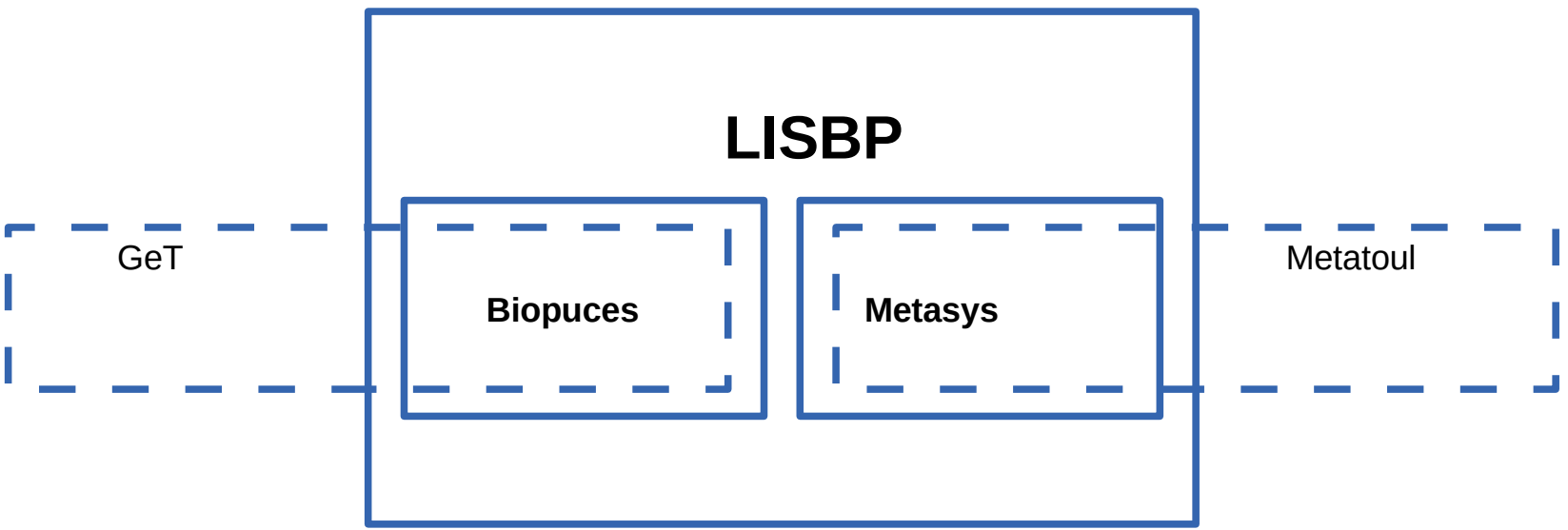
NAXSI
Un pare-feu applicatif pour NGINX

Matthieu Guionnet

jres Montpellier 2013

Mon environnement



* Laboratoire d'Ingénierie des Systèmes Biologiques et des Procédés

NGINX
Serveur HTTP et proxy inversé

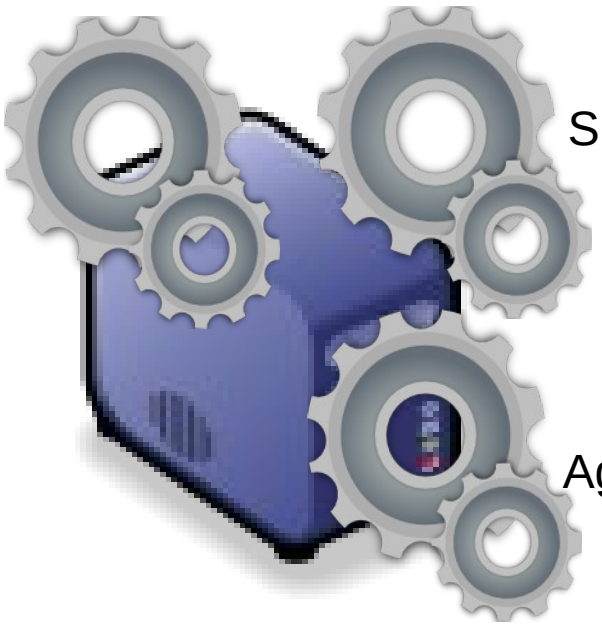
- Libre
- Bonnes performances
- Faible empreinte mémoire

Site web

Site web

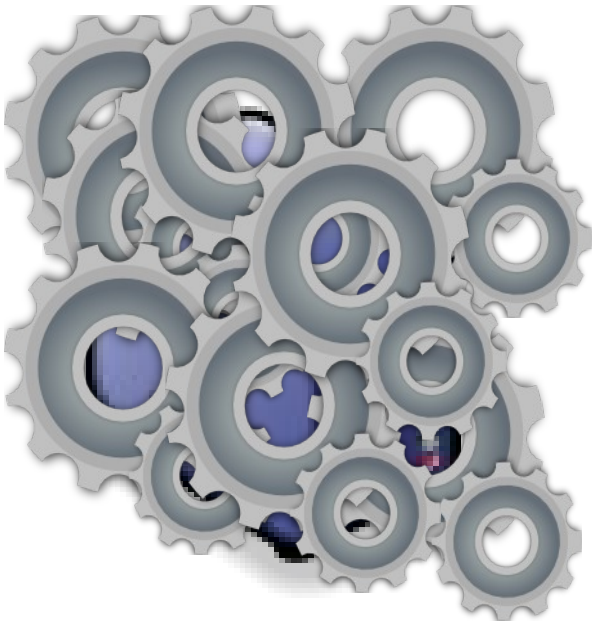
Agenda

CVS



Site web

Agenda



Python 2.6 PHP 5.x

Python 2.7 PHP 4.x

Perl 6 Perl 5

Python 3 R

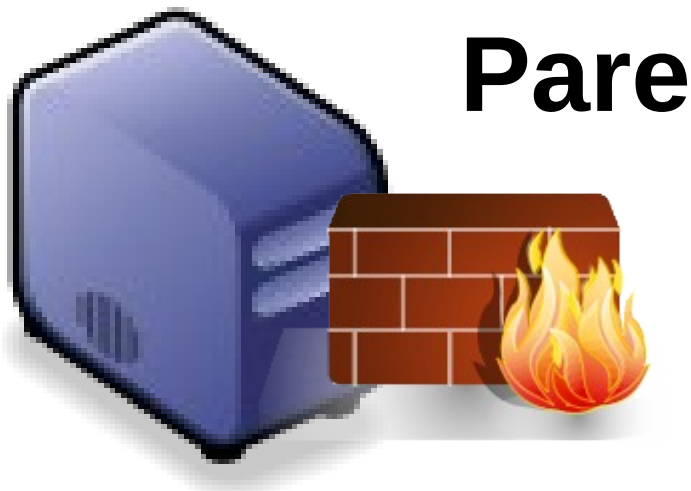
Ruby

Java

Le top 10 des risques de sécurité applicatifs web par l'Open Web Application Security Project (OWASP)

- **A1 - Injection**
- A2 - Violation de gestion d'authentification et de session
- **A3 - Cross-Site Scripting (XSS)**
- A4 - Références directs non sécurisées à un objet
- A5 - Mauvaise configuration sécurité
- A6 - Exposition de données sensibles
- A7 - Manque de contrôle d'accès au niveau fonctionnel
- **A8 - Falsification de requête intersite (CRSF)**
- A9 -Utilisation de composants avec des vulnérabilités connues
- A 10 - Redirections et renvois non validés

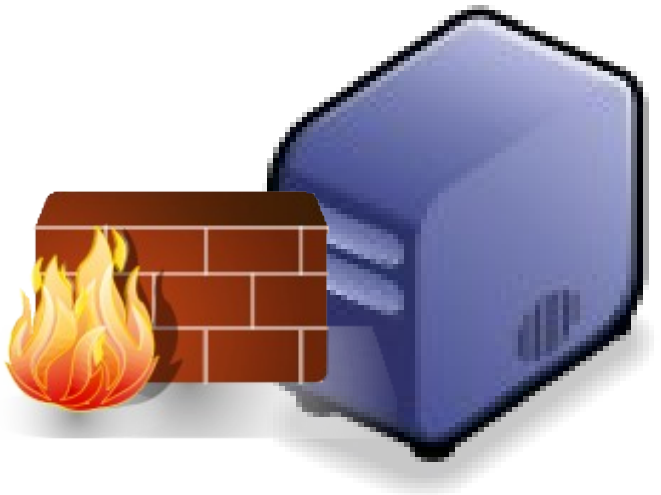
Pare-feu applicatif



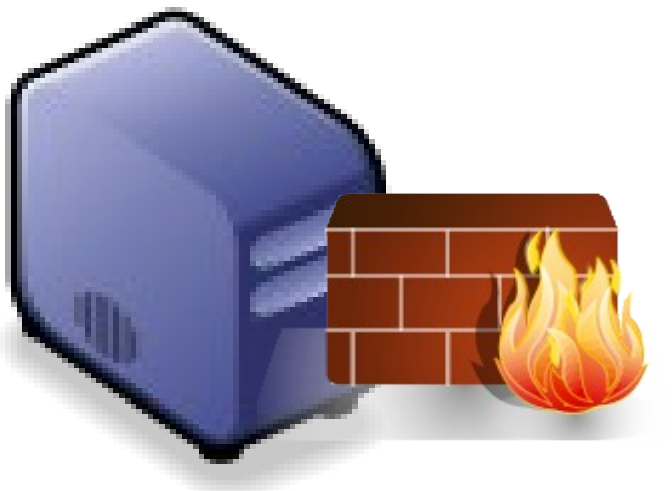
Apache HTTPD

- Libre
- Très connu
- Plein de modules

- **Modsecurity**



NAXSI



- Libre
- Performances
- Sans entretien

L'exemple à ne pas suivre

```
def my_view(request):
    if request.GET:
        q = request.GET['q']
        results = commands.getoutput('sqlite3 -line badproject /db/ database .db\
                                      \' select nom , identifiant from utilisateur where \
                                      nom = \"' + q + '\"\'' )
    else:
        q = ''
        results = ''
    return {results ': results }
```

Injections SQL

http :// monsite /?q=\"%3B+ select +*+ from+ utilisateur %3B

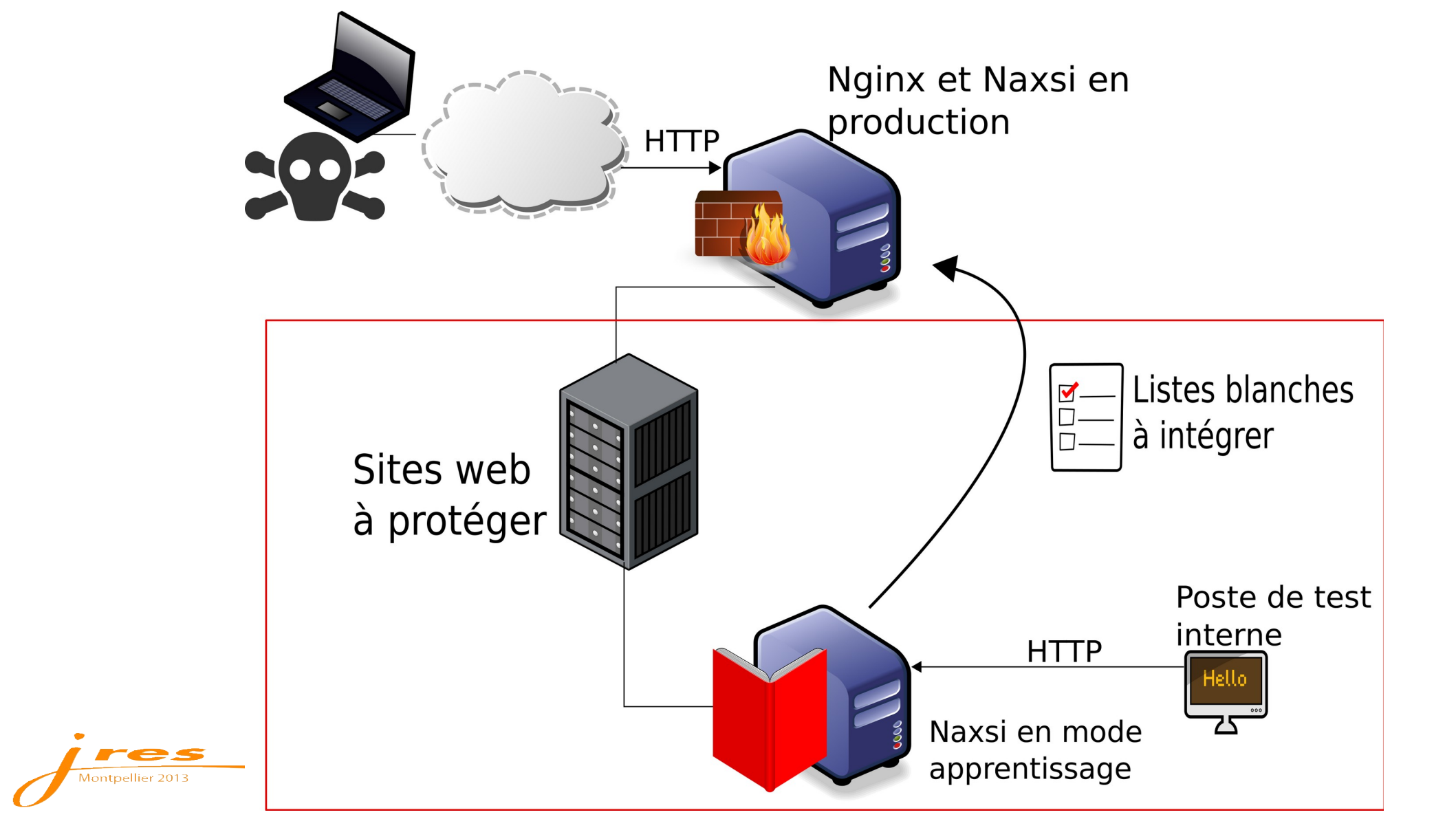
http :// monsite /?q=\"%3B+ delete +from+ utilisateur %3B

Modsecurity

- Base de signatures
- Recherche de motifs

Naxsi

- Score sur mots ou caractères
- Seuil de détection


Nginx et Naxsi en
production
HTTP
Sites web
à protéger
Listes blanches
à intégrer
Poste de test
interne
HTTP
Hello
Naxsi en mode
apprentissage