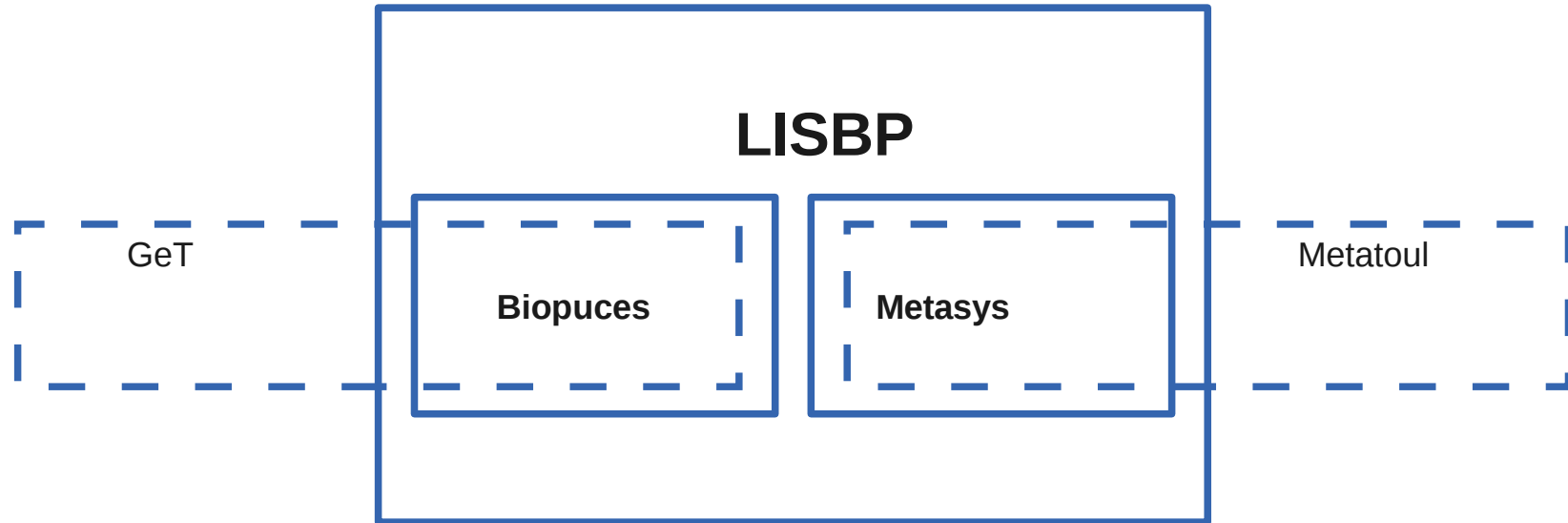


NAXSI

Un pare-feu applicatif pour NGINX

Mon environnement



NGINX

Serveur HTTP et proxy inversé



- Libre
- Bonnes performances
- Faible empreinte mémoire



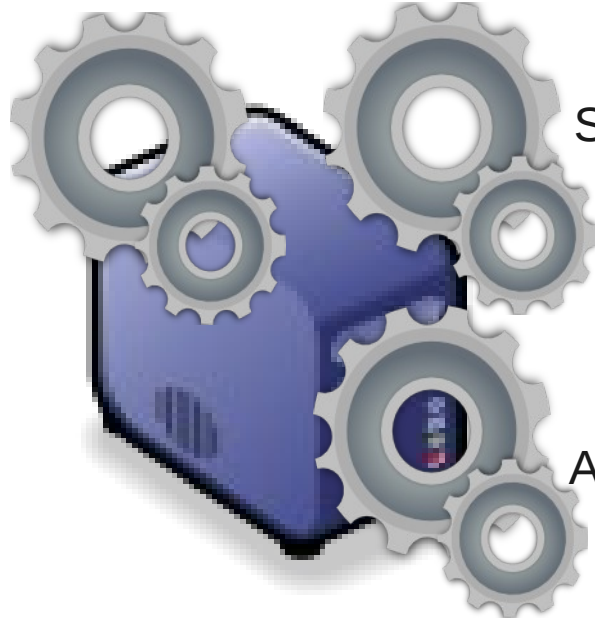
Site web



Site web

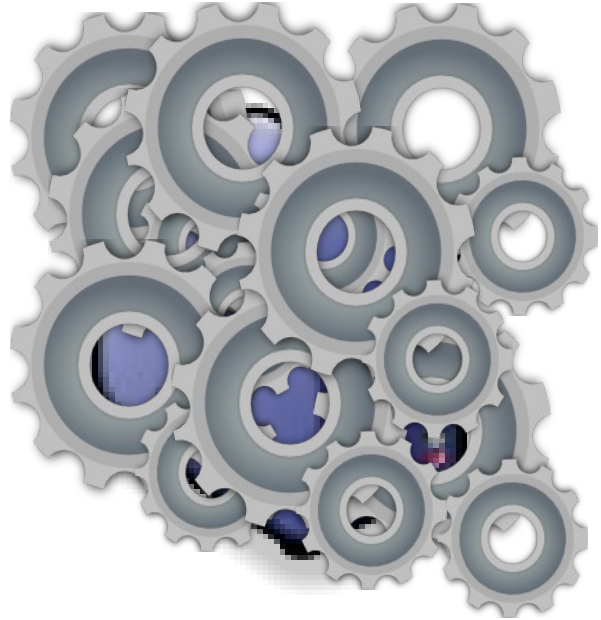
Agenda

CVS



Site web

Agenda





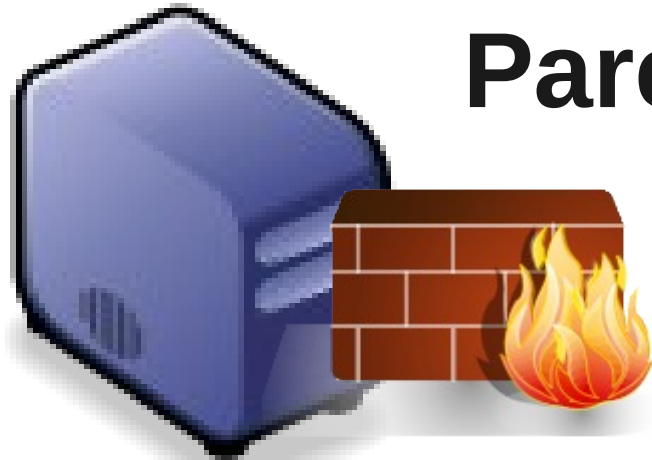
Python 2.6 **PHP 5.x**
Python 2.7 **PHP 4.x**
Perl 6 **Perl 5**
Python 3 **R**
Ruby
Java

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



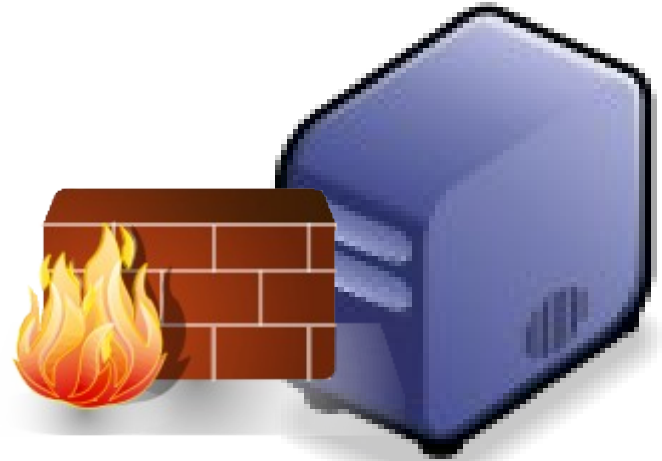
- **A1 - Injection**
- A2 - Violation de gestion d'authentification et de session
- **A3 - Cross-Site Scripting (XSS)**
- A4 - Références directs non sécurisées à un objet
- A5 - Mauvaise configuration sécurité
- A6 - Exposition de données sensibles
- A7 - Manque de contrôle d'accès au niveau fonctionnel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

Pare-feu applicatif

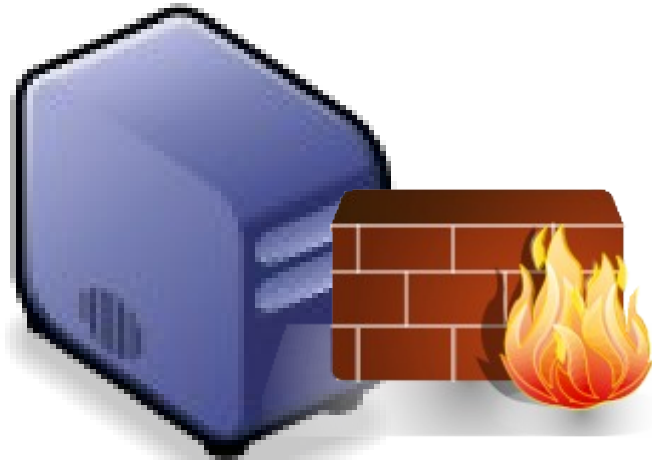


Apache HTTPD

- Libre
- Très connu
- Plein de modules
- **Modsecurity**



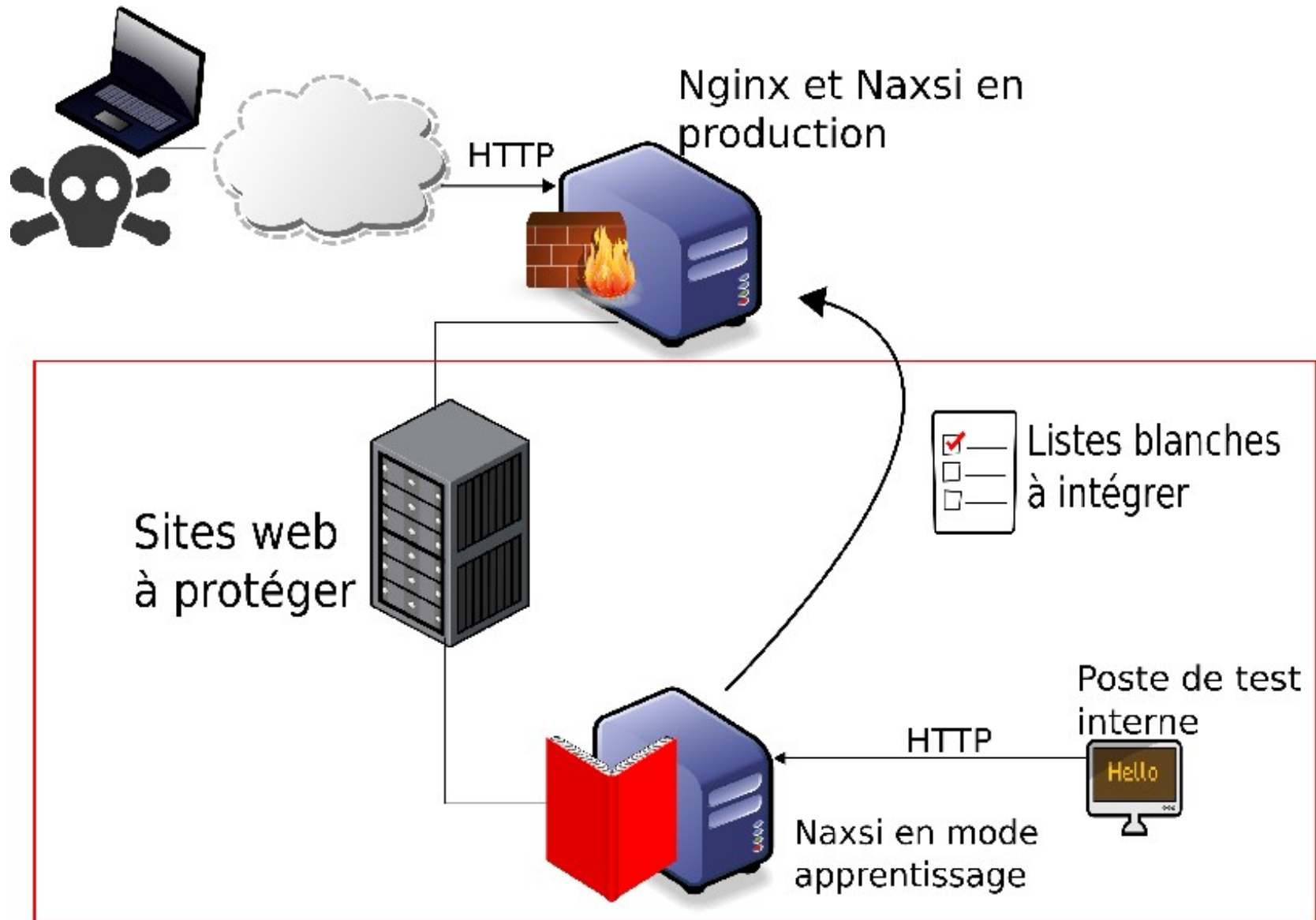
NAXSI



- Libre
- Performances
- Sans entretien

Comment faire pour configurer NAXSI

- configurer le serveur web Nginx
- définir son mode de fonctionnement, apprentissage ou non
- indiquer quelles sont les règles à utiliser et leurs scores
- définir les seuils de détections
- que faire en cas de détection, typiquement quelle page d'erreur HTTP retourner
- insérer la liste blanche des requêtes HTTP obtenue après la période d'apprentissage.



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://monsie /?q=\"%3B+ select +*+ from+ utilisateur %3B
```

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

Modsecurity

- Base de signatures
- Recherche de motifs

Naxsi

- Score sur mots ou caractères
- Seuil de détection

Conclusion

Naxsi

- objectifs de rapidité atteints

Mais

- L'efficacité d'une phase d'apprentissage est difficilement évaluable
- Le projet est encore jeune et les changements de version peuvent être très fréquents

<https://github.com/nbs-system/naxsi>