```
==== docker ps ====
NAMES      IMAGE                           STATUS                          PORTS
waf        owasp/modsecurity-crs:nginx    Up About a minute (unhealthy)   8080/tcp, 0.0.0.0:
8080->80/tcp, [::]:8080->80/tcp
web        example/web-proxy:latest       Up 34 minutes                   80/tcp, 8080/tcp
mocksite   nginx:stable-alpine            Up 35 minutes                   80/tcp

==== curl normal (http://localhost:8080/) ====
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   615  100   615    0     0   191k      0 --:--:-- --:--:-- --:--:--  200k
HTTP/1.1 200 OK
Server: nginx/1.28.0
Date: Thu, 23 Oct 2025 13:25:50 GMT
Content-Type: text/html
Content-Length: 615
Connection: keep-alive
Last-Modified: Wed, 23 Apr 2025 12:59:25 GMT
ETag: "6808e42d-267"
Accept-Ranges: bytes

<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>

==== curl SQLi payload ====
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   153  100   153    0     0  55250      0 --:--:-- --:--:-- --:--:-- 76500
HTTP/1.1 403 Forbidden
Server: nginx/1.28.0
Date: Thu, 23 Oct 2025 13:25:50 GMT
Content-Type: text/html
Content-Length: 153
Connection: keep-alive

<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx/1.28.0</center>
</body>
</html>

==== waf logs (tail 200) ====
/docker-entrypoint.sh: /docker-entrypoint.d/ is not empty, will attempt to perform configur
ation
/docker-entrypoint.sh: Looking for shell scripts in /docker-entrypoint.d/
/docker-entrypoint.sh: Launching /docker-entrypoint.d/01-check-low-port.sh
```

```
/docker-entrypoint.sh: Launching /docker-entrypoint.d/10-generate-certificate.sh
/usr/local/bin/generate-certificate: generating new certificate
Warning: No -copy_extensions given; ignoring any extensions in the request
/usr/local/bin/generate-certificate: generated /etc/nginx/conf/server.key and /etc/nginx/co
nf/server.crt
/docker-entrypoint.sh: Launching /docker-entrypoint.d/10-listen-on-ipv6-by-default.sh
10-listen-on-ipv6-by-default.sh: info: Getting the checksum of /etc/nginx/conf.d/default.co
nf
10-listen-on-ipv6-by-default.sh: info: /etc/nginx/conf.d/default.conf differs from the pack
aged version
/docker-entrypoint.sh: Sourcing /docker-entrypoint.d/15-local-resolvers.envsh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/20-envsubst-on-templates.sh
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/modsecurity.d/modsecu
rity.conf.template to /etc/nginx/modsecurity.d/modsecurity.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/modsecurity.d/modsecu
rity-override.conf.template to /etc/nginx/modsecurity.d/modsecurity-override.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/modsecurity.d/setup.c
onf.template to /etc/nginx/modsecurity.d/setup.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/conf.d/default.conf.t
emplate to /etc/nginx/conf.d/default.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/conf.d/modsecurity.co
nf.template to /etc/nginx/conf.d/modsecurity.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/conf.d/logging.conf.t
emplate to /etc/nginx/conf.d/logging.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/nginx.conf.template t
o /etc/nginx/nginx.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/includes/cors.conf.te
mplate to /etc/nginx/includes/cors.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/includes/location_com
mon.conf.template to /etc/nginx/includes/location_common.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/includes/proxy_backen
d.conf.template to /etc/nginx/includes/proxy_backend.conf
20-envsubst-on-templates.sh: Running envsubst on /etc/nginx/templates/includes/proxy_backen
d_ssl.conf.template to /etc/nginx/includes/proxy_backend_ssl.conf
/docker-entrypoint.sh: Launching /docker-entrypoint.d/30-tune-worker-processes.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/90-copy-modsecurity-config.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/91-update-resolver.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/92-update-real_ip.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/93-update-proxy-ssl-config.sh
/docker-entrypoint.sh: Launching /docker-entrypoint.d/94-activate-plugins.sh
# # #
Running CRS plugin activation
- - -

- - -
Finished CRS plugin activation
# # #

/docker-entrypoint.sh: Launching /docker-entrypoint.d/95-configure-rules.sh
# # #
Running CRS rule configuration
- - -
Detected CRS config file version: v3
Configuring 900000 for BLOCKING_PARANOIA with paranoia_level=1
Configuring 900110 for ANOMALY_INBOUND with inbound_anomaly_score_threshold=5
Configuring 900110 for ANOMALY_OUTBOUND with outbound_anomaly_score_threshold=4
- - -
Finished CRS rule configuration
# # #

/docker-entrypoint.sh: Ignoring /docker-entrypoint.d/configure-rules.v3.conf
/docker-entrypoint.sh: Ignoring /docker-entrypoint.d/configure-rules.v4.conf
/docker-entrypoint.sh: Configuration complete; ready for start up
2025/10/23 13:24:08 [notice] 1#1: ModSecurity-nginx v1.0.4 (rules loaded inline/local/remot
e: 0/925/0)
2025/10/23 13:24:08 [notice] 1#1: libmodsecurity3 version 3.0.14
172.18.0.1 - - [23/Oct/2025:13:24:37 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/8.5.0" "-"
2025/10/23 13:24:37 [error] 502#502: *3 [client 172.18.0.1] ModSecurity: Access denied with
 code 403 (phase 2). Matched "Operator ‘Ge’ with parameter ‘5’ against variable ‘TX:ANOMALY
```

```
_SCORE’ (Value: ‘5’ ) [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUA
TION.conf"] [line "81"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total
Score: 5)"] [data ""] [severity "2"] [ver "OWASP_CRS/3.3.7"] [maturity "0"] [accuracy "0"]
[tag "modsecurity"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"]
 [tag "attack-generic"] [hostname "localhost"] [uri "/"] [unique_id "176122587793.408194"]
[ref ""], client: 172.18.0.1, server: _, request: "GET /?id=1%27%20OR%20%271%27=%271%27 HTT
P/1.1", host: "localhost:8080"
172.18.0.1 - - [23/Oct/2025:13:24:37 +0000] "GET /?id=1%27%20OR%20%271%27=%271%27 HTTP/1.1"
 403 153 "-" "curl/8.5.0" "-"
{"transaction":{"client_ip":"172.18.0.1","time_stamp":"Thu Oct 23 13:24:37 2025","server_id
":"9120626f7f31aac27fc9532a8927cbe834770c6c","client_port":42878,"host_ip":"172.18.0.3","ho
st_port":80,"unique_id":"176122587793.408194","request":{"method":"GET","http_version":1.1,
"uri":"/?id=1%27%20OR%20%271%27=%271%27","headers":{"Host":"localhost:8080","User-Agent":"c
url/8.5.0","Accept":"*/*"}},"response":{"body":"<html>\r\n<head><title>403 Forbidden</title
></head>\r\n<body>\r\n<center><h1>403 Forbidden</h1></center>\r\n<hr><center>nginx/1.28.0</
center>\r\n</body>\r\n</html>\r\n","http_code":403,"headers":{"Server":"nginx/1.28.0","Date
":"Thu, 23 Oct 2025 13:24:37 GMT","Content-Length":"153","Content-Type":"text/html","Connec
tion":"keep-alive"}},"producer":{"modsecurity":"ModSecurity v3.0.14 (Linux)","connector":"M
odSecurity-nginx v1.0.4","secrules_engine":"Enabled","components":["OWASP_CRS/3.3.7\""]},"m
essages":[{"message":"SQL Injection Attack Detected via libinjection","details":{"match":"d
etected SQLi using libinjection.","reference":"v9,13","ruleId":"942100","file":"/etc/modsec
urity.d/owasp-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf","lineNumber":"46","data":
"Matched Data: s&sos found within ARGS:id: 1’ OR ’1’=’1’","severity":"2","ver":"OWASP_CRS/3
.3.7","rev":"","tags":["application-multi","language-multi","platform-multi","attack-sqli",
"paranoia-level/1","OWASP_CRS","capec/1000/152/248/66","PCI/6.5.2"],"maturity":"0","accurac
y":"0"}},{"message":"Inbound Anomaly Score Exceeded (Total Score: 5)","details":{"match":"M
atched \"Operator ‘Ge’ with parameter ‘5’ against variable ‘TX:ANOMALY_SCORE’ (Value: ‘5’ )
","reference":"","ruleId":"949110","file":"/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-B
LOCKING-EVALUATION.conf","lineNumber":"81","data":"","severity":"2","ver":"OWASP_CRS/3.3.7"
,"rev":"","tags":["modsecurity","application-multi","language-multi","platform-multi","atta
ck-generic"],"maturity":"0","accuracy":"0"}}]}}
172.18.0.1 - - [23/Oct/2025:13:25:50 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/8.5.0" "-"
2025/10/23 13:25:50 [error] 501#501: *6 [client 172.18.0.1] ModSecurity: Access denied with
 code 403 (phase 2). Matched "Operator ‘Ge’ with parameter ‘5’ against variable ‘TX:ANOMALY
_SCORE’ (Value: ‘5’ ) [file "/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-BLOCKING-EVALUA
TION.conf"] [line "81"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total
Score: 5)"] [data ""] [severity "2"] [ver "OWASP_CRS/3.3.7"] [maturity "0"] [accuracy "0"]
[tag "modsecurity"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"]
 [tag "attack-generic"] [hostname "localhost"] [uri "/"] [unique_id "176122595074.387359"]
[ref ""], client: 172.18.0.1, server: _, request: "GET /?id=1%27%20OR%20%271%27=%271%27 HTT
P/1.1", host: "localhost:8080"
172.18.0.1 - - [23/Oct/2025:13:25:50 +0000] "GET /?id=1%27%20OR%20%271%27=%271%27 HTTP/1.1"
 403 153 "-" "curl/8.5.0" "-"
{"transaction":{"client_ip":"172.18.0.1","time_stamp":"Thu Oct 23 13:25:50 2025","server_id
":"9120626f7f31aac27fc9532a8927cbe834770c6c","client_port":37948,"host_ip":"172.18.0.3","ho
st_port":80,"unique_id":"176122595074.387359","request":{"method":"GET","http_version":1.1,
"uri":"/?id=1%27%20OR%20%271%27=%271%27","headers":{"Host":"localhost:8080","User-Agent":"c
url/8.5.0","Accept":"*/*"}},"response":{"body":"<html>\r\n<head><title>403 Forbidden</title
></head>\r\n<body>\r\n<center><h1>403 Forbidden</h1></center>\r\n<hr><center>nginx/1.28.0</
center>\r\n</body>\r\n</html>\r\n","http_code":403,"headers":{"Server":"nginx/1.28.0","Date
":"Thu, 23 Oct 2025 13:25:50 GMT","Content-Length":"153","Content-Type":"text/html","Connec
tion":"keep-alive"}},"producer":{"modsecurity":"ModSecurity v3.0.14 (Linux)","connector":"M
odSecurity-nginx v1.0.4","secrules_engine":"Enabled","components":["OWASP_CRS/3.3.7\""]},"m
essages":[{"message":"SQL Injection Attack Detected via libinjection","details":{"match":"d
etected SQLi using libinjection.","reference":"v9,13","ruleId":"942100","file":"/etc/modsec
urity.d/owasp-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf","lineNumber":"46","data":
"Matched Data: s&sos found within ARGS:id: 1’ OR ’1’=’1’","severity":"2","ver":"OWASP_CRS/3
.3.7","rev":"","tags":["application-multi","language-multi","platform-multi","attack-sqli",
"paranoia-level/1","OWASP_CRS","capec/1000/152/248/66","PCI/6.5.2"],"maturity":"0","accurac
y":"0"}},{"message":"Inbound Anomaly Score Exceeded (Total Score: 5)","details":{"match":"M
atched \"Operator ‘Ge’ with parameter ‘5’ against variable ‘TX:ANOMALY_SCORE’ (Value: ‘5’ )
","reference":"","ruleId":"949110","file":"/etc/modsecurity.d/owasp-crs/rules/REQUEST-949-B
LOCKING-EVALUATION.conf","lineNumber":"81","data":"","severity":"2","ver":"OWASP_CRS/3.3.7"
,"rev":"","tags":["modsecurity","application-multi","language-multi","platform-multi","atta
ck-generic"],"maturity":"0","accuracy":"0"}}]}}

==== web logs (tail 200) ====
2025/10/23 12:51:15 [notice] 1#1: using the "epoll" event method
2025/10/23 12:51:15 [notice] 1#1: nginx/1.28.0
```

```
2025/10/23 12:51:15 [notice] 1#1: built by gcc 14.2.0 (Alpine 14.2.0)
2025/10/23 12:51:15 [notice] 1#1: OS: Linux 6.14.0-1012-aws
2025/10/23 12:51:15 [notice] 1#1: getrlimit(RLIMIT_NOFILE): 1048576:1048576
2025/10/23 12:51:15 [notice] 1#1: start worker processes
2025/10/23 12:51:15 [notice] 1#1: start worker process 6
2025/10/23 12:51:15 [notice] 1#1: start worker process 7
172.18.0.3 - - [23/Oct/2025:12:51:56 +0000] "HEAD / HTTP/1.1" 200 0 "-" "curl/7.88.1" "-"
172.18.0.3 - - [23/Oct/2025:12:57:15 +0000] "HEAD / HTTP/1.1" 200 0 "-" "curl/7.88.1" "-"
172.18.0.3 - - [23/Oct/2025:13:24:37 +0000] "GET / HTTP/1.0" 200 615 "-" "curl/8.5.0" "172.
18.0.1"
172.18.0.3 - - [23/Oct/2025:13:25:50 +0000] "GET / HTTP/1.0" 200 615 "-" "curl/8.5.0" "172.
18.0.1"
```