**Instalando e configurando o ModSecurity e o CRS**

Este artigo explica como instalar o Apache HTTP Server, o ModSecurity e as regras do projeto OWASP ModSecurity Core Rule Set.

Overview

O objetivo deste artigo é definir os passos necessários para a instalação e configuração do Apache HTTP Server, ModSecurity e as regras do projeto OWASP ModSecurity Core Rule Set. Para isso, será necessário executar os passos do Tutorial 2 - Instalando o OWASP Juice Shop e executar os passos a seguir.

Passo a Passo

**Passo 1: Instale o Apache HTTP Server**

|  |
| --- |
| # zypper –n in apache2 |

**Passo 2: Instale o ModSecurity 2.9.3 a partir do código-fonte**

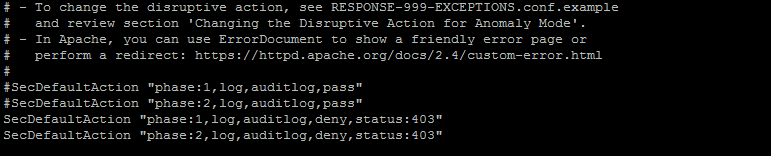
|  |
| --- |
| # zypper –n in apache2-devel libtool libyajl-devel pcre-devel libxml2-devel  # cd /opt  # wget https://github.com/SpiderLabs/ModSecurity/archive/v2.9.3.tar.gz  # tar xzvf v2.9.3.tar.gz  # cd ModSecurity-2.9.3  # ./autogen.sh  # ./configure  # make  # make install  # cp modsecurity.conf-recommended /etc/apache2/conf.d/modsecurity.conf  # cp unicode.mapping /etc/apache2/conf.d/  # a2enmod unique\_id  # a2enmod security2 |

**Passo 3: Instale as regras do OWASP ModSecurity Core Rule Set**

|  |
| --- |
| # cd /etc/apache2/conf.d/  # wget https://github.com/SpiderLabs/owasp-modsecurity-crs/archive/v3.2.0.tar.gz  # tar xzvf v3.2.0.tar.gz  # cd owasp-modsecurity-crs-3.2.0  # cp crs-setup.conf.example crs-setup.conf |

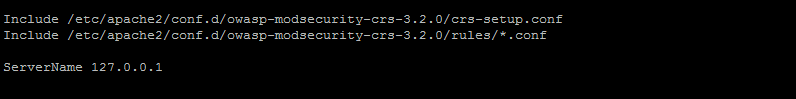
**Passo 4: Edite o arquivo crs-setup.conf e faça as modificações a seguir**

Edite o arquivo crs-setup.conf e altere a ação padrão, trocando os parâmetros do SecDefaultAction de **pass** para **deny**. A imagem a seguir apresenta a parte do arquivo de configuração que foi modificada.



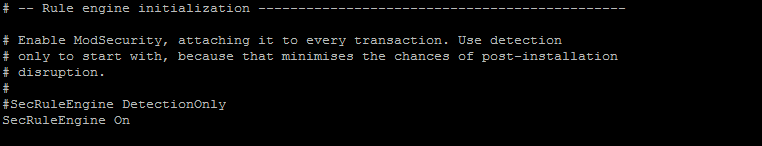
**Passo 5: Adicione as regras do OWASP ModSecurity CRS no arquivo httpd.conf**

Edite o arquivo /etc/apache2/httpd.conf e adicione as configurações a seguir no final do arquivo (o ServerName também deverá ser adicionado):



**Passo 6: Configure o SecRuleEngine para processar as regras e realizar os bloqueios**

Edite o arquivo /etc/apache2/conf.d/ modsecurity.conf e mude a configuração SecRuleEngine de DetectionOnly para On, conforme apresentado na imagem a seguir:



**Passo 7: Configure o proxy reverso do Apache HTTP para o Juice Shop**

Para configurar o proxy reverso, crie o arquivo juiceshop.conf e adicione as configurações necessárias, conforme os comandos a seguir:

|  |
| --- |
| # vi /etc/apache2/vhost.d/juiceshop.conf  <VirtualHost \*:80>  ServerAdmin webmaster@juice-sh.op  ServerName juice-sh.op  ProxyVia On  ProxyRequests Off  ProxyPreserveHost On  ProxyErrorOverride On  ProxyPass /error !  <Proxy \*>  Require all granted  Options None  </Proxy>  <LocationMatch "/">  ProxyErrorOverride Off  <RequireAll>  Require method GET POST  </RequireAll>  ProxyPass http://localhost:3000/  ProxyPassReverse http://localhost:3000/  </LocationMatch>  <Location "/rest/user/login">  ProxyErrorOverride Off  <RequireAll>  Require method POST  </RequireAll>  ProxyPass http://localhost:3000/rest/user/login  ProxyPassReverse http://localhost:3000/rest/user/login  </Location>  </VirtualHost> |

**Passo 8: Inicie o OWASP Juice Shop e o Apache HTTP Server**

Para iniciar o OWASP Juice Shop, abra o Terminal e digite os comandos a seguir:

|  |
| --- |
| # cd /opt/juice-shop  # npm start |

Para iniciar o Apache HTTP Server, abra um novo Terminal e digite os comando a seguir:

|  |
| --- |
| # rcapache2 start |

Para acessar a página do OWASP Juice Shop diretamente, use o endereço <http://localhost:3000>. Já para acessá-lo através do Apache HTTP Server e testar as regras debloqueio, use o endereço <http://localhost/>.

O acesso ao OWASP Juice Shop usando a porta 80 estará utilizando um proxy reverso do Apache HTTP Server, com o ModSecurity e as regras do projeto OWASP ModSecurity Core Rule Set.

Referências

1. Documentação do Servidor HTTP Apache versão 2.4 disponível em:

<http://httpd.apache.org/docs/2.4/>

1. ModSecurity Reference Manual disponível em: <https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual-(v2.x)>
2. OWASP ModSecurity Core Rule Set disponível em:

<https://owasp.org/www-project-modsecurity-core-rule-set/>