ModSecurity Core Rule Set 2.0

Bünyamin Demir, Ekim 2009, WGT E-Dergi 2. Sayı

Bir çoğumuz ModSecurity hakkında az da olsa kulak aşinalığı edinmişizdir. Fakat yine de hatırlatacak olursak; Apache`ye bir modül olarak eklenebilen web uygulama güvenlik duvarı diyebiliriz. Bu yazımızda bahsedeceğimiz ise bu güvenlik duvarı için hazırlanmış olan temel kural topluluğudur. Bu kural topluluğuna "Core Rule Set" adı verilmiştir. Core Rule Set önceleri Breach Security tarafından idame ettiriliyordu (hala farklı olduğunu düşünmüyorum), fakat şu an 2.0 ile birlikte bir OWASP projesi haline dönüştürüldü ve katılımın fazla olması sağlandı. Kısmen bu amaca da ulaşıldığını görüyorum. Tabi bunda en büyük pay kendine ait bir mail listesi açılmasıdır.

Neden "Core Rule Set" denilmiştir?

Aslında ModSecurity denetlemelerini kural veya kural topluluklarıyla yapmaktadır. Dolayısıyla bu da size farklı kural set`leri yazmamıza olanak tanır. Fakat adından da anlaşılabileceği gibi, çeşitli tecrübeler sonucu, kullanılması uygun görülmüş kuralları bir set haline getirip yayınlamayı uygun görmüşler -ki bu uygulamanın faydalı olduğunu düşünüyürum-. Zira ModSecurity kuralları yazmak iyi regexp bilgisi yanında ModSecurity`yi iyi anlayıp, hazmetmek gerektirecektir.

Bu yazımda değinmek istediğim iki husus var. Birincisi, Core Rule Set 2.0 ile getirilen değişiklikler, ikincisi ise, eksik gördüğüm hususlar olacaktır.

Core Rule Set 2.0 Değişiklikleri

Öncelikle eklenen özellikleri önemine göre madde halinde sıralayalım;

- Anomali Puanlama (Anomaly Scoring)
- Snort kurallarının ModSecurity kurallarına dönüştürülmesi (Converted Snort Rules)
- Ağırlıkların güncellenmesi (Updated Secerity Ratings)
- HTTP Parametre manipülasyonu için kural eklenmesi
- RFI denetlemesi (RFI Detection)
- Etkilerin korelasyonu (Correlated Events)

En çok dikkati çeken kısım ise anomali puanlamadır. Bu sayede bir değişken tanımlanıp, bu değişken her bir kural içinde puanlanabiliyor ve eğer puan sizin belirlediğiniz sınıra ulaşırsa etkiyi (action) icra ediyor (diğer bir deyişle blokluyor diyebiliriz.)

Eski yapıda her bir etki, içinde bulunduğu kural için icra ediliyordu. Ancak zincir kurallar ile birden fazla durum kontrolü yapılarak (IP, HOST v.s) etki icra ediliyordu. Bu yapının benzerisini SpamAssassin de kullanmaktadır.

Biraz daha teknik detaya inersek;

```
SecRule TX:/^PM_SQLI_DATA_*/ "\bsys\.user_catalog\b" \
"phase:2,capture,t:none,ctl:auditLogParts=+E,block,nolog,auditlog , msg:'Blind SQL Injection
Attack',id:'959517',tag:'WEB_ATTACK/SQL_INJECTION',logdata:'%{TX.0}',severity:'2',setvar:'t
x.msg=%{rule.msg}',setvar:tx.sqli_score=+1,setvar:tx.anomaly_score=+20,setvar:tx.%{rule.id}
-WEB_ATTACK/SQL_INJECTION-%{matched_var_name}=%{matched_var}"
```

Bu kural icra edilirken anomal_score değişkeni 20 arttırılıyor.

```
SecRule TX:ANOMALY_SCORE "@ge 20" \
   "phase:2,t:none,nolog,auditlog,deny,msg:'Anomaly Score Exceeded (score
%{TX.ANOMALY_SCORE}): %{tx.msg}',setvar:tx.inbound_tx_msg=%{tx.msg}"
```

Görüleceği gibi 20 den büyük-eşit mi diye kontrol eder. Eğer kurallar için de vermiş olduğunuz puanlama TX:ANOMALY_SCORE "@ge 20" sınırı ile doğrulanıyorsa, kuralın etkisi icra edilir. Tabi bu skor yapısı tamamen sizin insiyatifinizde, benim verdiğim değerler ön tanımlı gelmektedir.

Skor arttırmak gibi, düşürme işlemi de gerçekleştirilebilir. Örnek olarak;

```
SecRule MATCHED_VAR_NAME "TX\:(.*)"
"capture,t:none,setvar:!tx.%{tx.1},setvar:tx.anomaly_score=-20"
```

tanımı yapılmıştır.

Core Rule Set 2.0 Eksiklikleri

Gerçi bunlar tamamen benim tespitlerimden kaynaklanmaktadır. Sizler muhakkak benle aynı görüşleri paylaşmayabilirsiniz.

- Eskiden olduğu gibi eğer bloklama gerçekleşiyorsa size bir ruleid gönderiliyor. Fakat şu an bir bloklama işlemi birden fazla kural ile tetiklenebildiği için, siz hangi kuralların bu skoru oluşturduğunu göremiyorsunuz.

  Örneğin;

  K1 kuralı, ruleid=5, score +=10
  K2 kuralı, ruleid=11, score +10

  ve bizim sınırımız da 20 olsun. Bu iki kuraldan geçtikten sonra bloklama işlemi olacaktır. Fakat blok yapılan ruleid=11 gözükecektir
- Bazı kural gruplarının id si bulunmamaktadır. Bunları ancak dosya içinde alt alta görebiliyorsunuz. Dolayısıyla herhangi bir güncelleme işlemini otomatize yapmanız zor (Tabi Core Rule Set geliştiricileri bunun üstünde çalıştıklarını belirtiyorlar ama her bir parametre için bir ID tanımlanmış olsaydı, muhtemelen bukadar zorluk çekilmeyecekti.).

Yine de bir önceki kural setine göre daha esnek olduğunu söyleyebilirim. Sadece kural yazıcılar için iş (bence) biraz daha zorlaştırılmış. Tabi eski halinin de kolay olduğunu idda edemiyorum.

Referanslar

[1] OWASP Core Rule Set Projesi
[2] ModSecurity Projesi