Naxsi – Nginx-basierte WebApplicationFirewall

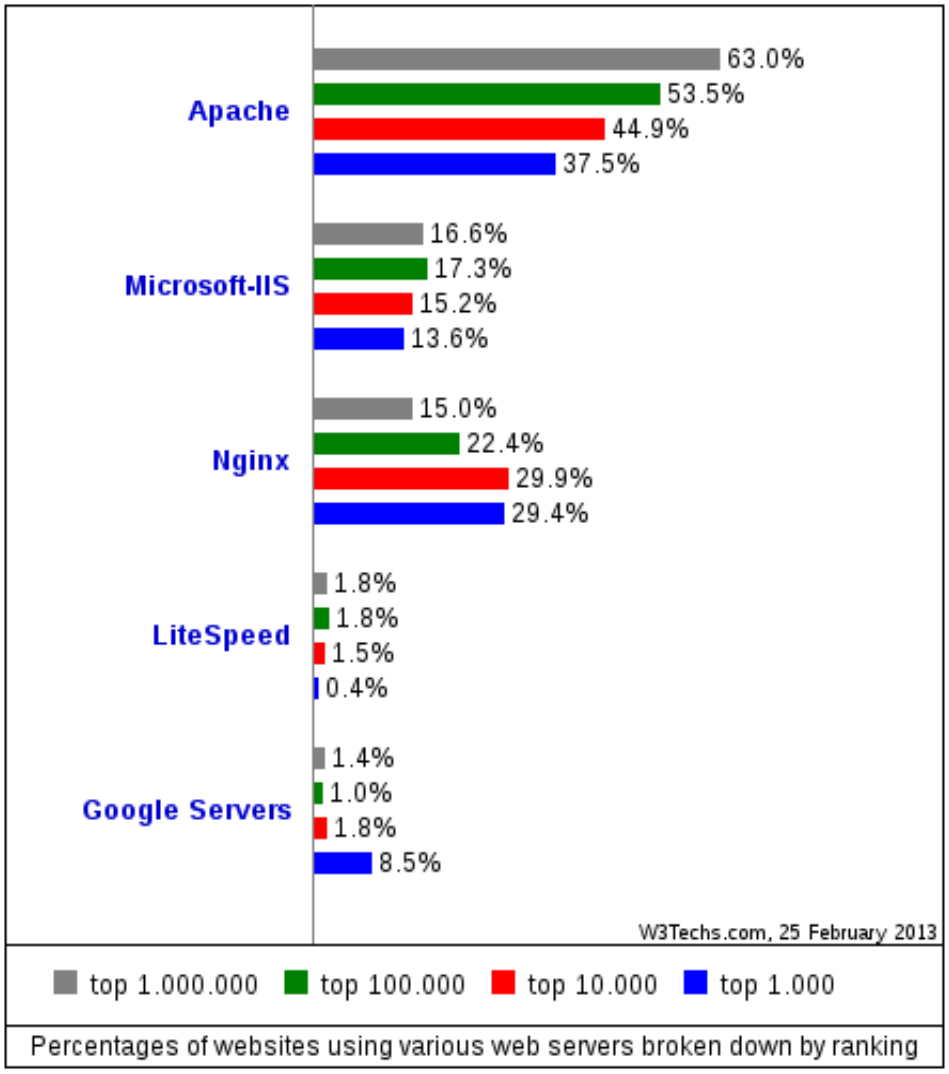
OWASP – German Chapter / Hamburg
14.03.2013

- **MARE system (Kiel)**
  http://www.mare-system.de/
  Hosting-Provider für ECommerce-Infrastruktur

- Über mich
  9 Jahre als SysAdmin und System-Architekt
  Mitarbeit in div. OSS-Projekten
  (Emerging Threats, Icinga, Naxsi, Dorvakt)

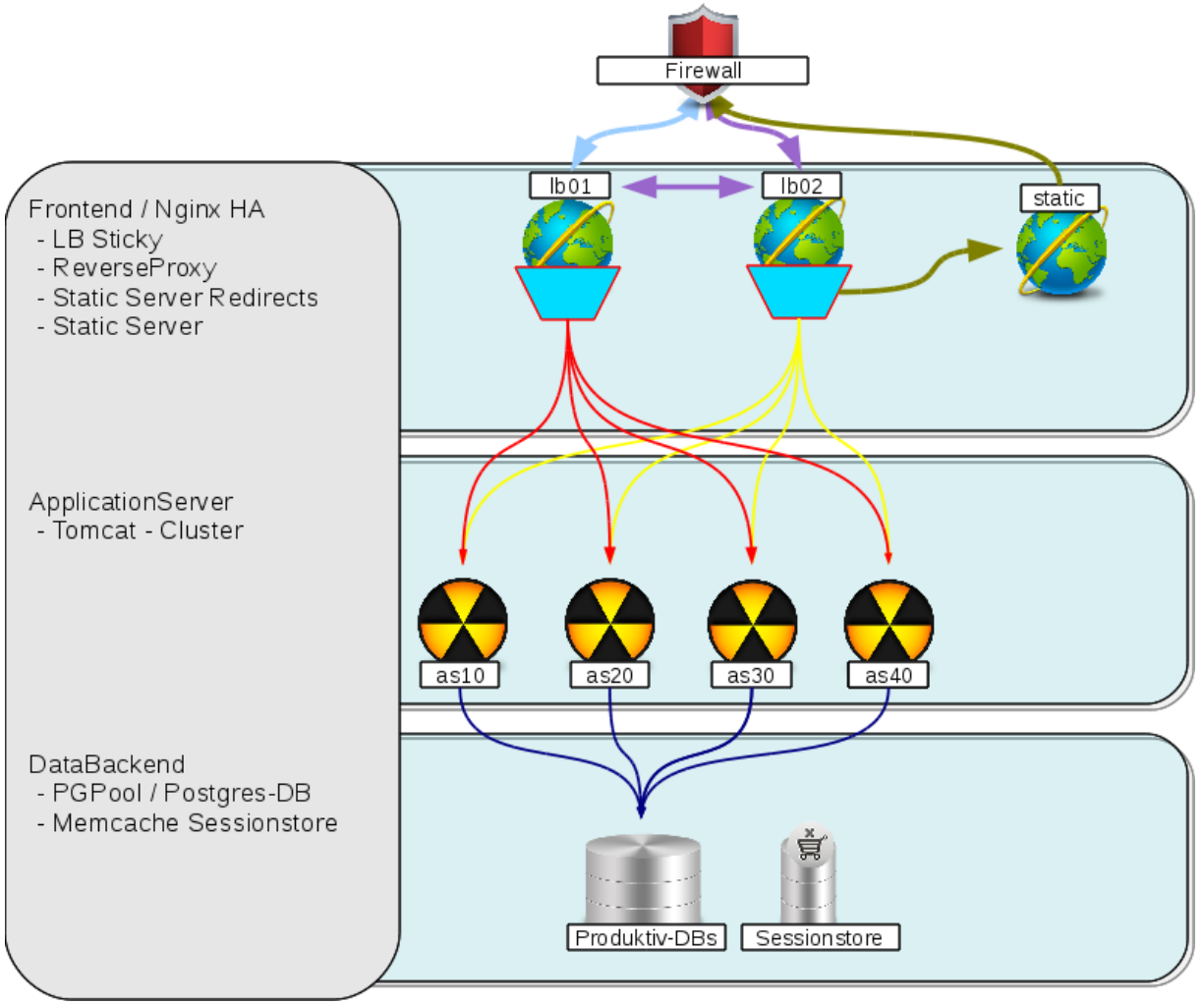
Naxsi - Intro

- Powered by NGINX:
  - Netflix
  - Pinterest
  - SoundCloud
  - CloudFlare
  - Github
  - Heroku
  - WordPress.com



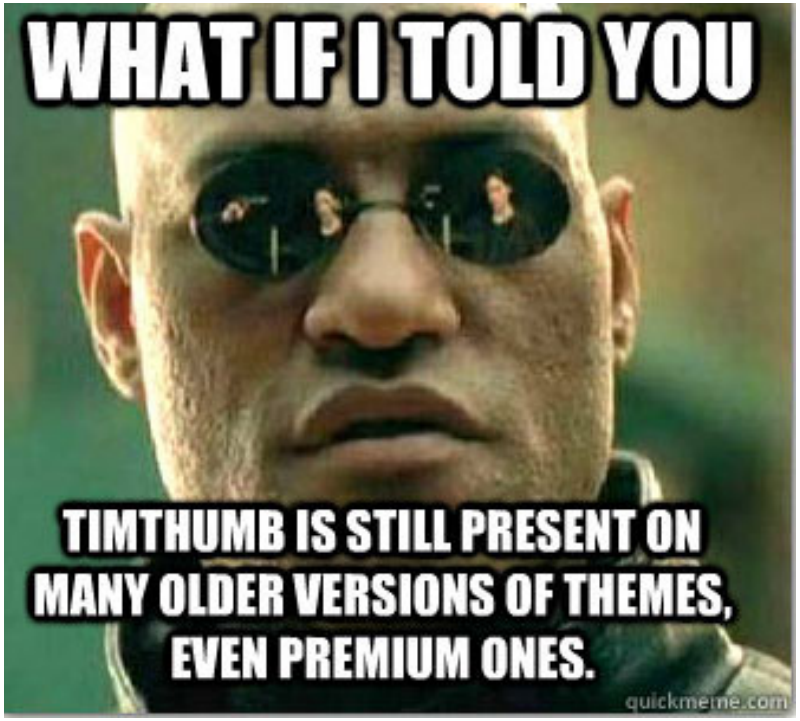
NAXSI

- NGINX - Beispiel



NAXSI

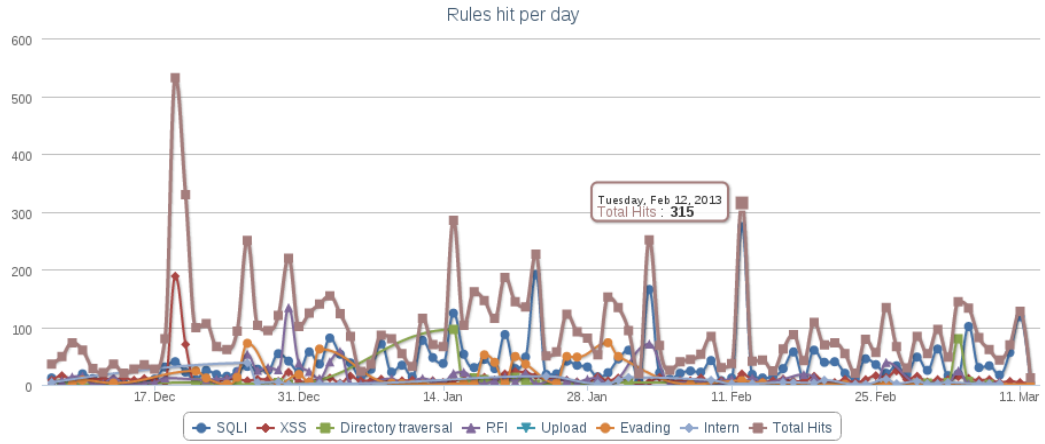
- Bedrohungen für (Web)Server und Webapps
  - Scanner
  - Skiddos
  - Sicherheitslücken
  - Humanpotential

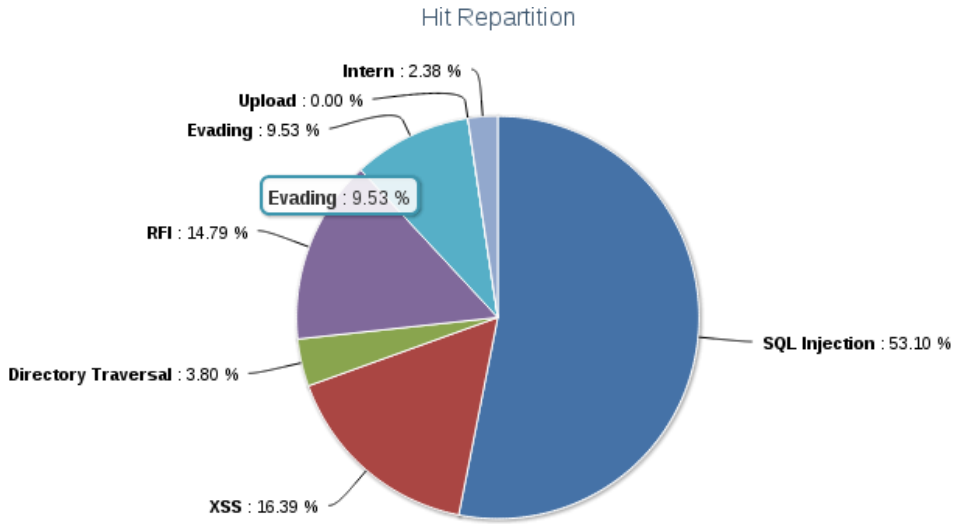


NAXSI

Naxsi – WAF

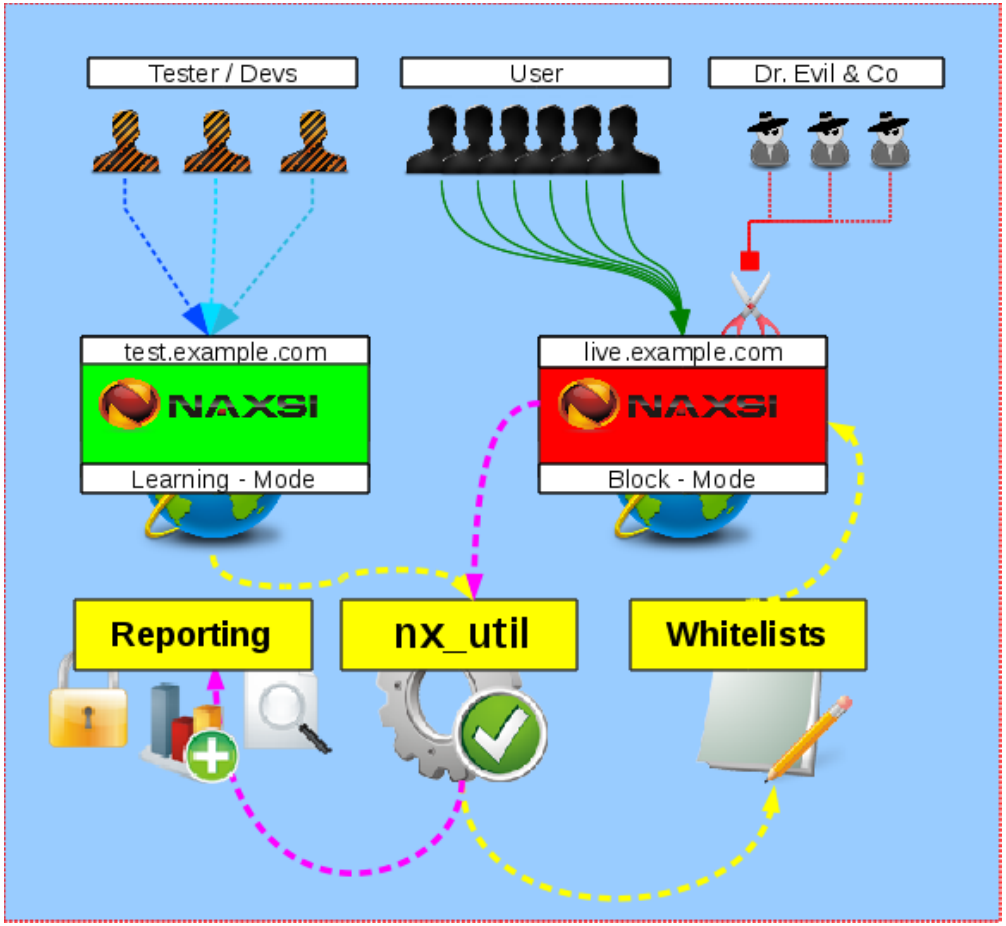
- Nginx - Modul
- core_ruleset
- nx_util
- Community (ML, IRC)





Naxsi – Modi

- Learning – Mode
  - generiert Whitelists
  - nx_util
  - Live oder Logfiles
- Block – Mode
  - Standalone
  - Reports mit nx_util



NAXSI

Naxsi - Core_Rules

- Core_Ruleset
  - SQL Injections IDs (16)
  - Obvious RFI IDs (6)
  - Directory traversal IDs (6)
  - Evading tricks IDs (6)
  - File uploads (1)

- Naxsi – Config
  - /Location - basiert

```
#LearningMode;
SecRulesEnabled;
#SecRulesDisabled;
DeniedUrl "/RequestDenied";

## check rules
CheckRule "$SQL >= 8" BLOCK;
CheckRule "$RFI >= 8" BLOCK;
CheckRule "$TRAVERSAL >= 4" BLOCK;
CheckRule "$EVADE >= 4" BLOCK;
CheckRule "$XSS >= 8" BLOCK;
```

NAXSI

Regeln

- Designator
- Suchpattern (str/rx)
- Message
- MatchingZone
- Score
- ID

Matching-Zones (mz)

- **URL**
- **ARGS**
- **BODY**
- **$HEADERS_VAR:[value]**
  - **$HEADERS_VAR:User-Agent**
  - **$HEADERS_VAR:Cookie**
  - **$HEADERS_VAR:Content-Type**
  - **$HEADERS_VAR:Connection**

```
MainRule "str:/manager/html/upload" "msg:DN SCAN Tomcat "
"mz:URL" "s:$UWA:8" id:42000217 ;
```

Naxsi - Regeln

```
MainRule "str:|" "msg:mysql keyword (|)"  "mz:BODY|URL|ARGS|$HEADERS_VAR:Cookie"
"s:$SQL:8" id:1005;
```

```
MainRule "str:/w00tw00t" "msg:DN SCAN DFind w00tw00t GET-Requests" "mz:URL"
"s:$ATTACK:8,$UWA:8" id:42000046 ;
```

```
MainRule "rx:type( *)=( *)[\"|']symbol[\"|']" "msg:DN APP_SERVER Possible RAILS -
Exploit using type=symbol" "mz:BODY" "s:$ATTACK:8" id:42000233 ;
```

```
 MainRule "str:basic ywrtaw46ywrtaw4=" "msg:APP_SERVER Tomcat admin-admin credentials"
"mz:$URL/manager|$HEADERS_VAR:Authorization" "s:$ATTACK:8" id:42000216 ;
```

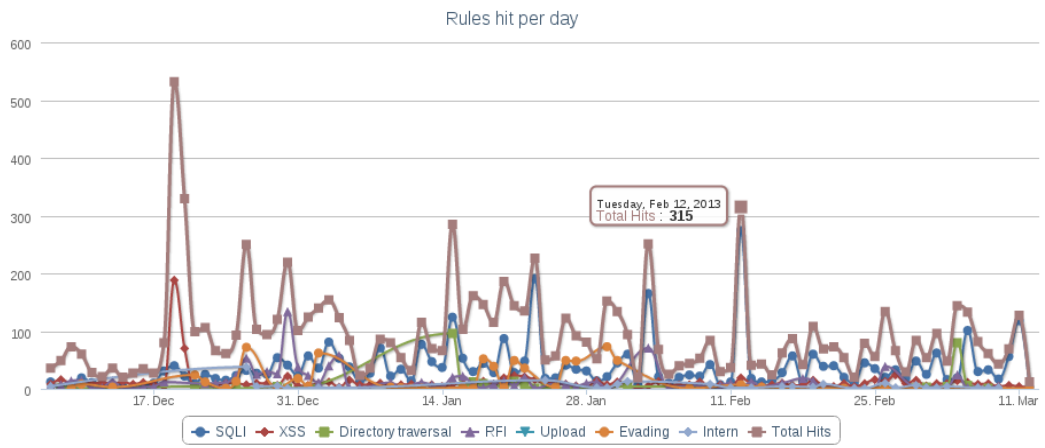
Naxsi - Whitelists

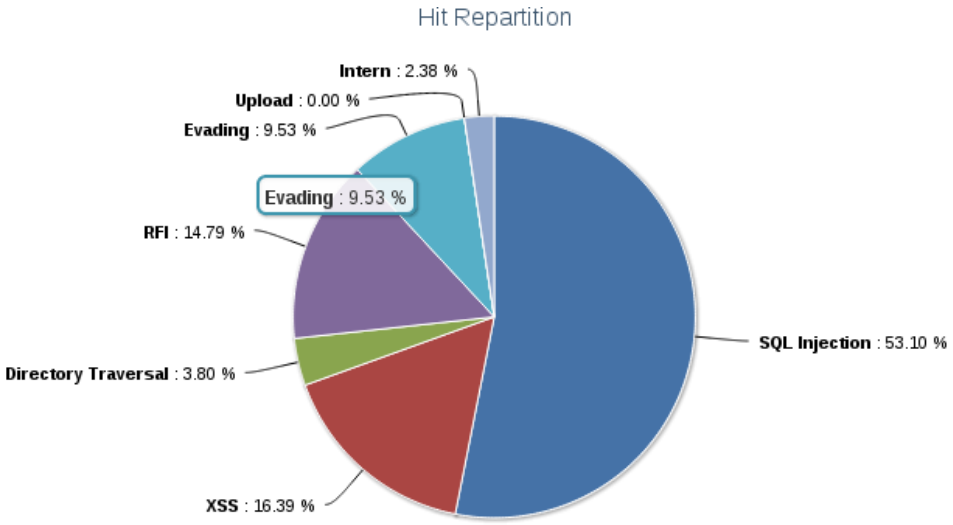
- Whitelists
  - Ausnahmen definieren
  - Testmodus / Staging
  - nx_utils
  - per Location

```
########### Optimized Rules Suggestion ##################
# total_count:727 (8.0%), peer_count:109 (10.45%) | ?
BasicRule wl:1008 "mz:$ARGS_VAR:amp|NAME";
# total_count:678 (7.46%), peer_count:46 (4.41%) | ?
#BasicRule wl:1315 "mz:$ARGS_VAR:!|NAME";
# total_count:644 (7.08%), peer_count:48 (4.6%) | ?
#BasicRule wl:1402 "mz:$HEADERS_VAR:content-type";
# total_count:571 (6.28%), peer_count:115 (11.03%) | ?
BasicRule wl:1008 "mz:URL";
# total_count:556 (6.11%), peer_count:55 (5.27%) | ?
BasicRule wl:42000039 "mz:$HEADERS_VAR:user-agent";
# total_count:461 (5.07%), peer_count:123 (11.79%) | ?
BasicRule wl:42000122 "mz:URL";
# total_count:331 (3.64%), peer_count:66 (6.33%) | ?
BasicRule wl:1100 "mz:$ARGS_VAR:src";
# total_count:319 (3.51%), peer_count:8 (0.77%) | ?
#BasicRule wl:1315 "mz:$HEADERS_VAR:cookie";
# total_count:277 (3.05%), peer_count:135 (12.94%) | ?
BasicRule wl:1008 "mz:$URL:/|$ARGS_VAR:c";
# total_count:243 (2.67%), peer_count:4 (0.38%) | ?
#BasicRule wl:1200 "mz:URL";
# total_count:214 (2.35%), peer_count:31 (2.97%) | ?
#BasicRule wl:1100 "mz:$ARGS_VAR:display";
# total_count:204 (2.24%), peer_count:52 (4.99%) | ?
#BasicRule wl:42000004 "mz:URL";
# total_count:182 (2.0%), peer_count:49 (4.7%) | ?
#BasicRule wl:42000002 "mz:URL";
# total_count:177 (1.95%), peer_count:13 (1.25%) | ?
#BasicRule wl:42000227 "mz:$HEADERS_VAR:user-agent";
# total_count:142 (1.56%), peer_count:23 (2.21%) | ?
#BasicRule wl:1010 "mz:URL";
# total_count:140 (1.54%), peer_count:43 (4.12%) | ?
#BasicRule wl:42000089 "mz:URL";
```

NAXSI

- NX_UTIL
  - eigener Dienst
  - /RequestDenied
  - füllt Datenbank
  - Reporting-Tool
  - Whitelists





Naxsi + Doxi - Rules

```
--[ 7days - time-based analysis ]--------------------

> global result | 523 events
      ID |  Count
-----------------------------------
    1008 |      162 | ; in stuff
    1315 |       75 | double encoding !
    1100 |       44 | http:// scheme
42000077 |       39 | DN WEB_SERVER LIBWWW_perl-UA detected
    1005 |       31 | mysql keyword (|)
    1000 |       30 | sql keywords
42000227 |       28 | DN SCAN Scanner ZmEu exploit scanner
42000122 |       26 | DN SCAN WP Timthumb - Access
      10 |       20 | unknown ID 10
    1001 |       13 | double quote
42000181 |        6 | DN SCAN Scanner webster pro
    1010 |        5 | parenthesis, probable sql/xss
42000082 |        5 | DN WEB_SERVER Tomcat - Manager - Access
       2 |        4 | unknown ID 2
    1200 |        4 | double dot
    1310 |        4 | [, possible js
    1311 |        4 | ], possible js
42000244 |        4 | DN SCAN PHPMyAdmin - Scanner (2)
      12 |        3 | unknown ID 12
    1002 |        2 | 0x, possible hex encoding
    1402 |        2 | Content is neither mulipart/x-www-form..
42000145 |        2 | DN SCAN Scanner morfeus
42000243 |        2 | DN SCAN PHPMyAdmin - Scanner
    1009 |        1 | equal in var, probable sql/xss
    1013 |        1 | simple quote
42000003 |        1 | DN APP_SERVER ASP_file access
42000004 |        1 | DN APP_SERVER CGI_file access
42000043 |        1 | DN SCAN WhatWeb Web Application Fingerprint Scanner Defau
42000151 |        1 | DN SCAN Scanner whatweb
42000229 |        1 | DN APP_SERVER ColdFusion - Vuln-URL-Access administrator
42000248 |        1 | DN SCAN SQL-Injection Scanner CZxt2s
```

- Doxi – Rules
  - erweitere Rulesets
  - “Known Bad”
  - ~150 Regel von ET
    - app_server.rules (16)
    - web_server.rules (56)
    - web_app.rules (13)
    - malware.rules (34)
    - scanner.rules (131)

NAXSI

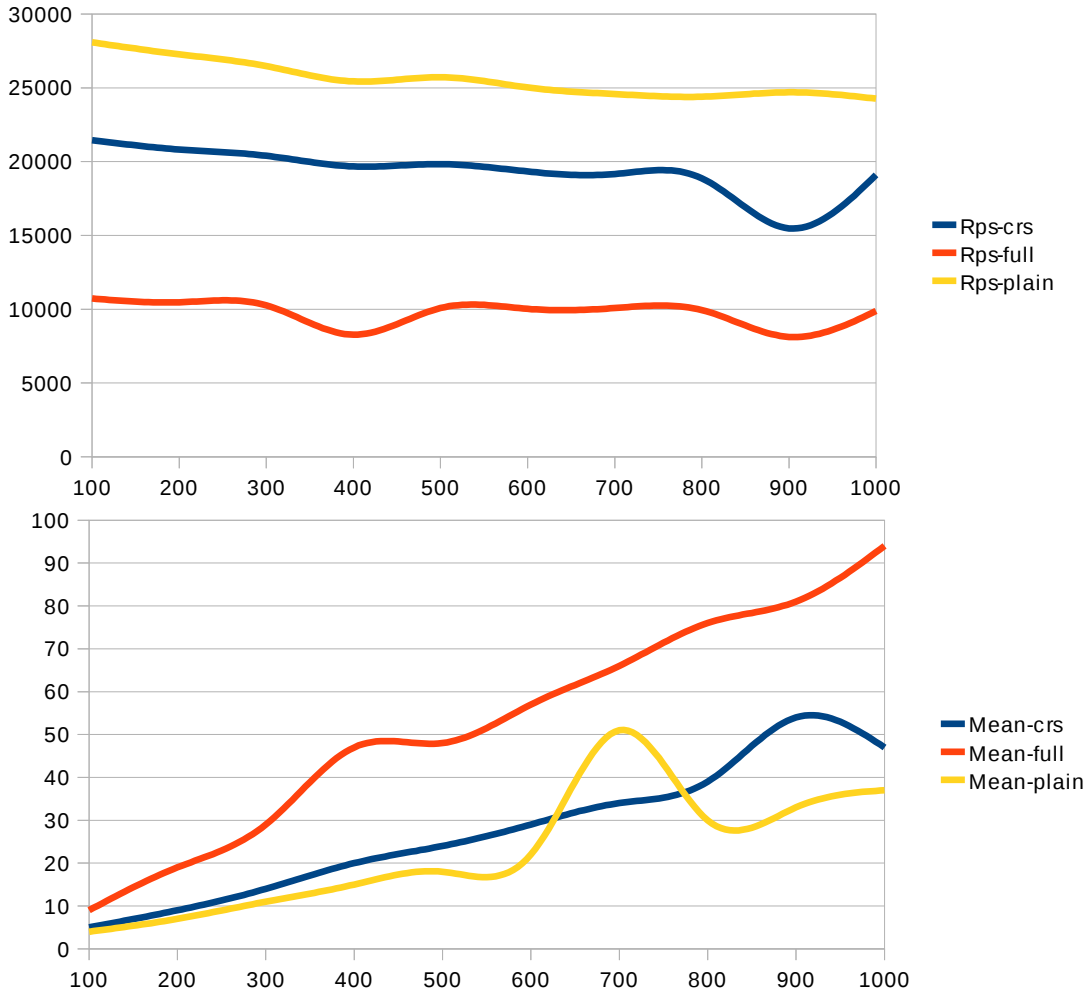
- dx-update

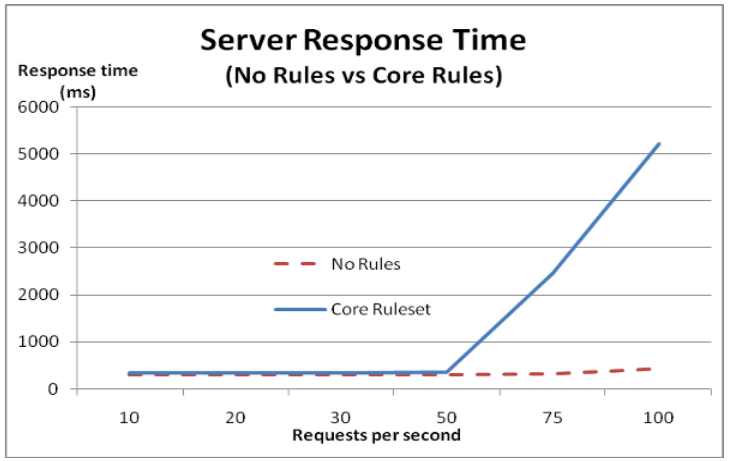
```
DOXI_Update



./dx-update - updating naxsi-rulesets from online-repo or local dir

Usage:
    ./dx-update [options]

Options
    -h          help
    -x          execute full update (w/ git pull -> rules_update
                from doxi@bitbucket
    -l          execute local update (sync from doxi-rules/ to
                nginx/doxi-rules)
    -n          config-test only, no nginx-restart
    -s          just update rules, no sync


    -v          version
```

- dx-result

```
DOXI_Result



./dx-result - getting results out of a naxsi-database

Usage:
    ./dx-result [options]

Options

    -x          execute normal results (default)
                24hrs/7days/30days/all
    -r          get most recent results (limit 100)
    -i [sid]    get result for a certain rules-id
                24hrs/7days/30days/all
    -I [ip]     get result for a certain ip
                24hrs/7days/30days/all
    -k          display known rules
    -j [sid]    display info for given signature-id / whole sig

    -h          help
    -v          version
```

Naxsi - Benchmarks



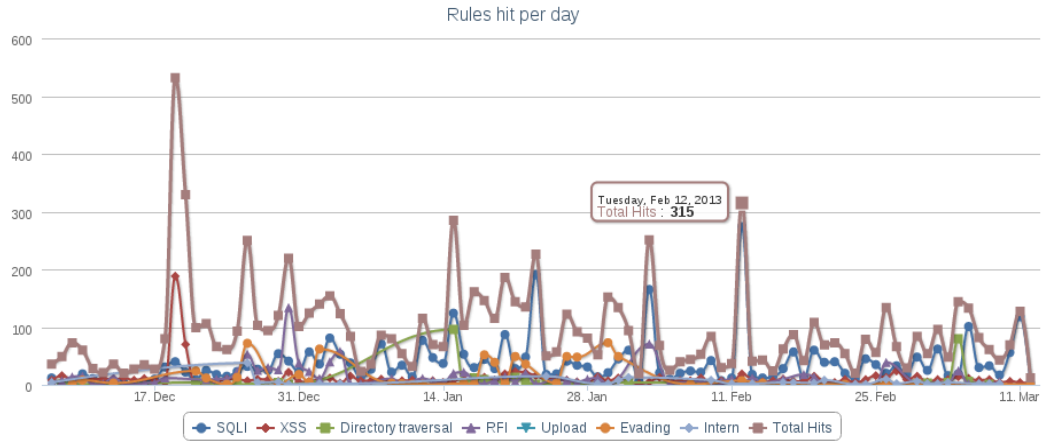


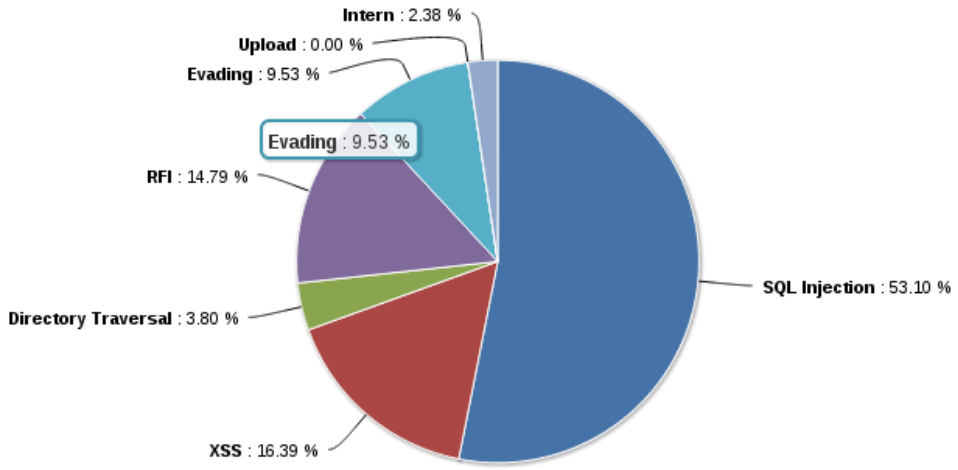
http://nguyenvulong.wordpress.com/page/3/

NAXSI

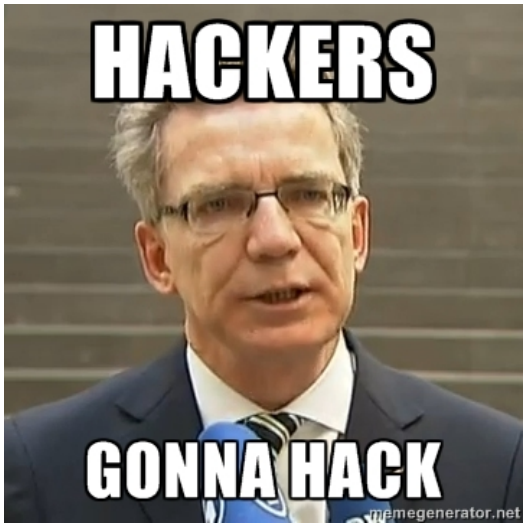
Naxsi - Reporting

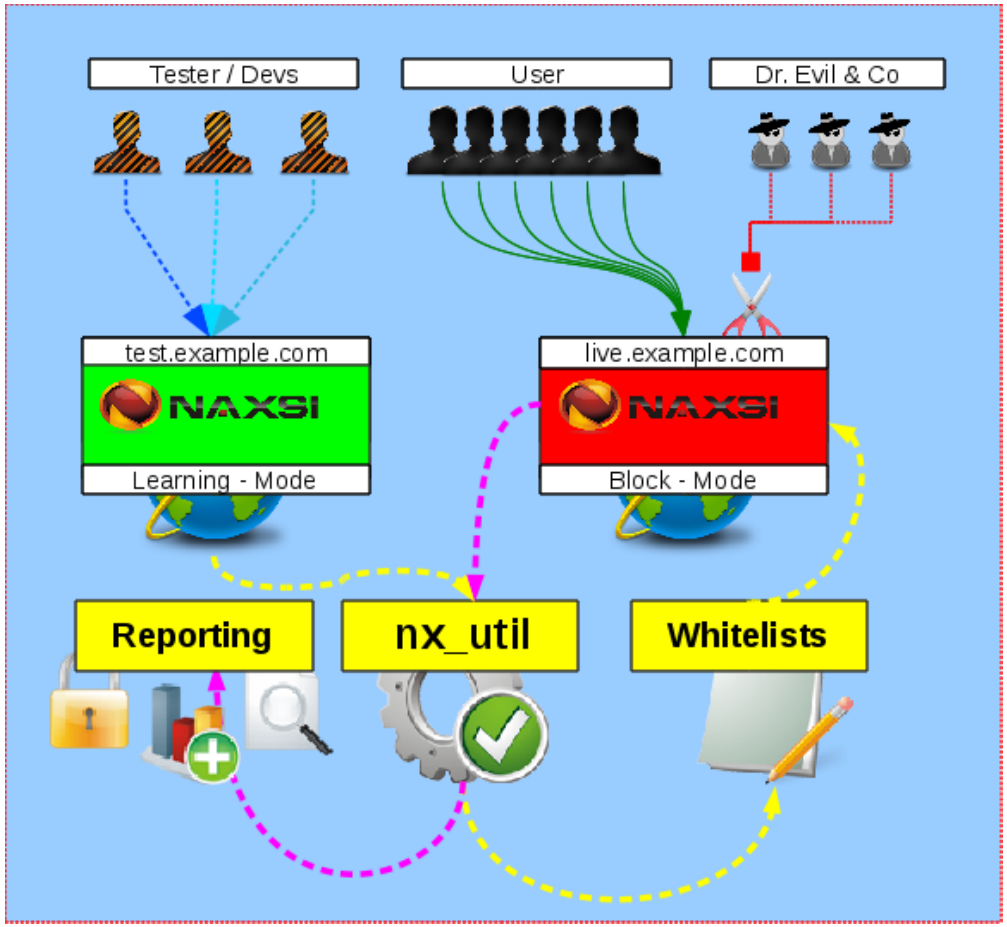
- nx_util
  - neue Version
  - Filter per CLI
  - Reports als HTML
- dx-result
  - andere Sicht auf Event-DB
  - Blacklists





- Fragen?





NAXSI