Une approche positive du filtrage applicatif Web

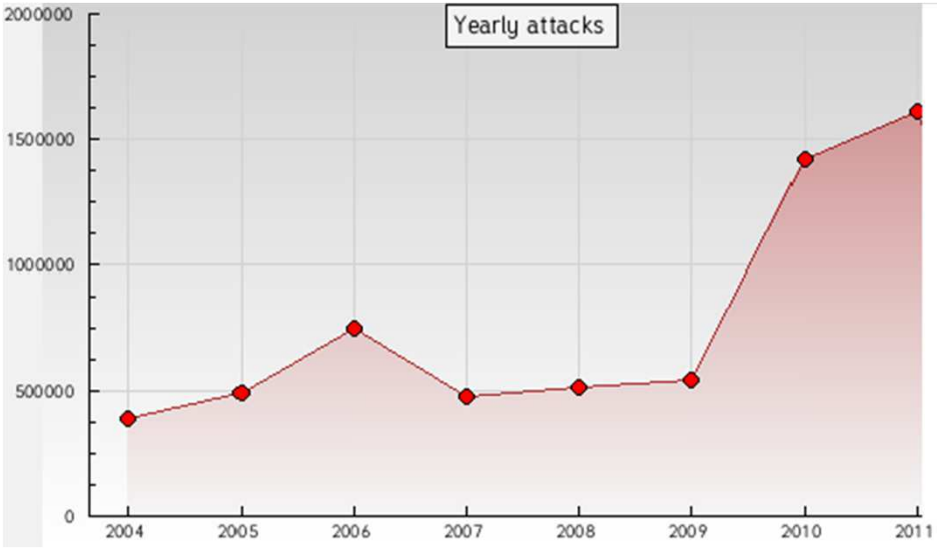
Didier « grk » Conchaudron
Sébastien « blotus » Blot

NAXSI

Un peu de background

Une hécatombe

Juste en 2011:
Sony, RSA, Orange,
MySQL.com, HBgary & 600+
autres



(Nb of annual defaces, source: zone-h)

- Faible niveau technique requis pour l'exploitation (SQLi)
- La plupart des acteurs manquent de sensibilité
- Globalement, le niveau de sécurité des applicatifs web évolue peu, ou pas assez vite
- A cause de ces facteurs, le nombre d'attaques croit de manière inquiétante

…qui n'affecte pas seulement les « petits »!

- Juste sur le mois de mai 2012:
  - Govs ou affiliés:
    - France
    - Bahrain
    - US
    - Thailand
    - Canada
    - Israel

```
username        user_password   user_email
$vo[illegible]  b35d1ac9729539d9f8ef87508e8b2be0        ki[illegible]@mail.ru
&a[illegible]3;         5e0ed8d03d765e4fb5128b6ba7bc8481        b[illegible]@hotmail.com
[illegible]3d5a7af23179acea3550fc6301300        Em[illegible]@mail.bij.pl
[illegible]     1e3c47bf39af11993cfdc689693b7012        je[illegible]@gmail.com
[illegible]     297dbe7699dcfa60609bf9e667e2e4dc        ev[illegible]@gmail.com
[illegible]     adefb16336d900168c9bfc40af5b18ef        lo[illegible]@gmx.com
[illegible]     f52eda79661df6bea25849e48c189f29        gy[illegible]@gmail.com
[illegible]     0d4d1b3bf4c8d5696d87cfb9b131ed75        nob[illegible]@gmail.com
[illegible]     81dc9bdb52d04dc20036dbd8313ed055        ad[illegible]@hotmail.com
[illegible]     fcb9582799a1bd68003dde3f22bc8c6b        a[illegible]@evi[illegible].com
[illegible]     7de3f3d71d7486009e63d9dfe11a0634        pa[illegible]@ya[illegible]im.ws
[illegible]     d4d1cc9634ec25cb316c256702a3695f
krovo[illegible]@hiph[illegible].webhop.net
[illegible]     622d308c8459213cd61de335dc2d4c75        u[illegible]@gmail.com
[illegible]     9dea477929069fef9e439107bea1ca81        c[illegible]@gmail.com
[illegible]     6086d3db17ba993aeb2afdfe9d3b8271        k[illegible]@mail.ru
[illegible]     c0b6a6994c4a62422fabb5b4074e80a5        y[illegible]@gmail.com
```

- En moyenne, plus de 300k couples de login/passwd dumpés chaque mois

Moar numbers!

- En tests d'intrusion en boite blanche
  - 92% de vulnérabilités critiques!
  - 50% des sites ont des vulnérabilités préoccupantes
- Répartition des vulnérabilités
  - 65% vecteurs de fuite d'informations
  - 38% de XSS
  - 13% d'injection de code SQL
- 50% des sites web mettent de 75 à 230 jours pour corriger les vulnérabilités

NAXSI

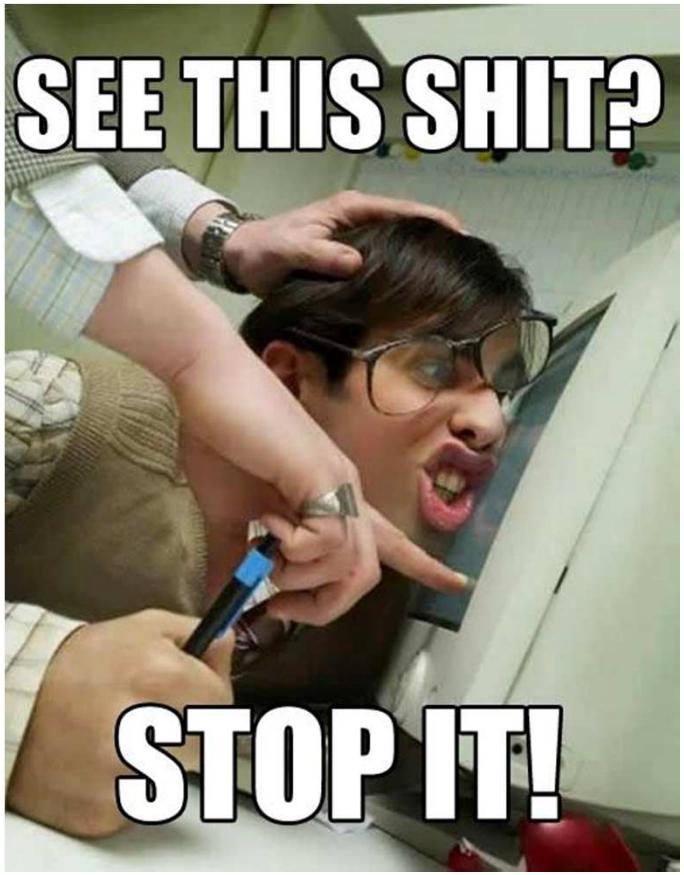
La raison derrière tout ca …

Applications web

IT classique

Et pourtant, des solutions existent…

- Meilleure mitigation : **Patch**

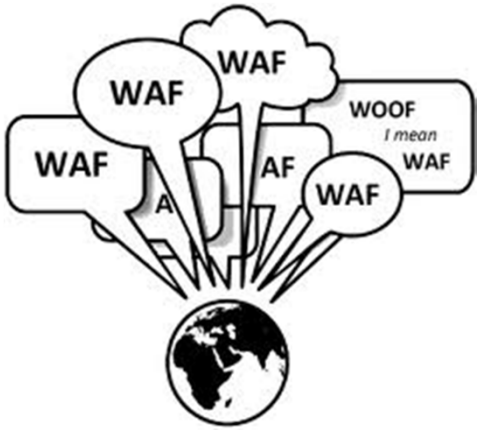


…pas toujours possible :

- Application trop complexe ou trop critique
- Manque de compétence, perte de connaissances

Le niveau de sécurité réel de votre applicatif ne peut être connu qu'après des (couteux ?) **tests de sécurité**

…ou l'emploi d'un WAF



- Le WAF est censé être à HTTP ce que le firewall est au Link layer (level 2 OSI)
- Un marché constitué essentiellement d'appliances propriétaires et quelques OSS
- Boom commercial depuis 5 ans

Les WAF

- Commerciaux :
  - Pas toujours abordables pour de petites sociétés, très couteux en montée à l'échelle
  - De qualité très hétérogène
- Open source :
  - Problèmes de performances
  - Pas assez « corporate » pour la plupart des utilisateurs ?
  - Coût de maintenance élevé
- Saas: le tout début

Et pourtant…

WHY U NO PROTECT ?

- Point de vue du pentester :
  - Les sites web sont souvent les points d'entrée les plus vulnérables …
  - Et les plus exposés aussi !
- Point de vue de l'hébergeur :
  - Les propriétaires de sites web, même quand c'est au cœur de leur business, s'en soucient peu … et se font compromettre !
- Point de vue du consultant :
  - Les DSI sont toujours réticentes/craintives à l'idée de mettre en place un WAF
  - Et ceux qui passent le pas vont généralement se tourner vers les gros WAF propriétaires coûteux (Hi Imperva !)

NAXSI

Rentrons dans le vif du sujet !

L'avènement de NAXSI

- Idée de Thibault Koechlin « bui » en avril 2011
- Projet officiel OWASP
- Financé par NBS System
  - Conseil et audit en sécurité, pentest, forensics
  - Hosting infogéré LAMP haute performance et sécurité

www.nbs-system.com

NAXSI

Pourquoi NAXSI?

- Dans l'idée d'offrir du hosting « sécurisé » pour certains de nos clients, nous avons rencontrés plusieurs problèmes :
  - Les WAFs commerciaux sont bien trop chers pour des grosses infrastructures redondées (spécialement avec beaucoup de clients)
  - Le WAF open-source analysé (mod_security) n'est pas assez rapide (ce qui signifie : filtrer seulement les requêtes POST si l'on ne veut pas dégrader l'expérience utilisateur)
  - Les deux requièrent des investissement importants pour garder les signatures à jour

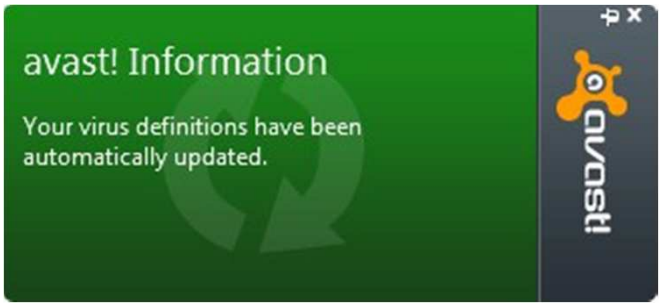
NAXSI (Nginx Anti Xss & SQL Injection)

- Un WAF pour hébergeur :
  - Performances / Montée à l'échelle
  - Industrialisation
- Un WAF qui ne requière pas de mise à jour de signatures
  - Seulement de la reconfiguration lorsque le site évolue
- Et surtout car – pour une fois – la défense est plus sympa que l'attaque !

NAXSI, un WAF, pas un WAA 1/3

- NAXSI est un module pour le serveur web/reverse proxy Nginx
- Le design de NAXSI est plus proche de celui d'un firewall stateless que de celui d'un classique pare-feu applicatif

- La plupart des WAFs tiennent plus de l'antivirus que du pare-feu
  - Ils reposent sur une base importante de signatures qui doivent être mises à jour régulièrement.



- NAXSI repose aussi sur une base de signatures, cependant probablement pas ce à quoi vous vous attendiez …

NAXSI, un WAF, pas un WAA 2/3

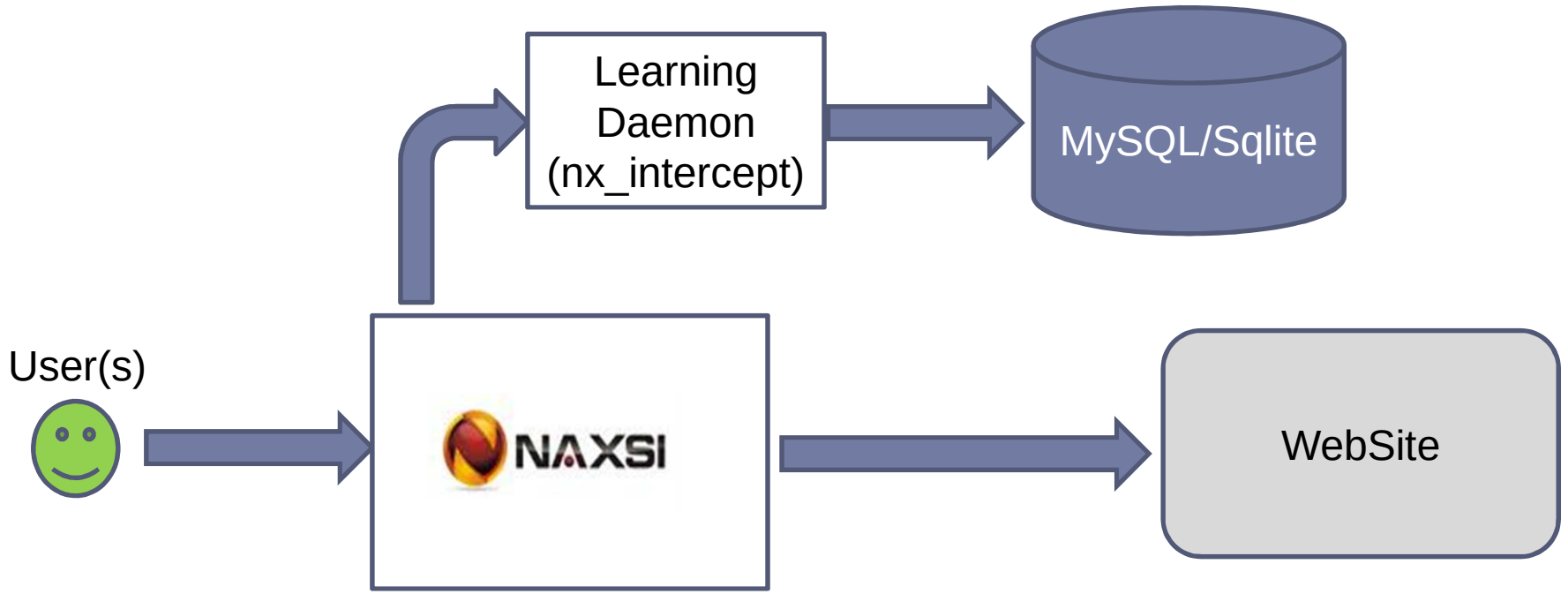
- NAXSI repose sur ~35 règles, ciblant: SQLi, XSS, RFI/LFI, file uploads …
  - Un pattern: généralement un caractère, un mot clé
  - Un/des scores: indiquant le type de menace associée
  - Match Zones: la zone dans laquelle on recherche le pattern
  - Et un ID unique
- Quand une requête atteint un score limite, une action est prise sur la requête

NAXSI, un WAF, pas un WAA 3/3

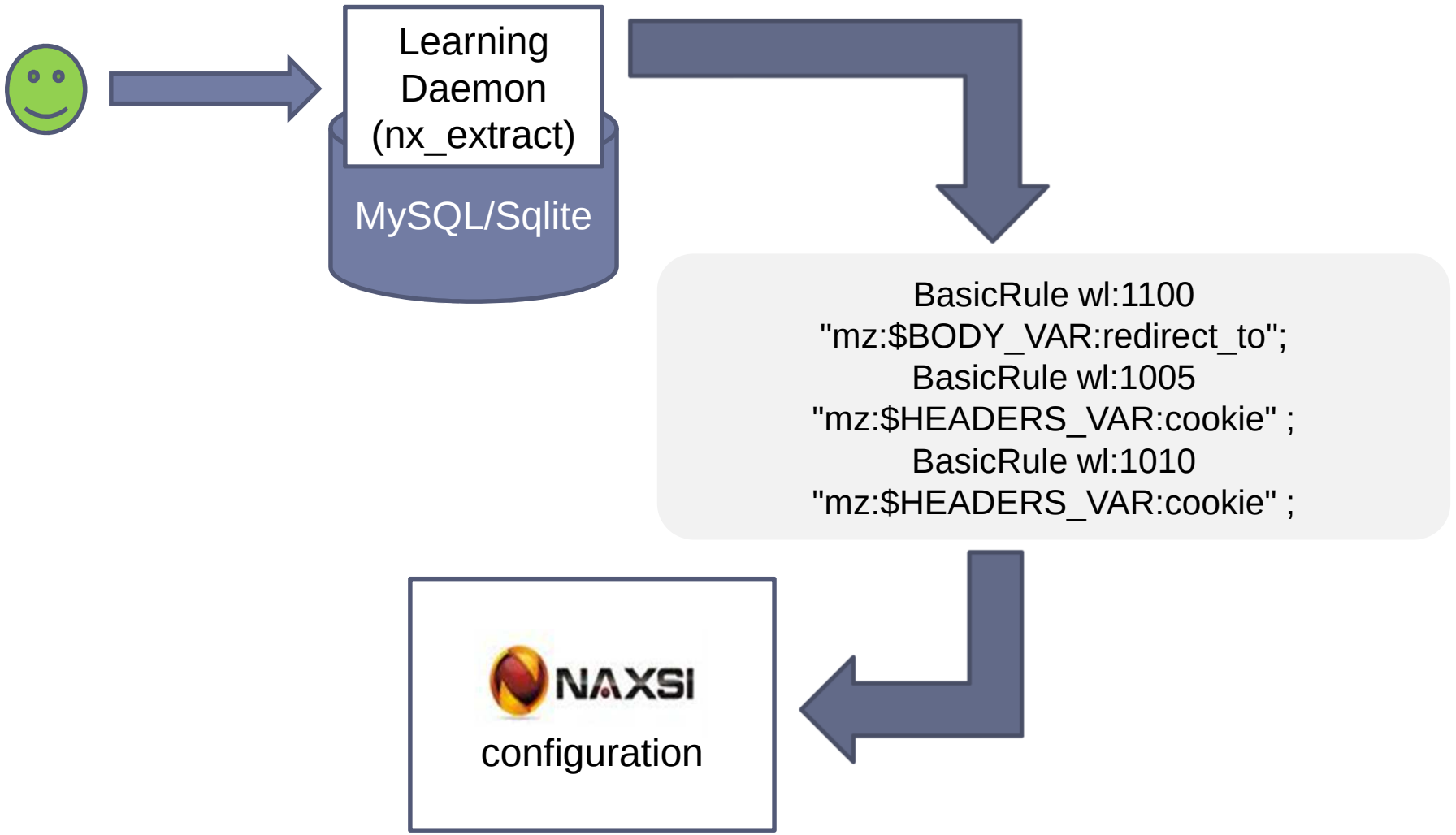
- Cette approche naïve a plusieurs avantages
  - Rapidité : pas de base massive et coûteuse de REGEX a traiter à la volée
  - Simplicité: NAXSI ne cherche pas à comprendre ou interpréter les données, ce qui limite le besoin pour de coûteuses fonctions de transformation
  - Auditabilité: 3,5K LOC

- Mais tout ceci à un prix :
  - Définition d'une liste blanche à l'aide d'un mode apprentissage!

Mode apprentissage 1/2



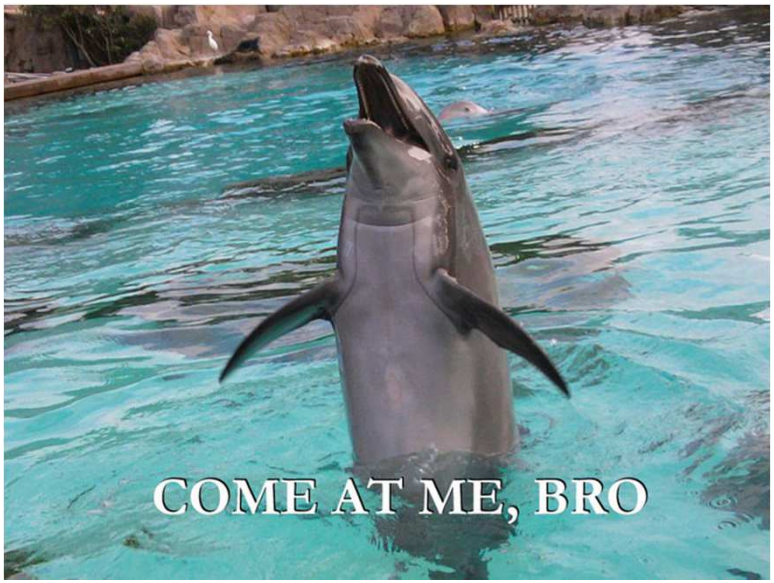
Mode apprentissage 2/2



NAXSI

NAXSI au banc d'essai

Robustesse du modèle de NAXSI vis-à-vis d'attaques obfusquées



Avantage d'un WAF sans signatures 1/2

0 div 1 union#foo*/*bar select#foo 1,2,current_user

0 div 1 union select 1,2,current_user

Mod_Security : Transformation sur les commentaires entrainant un bypass.

NAXSI : 2 mots clés SQL, 4 commentaire SQL

Avantage d'un WAF sans signatures 2/2

hUserId=22768&From Date=a1%27+or&ToDate=%3C%3Eamount+and%27

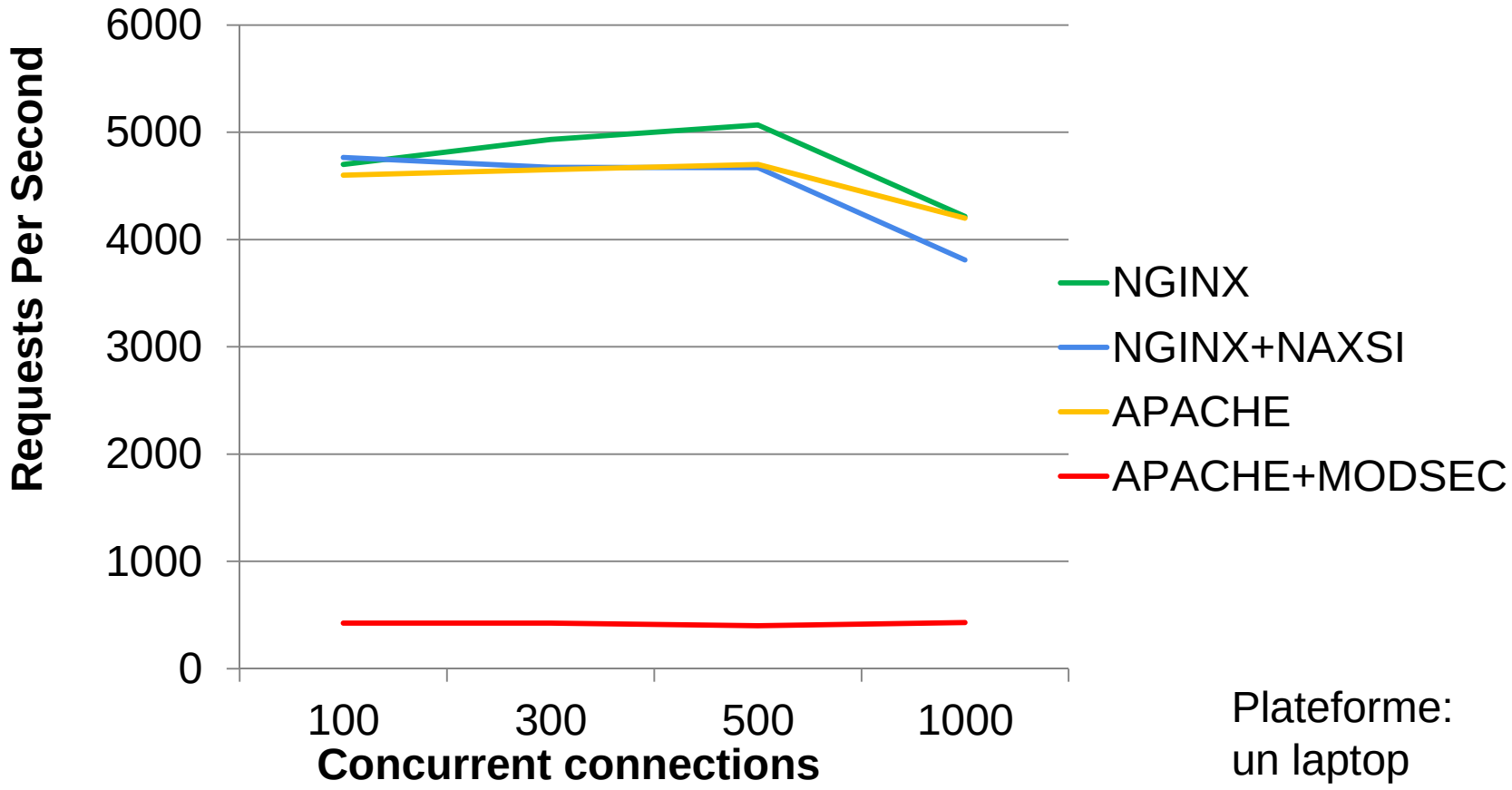
hUserId=22768&From Date=a1'+or&ToDate=<>amount+and")

Mod_Security : Victime d'attaque par fragmentation

NAXSI : Evalue la requête dans son ensemble, non pas « par variables »

Performances 1/2

- Simple GET /index.html sans arguments



Plateforme:
un laptop

Performances 2/2

- Avec apache-bench (1k requêtes concurrentes, 10k requêtes en tout, URL longue avec des arguments)

	Nginx	Nginx+NAXSI	Diff (%)
Total time	1.151 s	1.271 s	9,4%
Req Per Sec	8687.21	7866.73	9,4%
Time Per Req (mean)	0.115	0.127	9,4%
Transfert Rate	1220.48	1198.45	1,8%

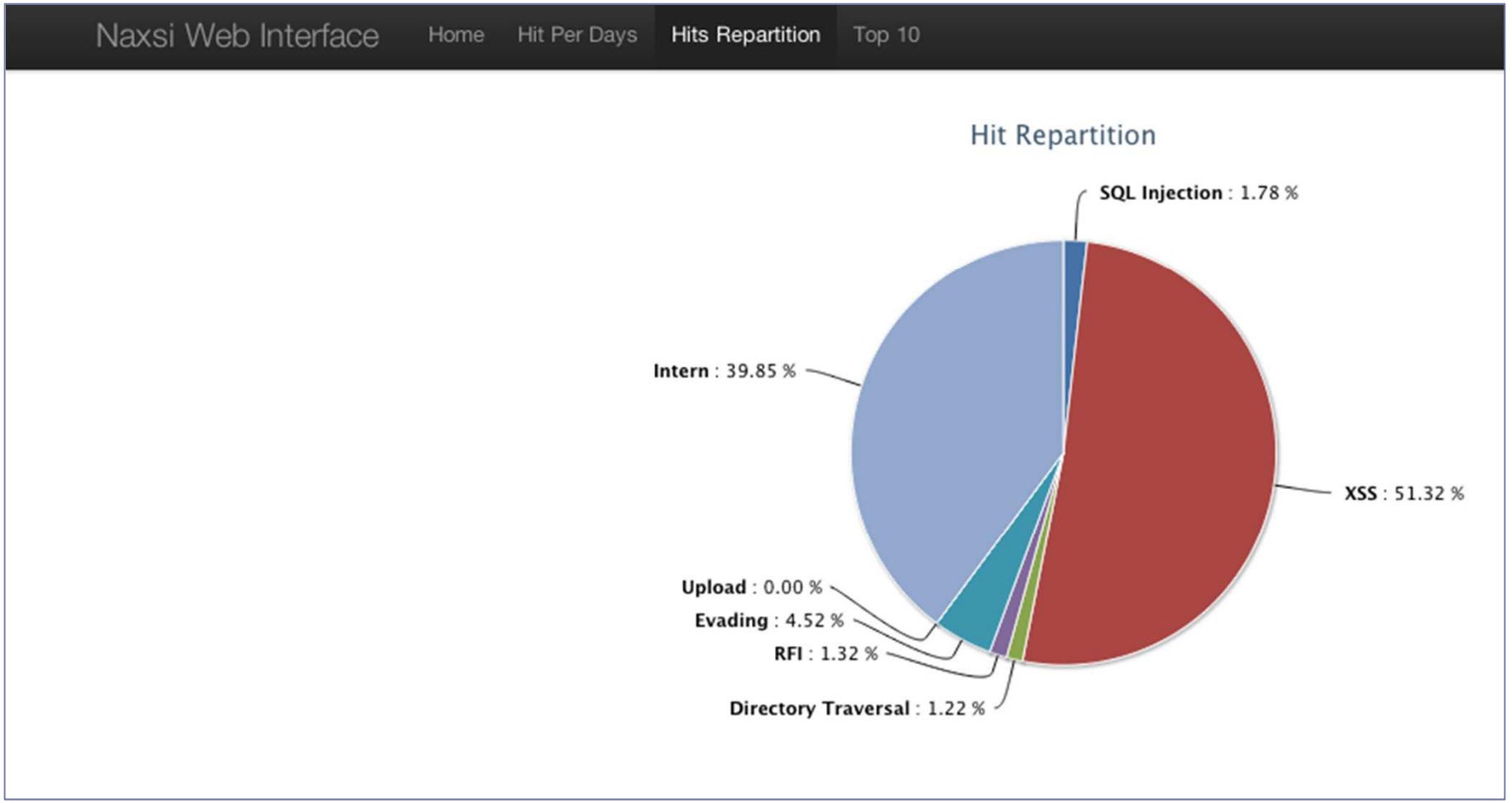
- Faible overhead de Naxsi versus perfs pures de Nginx

NAXSI comme WIDS

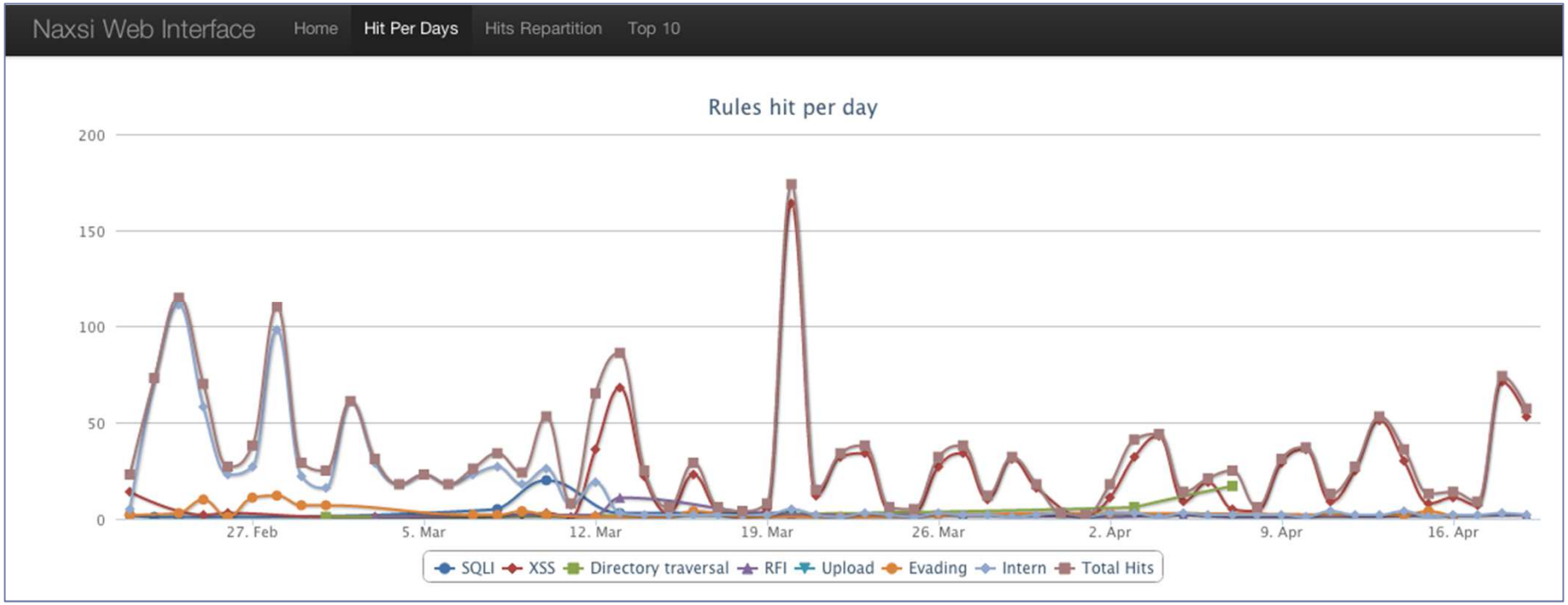
- Si vous avez une bonne raison (ou que vous êtes trop feignants), vous pouvez aussi utiliser NAXSI comme un IDS :
  - Laissez NAXSI en mode apprentissage (pas de requêtes bloquées)
  - Mettez un return 200; dans la location Nginx /RequestedDenied

- NAXSI ne bloquera aucune requête, mais toutes les exceptions seront loguées !

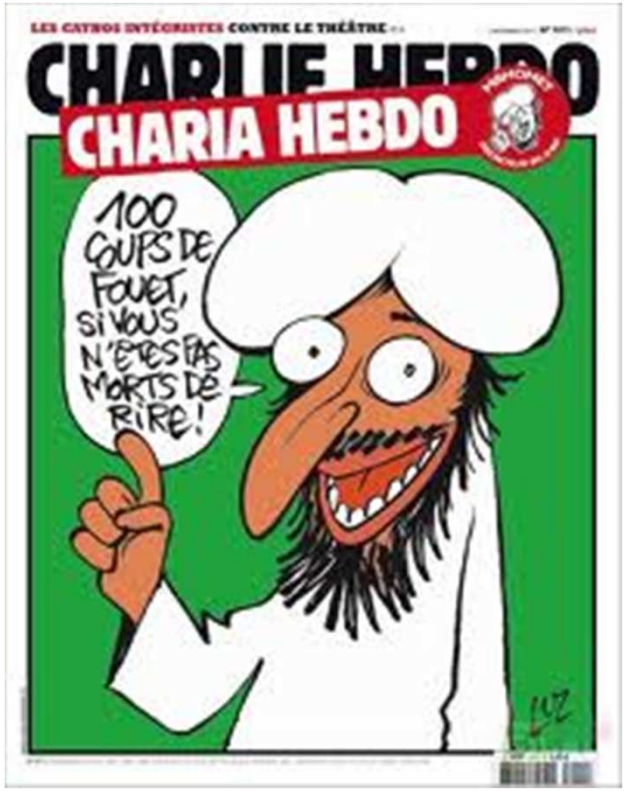
Reporting 1/2



Reporting 2/2



Retour d'expérience: l'histoire Charlie Hebdo



- Fin 2011, le journal satirique Charlie Hebdo voit ses locaux brûlés dans un incendie criminel
- Parallèlement, son site web est defacé 2 fois en 24h, le serveur DDOS
- NBS System propose son assistance et remet le site up en moins de 24h sur un serveur haute sécurité
- Depuis, mis à part un DDOS massif, le site reste inviolé
- Plus de 80% du trafic web suite à la remise en production a consisté en des tentatives d'intrusion web

NAXSI

Merci !

naxsi.googlecode.com

@NAXSI_WAF

#naxsi sur Freenode