IstioCon

IstioCon

Istio Web Application Firewall With WASM & Coraza

Zufar Dhiyaulhaq, GoTo Financial

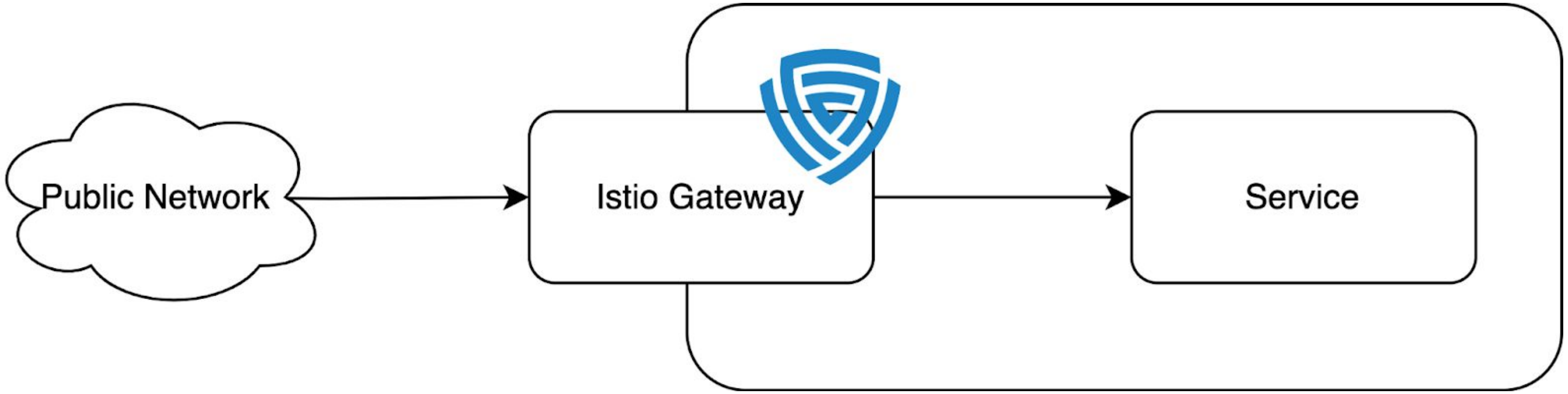
- there are few open source WAF solution in the market,
- Integration with Istio service mesh is complicated,
- Not all company can pay for enterprise WAF solution,
- ModSecurity is deprecated in 1 July, 2024.

- drop-in alternative to replace ModSecurity
- support ModSecurity SecLang rulesets
- 100% compatible with OWASP Core Rule Set
- Library at is core, extensible by default
- Seamless integration with Envoy & Istio service mesh

coraza

WEB APPLICATION FIREWALL

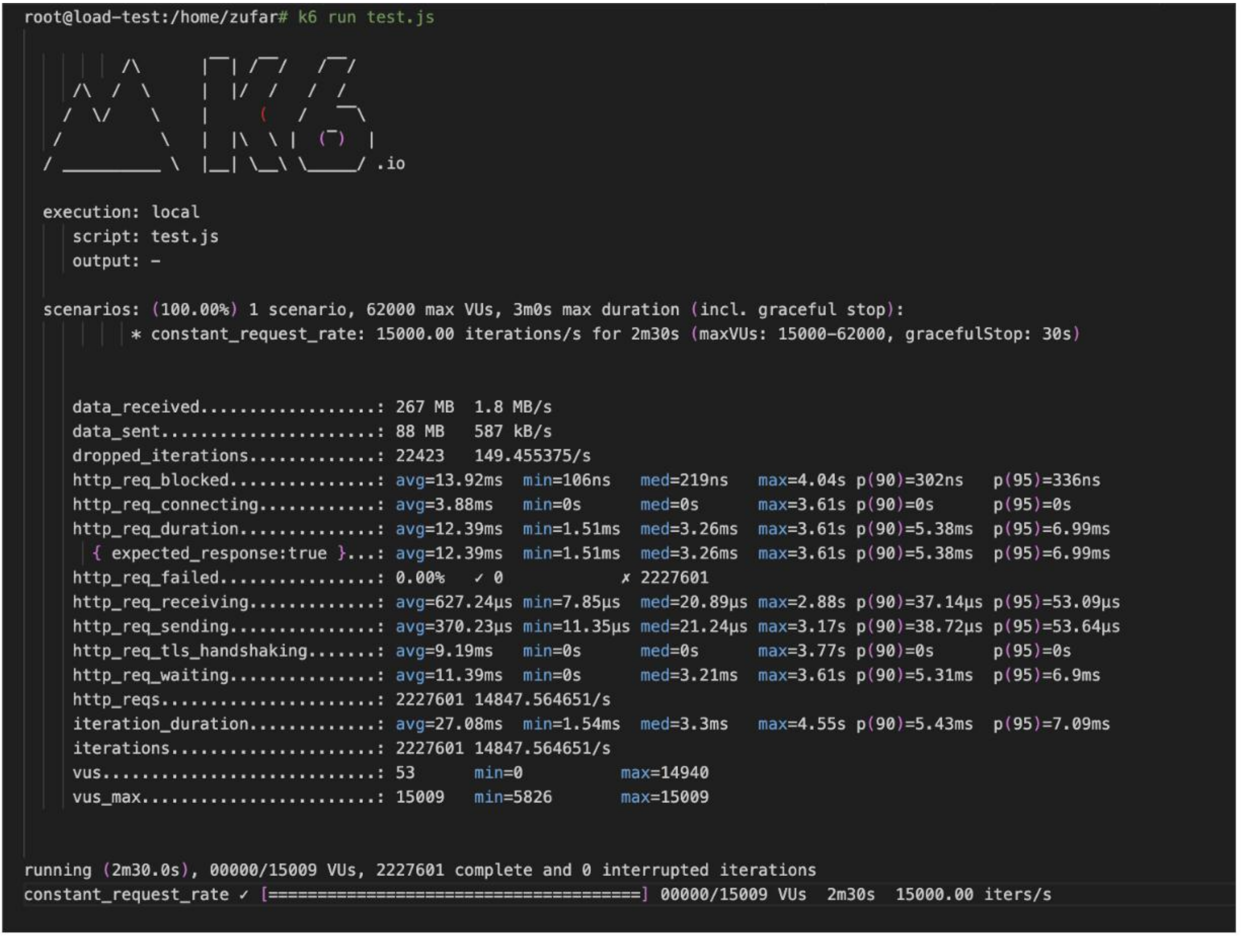
- Coraza has WebAsssembly implementation that supported by Envoy & Istio https://github.com/corazawaf/coraza-proxy-wasm
- Istio support this via **WASMPlugin** object.



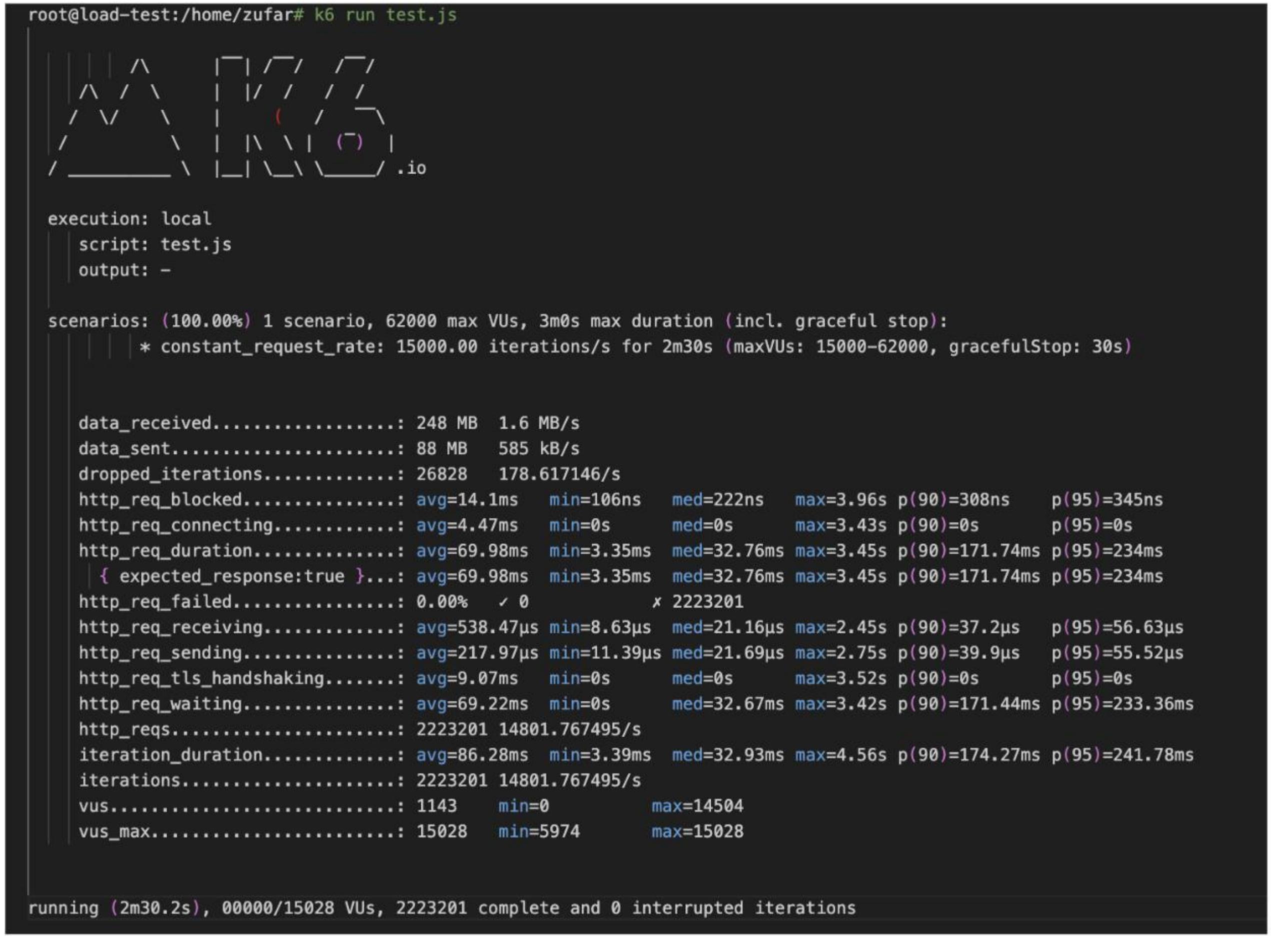
```yaml
apiVersion: extensions.istio.io/v1alpha1
kind: WasmPlugin
metadata:
  name: istio-public-gateway-waf-wp
  namespace: istio-system
spec:
  selector:
    matchLabels:
      app: istio-public-gateway
  url: oci://ghcr.io/corazawaf/coraza-proxy-wasm:0.1.2
  imagePullPolicy: Always
  pluginConfig:
    directives_map:
      crs:
      - Include @demo-conf
      - Include @crs-setup-demo-conf
      - Include @owasp_crs/*.conf
    default_directives: crs
```

```
pluginConfig:
  directives_map:
    crs_detection_only:
    - Include @demo-conf
    - Include @crs-setup-demo-conf
    - Include @owasp_crs/*.conf
    - SecRuleEngine DetectionOnly
    crs:
    - Include @demo-conf
    - Include @crs-setup-demo-conf
    - Include @owasp_crs/*.conf
  default_directives: crs_detection_only
  per_authority_directives:
    foo.gotofinancial.com: crs
    bar.gotofinancial.com: crs
```

With 15000 requests/second (CRS blocking), the average latency is added around 57ms



```
root@load-test:/home/zufar# k6 run test.js

          /\      |‾‾| /‾‾/   /‾‾/
     /\  /  \     |  |/  /   /  /
    /  \/    \    |     (   /   ‾‾\
   /          \   |  |\  \ |  (‾)  |
  / __________ \  |__| \__\ \_____/ .io

  execution: local
     script: test.js
     output: -

  scenarios: (100.00%) 1 scenario, 62000 max VUs, 3m0s max duration (incl. graceful stop):
           * constant_request_rate: 15000.00 iterations/s for 2m30s (maxVUs: 15000-62000, gracefulStop: 30s)


     data_received..................: 267 MB  1.8 MB/s
     data_sent......................: 88 MB   587 kB/s
     dropped_iterations.............: 22423   149.455375/s
     http_req_blocked...............: avg=13.92ms  min=106ns   med=219ns   max=4.04s p(90)=302ns   p(95)=336ns
     http_req_connecting............: avg=3.88ms   min=0s      med=0s      max=3.61s p(90)=0s      p(95)=0s
     http_req_duration..............: avg=12.39ms  min=1.51ms  med=3.26ms  max=3.61s p(90)=5.38ms  p(95)=6.99ms
       { expected_response:true }...: avg=12.39ms  min=1.51ms  med=3.26ms  max=3.61s p(90)=5.38ms  p(95)=6.99ms
     http_req_failed................: 0.00%   ✓ 0          ✗ 2227601
     http_req_receiving.............: avg=627.24µs min=7.85µs  med=20.89µs max=2.88s p(90)=37.14µs p(95)=53.09µs
     http_req_sending...............: avg=370.23µs min=11.35µs med=21.24µs max=3.17s p(90)=38.72µs p(95)=53.64µs
     http_req_tls_handshaking.......: avg=9.19ms   min=0s      med=0s      max=3.77s p(90)=0s      p(95)=0s
     http_req_waiting...............: avg=11.39ms  min=0s      med=3.21ms  max=3.61s p(90)=5.31ms  p(95)=6.9ms
     http_reqs......................: 2227601 14847.564651/s
     iteration_duration.............: avg=27.08ms  min=1.54ms  med=3.3ms   max=4.55s p(90)=5.43ms  p(95)=7.09ms
     iterations.....................: 2227601 14847.564651/s
     vus............................: 53      min=0        max=14940
     vus_max........................: 15009   min=5826     max=15009


running (2m30.0s), 00000/15009 VUs, 2227601 complete and 0 interrupted iterations
constant_request_rate ✓ [======================================] 00000/15009 VUs  2m30s  15000.00 iters/s
```



```
root@load-test:/home/zufar# k6 run test.js

          /\      |‾‾| /‾‾/   /‾‾/
     /\  /  \     |  |/  /   /  /
    /  \/    \    |     (   /   ‾‾\
   /          \   |  |\  \ |  (‾)  |
  / __________ \  |__| \__\ \_____/ .io

  execution: local
     script: test.js
     output: -

  scenarios: (100.00%) 1 scenario, 62000 max VUs, 3m0s max duration (incl. graceful stop):
           * constant_request_rate: 15000.00 iterations/s for 2m30s (maxVUs: 15000-62000, gracefulStop: 30s)


     data_received..................: 248 MB  1.6 MB/s
     data_sent......................: 88 MB   585 kB/s
     dropped_iterations.............: 26828   178.617146/s
     http_req_blocked...............: avg=14.1ms   min=106ns   med=222ns   max=3.96s p(90)=308ns    p(95)=345ns
     http_req_connecting............: avg=4.47ms   min=0s      med=0s      max=3.43s p(90)=0s       p(95)=0s
     http_req_duration..............: avg=69.98ms  min=3.35ms  med=32.76ms max=3.45s p(90)=171.74ms p(95)=234ms
       { expected_response:true }...: avg=69.98ms  min=3.35ms  med=32.76ms max=3.45s p(90)=171.74ms p(95)=234ms
     http_req_failed................: 0.00%   ✓ 0          ✗ 2223201
     http_req_receiving.............: avg=538.47µs min=8.63µs  med=21.16µs max=2.45s p(90)=37.2µs   p(95)=56.63µs
     http_req_sending...............: avg=217.97µs min=11.39µs med=21.69µs max=2.75s p(90)=39.9µs   p(95)=55.52µs
     http_req_tls_handshaking.......: avg=9.07ms   min=0s      med=0s      max=3.52s p(90)=0s       p(95)=0s
     http_req_waiting...............: avg=69.22ms  min=0s      med=32.67ms max=3.42s p(90)=171.44ms p(95)=233.36ms
     http_reqs......................: 2223201 14801.767495/s
     iteration_duration.............: avg=86.28ms  min=3.39ms  med=32.93ms max=4.56s p(90)=174.27ms p(95)=241.78ms
     iterations.....................: 2223201 14801.767495/s
     vus............................: 1143    min=0        max=14504
     vus_max........................: 15028   min=5974     max=15028


running (2m30.2s), 00000/15028 VUs, 2223201 complete and 0 interrupted iterations
```

Demo

Thank You