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有効化
SecRuleEngine On
## ModSecurity検知モード
### 検知モードで動かす場合はSecRuleEngine Onをコメントアウトしてこちらを有効化します
```

```
#SecRuleEngine DetectionOnly

## ファイルのアップロードをできるようにします。
SecRequestBodyInMemoryLimit 524288000
SecRequestBodyLimit 524288000

## テスト用の検知パラメータを付け加えます。
    SecRule ARGS:modsecparam "@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有効化
+SecRuleEngine On
+## ModSecurity検知モード
+### 検知モードで動かす場合はSecRuleEngine Onをコメントアウトしてこちらを有効化します
+#SecRuleEngine DetectionOnly
+
+## ファイルのアップロードをできるようにします。
+SecRequestBodyInMemoryLimit 524288000
+SecRequestBodyLimit 524288000
+
+## テスト用の検知パラメータを付け加えます。
+    SecRule ARGS:modsecparam "@contains test" "id:4321,deny,status:403,msg:'ModSecurity test rule has triggered'"
+
```

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

```
sudo apache2ctl configtest
```

`Syntax OK`???????

- Apache???

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

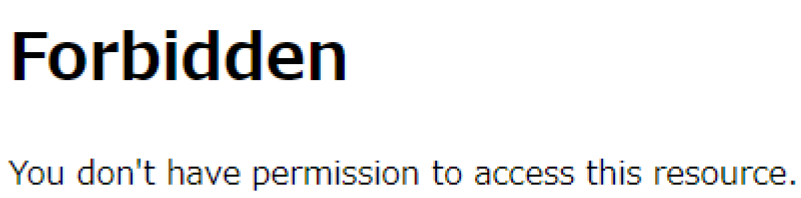
- Apache?????

```
systemctl status apache2.service
```

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

mod_security????

1. ??????????????Web?????????????????????????
2. ??????????`?modsecparam=test`?????????????



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

????????

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

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

????

```
ModSecurity: Access denied with code 403 (phase 2). String match "test" at ARGS:modsecparam. [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有効化
#SecRuleEngine On
## ModSecurity検知モード
### 検知モードで動かす場合はSecRuleEngine Onをコメントアウトしてこちらを有効化します
SecRuleEngine DetectionOnly
```

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

Revision #1
Created 9 September 2024 13:00:24 by manualmaton

Updated 9 September 2024 14:06:36 by manualmaton