Top 3
Outils de l'OWASP

Florian Bernard
Principal Engineer
OpenAirlines

Devoxx France - 16 Avril 2025

OWASP

- **O**pen ~~Web~~ **W**orldwide **A**pplication **S**ecurity **P**roject
- Fondation à but non lucrative axée sur la communauté
- Ressources et outils autour de la sécurité des applications
- Conférences et évènements
- OWASP Top 10
- https://owasp.org/

OWASP - Top 10

- 10 risques de sécurité les plus critiques dans les applications web
- Mise à jour tous les 4 ans
- Sensibilisation et atténuation
- Référence pour les audits de sécurité
- Top 10 pour les LLMs les applications GenAI
- https://owasp.org/www-project-top-ten/

OWASP - Top 10

#1 Broken Access Control: En 2013, une faille dans Facebook a permis à n'importe quel utilisateur de supprimer des photos de n'importe quel compte sans autorisation.

#2 Cryptographic Failures: La faille Heartbleed de 2014 a été une défaillance cryptographique majeure.

#3 Injection: En 2008, Heartland Payment Systems a été victime d'une attaque massive par injection SQL, qui a entraîné l'exposition d'environ 130 millions de numéros de cartes de crédit et de débit.

OWASP - Tools

Build → dependency track

Test → ZAP by Checkmarx

Run → modsecurity

Open Source Web Application Firewall

Dependency Track

- **Création:** Septembre 2017
- **Licence:** Apache License 2.0
- **Editeur:** OWASP
- **Description:** Identifier et monitorer des vulnérabilités dans les dépendances logicielles

dependency track

Software Bill of Materials (SBOM)

CycloneDX

Vulnerability Intelligence

NVD
GitHub
VulnDB
snyk
OSV | Open Source Vulnerabilities
sonatype | OSS INDEX

Supported Repositories

RubyGems
pypi
Maven
nuget
npm
hex
Composer

dependency track

Supported Notification Platforms

slack
webhooks
Mattermost
webex by CISCO
Microsoft Teams

API Integration

OPENAPI INITIATIVE
Jenkins

Vulnerability Aggregation

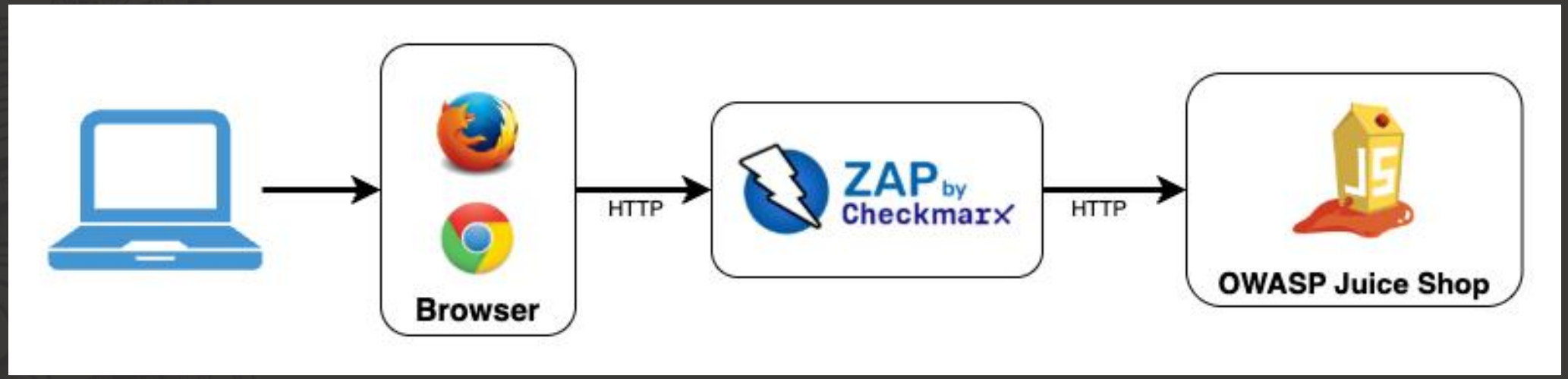
ThreadFix
FORTIFY
KENNA Security
CodeDx
DEFECTDOJO
Security Compass
Jira Software

Zed Attack Proxy (ZAP)

- **Création:** Septembre 2010
- **Licence:** Apache License 2.0
- **Editeur:** Checkmarx (initialement OWASP)
- **Description:** Outil de test de sécurité pour identifier les vulnérabilités dans les applications web (Dynamic Application Security Testing)

ZAP by Checkmarx

Zed Attack Proxy (ZAP)



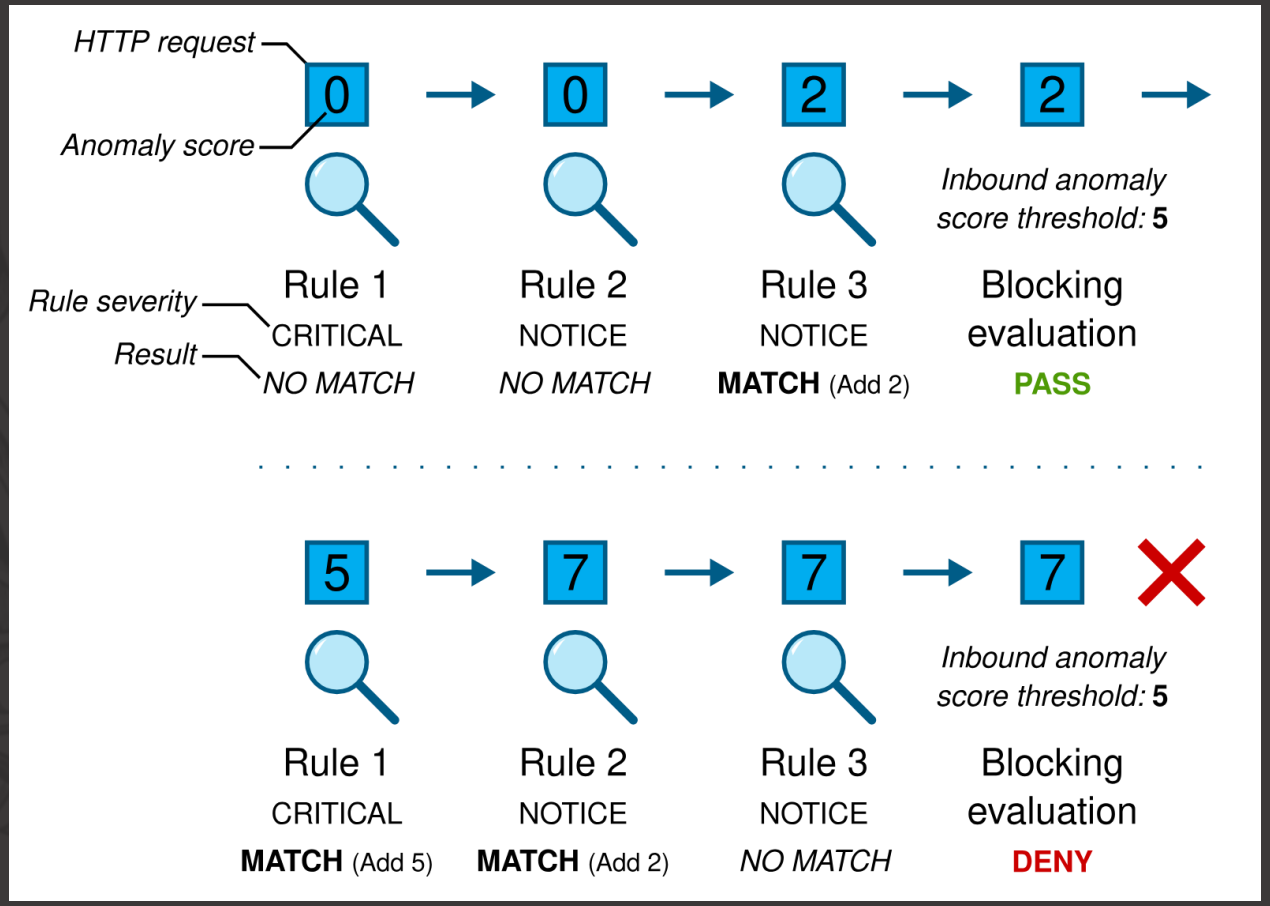
ZAP by Checkmarx

ModSecurity

- **Création:** Novembre 2002
- **Licence:** Apache License 2.0
- **Editeur:** OWASP (initialement Trustwave SpiderLabs)
- **Description: W**eb **A**pplication **F**irewall (WAF) permettant de filtrer dynamiquement des requêtes et réponses web.

modsecurity
Open Source Web Application Firewall

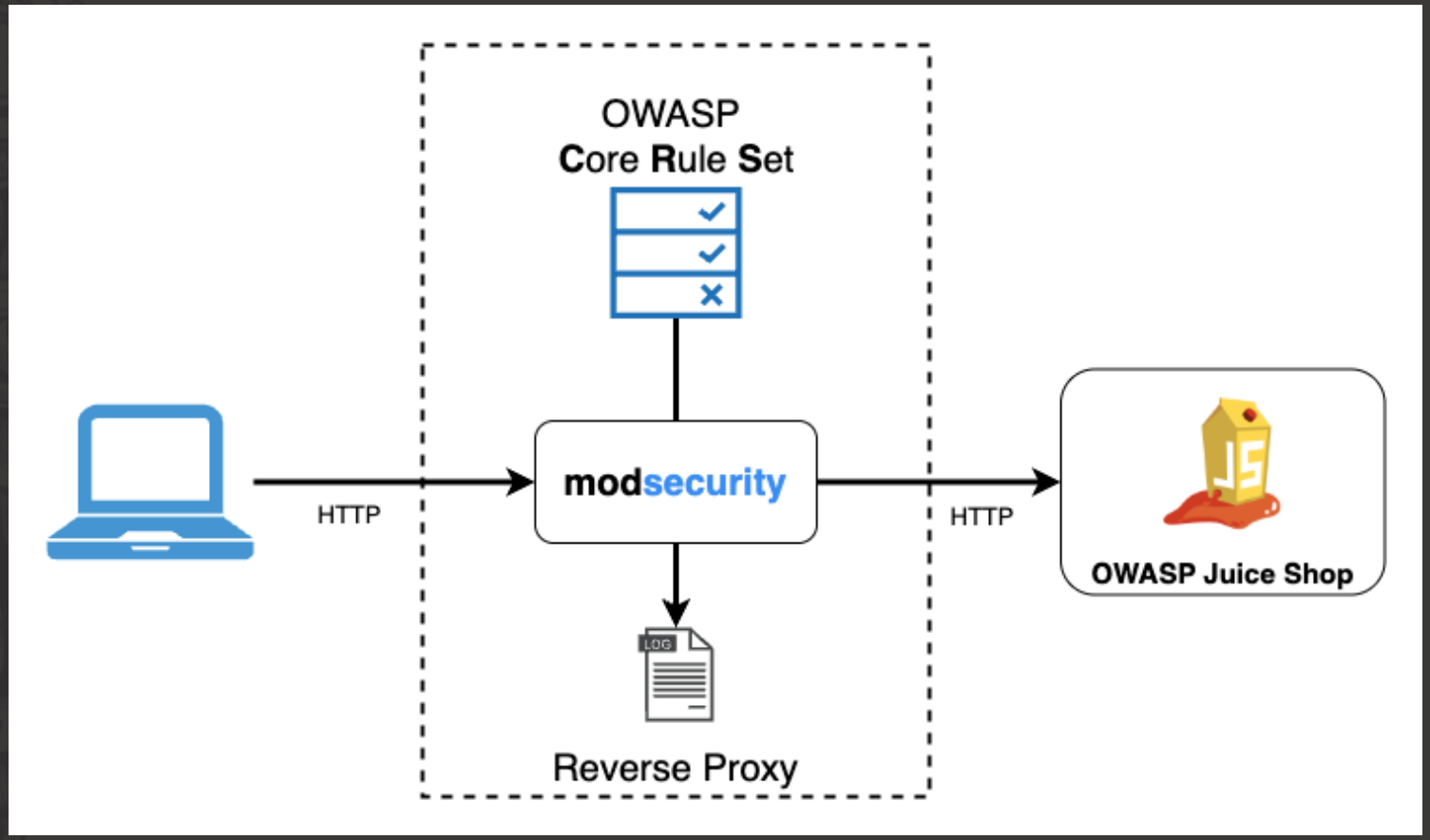
ModSecurity



modsecurity

Open Source Web Application Firewall

ModSecurity



modsecurity
Open Source Web Application Firewall

Conclusion

- 3 outils faciles à utiliser
- Gratuits et Open Source
- Utilisation ponctuelle ou automatisée (CI/CD)
- Commencer à les utiliser c’est déjà améliorer la sécurité
- Applications volontairement vulnérables
  - Juice Shop (Javascript)
  - WebGoat (Java)

Merci !!!

@flobtech.bsky.social

OpenAirlines

https://www.openairlines.com

OWASP®

https://owasp.org