Nginx - WAF

- Install Nginx and ModSecurity.

```
sudo apt-get update
sudo apt-get install nginx -y
sudo apt-get install libnginx-mod-security -y
sudo apt-get intall git -y
```

- Enable ModSecurity module in Nginx configuration.

```
sudo sed -i 's/# include \/etc\/nginx\/modules-enabled\/\*\.conf;/include \/etc\/nginx\/modules-enabled\/\*\.conf;/' /etc/nginx/nginx.conf
```

- Configure ModSecurity rules

```
sudo mv /etc/nginx/mods-available/mod-security.conf /etc/nginx/mods-available/mod-security.conf.orig
sudo cp /usr/share/modsecurity-crs/modsecurity.conf-recommended /etc/nginx/mods-available/mod-security.conf
sudo mv /etc/nginx/mods-available/modsecurity.conf /etc/nginx/mods-available/modsecurity.conf.orig
sudo sed -i 's/SecRuleEngine DetectionOnly/SecRuleEngine On/' /etc/nginx/mods-available/modsecurity.conf
sudo sed -i 's/SecResponseBodyAccess On/SecResponseBodyAccess Off/' /etc/nginx/mods-available/modsecurity.conf
```

- Download and configure the OWASP Core Rule Set.

```
sudo git clone https://github.com/SpiderLabs/owasp-modsecurity-crs.git /usr/share/modsecurity-crs
sudo cp /usr/share/modsecurity-crs/crs-setup.conf.example /usr/share/modsecurity-crs/crs-setup.conf
sudo mv /etc/nginx/mods-available/modsecurity-crs.conf /etc/nginx/mods-available/modsecurity-crs.conf.orig
sudo cp /usr/share/modsecurity-crs/rules/*.conf /etc/nginx/mods-available/
sudo cp /usr/share/modsecurity-crs/rules/*.data /etc/nginx/mods-available/
sudo cp /usr/share/modsecurity-crs/rules/*.txt /etc/nginx/mods-available/
sudo cp /usr/share/modsecurity-crs/rules/*.sls /etc/nginx/mods-available/
sudo sed -i 's/Include \/etc\/nginx\/modsecurity.conf/Include \/etc\/nginx\/mods-available\/modsecurity.conf/' /etc/nginx/mods-available/modsecurity-crs.conf
```

- Backup Config Nginx Default.

```
sudo cp /etc/nginx/sites-available/default /etc/nginx/sites-available/default.orig
```

- Download and configure the OWASP Core Rule Set.

```
server {
    listen 80;
    listen [::]:80;
    server_name example.com;

    location / {
        proxy_pass http://localhost:8000;
        proxy_set_header Host \$host;
        proxy_set_header X-Real-IP \$remote_addr;
        proxy_set_header X-Forwarded-For \$proxy_add_x_forwarded_for;

        # ModSecurity settings
        modsecurity on;
        modsecurity_rules_file /etc/nginx/mods-available/modsecurity-crs.conf;
    }
}
```

- Restart Nginx to apply changes

```
sudo systemctl restart nginx
```

Revision #3
Created 7 July 2024 01:52:03 by Kevin
Updated 19 February 2025 03:31:02 by Kevin