**Utho Product WAP Deployment on AlmaLinux 9.2**

**1. Overview**

This document provides a step-by-step guide to deploying opensource wap with **NGINX** & **ModSecurity v3** on **AlmaLinux 9.2**. The setup includes:

* **NGINX as a Reverse Proxy**
* **ModSecurity for Web Application Firewall (WAF)**
* **GeoIP Filtering** (Allow access only from India by default as per this setup)

**2. System Requirements**

**Supported OS:**

* AlmaLinux 9.2 (64-bit)

**Required Packages:**

* NGINX
* Mod Security v3
* GeoLite2 Country Database
* GCC, Make, and Dependencies

**3. Deployment Steps**

**Step 1: Run Deployment Script**

The provided script deployement.sh installs and configures everything automatically.

**Run the script:**

chmod +x deployement.sh

sudo ./deployement.sh

**Step 2: Verify Installation**

Check if NGINX is running:

sudo systemctl status nginx

If fail then paste nginx.conf contents to the /etc/nginx/nginx.conf which is attached

Check if GeoIP database is available:

ls -l /usr/share/GeoIP/GeoLite2-Country.mmdb

**4. ModSecurity Configuration**

**Main Configuration File: /etc/nginx/modsec/main.conf**

SecRuleEngine On

Include /etc/nginx/modsec/modsecurity.conf

Include /etc/nginx/modsec/crs/crs-setup.conf

Include /etc/nginx/modsec/crs/rules/\*.conf

# Enable GeoIP Filtering

SecGeoLookupDb /usr/share/GeoIP/GeoLite2-Country.mmdb

# Log only relevant events

SecAuditEngine RelevantOnly

SecAuditLogParts ABIJDEFHZ

SecAuditLogType Serial

SecAuditLog /var/log/nginx/modsec\_audit.log

SecAuditLogFormat JSON

# Allow access from India

SecRule REMOTE\_ADDR "@geoLookup" "phase:1,id:12345,t:none,pass,nolog"

# Block access from all other countries

SecRule GEO:COUNTRY\_CODE "!@streq IN" \

"phase:1,id:12346,deny,status:403,msg:'Access from restricted country'"

**Restart NGINX to Apply Changes**

sudo nginx -t

sudo systemctl restart nginx

**5. Testing the Setup**

**Legitimate Request (Should Work ✅)**

curl -A "Mozilla/5.0" -L "https://wecloud.remotedevadmin.in/"

**Blocked Requests (Should Return 403 🚫)**

**Test SQL Injection**

curl -A "Mozilla/5.0" -L "https://wecloud.remotedevadmin.in/index.php?id=1' OR '1'='1"

**Test XSS (Cross-Site Scripting)**

curl -A "Mozilla/5.0" -L "https://wecloud.remotedevadmin.in/index.php?search=<script>alert('XSS')</script>"

**Test Country Restriction (Non-India IPs Should Fail)**

curl -A "Mozilla/5.0" --header "X-Forwarded-For: 192.42.116.218" -L "https://wecloud.remotedevadmin.in/"

**6. Log Monitoring**

**View NGINX Error Logs**

sudo tail -f /var/log/nginx/error.log

**View NGINX Access Logs**

sudo tail -f /var/log/nginx/access.log

**View ModSecurity Audit Logs**

sudo tail -f /var/log/nginx/modsec\_audit.log

**7. Summary**

✅ **NGINX** is installed and running as a Reverse Proxy  
✅ **ModSecurity** is configured with **OWASP CRS** rules by default  
✅ **GeoIP filtering** allows traffic only from India by default  
✅ **Owasp top 10 vulnerabilities prevention** are active by default  
✅ **Logs** are stored in /var/log/nginx/ for debugging

🚀 **Your Web Application Firewall (WAF) is now deployed!**

For Dev team :

Customer need to provide examples:

server\_name wecloud.remotedevadmin.in;

SSl details :

ssl\_certificate /etc/letsencrypt/live/wecloud.remotedevadmin.in/fullchain.pem;

ssl\_certificate\_key /etc/letsencrypt/live/wecloud.remotedevadmin.in/privkey.pem;

include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot

ssl\_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot

proxy\_pass <http://157.20.214.104>; #backend server details with port if needed from backend response

Customer need to bind his domain with wap server ip and add his server ip as a proxy\_pass to serve response with filtered by wap.

[coreruleset](https://github.com/coreruleset/coreruleset) Rules need to add or remove in /etc/nginx/modsec/crs/crs-setup.conf

custom rules can be manage by this file /etc/nginx/modsec/main.conf

Logs need to visible to customer if any rules block his request, then he can block/unblock that rules.

Customer should be able to add and remove rules from above file as per there requirents.