



Özgür Uygulamalar ile Web Güvenliği

Bünyamin DEMİR

www.owasp.org/index.php/Turkey

www.webguvenligi.org

bunyamin@owasp.org



15 Ekim 2010

Copyright © The OWASP Foundation

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

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

Konuřmacı

Bünyamin Demir

- Web Uygulama Güvenliđi ve Veritabanı Güvenliđi Uzmanı
- OWASP-Türkiye Bölüm Yöneticisi
- Web Güvenliđi Topluluđu Üyesi

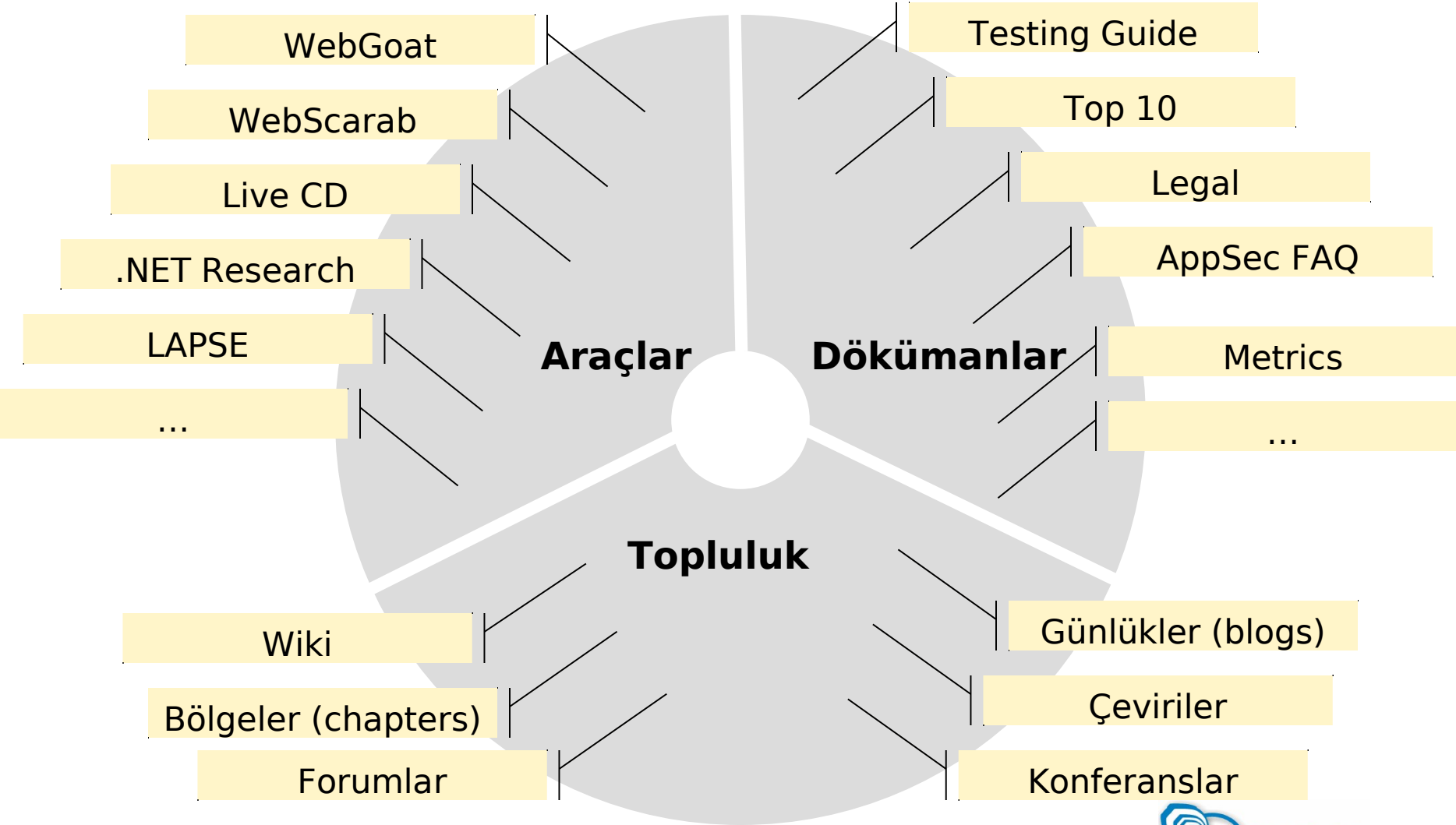
İçerik

- ▶ OWASP
 - Nedir?
 - Neler Yapar?
- ▶ OWASP-TR & WGT
 - Amaç ve Hedefler
 - Projeler
- ▶ Perspektifler
- ▶ WebGoat
 - Nedir?
 - Path Based Access Control
 - XSS
 - SQL Injection
- ▶ W3AF
 - Nedir?
 - Plugins
- ▶ ModSecurity
 - Nedir?
 - Nasıl Çalışır?
 - Konumlandırma
 - Ters Proxy Kullanımı

OWASP - Nedir?

- Open Web Application Security Projest (OWASP)
- Güvensiz yazılımların sebep oldukları açıkları bulup, bunlarla mücadele eden bir topluluktur.
- Tüm OWASP ürünleri ücretsiz ve açıktır.
- Kar amacı gütmmez
- Topluluga ait rakamlar
 - ▶ 120+ (Chapter)
 - ▶ 30+ Sponsor
 - ▶ 50+ Proje
 - ▶ 100+ E-posta listesi
 - ▶ Aylık beş milyon üzerinde ziyaret

OWASP Neler Yapar?



OWASP-TR / WGT Amaç ve Hedefler

- Web uygulaması güvenliğine ülkemizde gerekli duyarlılığın gösterilmesini sağlamak
- Web uygulaması güvenliği konusunda çalışan ve ilgi duyan arkadaşları bir platformda toplamak
- Güvenlik konulu makaleler, dökümanlar ve projelere yer ve destek sağlamak.
- Web uygulamalarının ortaya çıkardığı zararları en aza indirme yolunda çalışmalar yapmak
- Dünyada yapılan web uygulaması güvenliği konulu çalışmaların takibini sağlamak
- OWASP Vakfının Türkiye çalışmalarını sürdürmek
- Web uygulaması güvenliği projeleri geliştirmek.
- Web uygulaması güvenliği alanında yardımcı dökümanlar temin etmek.
- Özel ve kamu kuruluşları arası güvenlik konulu çalışmalar yapmak.
- Uluslararası konferanslar düzenlemek.
- Açık kaynak kodlu güvenlik çalışmalarına destek vermek.
- Üniversitelerimizde uygulamalı web güvenliği farkındalığı eğitimleri vermek.

OWASP-TR / WGT Projelerimiz

- [Web Uygulama Güvenliđi Kontrol Listesi 2010](#)
- [Web Güvenliđi E-Dergi \(dergi.webguvenligi.org\)](#)
- Jarvinen (Web tabanlı ModSecurity log analizi)
- OWASP-WeBekci (SoC 2008) ve MSALParser
- CAMMP (Chroot Apache Mysql ModSecurity PHP)
- SecureImage (.NET, Java ve PHP API)
- SecureTomcat (Tomcat J2EE sunucu güvenlik denetimi)
- Çeviri Projesi (~500 sayfa doküman)
- Otomatize Sql Entektörleri Analizi (SoC 2008)
- AntiCsurf (Cross Side Request Forgery için PHP API`si)
- ApacheLive (Apache sunucusunun Keep-alive parametresi için güvenlik kontrolü yapan bir araçtır)
- Web Güvenliđi Terimler Sözlüğü
- WIVET (Web Crawler'ın Teknik Yeteneklerinin Ölçülmesi ve Karşılaştırılması)

Perspektifler

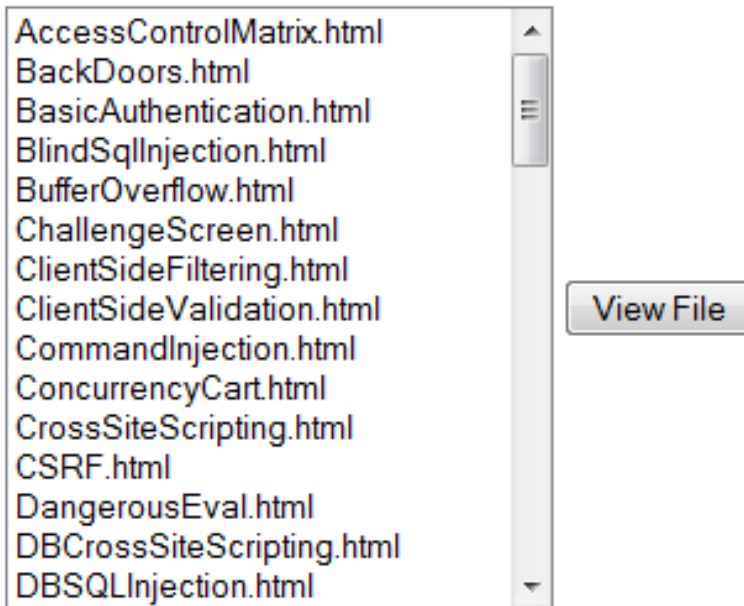
- Başlangıç
 - ▶ **OWASP WebGoat**
 - ▶ DVWA (*Damn Vulnerable Web App*)
 - ▶ OWASP WebScarab
- Saldırgan gözüyle bakış
 - ▶ Burp
 - ▶ OWASP CSRFTester
 - ▶ **W3AF**
 - ▶ OWASP DirBuster
- Savunmacı gözüyle bakış
 - ▶ **ModSecurity**
 - ▶ OWASP ESAPI
 - ▶ OWSASP Testing Guide

Başlangıç - WebGoat

- Güvenlik açıklıkları barındıran bir OWASP projesidir (J2EE ile yazılmıştır).
- Web uygulama güvenliği bilincini arttırmak için hazırlanmış bir eğitim aracıdır. Bu araç sayesinde açıklıkları anlayabilme ve bunları exploit edebilme yeteneği kazandırılmak istenmektedir.
 - ▶ Yüzlerce açıklık içermektedir.
 - ▶ Açıklıkların detaylı çözümleri ve bu açıklıkları çözmek için yardımcı ipuçları barındırır.
 - ▶ Açıklıklar belli kategorilerde sunulmaktadır.
 - ▶ Kolayca yeni açıklıklar ilave edilebilir.
 - ▶ Güvenlik testleri için ideal bir çalışma ortamı sunulur.
- Kolay kuruluma sahiptir.

WebGoat - Path Based Access Control

Choose the file to view:

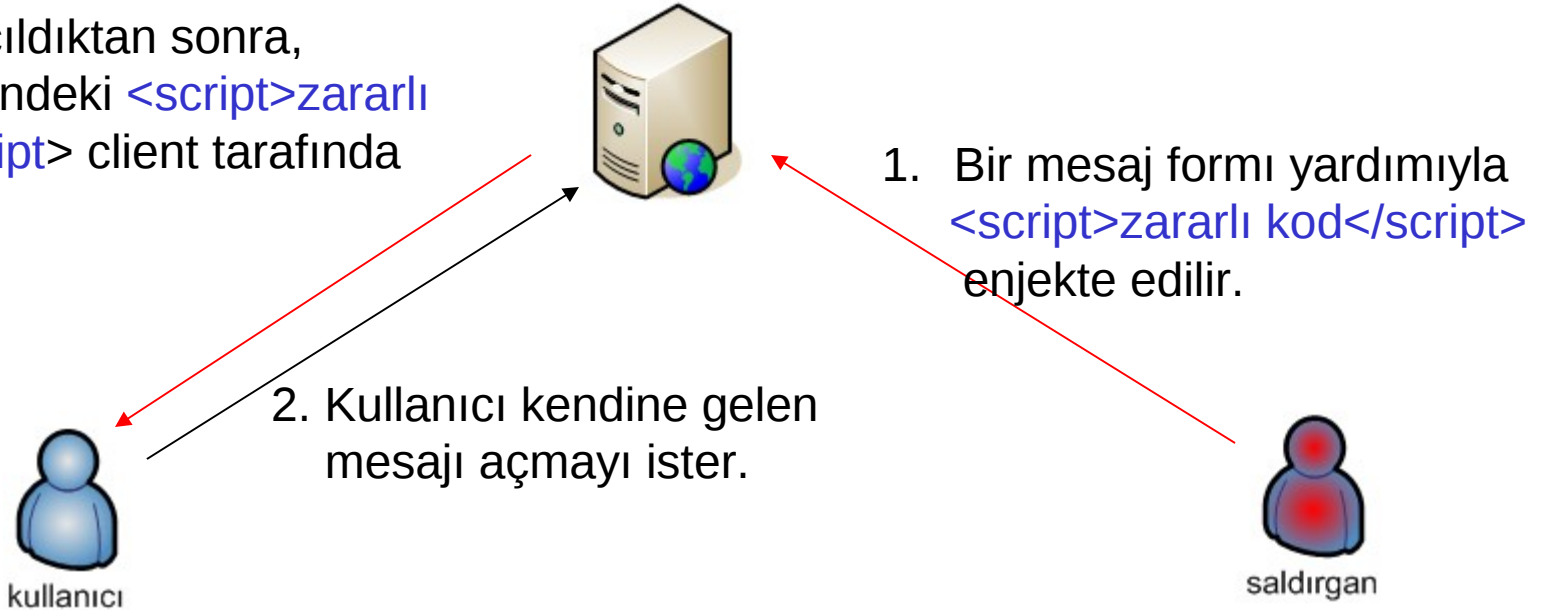


- Web uygulamalarında özellikle dizinlerden dosya okuturken karşımıza çıkan bir güvenlik açığıdır.
- Erişim sağlanan dizinin dışına çıkma imkanı varsa, bu imkan sayesinde stahmin edilen bazı dosyalara izinsiz erişim sağlanır.
- ../main.jsp ye erişim sağlanabilir.

Web Goat - Stored XSS

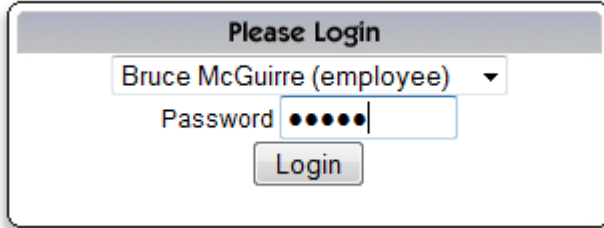
- Saldırgan tarafından girilen zararlı kod parçasının kurban tarafından çalıştırılmasından kaynaklanmaktadır.

3. Mesaj açıldıktan sonra, mesaj içindeki `<script>zararlı kod</script>` client tarafında çalışır.

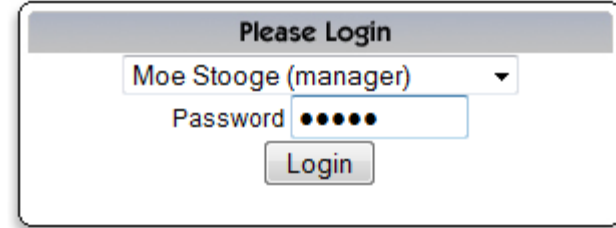


Web Goat - Stored XSS

1



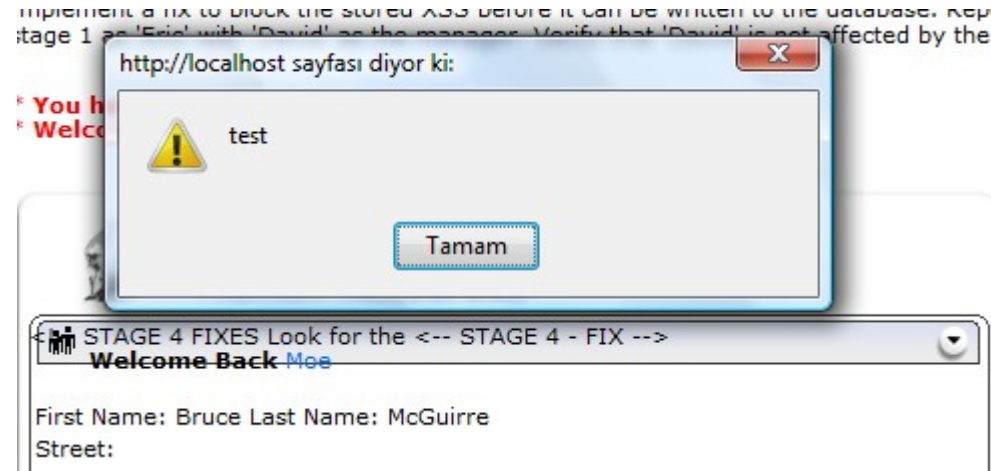
3



2



4



1. Bruce olarak sisteme girilir.
2. Bilgileri güncellerken "street" alanında xss açığı olduğu tespit edilir ve zararlı kod parçacığı yazılır.
3. Yönetici olan Moe sisteme girer.
4. Moe sisteme girdikten sonra kullanıcı profillerine bakarken Bruce'un girmiş olduğu zararlı kod parçacığı browser tarafından çalıştırılır.

WebGoat - Sql Injection

Sql Injection açığı bulunan bir formdan arka arkaya sql cümleciklerinin çalışma demosu.

User ID:

select userid, password, ssn, salary, email from employee where userid=

Submit

User ID:

select userid, password, ssn, salary, email from employee where userid=**1 or 1=1**

Submit

User ID	Password	SSN	Salary	E-Mail
101	larry	386-09-545	1200	larry@stooges.com
102	moe	936-18-4524	140000	moe@stooges.com
103	curly	961-08-0047	50000	curly@stooges.com

User ID:

select userid, password, ssn, salary, email from employee where userid=**1 or 1=1; update employee set salary=9999999 where userid=101**

Submit

User ID	Password	SSN	Salary	E-Mail
101	larry	386-09-545	9999999	larry@stooges.com
102	moe	936-18-4524	140000	moe@stooges.com
103	curly	961-08-0047	50000	curly@stooges.com

Saldırgan - W3AF

- Web Uygulama Açıklık Tarayıcısı
- Andres Riancho (Bonsai Information Security)
- Açık kaynak kodlu (GPLv2)
- Python ile yazılmış
- Exploit: [blind] SQL injections, OS commanding, remote file inclusions, local file inclusions, XSS, unsafe file uploads and more!



w3af

Saldırgan - W3AF - Plugins

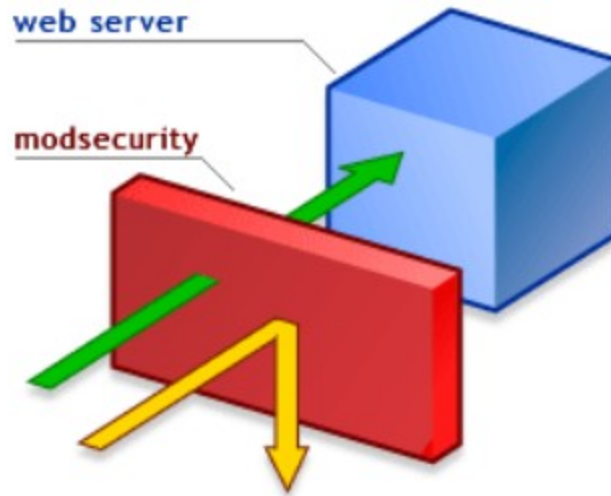
1. sql_webshell
2. davShell
3. sqlmap
4. xssBeef
5. remote file include shell
6. OS Commanding shell



w3af

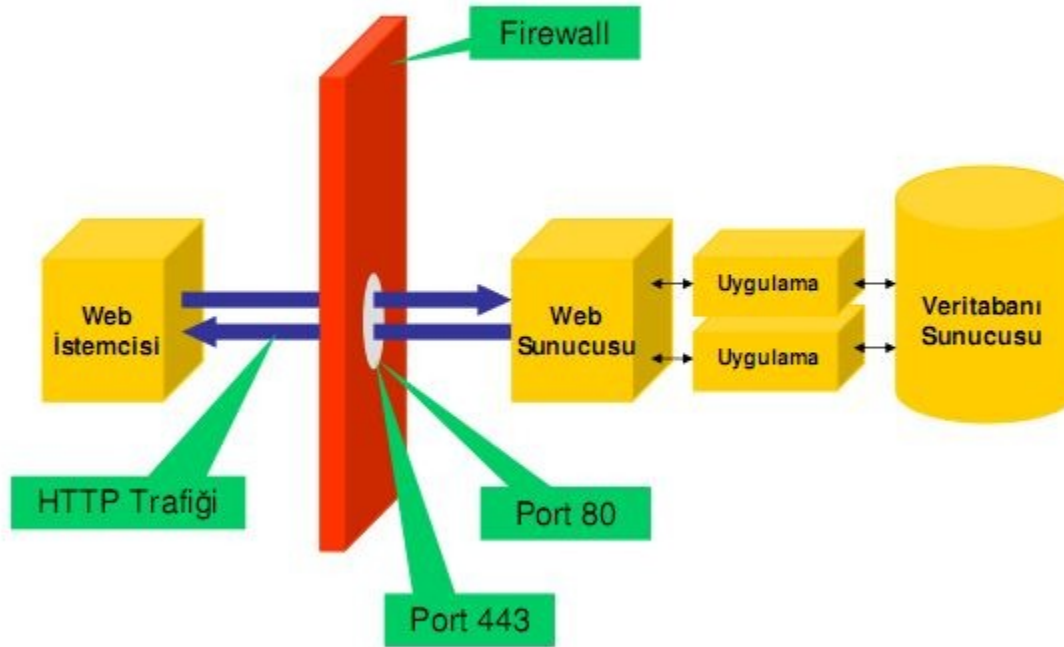
Savunmacı - ModSecurity

- Web uygulama güvenlik duvarı
- Trustwave firması tarafından desteklenmektedir
- Apache`nin bir modülü olarak çalışır (mod_Security)
- OWASP ModSecurity Core Rule Set (Kural seti)



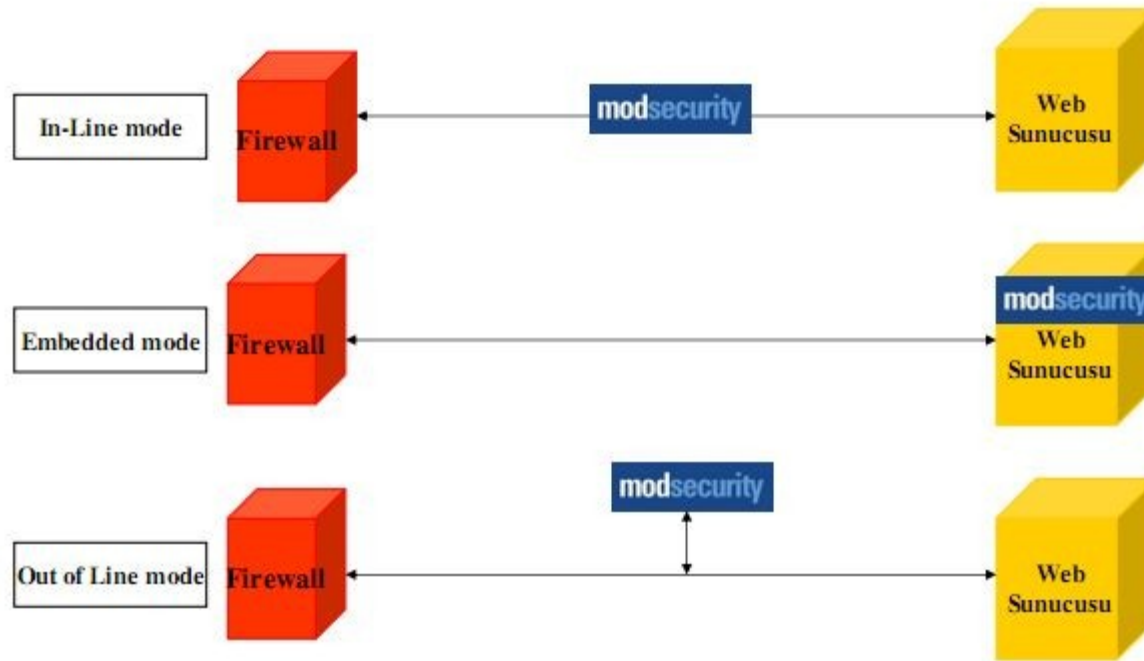
Savunmacı - ModSecurity - Nasıl Çalışır?

HTTP Trafikini Denetler

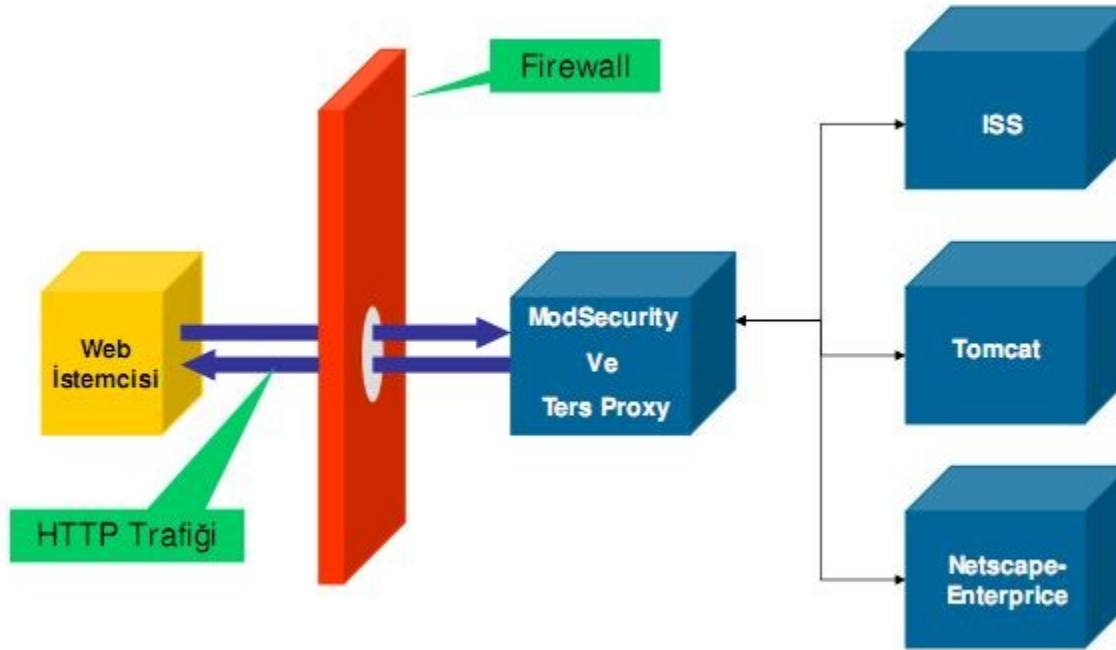


Savunmacı - ModSecurity - Konumlandırma

ModSecurity Kurulum ve Kullanım modelleri



Savunmacı - ModSecurity - Ters Proxy Kullanımı



Teşekkürler!



OWASP

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



www.webguvenligi.org

www.owasp.org

E-posta listesine kayıt olmak için

google: owasp turkey mail list

