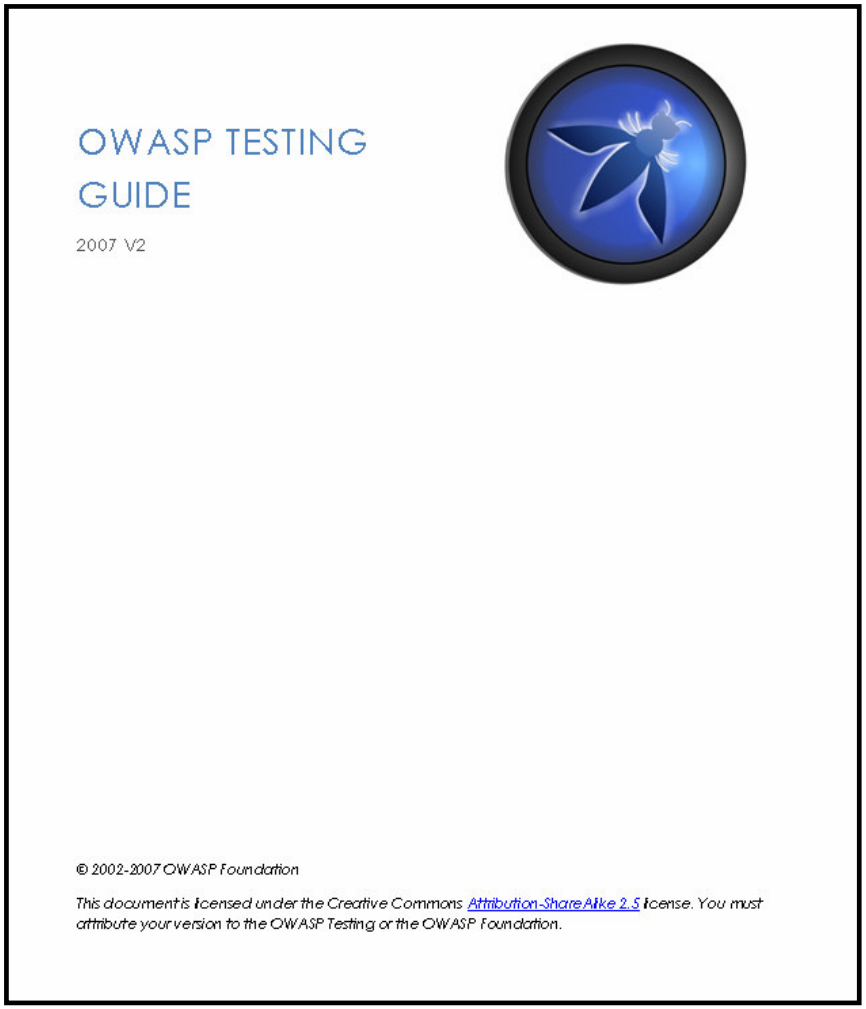
- Open Web Application Security Projest (OWASP)
- Güvensiz yazılımların sebep oldukları açıkları bulup, bunlarla mücadele eden bir topluluktur.
- Kar amacı gütmez
- Topluluğa ait rakamlar
  - 85 Bölge (Chapter)
  - 41 Proje
  - 132 E-posta listesi
  - 5004 Bölge e-posta üyesi
  - 3465 Proje e-posta üyesi
  - Aylık bir milyon üzerinde ziyaret

OWASP Neler Yapar?



OWASP Testing Guide

- Çalışma ortamının oluşturulması (Testing Framework)
- Güvenlik testlerinin yapılması
- Rapor hazırlanması



OWASP Top 10

- Sık rastlanan on web güvenlik açığını içerir
- Açıklar hakkında özet bilgi ve linkler vardır
- Her yıl yenilenir
- Topluluktan herkes katkı ve yorum sunabilir

OWASP Projeleri

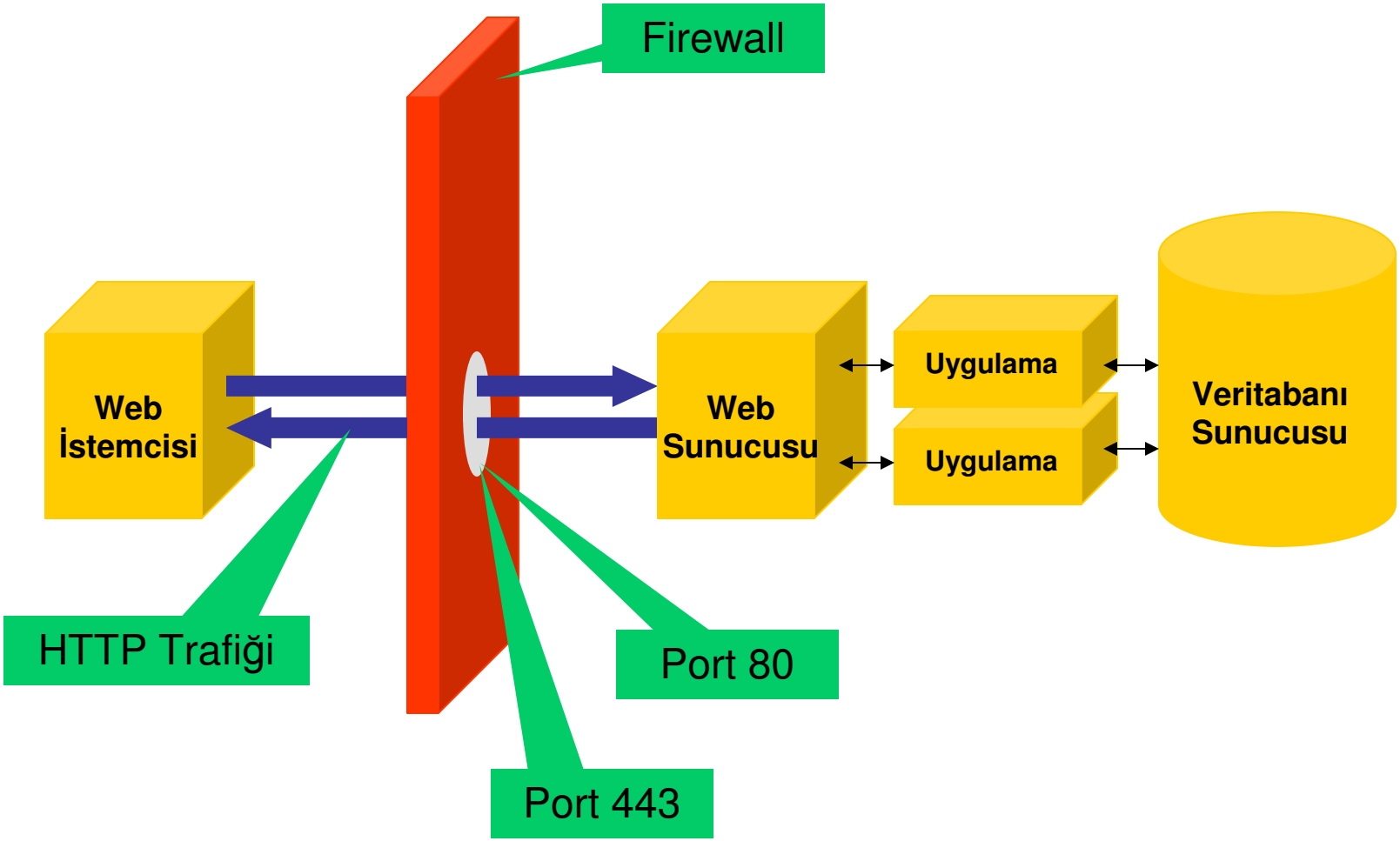
- Projelere maddi destek sağlar
- Güz ve bahar dönemi proje geliştirme yarışması
- WebGoat Projesi
  - Eğitim projesidir. Kullanıcıların web güvenliği hakkında bilgiler edinmesi için hazırlanmıştır. İçinde güvenlik açıkları içeren dersler bulunmaktadır ve sizlerden bu açıkları bulmanızı ister.
- WebScarab Projesi
  - Uygulamaların güvenlik açıklarınızı test etmeye yarar.
- Live CD Projesi
  - OWASP projelerini ve dökümanlarını barındıran CD dir.
- .NET Projesi
  - DotNet ortamını daha güvenli hale getirecek araçlar bulundurmaktadır.
- Legal Projesi
  - Yazılım alış verişindeki yasal düzenlemeleri yapmanıza yarayan bir projesidir

.....

Web Application Firewall`ın (WAF) Önemi ve Neden İhtiyaç Duyarız?

- Web uygulamaları ciddi güvenlik açıkları içerebilir.
- Web uygulamasının açığı bulunduğu andan giderilinceye kadar geçen zaman içinde yapılması gerekenler.
- Güvenli olmayan yazılımlar bir tarafa, WAF`lar HTTP trafiğini denetler.

HTTP Trafiğini Denetler



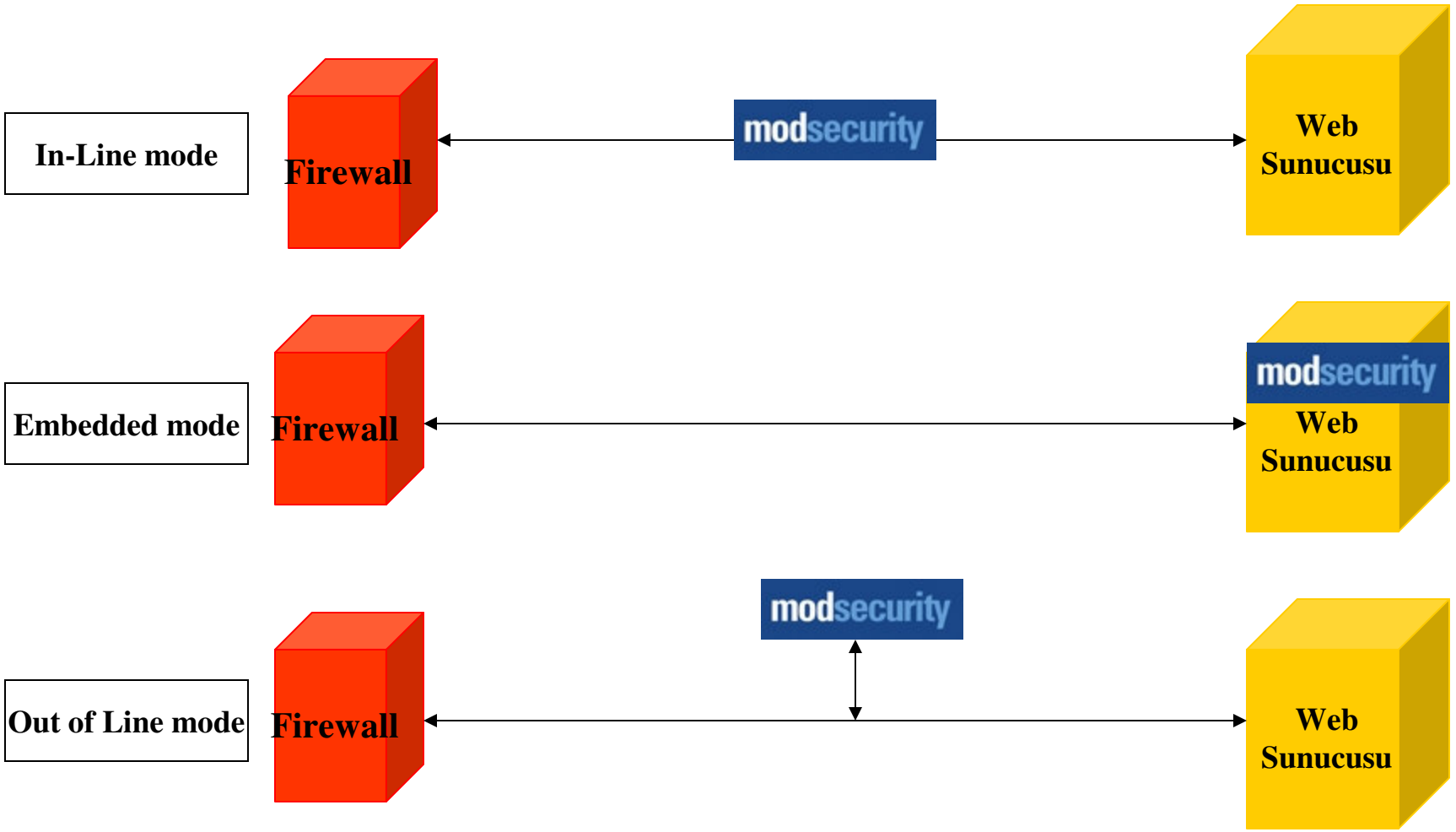
Web Güvenlik Duvarları İle Korunma Stratejileri

- Negatif Güvenlik Modeli:
  - Detaylara bakıp, bunların sonucuna göre kuralların işlenmesi sağlanır.
- Pozitif Güvenlik Modeli:
  - Sadece geçerli sayılan istekler kabul edilir. Bunun dışındaki tüm istekler reddedilir.
- Sanal Yamalama:
  - Yazılımlarda çıkan açıklar için yamalar yazılması.

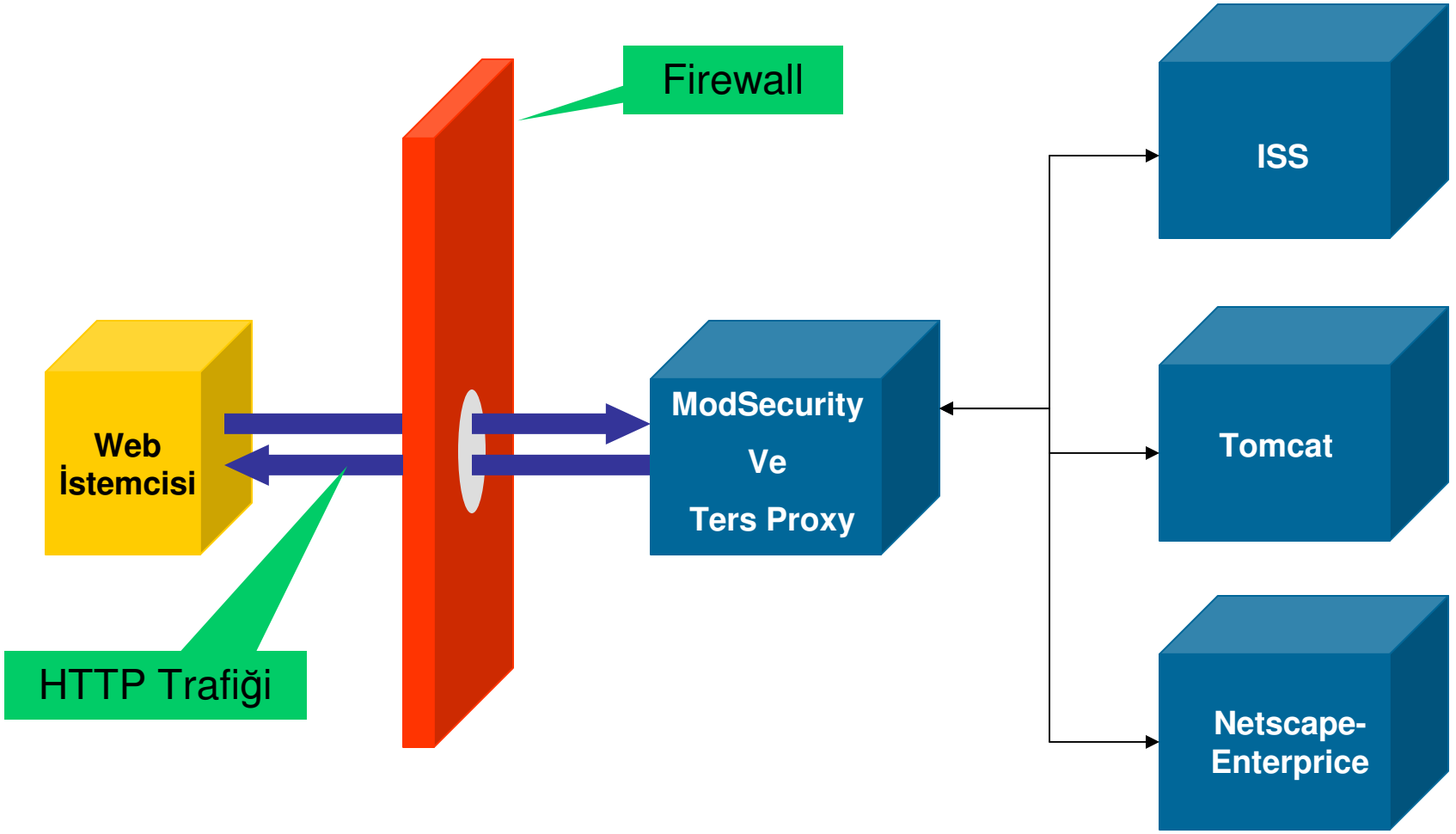
Gömülü Güvenlik Duvarlarının Avantajları

- ModSecurity gömülebilir web güvenlik duvarıdır
- Ağ yapısını değiştirmenize gerek kalmaz
- Eklenmesi ve kaldırılması çok az zaman alır
- No SPOF (Single Point Of Failure)
- Web servisinin prosesi içinde çalıştığı için çok az ek yük getirir
- Şifrelenmiş ve sıkıştırılmış veri ile bir sorun yaşanmaz.

ModSecurity Kurulum ve Kullanım modelleri



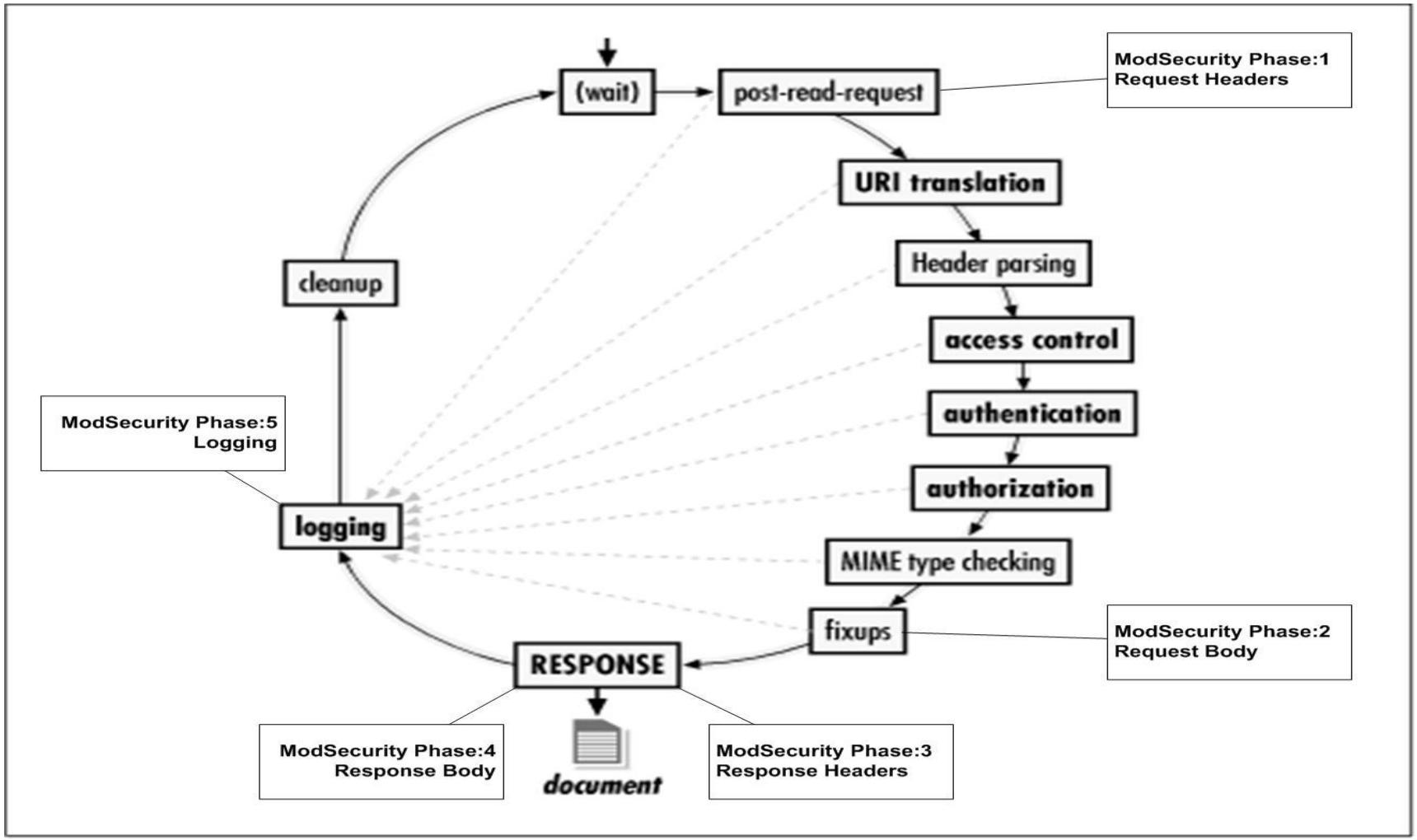
Ters (Reverse) Proxy Modeli



ModSecurity`i Ters Proxy Olarak Kullanmak

- Single point of access
- Performansı artırır
- Ağı izole eder
- Ağ topolojinizi dış dünyaya kapatır
- Arkasındaki sunucuların açıklarını perdelemiş olursunuz.

ModSecurity Kurallarının Uygulama Fazları



Konfigürasyon

- Temel parametreler
  - SecRuleEngine On
  - SecRequestBodyAccess On
  - SecResponseBodyAccess On
- Diğerleri
  - SecRequestBodyLimit
  - SecRequestBodyInMemoryLimit
  - SecResponseBodyLimit
  - SecResponseBodyMimeType
  - SecRuleInheritance
  - SecServerSignature
  - SecTmpDir
  - SecWebAppId
  - SecChrootDir

Kural Dili ve etkiler

- ARGS

  <LocationMatch "^/bilog/login.php$">
  SecRule ARGS:username "!^\w+$" "deny,log"
  </LocationMatch>

  http://www.site.com/bilog/login.php?username=1 geçer
  http://www.site.com/bilog/login.php?username=- takılır
- QUERY_STRING

  http://www.site.com/index.php?asayi=5&deneme=er
- REMOTE_ADDR

  SecRule REMOTE_ADDR "^192\.168\.5\.5$" auditlog,deny,severity:2
- REQUEST_COOKIES

  SecRule &REQUEST_COOKIES "@eq 0" deny,status:403
- REQUEST_HEADERS_ NAMES

  SecRule REQUEST_HEADERS_NAMES "^X-FORWARDED-FOR" "deny,status:403,msg:'Proxy Kullanıyor'"
- RESPONSE_BODY

  SecRule RESPONSE_BODY "ODBC Error" deny,log

Kayıt Analizi (Logging)

- Hata ayıklama (Debug Log)
  - 0 – Kayıt tutma!
  - 1 – İstek hataları
  - 2 – Uyarılar
  - 3 – Notlar
  - 4 – O an yapılan işlemler hakkında bilgi verir
  - 5 – Her işlemin içeriğinide tutar
  - 9 – Bütün işlemleri kayıt altına alır
  - 1 - 3 = apache error.log
  - SecDebugLogLevel 0
- İnceleme (Audit Log)
  - Yapılan her istek için ayrıntılı bir inceleme sağlatır
  - A,B,C,E,F,G,H,I,Z parametreleriyle amaca uygun kullanım sağlanır
  - SecAuditEngine RelevantOnly
- Guardian stili (Guardian Log)

Core Rules, Cool Rules ve OWASP-WeBekci Projesi

- Core Rules
  - Breach Security Inc. Tarafından geliştirilen kurallar
- Cool Rules
  - ModSecurity topluluğunun geliştirdiği kurallar
- OWASP-WeBekci Projesi
  - OWASP-Türkiye üyeleri tarafından OWASP bünyesine kazandırılmıştır
  - ModSecurity yönetim aracıdır
  - Php, MySql ve XAJAX framework`ü kullanılmıştır
  - Konfigurasyonun %80`ine destek vermektedir
  - System, error log ve guardian log stilleri desteklenmektedir
  - Tek değişkenli kurallar yazılabilmektedir.

- Yanlış güvenlik hisleri
  - Eğer Firewall varsa, güvendeyim
  - Eğer SSL kullanıyorsam, güvendeyim
  - Eğer Opera/Firefox kullanıyorsam, güvendeyim
  - Eğer Unix/Linux kullanıyorsam, güvendeyim

S&C

Teşekkürler!

OWASP
The Open Web Application Security Project
http://www.owasp.org

www.owasp.org

www.webguvenligi.org