

# Ubuntu????Mod\_Security????

Apache?WAF???????mod\_security??????

- AWS Lightsail???????????
- ????IP???????????

????????????????????Web Arena???????????????

??

- Ubuntu 24.04 (20.04???????????)
- Apache 2.4

? ??????aptitude????????????apt???????????

??????????

1. mod\_security???????????
2. mod\_security??????????
3. Apache????????mod\_security?????????
4. ????????????????

mod\_security??????????????

- ????????????

```
sudo aptitude update
```

- mod\_security??????

```
sudo aptitude install libapache2-mod-security2
```

- ????????

```
sudo apache2ctl -M |grep security
```

```
security2_module (shared)
```

??????????????????

ModSecurity???

- ??????????

```
sudo mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
```

????????????????????

## OWASP Core Rule Set (CRS)????????

- ???????

```
cd /usr/share/modsecurity-crs && pwd
```

- ?????????

```
sudo git clone https://github.com/coreruleset/coreruleset.git
```

- ?????????

```
sudo mv /usr/share/modsecurity-crs/coreruleset/crs-setup.conf.example /usr/share/modsecurity-  
crs/coreruleset/crs-setup.conf
```

## mod\_security????CRS????????

- ???????

```
cd /etc/apache2/mods-available/ && pwd
```

- ?????????

```
sudo cp -pi security2.conf /path/to/backup/directory/security2.conf.$(date +%Y%m%d)
```

????????????????

- ???????

```
diff -u /path/to/backup/directory/security2.conf.$(date +%Y%m%d) security2.conf
```

????????????????

- ??????

```
/etc/apache2/mods-available/security2.conf ?????????????????????????????????root??
```

```
- </IfModule>  
+     # Include OWASP ModSecurity CRS rules if installed  
+     IncludeOptional /usr/share/modsecurity-crs/*.load  
+</IfModule>
```

- ?????????

```
sudo apache2ctl configtest
```

Syntax OK ??????

- Apache??

```
sudo systemctl restart apache2.service
```

- Apache????

```
systemctl status apache2.service
```

active (running) ??????

## Apache????????

????Apache??

- ???????

```
cd /etc/apache2/sites-available && pwd
```

- ?????????????????

```
sudo cp -pi your_site.conf /path/to/backup/directory/your_site.conf.$(date +%Y%m%d)
```

.conf????????????????????????????

- ???????

```
diff -u /path/to/backup/directory/your_site.conf.$(date +%Y%m%d) your_site.conf
```

????????????????

- ?????

/etc/apache2/sites-available/your\_site.conf ?????????????????????????????????root??

```
# Mod Security
```

```
## ModSecurity[ ]
```

```
SecRuleEngine On
```

```
## ModSecurity[ ]
```

```
### [ ]SecRuleEngine On[ ]
```

```
#SecRuleEngine DetectionOnly
```

```
## [redacted]
```

```
SecRequestBodyInMemoryLimit 524288000
```

```
SecRequestBodyLimit 524288000
```

```
## [redacted]
```

```
SecRule ARGS:modseccparam "@contains test" "id:4321,deny,status:403,msg:'ModSecurity test rule has triggered'"
```

- ??????

```
diff -u /path/to/backup/directory/your_site.conf.$(date +%Y%m%d) your_site.conf
```

```
+ # Mod Security
```

```
+
```

```
+ ## ModSecurity [redacted]
```

```
+ SecRuleEngine On
```

```
+ ## ModSecurity [redacted]
```

```
+ ### [redacted] SecRuleEngine On [redacted]
```

```
+ # SecRuleEngine DetectionOnly
```

```
+
```

```
+ ## [redacted]
```

```
+ SecRequestBodyInMemoryLimit 524288000
```

```
+ SecRequestBodyLimit 524288000
```

```
+
```

```
+ ## [redacted]
```

```
+ SecRule ARGS:modseccparam "@contains test" "id:4321,deny,status:403,msg:'ModSecurity test rule has triggered'"
```

```
+
```

- ??????????

```
sudo apache2ctl configtest
```

Syntax OK ??????

- Apache???

```
sudo systemctl restart apache2.service
```

- Apache????

```
systemctl status apache2.service
```

```
active (running) ??????
```

mod\_security???

1. ?????????Web????????????????
2. ??????????modseccparam=test????????

# Forbidden

You don't have permission to access this resource.

????????????????

???????

```
sudo cat /path/to/sites_log/directory/sites_error.log
```

????????????????

???

```
ModSecurity: Access denied with code 403 (phase 2). String match "test" at ARGS:modseccparam. [file
"/etc/apache2/sites-enabled/your_site.conf"] [line "53"] [id "4321"] [msg "ModSecurity test rule has triggered"]
[hostname "host_address"] [uri "/" ] [unique_id "xxxxxxx"]
```

????????????????

??

Wordpress?Redmine??Web????????????????????????????(???)

???????????

```
## ModSecurity[]
#SecRuleEngine On
## ModSecurity[]
### []SecRuleEngine On[]
SecRuleEngine DetectionOnly
```

????????????????

