# Headers, Websockets + More: Webserver und Webapp-Sicherheit im Jahre 2014

Markus Manzke
SLAC 2014 / Berlin
13.03.2014

"If you spend more on coffee than on IT security,
then you will be hacked."

**-- Richard A. Clark / 2002**

- Über mich

  12 Jahre als SysAdmin und System-Architekt für webbasierte Infrastruktur
  von klein bis mittel(stands)groß
  Mitarbeit in div. OSS-Projekten (Emerging Threats, Icinga, Naxsi, Nginx)
  Vorträge/Artikel: CeBIT, OWASP, ix, ADMIN-MAGAZIN, Barcamps

- **MARE system (Kiel)**

  **http://www.mare-system.de/**
  Hosting-Provider für Ecommerce-Infrastruktur

- **8ack**

  **http://www.8ack.de**
  Security-Information und News, von Profis für Profis

# Inhalt

- Webserver-Header
  Analyse, Probleme, Best Practices
- Content Security Policy et al
  neue Userschutz-Technologie
- Websockets
  Einsatzgebiete, DOs & DONTs
- Reverse Proxy
  Einsatzgebiete & Best Practices
- WebApplicationFirewalls
  Einsatzszenarien, Überblick und Vergleich populärer Open-Source-Lösungen
  Layer 7 DDoS - Schutz

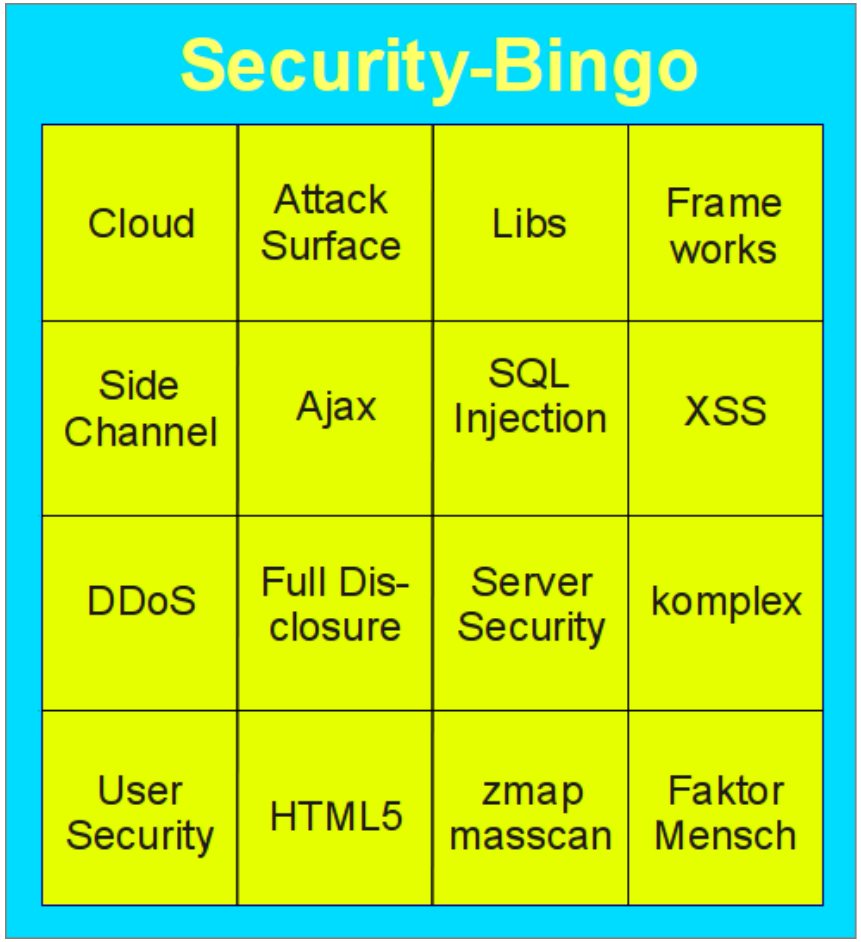
# Web-Security: Grundsätzliche Probleme

- Problem:

  24/7, Accept: World & Dog
  Abhängig von Appservern, Libs,
  Frameworks, Appliances:
  kleine Ursache, große Wirkung
  komplex, vernetzt & verwoben (OAuth)
  Verteidigung: 24/7, Grundrauschen
  Angreifer: kann warten und die Route
  wählen, ausgereifte Toolbox, Scanner

- Lösung

  Wissen
  Policy + Architektur
  Disziplin
  Glück



# Webserver-Header

- verräterische Header
  AppServer-Leaks
  lazy Admins / Eastereggs
  Infrastruktur-Leaks

- Analyse-Tools
  Shodan/zmap/masscan
  Console-Output

- Todo:
  Attack-Surface minimieren
  Header-Check
  Header-Hygiene

# Attacke!

- Angriffsvorbereitung via Header-Analyse
- Bsp1: zentraler Schul-Proxy Iowa/Arrowhead
  5 Minuten bis zum potentiellen Exploit
- Bsp2: myXYZ.de
  10 Minuten bis zum potentiellen Exploit

# Userschutz durch Security-Header

- Content Security Policy (CSP)
  XSS/Script-Injection-Schutz
  Definieren der Quellen für Script, Fonts, Grafiken, Iframes
  Whitelist-Ansatz
  Learning-Mode / Reporting
- X-Frame-Options
  Clickjacking-Schutz
  SAMEORIGIN / DENY / ALLOW
- X-Content-Type-Options/X-XSS-Protection
  Schützt vor XSS und Mime-Sniffing
- Cross Origin Resource Sharing (CORS)
  Aufbrechen der Same-Origin-Policy (scriptbasierte XMLHttpRequests)

# Userschutz durch Security-Header

- Strict-Transport-Security (HSTS, SSL/TLS)
  zwingt den Browser auf HTTPS
- Cookies
  HTTPOnly / Secure

- Pro
  erhöhter Userschutz (XSS, Clickjacking, Session-Stealing, SSL erzwingen)
- Contra
  Browserabhängig
  Implementierungsaufwand (might break stuff)

- Websockets
  TCP over HTTP
  bidirektionale Verbindung Server ↔ Client (2-Way-Push)
  kein HTTP-Overhead
- DONT
  statische Inhalte, CSS; JS; HTML
- DO
  dynamische Daten innerhalb der Webapp
  (vulgo: AJAX-Requests)

- Sicherheit ... Sicherheit?

  eigenes Security-Modell implementieren

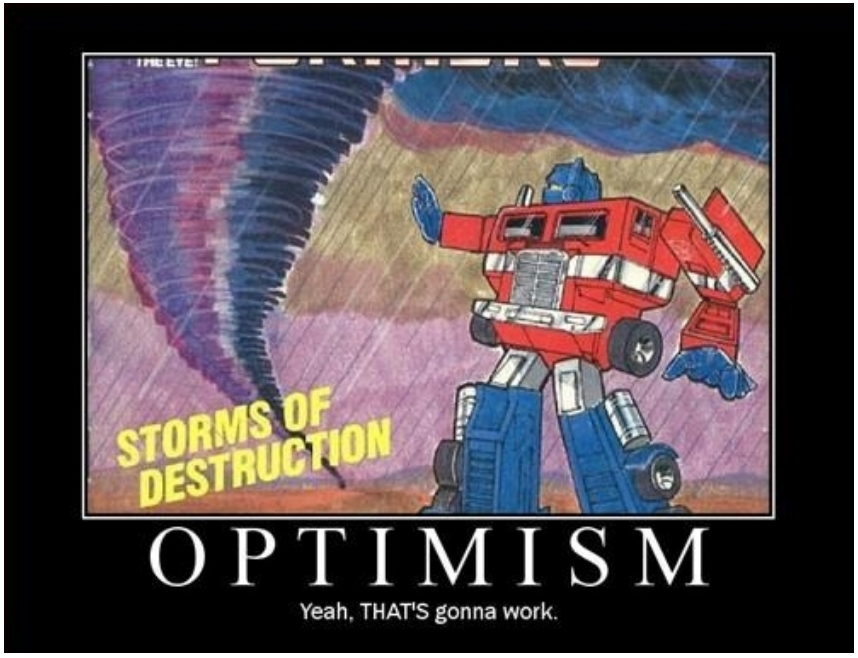
  keine HTTP/IP-Restriktionen

  keine Session/Cookies

  alles noch sehr Alpha

  WS-Server eigene Instanzen

  keine WAF/IDS-Abdeckung momentan



- Reverse Proxy Best Practices

  Header-Kontrolle / Verstecken der Infrastruktur

  Loadbalancing + Performance

  Abfangen von Requests vor Appservern (Static/Cache)

  Cookie-Mangling: Secure / HTTPOnly

  Hotpatching / serverseitige Workarounds
  (CVE 2014-0050 Tomcat DDoS)

  WAF / Limit-Filter

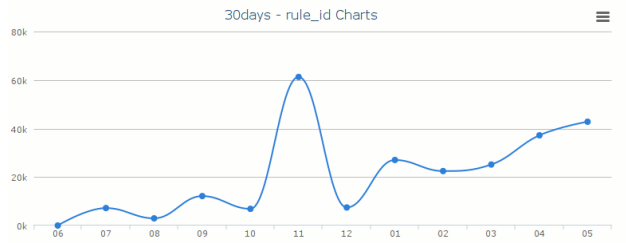
- WAF – Protect your Interwebs

  Schutz vor Schmutz
  White/Blacklisting
  Signatur-basiert
  Profiling
  - browserbasierte Webapps
  - APIs

  Hotpatching

- Contra

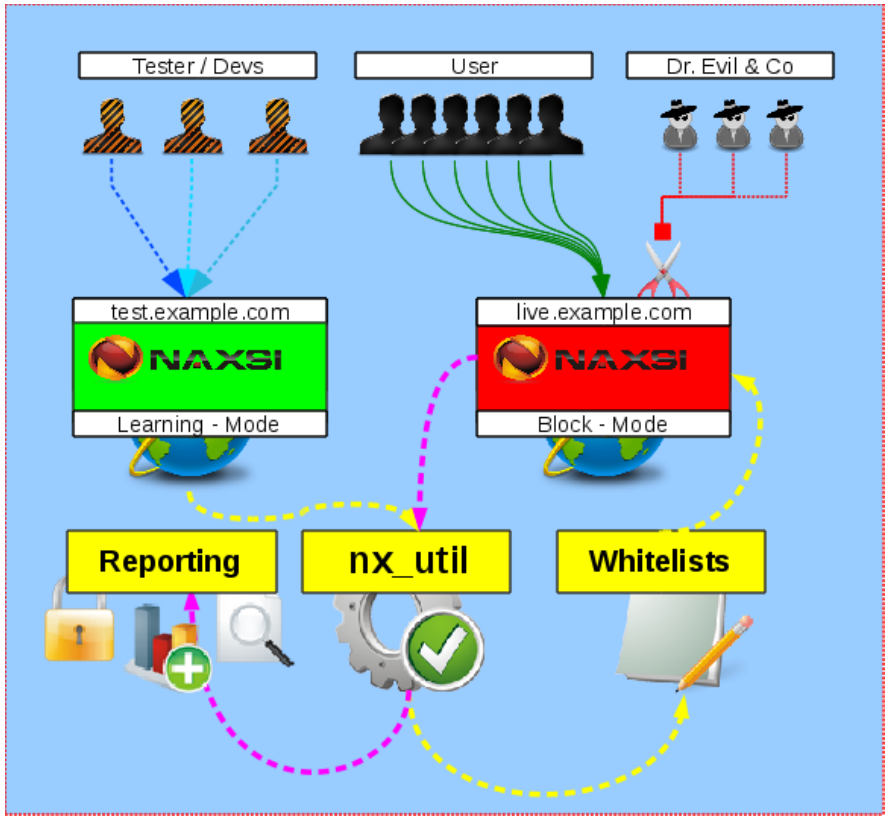
  Implementierung
  Change-Management
  unbekannte Angriffsvektoren
  immer einen Schritt hinterher
  Performance



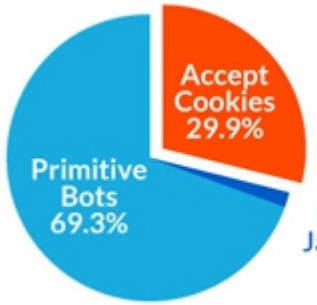

DX-Console Dashboard Latest Events | Filter | [ n: 3298 ] |

| | | |
|---|---|---|
| 34 | 42000082 | DN WEB_SERVER Tomcat - Manager - Access |
| 33 | 42000032 | DN WEB_SERVER PHP-EVAL - Attempt |
| 33 | 42000227 | DN SCAN Scanner ZmEu exploit scanner |
| 29 | 42000020 | DN APP_SERVER ASPX_file access |
| 29 | 42000021 | DN WEB_SERVER Tilde in URI, potential .php source disclosure vulnerability |
| 25 | 42000203 | DN SCAN Scanner Paros Proxy Scanner |
| 24 | 42000285 | DN WEB_SERVER Joomla JCE-Exploit-Scan |
| 22 | 1103 | php:// scheme |
| 22 | 42000003 | DN APP_SERVER ASP_file access |
| 20 | 2 | 2 |
| 20 | 42000305 | DN SCAN Possible HNAP-Exploit-Attempt |
| 19 | 42000002 | DN APP_SERVER PHP-file-access |
| 17 | 42000337 | DN WEB_SERVER PHP-CGI-Scan |
| 14 | 1402 | Content is neither mulipart/x-www-form.. |
| 13 | 42000073 | DN SCAN Python-urllib UA, possible Scanner |
| 13 | 42000311 | DN SCAN poss. malicious Scanner using Fake UA Apache/Synapse |
| 13 | 42000319 | DN SCAN Possible WHMCS - Scan |
| 12 | 1004 | mysql comment (*/) |
| 12 | 42000077 | DN WEB_SERVER LIBWWW_perl-UA detected |
| 12 | 42000310 | DN SCAN Abnormal double http:// in HTTP header, |

- Mod-Security
  Apache
  ausgereift
  Core-Rule-Set
  sehr komplex
  hoher Aufwand für Regeln + Whitelisting
- Naxsi
  Nginx
  stabil
  Core-Rule-Set
  einfach
  Learning-Mode, Reporting-Tool, Whitelisting
- Lua-WAF
  Nginx
  Profile, Logik, all you can Script



- Layer 7 DDoS
  legitime Requests
  App-Server überfluten → Ressourcen verbrauchen
  ca 20% der DDoS-Attacken sind L7-Attacken (Imperva)
  Bots werden intelligenter




Number of DDoS bot visitors has increased by more than **240%** during the last 12 months.

- Schutzmaßnahmen
  Monitoring + Notfallplan
  JS-Canary/Cookie
  Ratelimits (bedingt)
  Request-Shaping (bedingt)
  IP-Block vs Request-Block

- SSL + TLS
  Authentizität der Verbindung
  Transport-Verschlüsselung
  ganz oder garnicht
  HSTS
  SPDY
  PFS

- Contra
  Performance
  Kompatibilität
  might break stuff

- Tools
  testssl.sh
  ssllabs.com

# Fragen?