Objetivo:
criar um conjunto de regras protecao para uma das aplicacoes disponiveis em
https://github.com/globocom/secDevLabs

Aplicacao escolhida → secDevLabs/owasp-top10-2021-apps/a3/gossip-world/

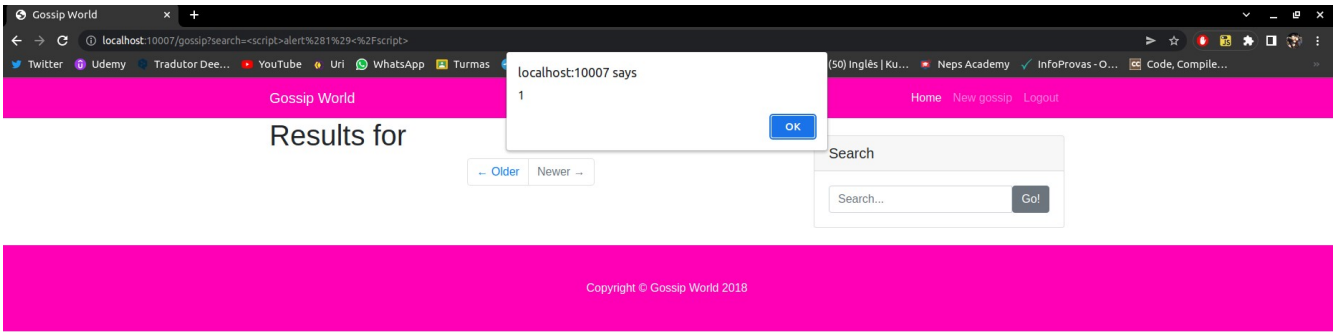
pre requisitos:
docker → https://docs.docker.com/engine/install/
docker compose → https://docs.docker.com/compose/install/

Configurando o ambiente:
seguimos o passo a passo descrito no arquivo tag de waf.
A seguir, estão descritos alguns passos para a criação de um ambiente semelhante ao utilizado no GET.

1. Instale uma VM com Debian ou Ubuntu
2. Instale o nginx
2.1 sudo add-apt-repository ppa:ondrej/nginx-mainline -y
2.2 apt update
2.3 apt install nginx-core nginx-common nginx nginx-full
3. Instale o código fonte do nginx
3.1 habilite os respositórios deb-src em /etc/apt/sources.list.d/ondrej-ubuntu-nginx-mainline-*.list (basta descomentar a linha)
3.2 apt update; apt install dpkg-dev
3.3 mkdir -p /usr/local/src/nginx; cd /usr/local/src/nginx; apt source nginx
4. Instale o modsecurity
4.1 apt install git
4.2 git clone --depth 1 -b v3/master --single-branch https://github.com/SpiderLabs/ModSecurity /usr/local/src/ModSecurity/
4.3 apt install gcc make build-essential autoconf automake libtool libcurl4-openssl-dev liblua5.3-dev libfuzzy-dev ssdeep gettext pkg-config libpcre3 libpcre3-dev libxml2 libxml2-dev libcurl4 libgeoip-dev libyajl-dev doxygen uuid-dev
4.4 git submodule init
4.5 git submodule update
4.6 ./build.sh
4.7 ./configure
4.8 make -j1 ; sudo make install
5. Instale o conector de nginx do modsecurity
5.1 git clone --depth 1 https://github.com/SpiderLabs/ModSecurity-nginx.git /usr/local/src/ModSecurity-nginx/
5.2 cd /usr/local/src/nginx/nginx-*/
5.3 apt build-dep nginx
5.4 ./configure --with-compat --add-dynamic-module=/usr/local/src/ModSecurity-nginx
5.5 make modules
5.6 sudo cp objs/ngx_http_modsecurity_module.so /usr/share/nginx/modules/
6. Inicie o nginx
6.1 systemctl start nginx
7. Copie os arquivos de exemplo e depois reinicie o nginx
7.1 systemctl restart nginx

observacoes:
- Alguns comandos não foram necessarios, já havia instalado anteriormente o git (passo 4.1)
- fiz um backup do arquivo original → mv /etc/nginx/nginx.conf /etc/nginx/nginx.conf.bkp

vulnerabilidade pre mudancas:
comando → <script>alert(1)</script>



vunerabilidade sql corrigida:

vunerabilidade xss corrigida:

vale destacar que devemos acessar pela porta 80, pois, é nela que o WAF está configurado.