ModSecurity

ModSecurity (často označovaný jako **ModSec**) je open-source nástroj pro detekci a prevenci útoků na webové aplikace. Funguje jako „štíhlá“ vrstva mezi internetem a webovým serverem, která v reálném čase analyzuje veškerý příchozí a odchozí HTTP provoz.

Je považován za „švýcarský nůž“ bezpečnosti webových serverů, protože umožňuje definovat extrémně detailní pravidla pro filtrování požadavků.

Jak ModSecurity funguje?

ModSec nefunguje jen na základě jednoduchých seznamů zakázaných slov. Jeho síla spočívá v **Engine**, který provádí:

- **Analýzu protokolu:** Kontroluje, zda jsou HTTP požadavky v souladu se standardy (brání anomáliím).
- **Real-time monitorování:** Sleduje provoz v reálném čase a okamžitě zasahuje při detekci podezřelého vzorce.
- **Logování:** Nabízí velmi podrobné protokoly o každém pokusu o útok, což je klíčové pro forenzní analýzu.

OWASP Core Rule Set (CRS)

Samotný ModSecurity je pouze „motor“. Aby věděl, co má blokovat, potřebuje sadu pravidel. Tou nejznámější je **OWASP Core Rule Set (CRS)**. Tato sada pravidel chrání web před:

- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Local/Remote File Inclusion (LFI/RFI)
- Command Injection
- Útoky typu Session Fixation

Podporované platformy

Ačkoliv začínal jako modul pro **Apache**, dnes je k dispozici pro:

- **Nginx:** Často se používá jako součást „Ingress Controlleru“ v Kubernetes.
- **Microsoft IIS:** Pro servery běžící na Windows.

Hlavní výhody a nevýhody

Vlastnost	Popis
Cena	Je zcela zdarma (Open Source).
Flexibilita	Umožňuje psát vlastní pravidla pro specifické potřeby aplikace.
Virtual Patching	Dokáže okamžitě zablokovat novou zranitelnost (Zero-day) pomocí pravidla, aniž by se měnil kód webu.
Náročnost	Špatně nastavený ModSec může způsobit vysokou zátěž CPU nebo blokovat legitimní uživatele (tzv. False Positives).

Co je to "Virtual Patching" v ModSecurity?

Toto je jedna z nejvíce oceňovaných funkcí. Pokud se v populárním systému (např. WordPress) objeví kritická chyba, trvá dny i týdny, než vyjde aktualizace a majitelé webů ji nainstalují. S ModSecurity stačí přidat **jedno pravidlo**, které tento specifický útok zablokuje na úrovni firewallu. Web je tak „virtuálně opraven“ okamžitě, i když jeho zdrojový kód je stále zranitelný.

Související pojmy: WAF, SQL Injection, OWASP, Apache, Nginx, Virtual Patching, HTTP.