Implementing and Testing a Web Application Firewall (WAF)

IZRADILI: FILIP DRVODERIĆ, MATIJA ŽNIDARIĆ, LUKA VIDEC, BORNA ŠOŠTAR

KOLEGIJ: SIGURNOST INFORMACIJSKIH SUSTAVA

AKADEMSKA GODINA: 2025./2026.

Sadržaj

Uvod

Nagli porast broja web aplikacija = porast broja napada na aplikacijski sloj

Firewall i IDS/IPS ne mogu prepoznati napade unutar HTTP/HTTPS prometa

Najčešće prijetnje: SQL Injection, XSS, CSRF

Potrebna dodatna razina zaštite koja analizira aplikacijski promet

Rješenje? Web Application Firewall!

Što je Web Application Firewall

- Sigurnosni sustav koji filtrira, nadzire i blokira HTTP/HTTPS promet između korisnika i web aplikacije
- Djeluje na aplikacijskom sloju
- Analizira dolazne zahtjeve i odgovore web aplikacije
- Može se implementirati kao: hardware, software ili cloud servis
- Cilj: spriječiti iskorištavanje ranjivosti u samom kodu aplikacije

Uloga WAF-a

- Djeluje kao posrednik između korisnika i web aplikacije
- Filtrira zlonamjerne zahtjeve prije nego dođu do poslužitelja
- Smanjuje rizik od kompromitacije aplikacije i krađe podataka
- Pruža dodatni sigurnosni sloj uz druge mehanizme (Firewall, IDS/IPS)
- Omogućuje real-time zaštitu i praćenje sigurnosnih događaja
- Ključan je dio strategije Defense in Depth

Arhitektura WAF-a

- Postavlja se između korisnika i web aplikacije
- Analizira HTTP/HTTPS promet u stvarnom vremenu
- Može raditi kao:
  - Reverse Proxy - svi zahtjevi prolaze kroz WAF prije poslužitelja
  - Transparent Bridge - promet prolazi kroz WAF bez promjene IP adresa
  - Out of Band - WAF nadzire promet pasivno (kopija prometa)
- Moderni WAF-ovi često su integrirani s load balancerima i SIEM sustavima

Vrste WAF-ova

On premises WAF - instaliran lokalno	• Potpuna kontrola nad konfiguracijom i podacima • Veći troškovi hardvera i održavanja
Cloud based WAF - usluga koju pruža treća strana	• Brza implementacija i automatska ažuriranja • Manja kontrola nad fizičkom infrastrukturom
Hybrid WAF - kombinira lokalnu i cloud zaštitu	• Fleksibilnost i skalabilnost • Pogodan za velike sustave i distribuirane aplikacije

Glavne funkcionalnosti

- Filtriranje i analiziranje HTTP/HTTPS prometa u stvarnom vremenu
- Validacija korisničkog unosa i blokiranje sumnjivih parametara
- Pravila za prepoznavanje napada i neželjenog ponašanja
- Rate limiting - ograničavanje broja zahtjeva prema aplikaciji
- Session Management - zaštita kolačića i autentifikacijskih podataka
- Logging i izvještavanje o sigurnosnim događajima
- Integracija s drugim sigurnosnim alatima

Mehanizmi detekcije

Signatuare based detection

- Prepoznaje poznate obrasce napada
- Koristi predefinirane signiture – skupove pravila i uzoraka
- Brz i učinkovit, ali ne prepoznaje nove (zero-day) prijetnje

Anomaly based detection

- Analizira normalno ponašanje aplikacije i traži odstupanja.
- Otkriva napade koji nemaju poznate potpise.
- Često koristi machine learning

Hybrid detection

- Kombinira signature i anomaly metode za veću preciznost
- Smanjuje broj false positives i false negatives

Prednosti

- Pruža dodatni sloj zaštite uz mrežne i sustavske sigurnosne mehanizme
- Brza implementacija – ne zahtijeva promjene u izvornom kodu aplikacije
- Zaštita u stvarnom vremenu od širokog raspona prijetnji
- Detaljni logovi i nadzor prometa za kasniju analizu
- Može kompenzirati ranjivosti u starijim (legacy) aplikacijama

Ograničenja

- Mogućnost false positive blokiranja legitimnih zahtjeva
- Potrebna stalna konfiguracija i održavanje pravila
- Dodatno opterećenje performansi (latency, bandwidth)
- Ne zamjenjuje siguran razvoj aplikacije (secure coding)

Vrste napada koje WAF sprječava

SQL Injection - umetanje zlonamjernih SQL upita radi pristupa bazi podataka

Cross Site Scripting - umetanje skripti u web-stranice radi krađe kolačića ili podataka

Cross Site Request Forgery - napad kojim se korisnika prisiljava da nenamjerno pošalje zahtjev

File Inclusion / Path Traversal - pristup osjetljivim datotekama na poslužitelju

Session Hijacking - krađa ili preuzimanje korisničke sesije

DDos - preopterećenje aplikacijskog sloja velikim brojem zahtjeva

Praktični dio

- Postaviti virtualno okruženje (VirtualBox / VMware)
- Instalacija i konfiguracija WAF-a
- Definiranje napada
- Simulacija napada (OWASP ZAP)
- Prikupljanje i analiza podataka
- Optimizacija pravila
- Dokumentacija i izvještaj
- Rezultati analize

Literatura

- OWASP(2008). Best Practices: Use of Web Application Firewalls. Preuzeto 28.10.2025. s https://wiki.owasp.org/images/b/b0/Best_Practices_WAF_v105.en.pdf
- M. Prakash (2024). Web Application Firewall. Preuzeto 28.10.2025 s https://www.researchgate.net/publication/387187876_WEB_APPLICATION_FIREWALL
- CloudFlare (bez dat). What is a Web Application Firewall (WAF)? Preuzeto 28.10.2025. s https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/
- Fortinet (bez dat). How WAF Can Help Organizations Detect and Prevent Online Threats. Preuzeto 28.10.2025. s https://www.fortinet.com/resources/cyberglossary/waf
- Cisco (bez dat). Web application firewall (WAF). Preuzeto 28.10.2025 s https://www.cisco.com/site/us/en/learn/topics/security/what-is-web-application-firewall-waf.html