- Other OS Configs
  - CentOS Stream 9
  - Ubuntu 24.04 LTS
  - Ubuntu 22.04 LTS
  - Windows Server 2022
  - Windows Server 2019
  - Debian 12
  - Debian 11
  - Fedora 40
  - AlmaLinux 9

Server World Privacy Policy Support/Contact us 33404 / 114452921

Ubuntu 22.04

- Install
- NTP /
- DNS /
- Storage
- Virtualization
- Container
- Cloud
- Directory
- Web S
- Database
- FTP /
- Proxy
- Monit
- Security
- Language
- Desktop
- Others

- Others
- Ruby
- (01) Install Ruby 3.0
- .NET
- Podman
- PHP
- (01) Install Podman
- JavaScript / TypeScript
- (05) InfluxDB Next is
- Python
- Buildah
- Minikube
- (01) Install Minikube
- MySQL 8.0
- Docker
- (22) Neutron Network (FLAT)
- (01) Install Vagrant

- Set Disk Quota
- (01) Install Graphic Driver
- Display Disk Settings info
- (02) Install Container Toolkit
- Check Network Bandwidth
- Configure Network Bonding
- CentOS Stream 8
- (06) Enable Registry
- (44) Conf Manila (Storage Node)
- (07) Enable Prometheus
- (08) Enable Helm3

- CentOS 8
- CentOS 6
- CentOS 5
- Debian 10
- Debian 9
- Debian 8
- Debian 7
- Debian 6
- Fedora 39
- Fedora 38
- Fedora 37
- Fedora 36
- Fedora 35
- Fedora 34

- Fedora 33
- (45) Use Manila (Local Device)
- (46) Conf Designate (Control Node)
- (47) Conf Designate (Network Node)
- (48) How to use Designate
- (49) Conf Octavia (Control Node)
- (50) Conf Octavia (Network Node)
- (51) Create LoadBalancer Image
- (52) How to use Octavia
- (53) Configure Gnocchi
- (54) Conf Ceilometer (Network)
- (55) Conf Ceilometer (Compute)
- (56) How to use Ceilometer (Nova)
- (57) How to use Ceilometer (Glance)
- (58) How to use Ceilometer (Cinder)
- (59) Configure CloudKitty
- (60) How to use CloudKitty
- (61) Conf Trove (Control Node)
- (62) Conf Trove (Network Node)
- (63) How to use Trove
- OpenStack Caracal
- OpenStack Antelope
- OpenStack Zed
- OpenStack Yoga

Apache2 : Configure mod_security2022/05/12

Enable [mod_security] module to configure Web Application Firewall (WAF).

[1] Install [mod_security].

```
root@www:~#
apt -y install libapache2-mod-security2
```

[2] Enable [mod_security].

```
root@www:~#
cp -p /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf

root@www:~#
vi /etc/modsecurity/modsecurity.conf

    line 7 : [SecRuleEngine DetectionOnly] is set as default, it does not block actions
    # if you'd like to block actions, change to [SecRuleEngine On]
    SecRuleEngine DetectionOnly
.....
.....
```

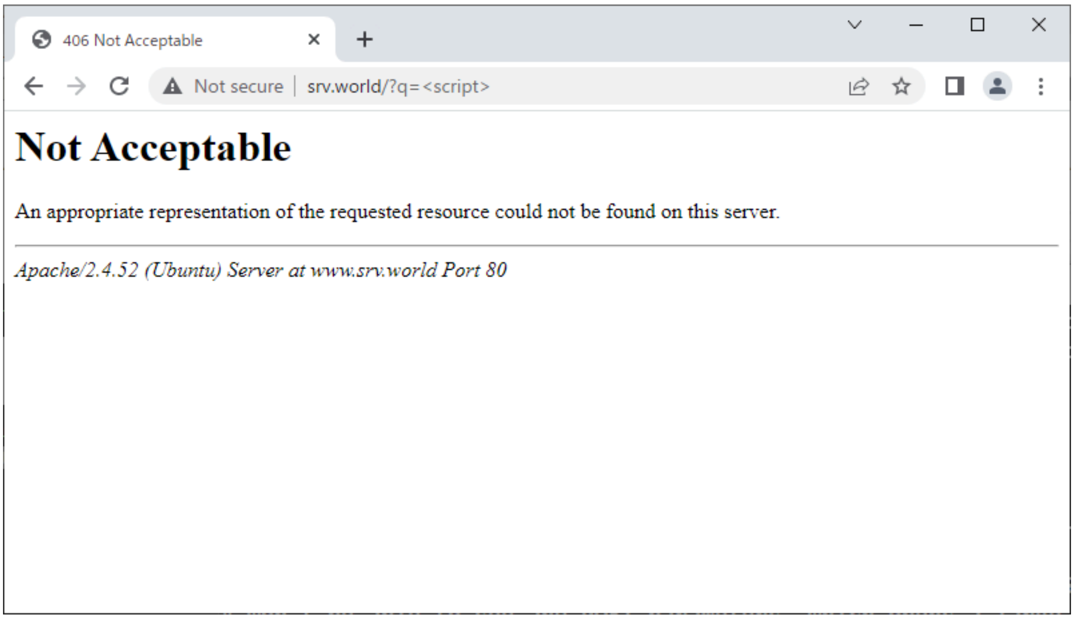
[3] It's possible to write a rule like follows.
⇒ SecRule VARIABLES OPERATOR [ACTIONS]
Each parameter has many kind of values, refer to official documents below.
https://github.com/SpiderLabs/ModSecurity/wiki

[4] For Example, set some rules and verify it works normally.

```
root@www:~#
vi /etc/modsecurity/localrules.conf
# default action when matching rules

SecDefaultAction "phase:2,deny,log,status:406"
# [etc/passwd] is included in request URI

SecRule REQUEST_URI "etc/passwd" "id:'500001'"
# [../] is included in request URI

SecRule REQUEST_URI "\.\./" "id:'500002'"
# [<SCRIPT] is included in arguments

SecRule ARGS "<[Ss][Cc][Rr][Ii][Pp][Tt]" "id:'500003'"
# [SELECT FROM] is included in arguments

SecRule ARGS "[Ss][Ee][Ll][Ee][Cc][Tt][[:space:]]+[Ff][Rr][Oo][Mm]" "id:'500004'"
```

```
root@www:~# systemctl restart apache2
```

[5] Access to the URI which includes words you set and verify it works normally.



Not Acceptable

An appropriate representation of the requested resource could not be found on this server.

Apache/2.4.52 (Ubuntu) Server at www.srv.world Port 80

[6] The logs for [mod_security] is placed in the directory like follows.

```
root@www:~# cat /var/log/apache2/modsec_audit.log


--622ba619-H--
Message: Access denied with code 406 (phase 2). Pattern match "<[Ss][Cc][Rr][Ii][Pp][Tt]" at ARGS:q. [file "/etc/modsecuri
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 10.0.0.5] ModSecurity: Access denied with code 406 (pha
Action: Intercepted (phase 2)
Stopwatch: 1652331282078532 1929 (- - -)
Stopwatch2: 1652331282078532 1929; combined=928, p1=759, p2=34, p3=0, p4=0, p5=135, sr=103, sw=0, l=0, gc=0
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.9.5 (http://www.modsecurity.org/); OWASP_CRS/3.3.2.
Server: Apache/2.4.52 (Ubuntu)
Engine-Mode: "ENABLED"

.....
.....
```

[7] General rules are provided and applied by default under the directory below. However maybe you need to customize them for your own web sites not to block necessary requests.

```
root@www:~# ll /usr/share/modsecurity-crs/rules


total 676
drwxr-xr-x 2 root root  4096 May 12 04:48 ./
drwxr-xr-x 4 root root  4096 May 12 04:48 ../
-rw-r--r-- 1 root root 13513 Aug 24  2021 REQUEST-901-INITIALIZATION.conf
-rw-r--r-- 1 root root 13555 Aug 24  2021 REQUEST-903.9001-DRUPAL-EXCLUSION-RULES.conf
-rw-r--r-- 1 root root 25812 Aug 24  2021 REQUEST-903.9002-WORDPRESS-EXCLUSION-RULES.conf
-rw-r--r-- 1 root root 10642 Aug 24  2021 REQUEST-903.9003-NEXTCLOUD-EXCLUSION-RULES.conf
-rw-r--r-- 1 root root  7822 Aug 24  2021 REQUEST-903.9004-DOKUWIKI-EXCLUSION-RULES.conf
-rw-r--r-- 1 root root  1876 Aug 24  2021 REQUEST-903.9005-CPANEL-EXCLUSION-RULES.conf
.....
.....
```

Matched Content

Ubuntu 22.04 : Apache2

- (01) Install Apache2
- (02) Configure Virtual Hostings
- (03) Configure SSL/TLS
- (04) Enable Userdir
- (05) Use CGI Scripts
- (06) Use PHP Scripts
- (07) PHP + PHP-FPM
- (08) Basic Authentication
- (09) Configure WebDAV Folder
- (10) Basic Authentication + PAM
- (11) Kerberos Authentication
- (12) Configure mod_md

- (13) Configure mod_proxy
- (14) Configure mod_security
- (15) Configure mod_ratelimit
- [Next Page]