Mod_Security??????????????Next cloud?????????

Nextcloud?mod_security??????????????????????????????????????Mod_security????????????????????????

????

1. ?????????????
2. ?????????
3. ??????????????????

??????

????

`/var/log/nextcloud_error.log`??????????????????

```
[Wed Sep 11 16:35:02.048442 2024] [security2:error] [pid 32762:tid 32762] [client aaa.bbb.ccc.ddd:56994] [client aaa.bbb.ccc.ddd] ModSecurity: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "92"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 5 - SQLI=0,XSS=0,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 5, 0, 0, 0"] [ver "OWASP_CRS/3.3.5"] [tag "event-correlation"] [hostname "nextcloud.hoge.com"] [uri "/ocs/v2.php/apps/user_status/api/v1/heartbeat"] [unique_id "ZuFIJU_udFaqxqrJvRLaPQAAAAA"]
```

????????

- ???????IP????
- ????????ID?
- ??????????

???

???????????

???????????copilot???????awk????????????

```
awk '/ModSecurity/ {
ip = gensub(/.*\[client ([0-9.]+):.*/, "\\1", "g", $0);
rule_id = gensub(/.*\[id "([0-9]+)"\].*/, "\\1", "g", $0);
print rule_id, ip;
```

```
}' /var/log/nextcloud/nextcloud_error.log | sort | uniq -c
```

???????????Mod_Security???????????????

```
 36 911100 127.0.0.1
267 911100 aaa.bbb.ccc.ddd
 65 920420 aaa.bbb.ccc.ddd
 36 949110 127.0.0.1
267 949110 aaa.bbb.ccc.ddd
 36 980130 127.0.0.1
267 980130 aaa.bbb.ccc.ddd
```

??????????????127.0.0.1?????????aaa.bbb.ccc.ddd????????????IP??????????????????Nextcloud???????????????????

Mod_security????????ID????????????????????

Mod_Security???????????????

Apache??????????????????????????

?????????

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

```
sudo cp -ci /etc/apache2/sites-available/nextcloud.conf /path/to/backup/directory/nextcloud.conf.$(date +%Y%m%d)
```

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

- ????????

```
diff -u /path/to/backup/directory/nextcloud.conf.$(date +%Y%m%d) /etc/apache2/sites-available/nextcloud.conf
```

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

- ??????

`/etc/apache2/sites-available/nextcloud.conf` ????????????????(?root??)

```
# Mod_security
## □□□□□□□□

SecRuleEngine DetectionOnly

## □□□□□□□□ID
```

```
SecRuleRemoveById 911100
SecRuleRemoveById 920420
SecRuleRemoveById 949110
SecRuleRemoveById 980130
```

- ????????

```
diff -u /path/to/backup/directory/nextcloud.conf.$(date +%Y%m%d) /etc/apache2/sites-available/nextcloud.conf
```

`SecRuleRemoveById ID` ??????????????????????

- ???

```
 ## 最初は検知モード

 SecRuleEngine DetectionOnly
+
+## 偽陽性と判断したID
+SecRuleRemoveById 911100
+SecRuleRemoveById 920420
+SecRuleRemoveById 949110
+SecRuleRemoveById 980130
+
 </VirtualHost>
```

???????????

- ????

```
sudo apache2ctl configtest
```

`Syntax OK` ???????

- ????

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

- Apache????

```
systemctl status apache2.service
```

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

????

??????

```
tail -f /var/log/nextcloud/nextcloud_error.log
```

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

- ????????Nextcloud?????????????????
- ??????ID?????????????????

Revision #3
Created 11 September 2024 17:26:52 by manualmaton
Updated 12 September 2024 09:09:04 by manualmaton