

MODSECURITY DENETİM KAYITLARINI ANLAMAK

Gökhan Alkan, gokhan@enderunix.org

İÇİNDEKİLER

MODSECURITY DENETİM KAYITLARINI ANLAMAK	1
1. ModSecurity Nedir ?	3
2. ModSecurity Nasıl Çalışır ?	3
3. ModSecurity Kayıt Bilgisi Tutma Özelliği Ve Direktifleri	4
3.1 SecAuditEngine.....	4
3.2 SecAuditLog.....	4
3.3 SecAuditLog2.....	5
3.4 SecAuditLogParts.....	5
3.5 SecAuditLogRelevantStatus.....	6
3.6 SecAuditLogStorageDir	6
3.7 SecAuditLogType	6
4. Uygulama - ModSecurity Denetim Kayıt Bilgilerini Ayrıştırmak Ve Jarvinen (Parsing ModSecurity Logs)	7
5. Kaynaklar	8

1. ModSecurity Nedir?

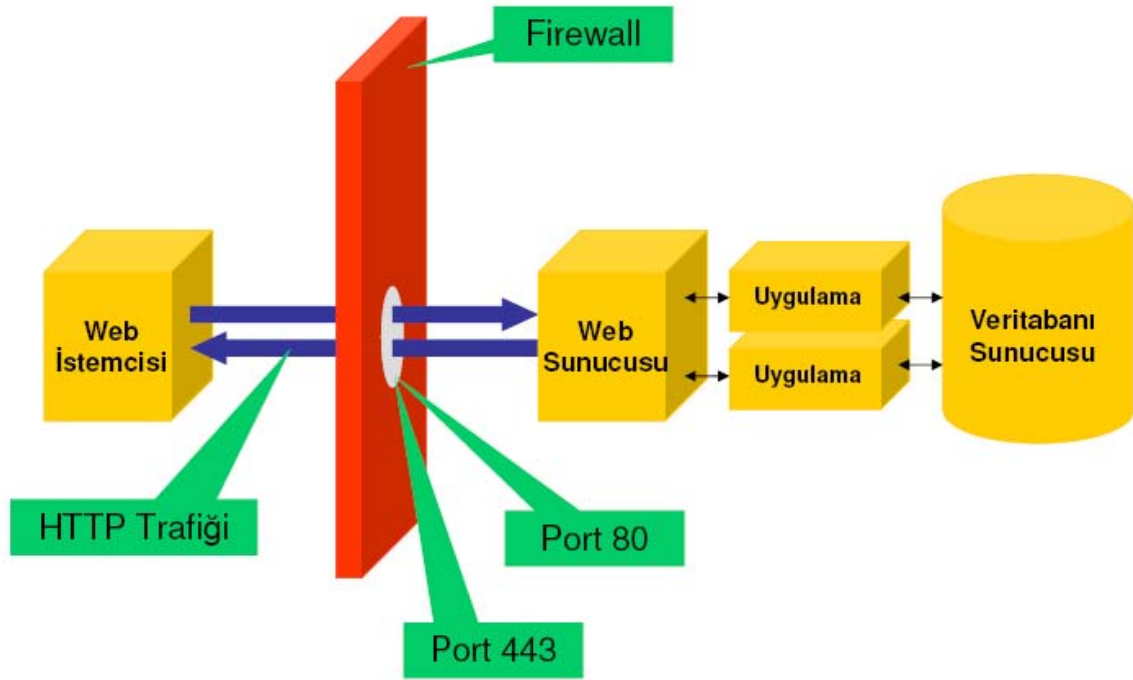
ModSecurity Ivan Ristic tarafından geliştirilen, Apache web sunucusunun bir modülü olarak çalışan açık kaynak kodlu, tehdit gözetleme ve engelleme sistemidir. Web uygulama güvenlik duvarı olarak da adlandırılan ModSecurity, hem tehdit gözetleme hem de engelleme sistemi olarak çalışabilmektedir. Kısaca yapılandırmasında gerçekleştirilen değerlere göre gelen istek için bir aksiyon alır.

2. ModSecurity Nasıl Çalışır?

ModSecurity Apache web sunucusunun bir modülü olarak çalışır. İstemciden gelen istek ve sunucu cevabının analizi aşağıdaki şekildedir

1. Birinci adımda, isteğin biçimi bir dizi gömülü kontrol tarafından analiz edilir. Bu kontroller yapılandırma değerleri kullanılarak değiştirilebilir.
2. İkinci adımda, istek kullanıcı tarafından tanımlanan girdi denetimine gider. Ne zaman bir eşleşme olursa, yine kullanıcı tarafından tanımlanan olaylar tetiklenir.
3. İstek Apache tarafından işlenir.
4. Eğer çıktı filtreleme aktifleştirilmiş ise, çıktı bir dizi kullanıcı tanımlı çıktı filtresine yönlendirilir. Eğer bir eşleşme olursa belirtilen davranışlar tetiklenir.

Genel olarak ModSecurity çalışma prensibi Şekil 1’de gösterilmiştir.



Şekil 1 ModSecurity Çalışma Prensibi

3. ModSecurity Kayıt Bilgisi Tutma Özelliği Ve Direktifleri

3.1 SecAuditEngine

Denetim kayıt bilgisi alma yeteneğini aktifleştirmek için kullanılır.

Örnek kullanım: *SecAuditEngine On*

Alabileceği değerler:

- On – Bütün işlem bilgileri kayıt altına alınır.
- Off – İşlem bilgileri kayıt altına alınmaz.
- RelevantOnly – Uyarı, hata ya da ilgili olduğu düşünülen durum kodları kayıt altına alınır.

3.2 SecAuditLog

Audit kayıt bilgisinin tutulacağı kayıt dosyasının tam yolunu belirtmek için kullanılır.

Örnek kullanım: *SecAuditLog /var/log/apache/logs/audit.log*

Bu dosya açılışta sunucu root hakları ile çalıştığında açık halde bulunmaktadır. Root kullanıcı haklarına erişim izni bulunmayan kullanıcıların bu dosyaya yazma hakları bulunmadığından ya da bulunduğu dizine yazma izni olmadığından emin olunmalıdır.

Eğer arka arkaya kayıt bilgi biçimi (serial audit logging format) kullanılıyorsa bu dosya denetim kayıt bilgilerinin (audit logs) saklanması için kullanılır. Eğer eşzamanlı (concurrent) kayıt bilgi formatı kullanılıyorsa bu dosya indeks olarak kullanılacaktır ve oluşturulmuş bütün kayıt bilgisi dosyalarının kaydını içerir. Eğer eşzamanlı denetim kayıt bilgisi (concurrent audit logging) kullanmayı düşünüyorsanız ve denetim kayıtlarını (audit logging) uzak bir sunucuya göndermeyi planlıyorsanız ya da ticari ModSecurity yönetim aracı (commercial ModSecurity Management Appliance) kullanmayı planlıyorsanız, ModSecurity kayıt bilgisi toplayıcı (ModSecurity Log Collector -mlogc-) yapılandırmanız ve kullanmanız gerekecektir. Bunun için aşağıdaki format denetim kayıt bilgisi biçimi (audit log format) için kullanılmalıdır.

```
SecAuditLog "|/path/to/mlogc /path/to/mlogc.conf"
```

3.3 SecAuditLog2

Eş zamanlı kayıt bilgisi (concurrent logging) etkinleştirildiğinde ikincil denetim kayıt indeks dosyasının (audit log index) tam yolunu tanımlamak için kullanılır.

Örnek kullanım: `SecAuditLog2 /var/log/apache/logs/audit2.log`

3.4 SecAuditLogParts

Esas denetim kayıt bilgisinin detaylarını tanımlar.

Örnek kullanım: `SecAuditLogParts ABCFHZ`

Kullanılabilir denetim kayıt seçenekleri:

- A – Denetim kayıt bilgisi başlığı (zorunlu)
- B – İstek başlığı
- C – İstek gövdesi
- D – Aracılık eden başlık bilgileri (intermediary response headers) için ayrılmıştır, henüz gerçekleştirilmedi.
- E – Arada bulunan cevap gövdesi (intermediary response body)
- F – Son başlık bilgisi (son olarak içeriğin iletiminde Apache tarafından eklenen tarih ve sunucu başlık bilgileri dışında kalan). Arada bulunan cevap gövdesi (Intermediary response body) ModSecurity cevap gövdesini engellemediği sürece gerçek cevap gövdesi ile aynıdır, bu durumda gerçek cevap gövdesi hata mesajını içerecektir (ya ön tanımlı Apache hata mesajı ya da ErrorDocument sayfası).
- G – Gerçek cevap gövdesi için ayrılmıştır, henüz gerçekleştirilmedi.

- H – Denetim kayıt artbilgisi (audit log trailer)
- I – C bölümünün yerine kullanılan bölümdür. multipart/form-data kodlaması kullanıldığı durumlar haricinde C bölümü ile aynı verileri kayıt altına alır. Bu durumda parametreler hakkında bilgiler içeren fakat dosyalar hakkında olmayan sahte bir application/x-www-form-urlencoded gövdesi içeren kayıt bilgisini tutacaktır.
- J – Ayrılmıştır. Bu bölüm uygulandığında multipart/form-data kodlaması kullanan aktarılmış dosyalar (uploades files) hakkında bilgi içerecektir.
- K – Eşleştirildikleri sırayla eşleşen her kuralın tam listesini içerir.
- Z – Son sınır bilgisi. Kayıt bilgisinin sonu olduğuna işaret eder. (zorunlu)

3.5 SecAuditLogRelevantStatus

Hangi cevap durum kodunun ilgili denetim kaydı için kullanılacağını yapılandırır.

Örnek kullanım: `SecAuditLogRelevantStatus ^(?:5|4\d{^4})`

Bu direktifin asıl kullanım amacı kullanıcıya sadece belirlenmiş HTTP cevap durum kodlarını oluşturan işlemler için denetim kayıt bilgisi (audit logging) yapılandırması için izin vermektir. Bu direktif genellikle toplam denetim kayıt bilgisini artırmak için kullanılır. Bu direktif kullanıldığında 200 OK durum kodu ile sonuçlanan başarılı saldırılar için kayıt bilgisi tutulmayacağı unutulmamalıdır.

3.6 SecAuditLogStorageDir

Eş zamanlı denetim kayıt bilgisinin (concurrent audit log) nerede tutulacağını yapılandırır.

`SecAuditLogStorageDir /var/log/apache/logs/audit`

SecAuditLogType direktifi eş zamanlı (concurrent) olarak ayarlanmalıdır. Apache servisi başlamadan önce dizin oluşturulmalı ve yeni dosyaların çalışma zamanında oluşturulması için web sunucu yazılımı kullanıcısının yazma hakkı olmalıdır.

3.7 SecAuditLogType

Kullanılacak kayıt denetim mekanizmasının çeşidini yapılandırır.

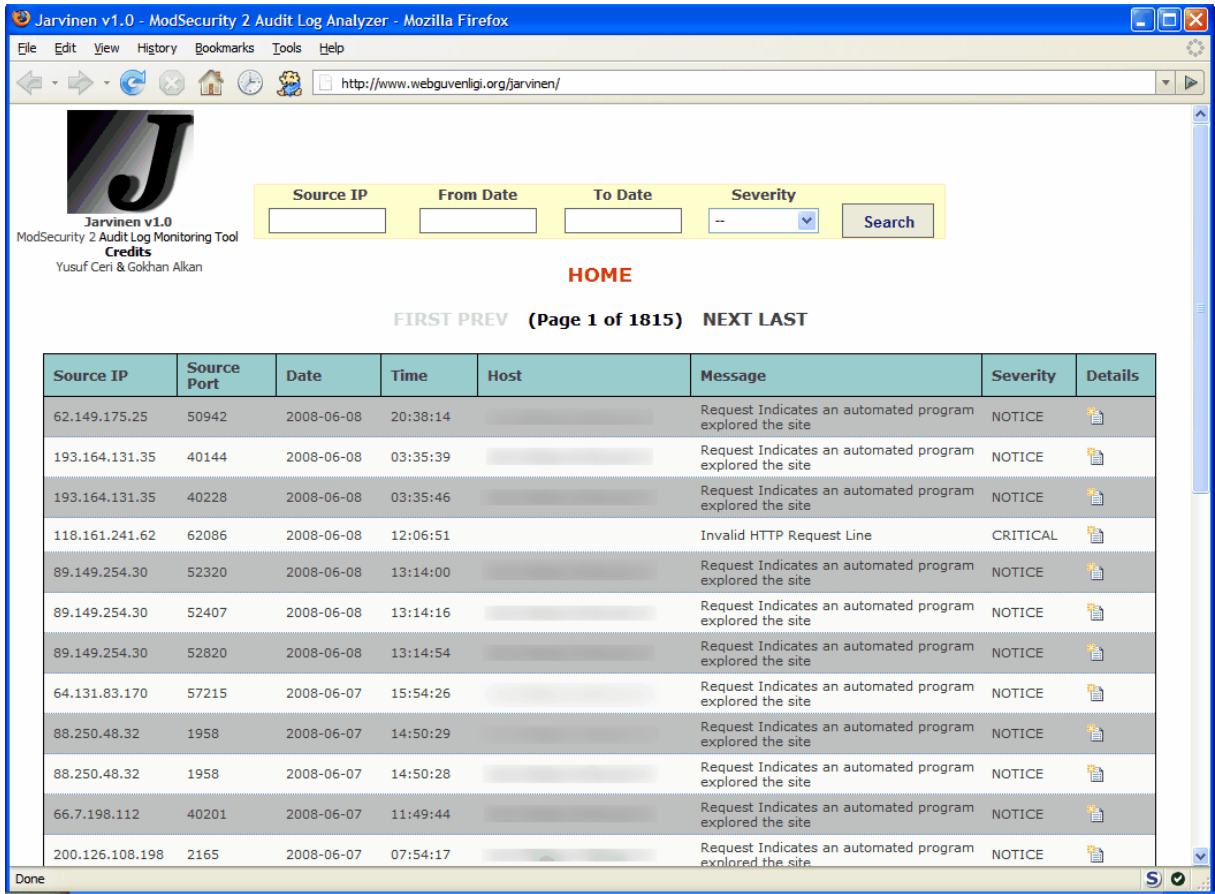
Örnek kullanım: `SecAuditLogType Serial`

Geçerli direktifler:

- Serial: Bütün denetim kayıt bilgileri (audit log) esas denetim kayıt dosyasında tutulacaktır.
- Concurrent: Denetim kayıt bilgileri ayrı tutulacaktır.

4. Uygulama - ModSecurity Denetim Kayıt Bilgilerini Ayrıştırarak Ve Jarvinen (Parsing ModSecurity Logs)

Eğer ModSecurity Console uygulamasını kullanmıyorsanız, ModSecurity denetim kayıt bilgilerini her gün izlemek ve analiz etmek oldukça zor olmaktadır. Jarvinen bu ihtiyacı karşılamak için yazılmış bir uygulamadır. Kısaca yaptığı iş, ModSecurity2 denetim kayıt bilgilerini ayrıştırıp bu bilgileri mysql veritabanına aktarmaktır. 2 parçadan oluşmaktadır. Betik programlama (shell script) kullanarak ModSecurity denetim kayıt bilgilerini ayrıştırıp veritabanına aktaran birinci parça ve php ile geliştirilmiş veritabanındaki ModSecurity denetim kayıt bilgilerini web arayüzünden kullanıcıya gösteren ikinci parça. Kabuk programlama kullanılması amaç uygulamanın taşınabilir olmasıdır. Bu şekilde kullanıcı fazladan bir yazılama gerek kalmadan Jarvinen uygulamasını çalıştırabilecektir. Uygulamanın kurulum ve yapılandırmasına ilişkin ayrıntılara <http://code.google.com/p/jarvinen/> adresinden ulaşılabilir. Web arayüzüne ilişkin örnek çıktılar aşağıda gösterilmiştir.



The screenshot shows the Jarvinen v1.0 web interface in a Mozilla Firefox browser. The browser address bar shows the URL <http://www.webguvenligi.org/jarvinen/>. The interface includes a search form with fields for Source IP, From Date, To Date, and Severity, and a Search button. Below the search form, there are navigation links: HOME, FIRST, PREV, (Page 1 of 1815), NEXT, and LAST. The main content area displays a table of log entries with columns for Source IP, Source Port, Date, Time, Host, Message, Severity, and Details. The table contains 12 rows of log data.

Source IP	Source Port	Date	Time	Host	Message	Severity	Details
62.149.175.25	50942	2008-06-08	20:38:14		Request Indicates an automated program explored the site	NOTICE	
193.164.131.35	40144	2008-06-08	03:35:39		Request Indicates an automated program explored the site	NOTICE	
193.164.131.35	40228	2008-06-08	03:35:46		Request Indicates an automated program explored the site	NOTICE	
118.161.241.62	62086	2008-06-08	12:06:51		Invalid HTTP Request Line	CRITICAL	
89.149.254.30	52320	2008-06-08	13:14:00		Request Indicates an automated program explored the site	NOTICE	
89.149.254.30	52407	2008-06-08	13:14:16		Request Indicates an automated program explored the site	NOTICE	
89.149.254.30	52820	2008-06-08	13:14:54		Request Indicates an automated program explored the site	NOTICE	
64.131.83.170	57215	2008-06-07	15:54:26		Request Indicates an automated program explored the site	NOTICE	
88.250.48.32	1958	2008-06-07	14:50:29		Request Indicates an automated program explored the site	NOTICE	
88.250.48.32	1958	2008-06-07	14:50:28		Request Indicates an automated program explored the site	NOTICE	
66.7.198.112	40201	2008-06-07	11:49:44		Request Indicates an automated program explored the site	NOTICE	
200.126.108.198	2165	2008-06-07	07:54:17		Request Indicates an automated program explored the site	NOTICE	

Şekil 2 ModSecurity2 Denetim Kayıt Bilgilerini Jarvinen Web arayüzü İle Analiz Edilmesi

