THE BRIDGE

CYBER SECURITY

Reglas de WAF

Regla WAF

- **Mod Security:**
  - Es un módulo de firewall de aplicaciones web (WAF) de código abierto y multiplataforma.
  - Obtenemos visibilidad del tráfico HTTP(S)
  - Permite protegernos de los ataques WEB como lo son:
    - inyecciones de SQL.
    - XSS (Cross Site Scripting).
    - Troyanos.
    - Agentes de usuario incorrectos.
    - Session hijacking (secuestro de sesiones)
    - Muchas otras vulnerabilidades… y además tiene una API para implementar protecciones avanzadas.

  - Funciona con Apache, Nginx e MS-IIS

- La seguridad se implementa usando reglas en cualquier de las cinco fases de un requerimiento Web:
  - **Encabezados de solicitud → REQUEST_HEADERS**
  - **Cuerpo de solicitud → REQUEST_BODY**
  - **Encabezados de respuesta → RESPONSE_HEADERS**
  - **Cuerpo de respuesta → RESPONSE_BODY**
  - **Registro → LOGGING**

modsecurity
Open Source Web Application Firewall

Rules

- Generalmente, las reglas tienen 4 partes:
    - **Directiva de configuración**
    - Variable(s)
    - Operador(es)
    - Acción(es)

    - https://github.com/SpiderLabs/ModSecurity/wiki/ModSecurity-Rules-Language-Porting-Specification#directives

- **Directivas de configuración:**
    - Las directivas de configuración para **ModSecurity** son similares a las directivas del servidor Apache.

    - Algunas solo se pueden usar una vez en el archivo de configuración principal.

    - Esto permite una actualización/migración más fácil de las reglas.

    - Los valores para las directivas más comunes son:
        - **SecRuleEngine**: Activa o desactiva que se procesen las reglas de seguridad, los valores son **ON**, **OFF** o **DetectionOnly**.

        - **SecRule**: Permite crear una regla de seguridad.

- https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual-(v3.x)#user-content-Configuration_Directives

Rules

- Generalmente, las reglas tienen 4 partes:
  - Directiva de configuración
  - **Variable(s)**
  - Operador(es)
  - Acción(es)

- **Variables:**
  - Notifica a ModSecurity **DÓNDE** tiene que mirar en busca de los patrones que va a evaluar

  - Algunas variables comunes son:
    - **REQUEST_URI**: This variable holds the full request URL including the query string data (**e.g., /index.php? p=X**). However, it will never contain a domain name, even if it was provided on the request line.

    - **ARGS**: Es una colección y se puede usar por sí solo (significa todos los argumentos, incluida la carga útil POST), con un parámetro estático (coincide con los argumentos con ese nombre) o con una expresión regular (coincide con todos los argumentos con un nombre que coincide con la expresión regular

    - **REQUEST_BODY**: Contiene el cuerpo de la solicitud sin procesar

    - **REQUEST_HEADERS**: una colección de todos los encabezados de solicitud o se puede usar para inspeccionar los encabezados seleccionados

- https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual-(v3.x)#user-content-Variables

Rules

- Generalmente, las reglas tienen 4 partes:
    - Directiva de configuración
    - Variable(s)
    - **Operador(es)**
    - Acción(es)

- **Operadores:**
    - Define QUÉ se está buscando o **QUÉ patrón se espera**
    - Se inicia con el símbolo "**@**".
    - El resultado del operado puede ser "**TRUE**" o "**FALSE**".
    - Algunos Operadores comunes son:
        - **eq**: Realiza una comparación numérica.
        - **Contains:** Busca el texto en alguna parte de la variable analizada.
        - **rx**: realiza una coincidencia de expresión regular del patrón proporcionado como parámetro. Este es el operador predeterminado

- https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual-(v3.x)#user-content-Operators

Rules

- Generalmente, las reglas tienen 4 partes:
  - Directiva de configuración
  - Variable(s)
  - Operador(es)
  - **Acción(es)**

- **Acción (es):**
  - Define QUÉ se debe hacer con el tráfico cuando se produce una coincidencia.

  - Algunos Operadores comunes son:
    - **id** : Asigna un ID único a la regla, esto ayuda para poder identificarla y poder acciones subsecuentes.

    - **Log**: Indica que el requerimiento debe generar un LOG de la transacción.

    - **Msg**: Genera un mensaje personalizado cuando la regla sea ejecutada.

    - **Pass**: Continúa procesando la próxima regla, aunque esta sea TRUE.

    - **deny**: Deniega la ejecución del requerimiento.

    - **Phase**: Indica en qué fase se va a realizar la verificación de la regla, los valores posibles son del 1 al 5.

    - **severity**: Establece el nivel de criticidad de la regla y puede ser del 0 al 7 o por texto (ejemplo “CRITICAL”)

- https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual-(v3.x)#user-content-Actions

Rules

- **Ejemplos de Reglas**
  - **SecRule REQUEST_URI "@streq /index.php" "id:99990,phase:1,t:lowercase,deny"**
    - **Directiva de configuración: SecRule**
      - Indica que es una regla de seguridad del WAF.
    - **Variables: REQUEST_URI**
      - Verifica en la URL
    - **Operador: "@streq /index.php"**
      - Realizar una comparación de caracteres: @streq
      - Valor a comparar: /index.php
    - **Acción: "id:99990,phase:1,t:lowercase,deny"**
      - Se establece el ID de la regla **(id:99990)**
      - Se establece que se va a ejecutar en la fase de **(REQUEST_HEADERS: phase:1)**
      - Se incluye que se va a realizar una transformación para que todo el texto sean letras minúsculas **(t:lowercase)**
      - Si se cumple la regla o sea que el valor es TRUE entonces se deniega este requerimiento **(deny)**

Documentacion Adicional

- Mod Security:
  - https://www.modsecurity.org/
- Mod Security Rules:
  - https://www.modsecurity.org/rules.html
- Mod Security Documentation:
  - https://github.com/SpiderLabs/ModSecurity/wiki
- Tutorial How to set up mod_security with apache on Debian/Ubuntu:
  - https://www.digitalocean.com/community/tutorials/how-to-set-up-mod_security-with-apache-on-debian-ubuntu
  - https://phoenixnap.com/kb/setup-configure-modsecurity-on-apache
- Continuous Security Monitoring using ModSecurity:
  - https://www.notsosecure.com/continuous-security-monitoring/

THE BRIDGE

Lorem ipsum Dolor sit amet, consectetur Adipiscing Elit. Etiam eget quam lacus.