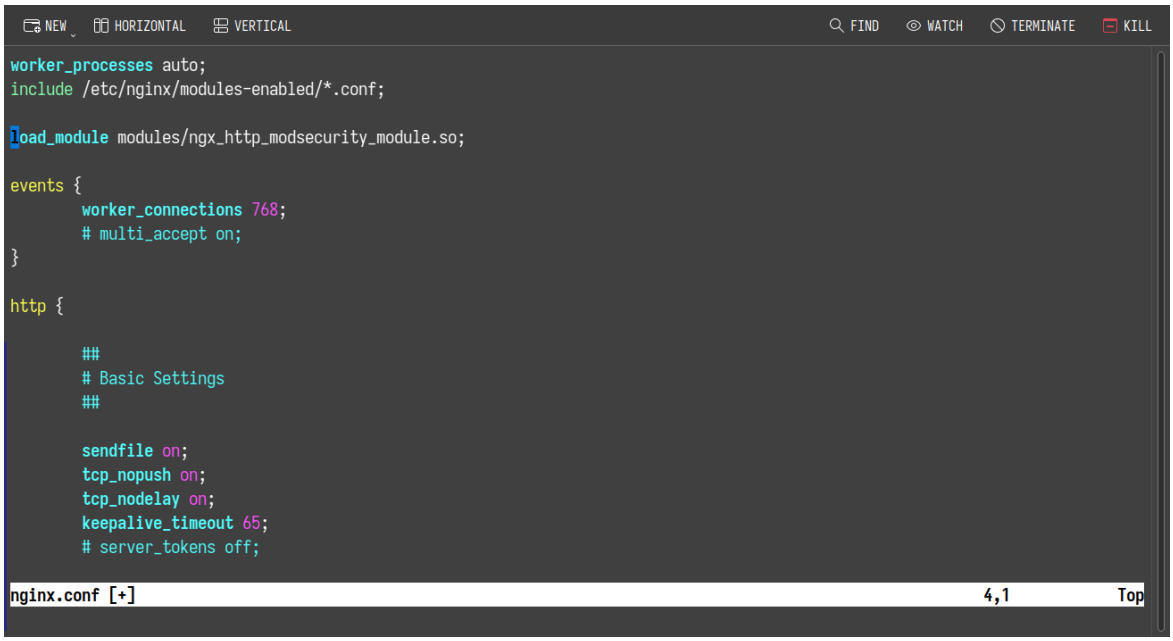
实验4

> 21009200991 盖乐

配置nginx

文档：https://docs.nginx.com/nginx-waf/

启用 nginx modsecurity 模块：



配置ModSecurity

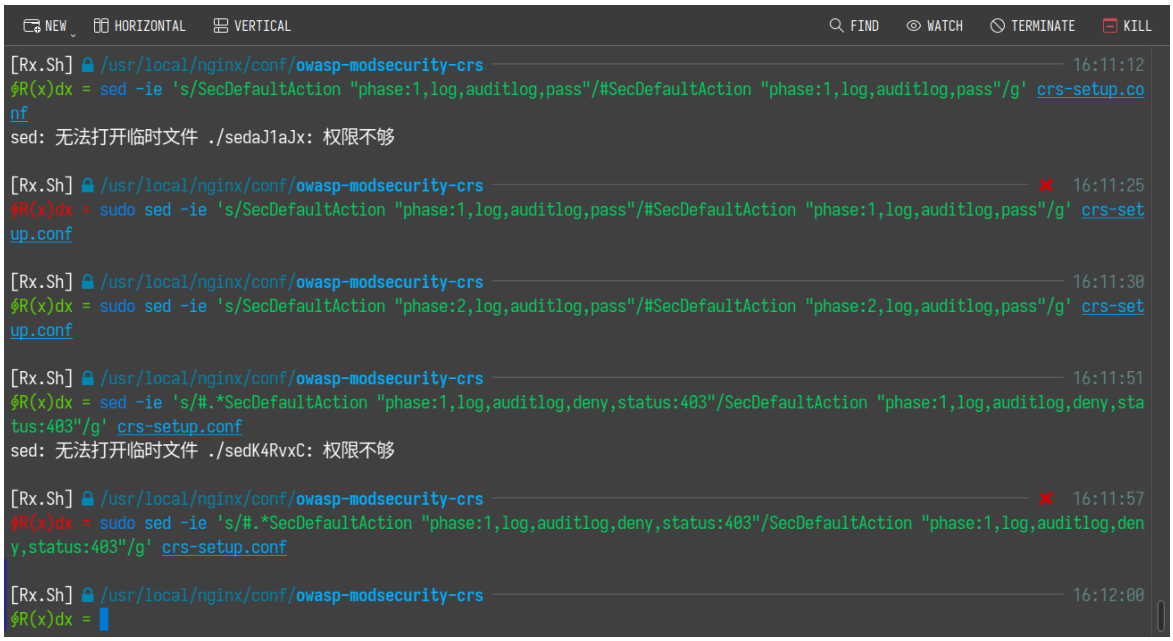
修改nginx配置：

```
NEW  HORIZONTAL  VERTICAL                                   FIND  WATCH  TERMINATE  KILL
server {
    listen 8080;
    listen [::]:8080;
    server_name localhost;
    modsecurity on;
    modsecurity_rules_file /etc/nginx/modsec/modsecurity.conf;
    root /var/www/html;
    location / {
        index index.html index.htm index.php;
    }

    location ~ \.php$ {
        # 404
        try_files $fastcgi_script_name =404;

        # default fastcgi_params
        include fastcgi_params;

        # fastcgi settings
        fastcgi_pass                    unix:/run/php-fpm7/php-fpm.sock;
        fastcgi_index                   index.php;
        fastcgi_buffers                 8 16k;
/etc/nginx/sites-available/basic_auth [+]                                  6,56          Top
:wq
```

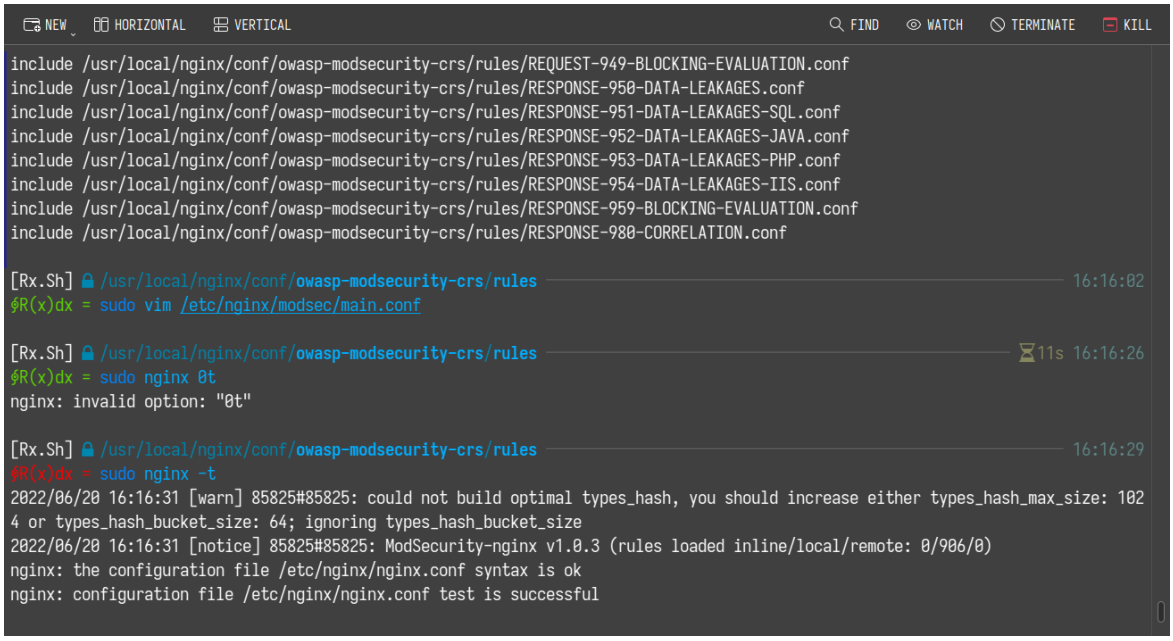
配置OWASP规则

配置 OWASP 规则:

```
NEW  HORIZONTAL  VERTICAL                                   FIND  WATCH  TERMINATE  KILL

[Rx.Sh] ~/Code                                                                  HU 16:10:40
$R(x)dx = git clone https://github.com/SpiderLabs/owasp-modsecurity-crs.git
正克隆到 'owasp-modsecurity-crs'...
remote: Enumerating objects: 10486, done.
remote: Total 10486 (delta 0), reused 0 (delta 0), pack-reused 10486
接收对象中: 100% (10486/10486), 3.34 MiB | 1.87 MiB/s, 完成.
处理 delta 中: 100% (7687/7687), 完成.

[Rx.Sh] ~/Code                                                                  4s 16:10:46
$R(x)dx = sudo cp -rf owasp-modsecurity-crs  /usr/local/nginx/conf/
[sudo] reverier 的密码:

[Rx.Sh] ~/Code                                                                  4s 16:10:55

[Rx.Sh] ~/Code                                                                  4s 16:11:01
$R(x)dx = cd /usr/local/nginx/conf/owasp-modsecurity-crs

[Rx.Sh] /usr/local/nginx/conf/owasp-modsecurity-crs                                16:11:04
$R(x)dx = cp crs-setup.conf.example  crs-setup.conf
cp: 无法创建普通文件 'crs-setup.conf': 权限不够

[Rx.Sh] /usr/local/nginx/conf/owasp-modsecurity-crs                                16:11:09
$R(x)dx = sudo cp crs-setup.conf.example  crs-setup.conf
```

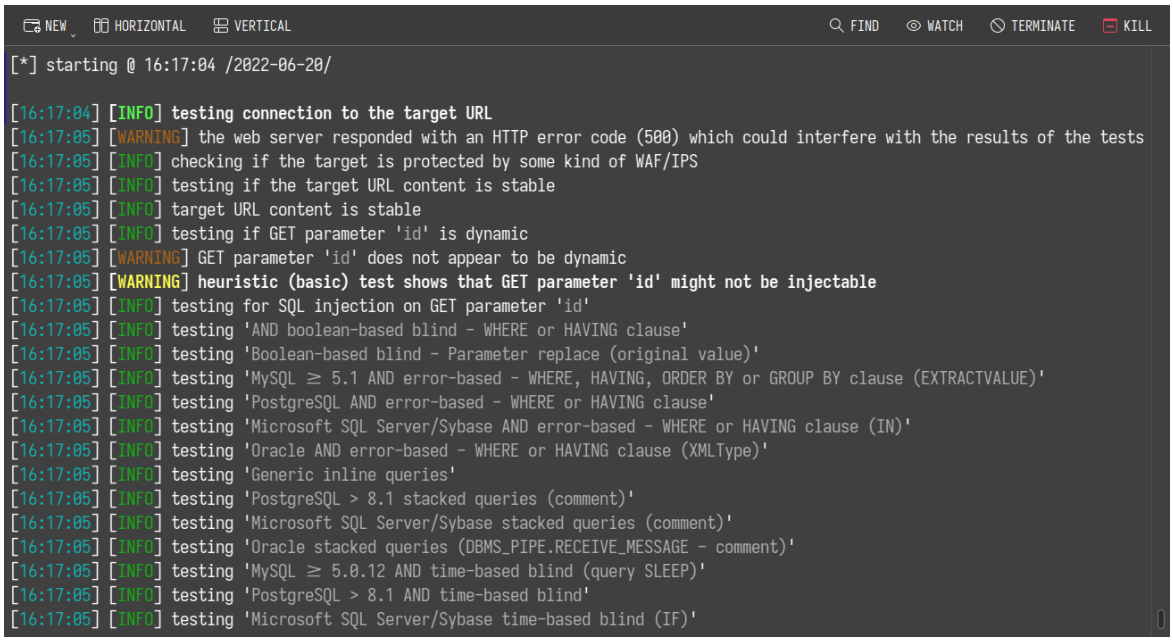


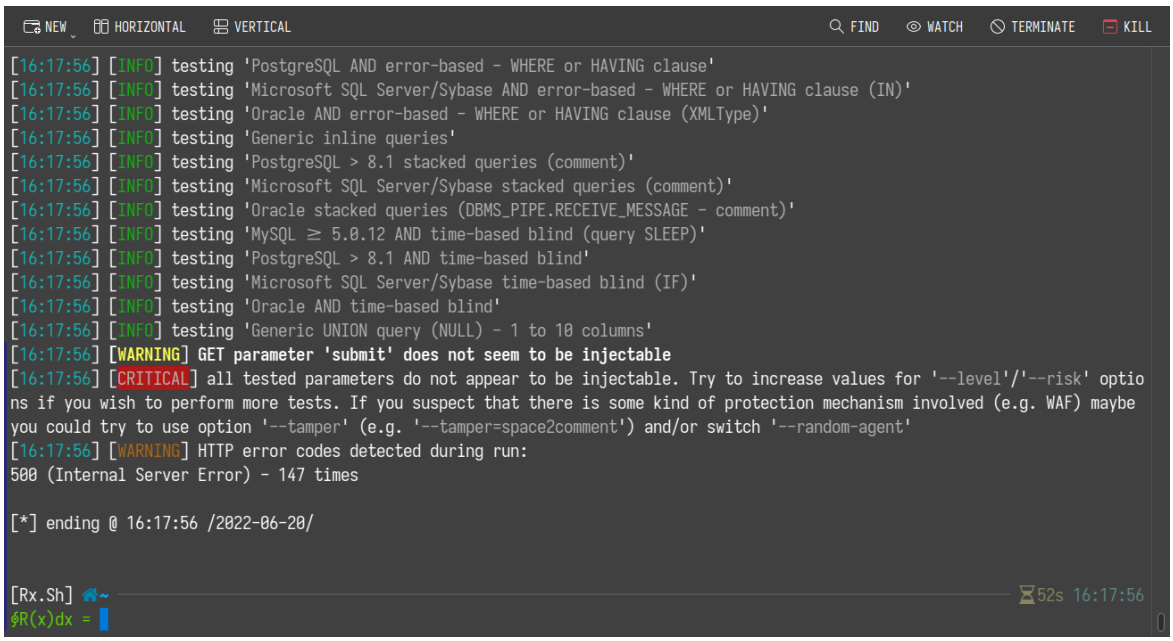
启用规则：



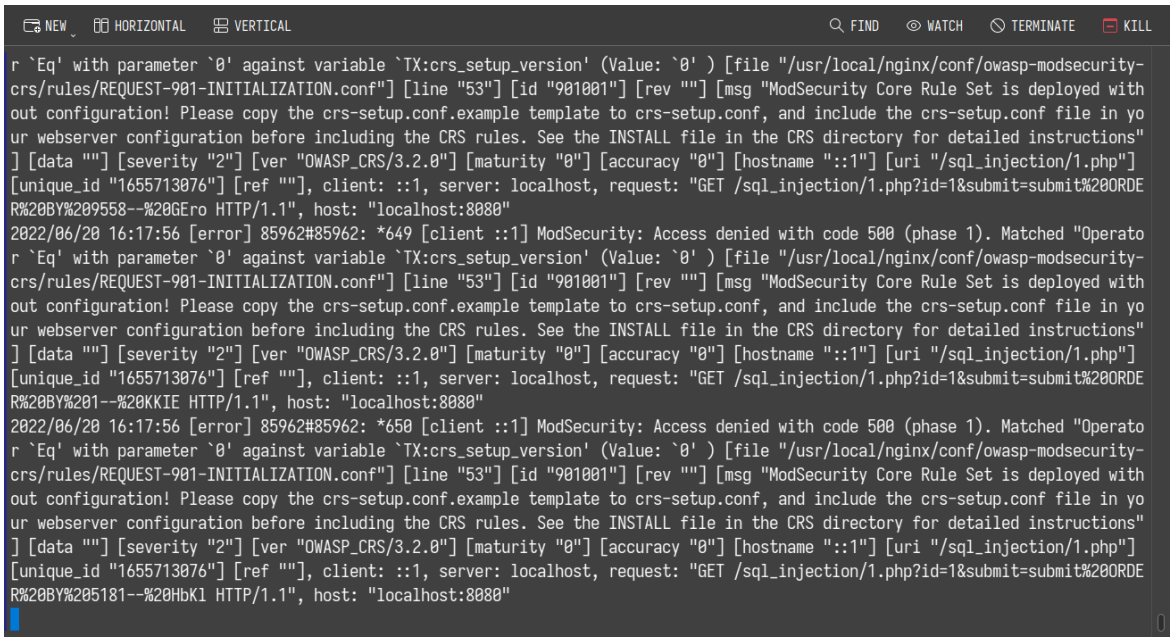
验证 WAF 是否生效

此时再次进行sqlmap扫描，可以发现已经被阻断：


NEW
HORIZONTAL
VERTICAL
FIND
WATCH
TERMINATE
KILL
[*] starting @ 16:17:04 /2022-06-20/
[16:17:04] [INFO] testing connection to the target URL
[16:17:05] [WARNING] the web server responded with an HTTP error code (500) which could interfere with the results of the tests
[16:17:05] [INFO] checking if the target is protected by some kind of WAF/IPS
[16:17:05] [INFO] testing if the target URL content is stable
[16:17:05] [INFO] target URL content is stable
[16:17:05] [INFO] testing if GET parameter 'id' is dynamic
[16:17:05] [WARNING] GET parameter 'id' does not appear to be dynamic
[16:17:05] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[16:17:05] [INFO] testing for SQL injection on GET parameter 'id'
[16:17:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:17:05] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[16:17:05] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[16:17:05] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[16:17:05] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[16:17:05] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[16:17:05] [INFO] testing 'Generic inline queries'
[16:17:05] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[16:17:05] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[16:17:05] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[16:17:05] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[16:17:05] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[16:17:05] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'


NEW
HORIZONTAL
VERTICAL
FIND
WATCH
TERMINATE
KILL
[16:17:56] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[16:17:56] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[16:17:56] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[16:17:56] [INFO] testing 'Generic inline queries'
[16:17:56] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[16:17:56] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[16:17:56] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[16:17:56] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[16:17:56] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[16:17:56] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[16:17:56] [INFO] testing 'Oracle AND time-based blind'
[16:17:56] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[16:17:56] [WARNING] GET parameter 'submit' does not seem to be injectable
[16:17:56] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[16:17:56] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 147 times
[*] ending @ 16:17:56 /2022-06-20/
[Rx.Sh] ~
52s 16:17:56
$R(x)dx =

查看日志：



成功被ModSecurity检测到并阻断。