Lynt SERVICES

Bezpečnost Wordpressu

Vláďa Smitka

vladimir.smitka@lynt.cz

@smitka (ale skoro nic nepíšu)

Lynt services s.r.o.

Skrytá reklama

Kvalita správce online kampaní je přímo úměrná počtu beanbagů od Google* ;-)

* maximum v ČR jsou 2 a ty mají jen 2 firmy

Kdo jste?

Správci serverů

- Spravuji firewall
- Nastavuji Apache/Nginx/IIS

Vývojáři

- Upravuji si šablony a pluginy v PHP
- Píšu si vlastní doplňky

Uživatelé

- Koupím šablonu, nahraji pár pluginů
- Jen si upravuji texty, zbytek řeší někdo jiný

Lynt SERVICES

6 nejlepších rad

Aktualizujte

Zálohujte

Používejte bezpečnostní plugin

Buďte opatrní

Smažte, co nepotřebujete

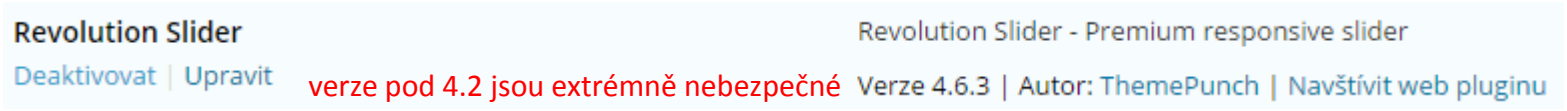
Nedávejte světu moc informací

Největší hrozba

Otázka: „Jaká je podle tebe aktuálně největší bezpečnostní hrozba Wordpressových webů?“

Odpověď: „Neaktualizovaný Slider Revolution.“

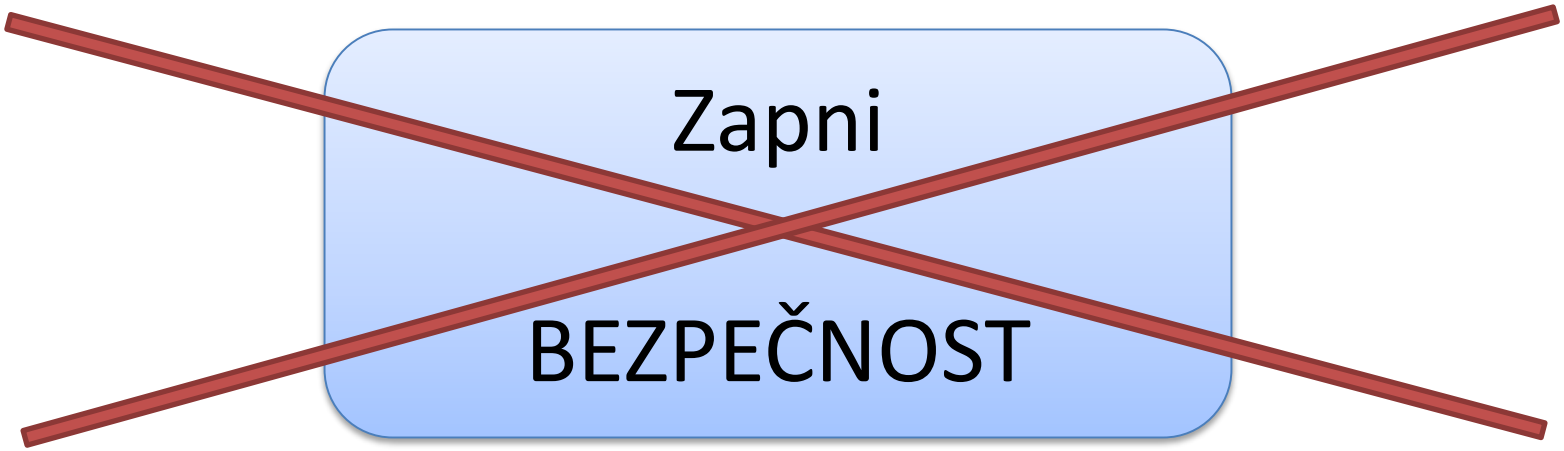
- Pravděpodobně nejčastěji kradený plugin
- Součást mnoha šablon, kde je však bez podpory a updatů
- Neobsahuje autoupdate – nutno aktualizovat ručně!
- Prvek, který se velmi snadno pozná



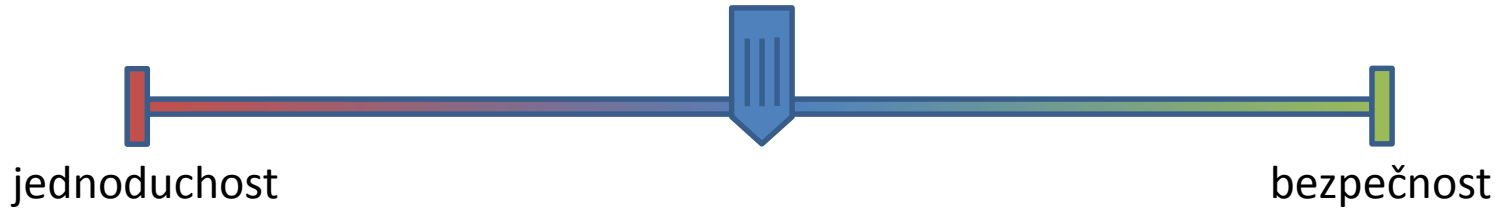
http://blog.sucuri.net/2014/09/slider-revolution-plugin-critical-vulnerability-being-exploited.html

Lynt SERVICES

Bezpečnost

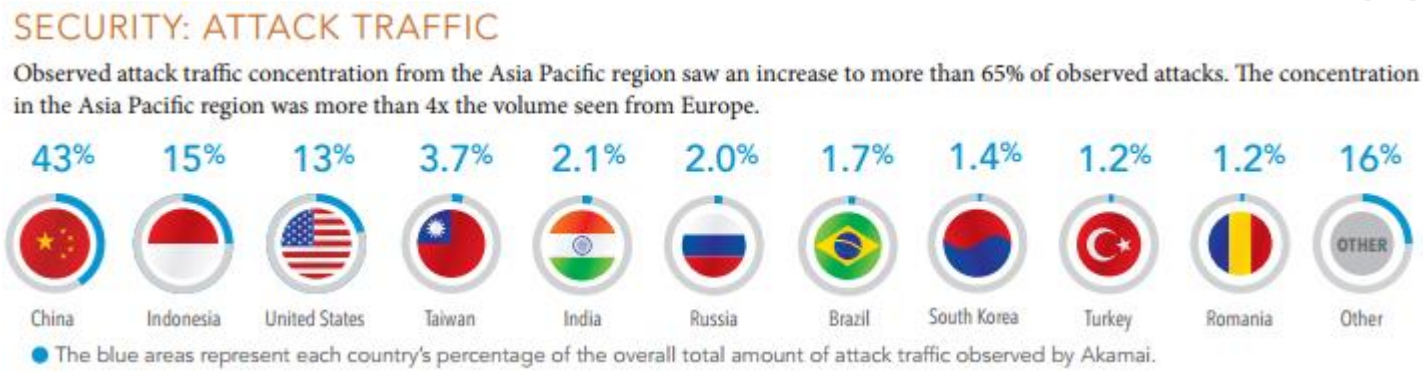


Bezpečnost



Co je bezpečné dnes, nemusí být bezpečné zítra.

Fakta



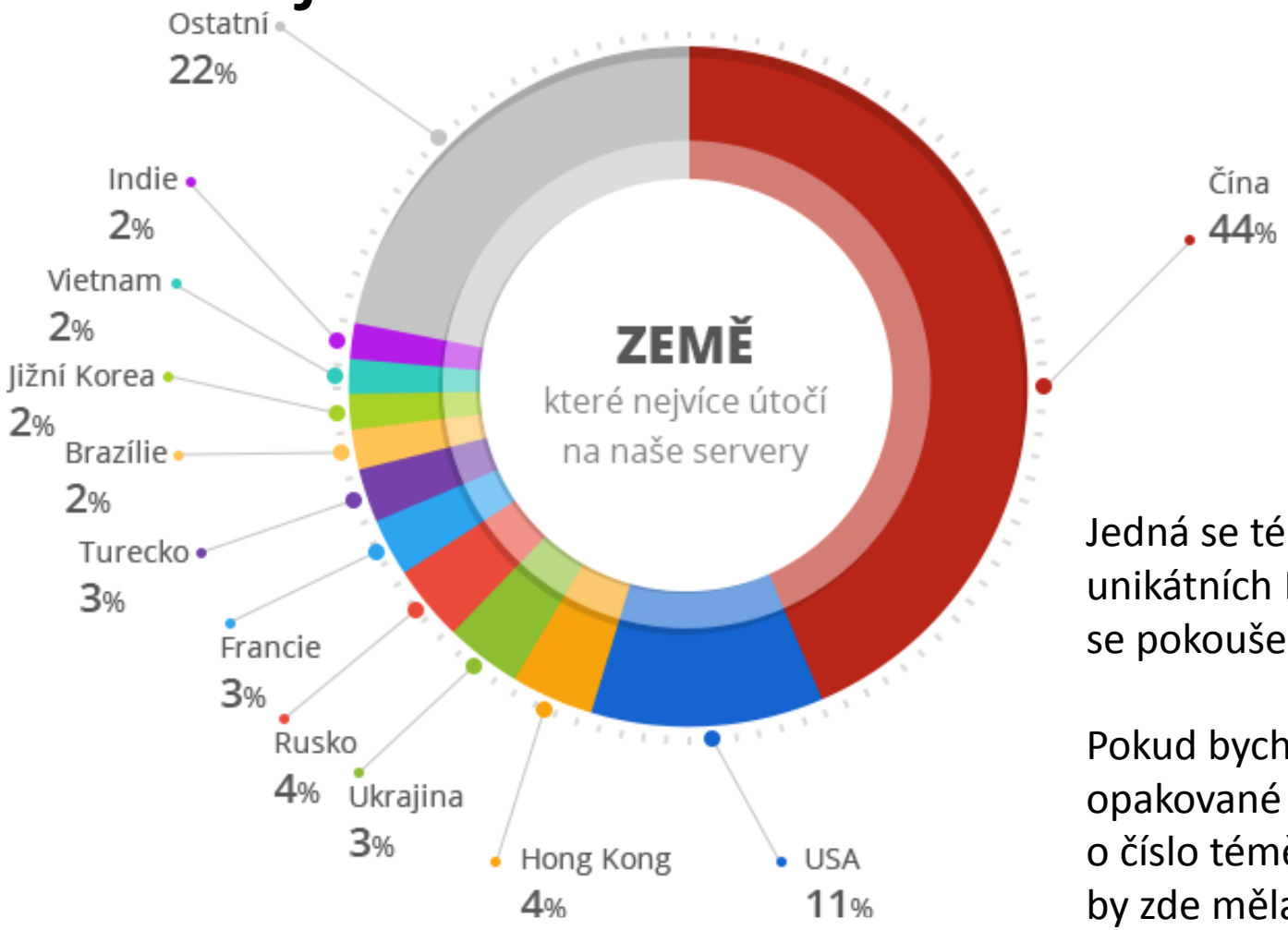
http://www.akamai.com/stateoftheinternet/

43% útoků přichází z Číny
Potřebuji čínský traffic?
Nemělo by smysl celou Čínu zablokovat?

Zablokovat USA?
Spíše ne, můžu zablokovat vyhledávače, CDN…

Zablokovat vše mimo ČR?
Určitě ne. IP geolokace není 100% přesná.
Firemní uživatelé se mohou připojovat přes centrálu v jiné zemi.
Čeští uživatelé mohou přistupovat např. z dovolené (dovolená v Číně?).

Poslední měsíc na jednom z našich serverů



Jedná se téměř o 1000 unikátních IP adres, které se pokoušely lámat hesla.

Pokud bychom zahrnuli opakované útoky, jedná se o číslo téměř 3x větší. Čína by zde měla 56% podíl.


NO, THANKS!

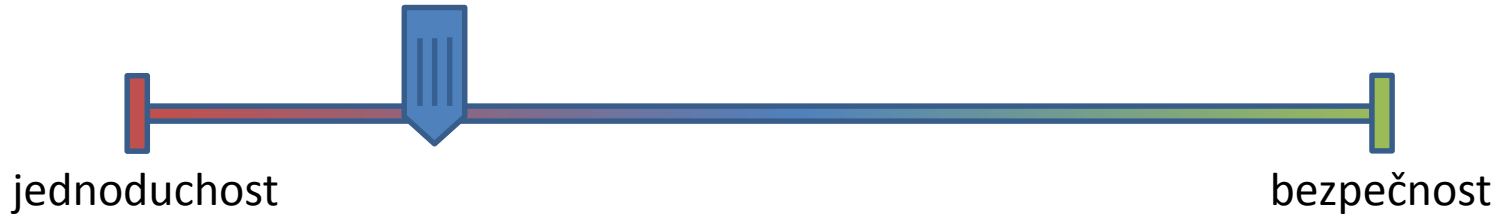
Jak zablokovat Čínu?

Seznam IP adres: http://www.ip2location.com/blockvisitorsbycountry.aspx

- Iptables
  - Nepoužívat vygenerovanou konfiguraci – tisíce pravidel, skrze které musí projít každý packet
  - iptables -A INPUT -m tcp -m state --state NEW -j CHINA_WALL
  - Pokročilé: optimalizace – více chainů podle části IP
- .htaccess/konfigurace nginx
- mod_geoIP
- Pluginy (např. placený Wordfence)
- HW krabička

- Další varianta – přístupy z blokovaných zemí přesměrovat na stránku s CAPTCHA

Aktualizovaný Wordpress v základu

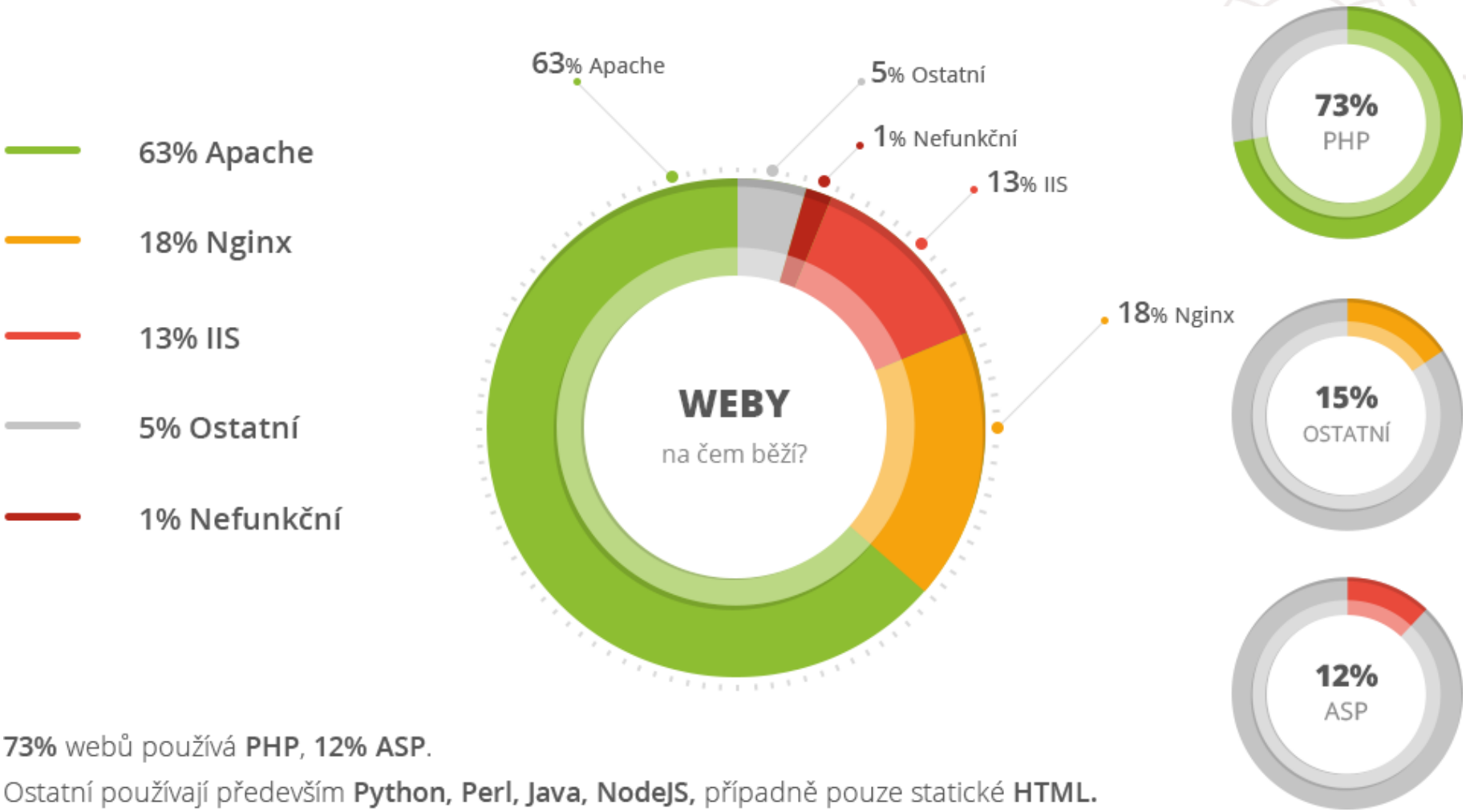


Jak jsme na tom s WP v ČR?

- Udělal jsem průzkum 1000 nejnavštěvovanějších českých webů
- Zkoumal jsem, jaké technologie používají a kolik z nich běží na Wordpressu
- Pro hrubé zhodnocení bezpečnosti jsem zkoumal, jakou verzi WP používají
- Namátkově jsem několik webů prozkoumal podrobněji

Lynt SERVICES

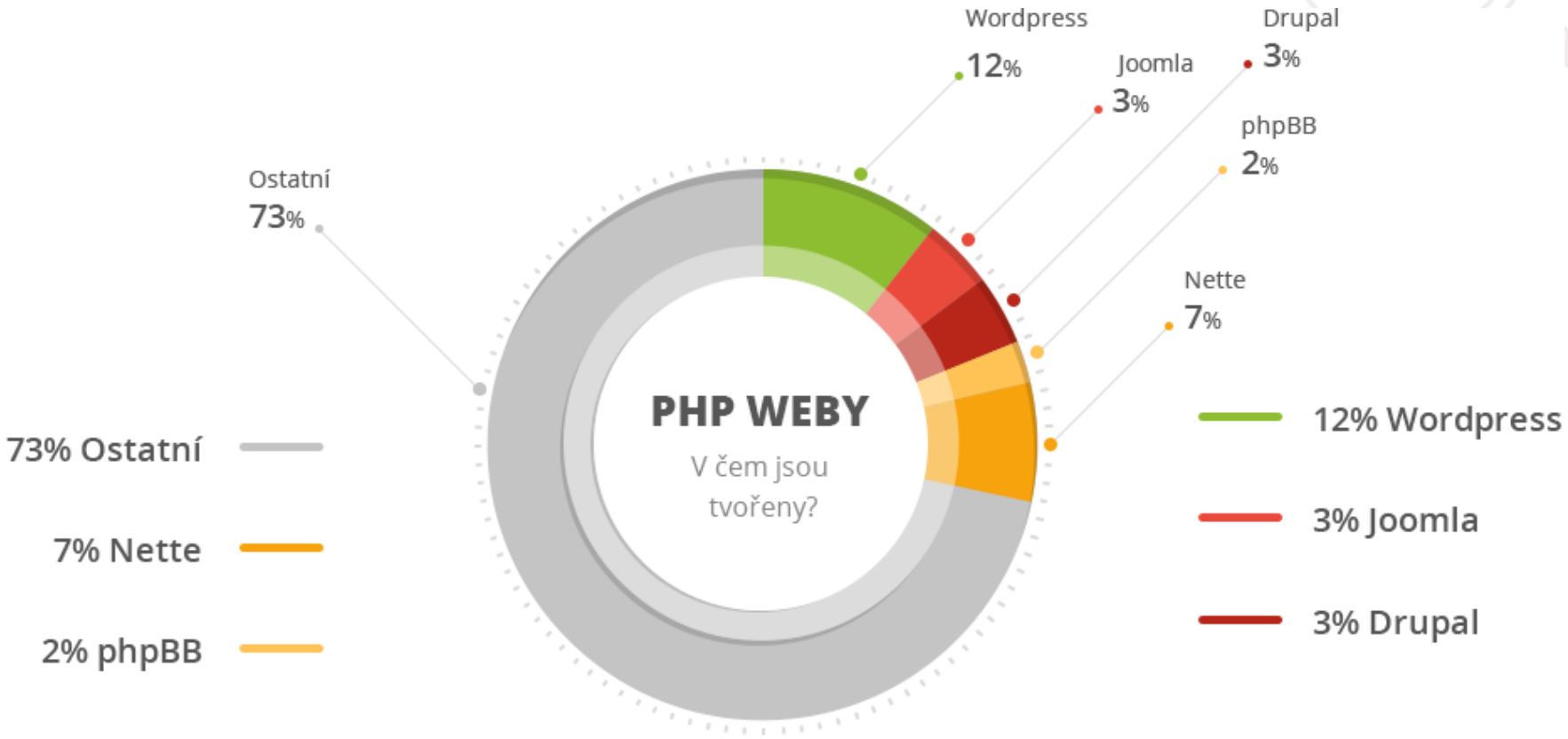
Technologie webů



73% webů používá **PHP**, **12% ASP**.

Ostatní používají především **Python, Perl, Java, NodeJS,** případně pouze statické **HTML.**

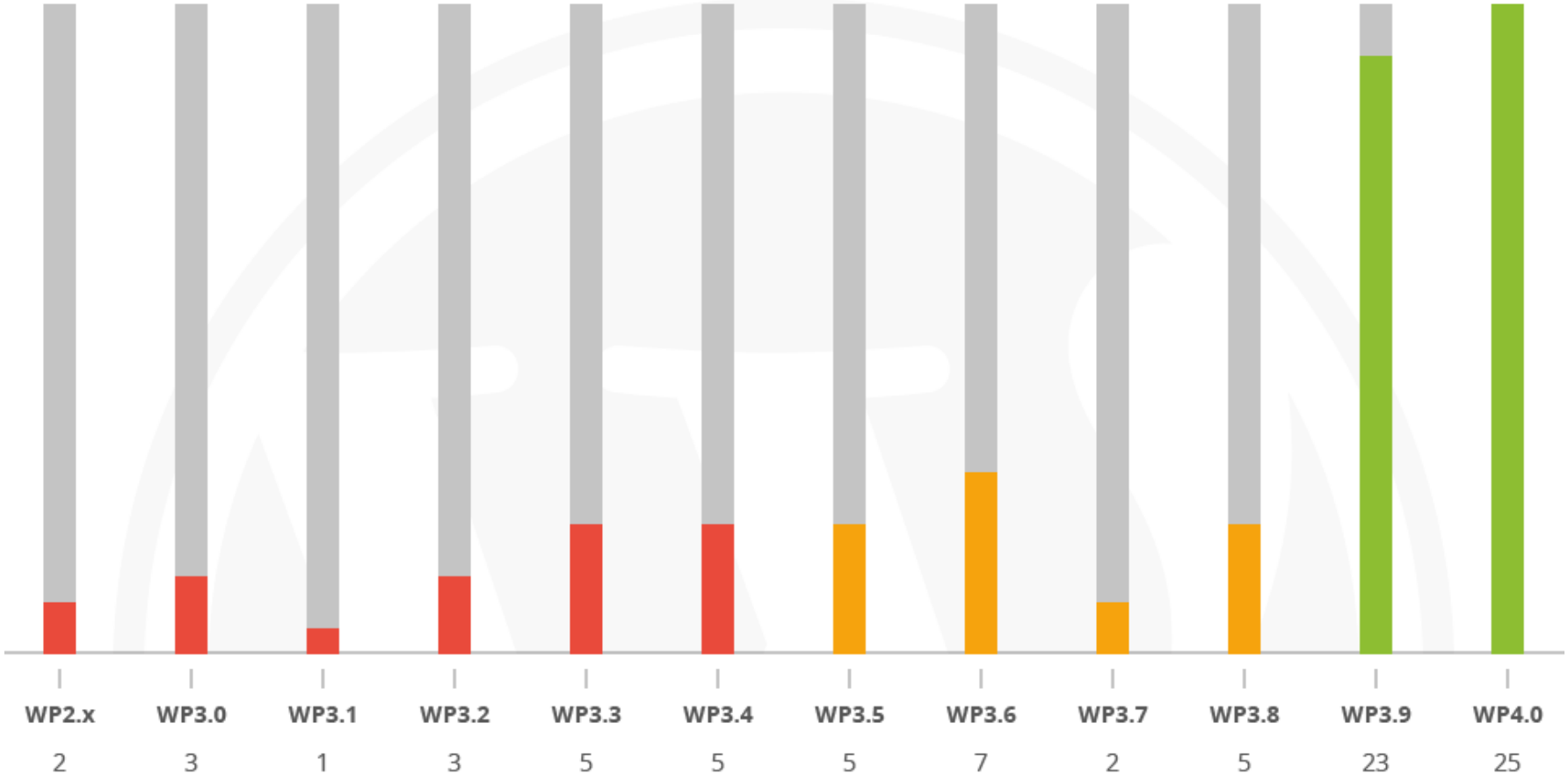
CMS a frameworky



Z těchto **73% webů na PHP** používá **12% Wordpress** (více než 80 webů z tisíce testovaných) – je tak s přehledem nejrozšířenějším z „velkých" CMS. Velká část webů používá také **PHP Framework Nette.** V části „ostatní" jsou většinou velké weby dělané na míru, nebo jejich autoři dbali na skrytí používaných technologií.

Lynt SERVICES

Verze Wordpress



Výsledky

Verzi jsem zjišťoval nejjednodušším možným způsobem - zadáním adresy /readme.html, případně /feed. Některé weby jsem dále zkoumal – nalezl jsem různé zranitelnosti typu SQL injections, LFI, XSS.

Více než polovina webů používá aktuální verze Wordpressu a jejich správci se starají o jejich aktualizaci. To však neznamená, že díky pluginům a šablonám neobsahují bezpečnostní chyby.

Téměř polovina nalezených webů používá zastaralou verzi Wordpressu a můžeme je považovat za nebezpečné.

Našel jsme dokonce několik webů, které používají více než 7 let starý Wordpress verze 2.

Téměř polovina Wordpress webů je potenciálně nebezpečná!
Aktualizujte!

Další info (článek + infografika): http://lynt.cz/blog/ceske-weby-a-wordpress

Neaktualizovaný Wordpress s pluginy

Lynt SERVICES

Readme.html

WordPress

Version 3.0.4

Semantic Personal Publishing Platform

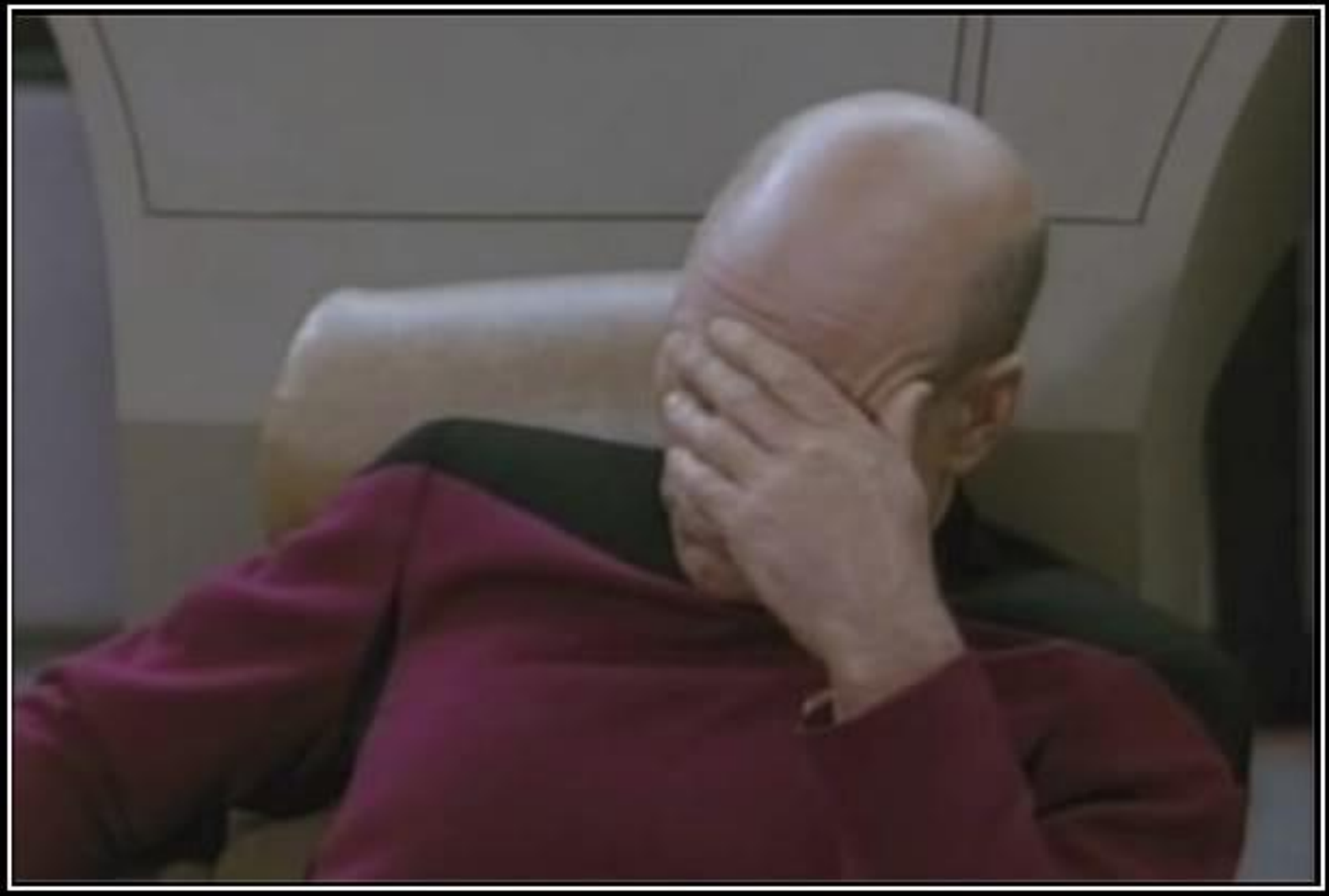
First Things First

Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and together we create something beautiful that I'm proud to be a part of. Thousands of hours have gone into WordPress, and we're dedicated to making it better every day. Thank you for making it part of your world.

— Matt Mullenweg

Installation: Famous 5-minute install

1. Unzip the package in an empty directory and upload everything.
2. Open wp-admin/install.php in your browser. It will take you through the process to set up a `wp-config.php` file with your database connection details.



FACEPALM

Because expressing how dumb that was in words just doesn't work.

Readme.html

WordPress

Version 2.0

Semantic Personal Publishing Platform

First Things First

Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and together we create something beautiful that I'm proud to be a part of. Thousands of hours have gone into WordPress, and we're dedicated to making it better every day. Thank you for making it part of your world.

— Matt Mullenweg

Installation: Famous 5-minute install

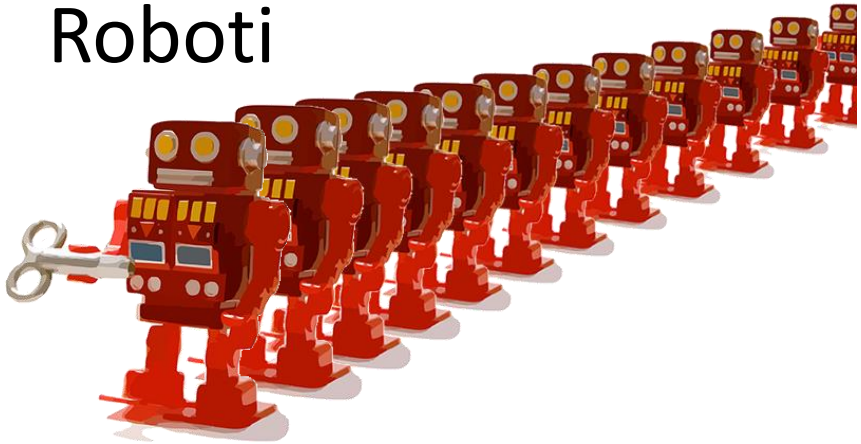
1. Unzip the package in an empty directory
2. Open up `wp-config-sample.php` with a text editor like WordPad or similar and fill in your database connection details
3. Save the file as `wp-config.php`
4. Upload everything.
5. Open /wp-admin/install.php in your browser. This should setup the tables needed for your blog. If there is an error, double check your wp-config.php file, and try again. If it fails again, please go to the support forums with as much data as you can gather.
6. **Note the password given to you.**

DOUBLE FACEPALM

FOR WHEN ONE FACEPALM DOESN'T CUT IT

Kdo

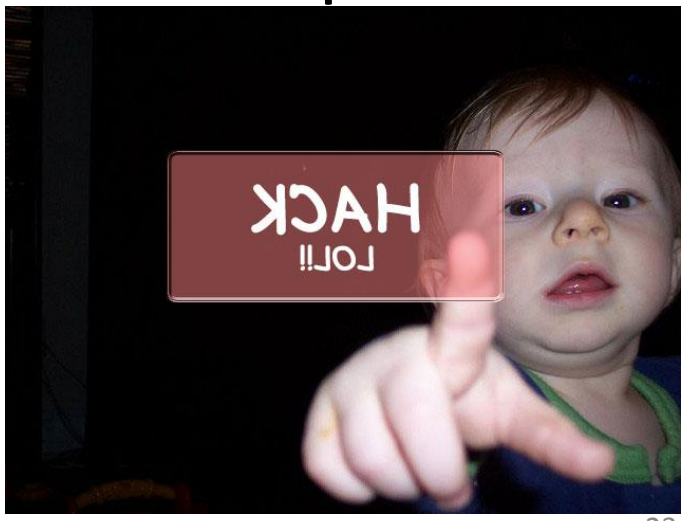
Roboti



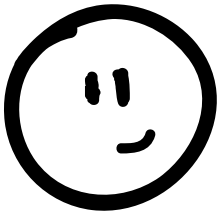
Anonymní hackeři

Motivovaní hackeři

Děti - script kiddies



Co



Vložení svého odkazu

Vložení svého javascriptu

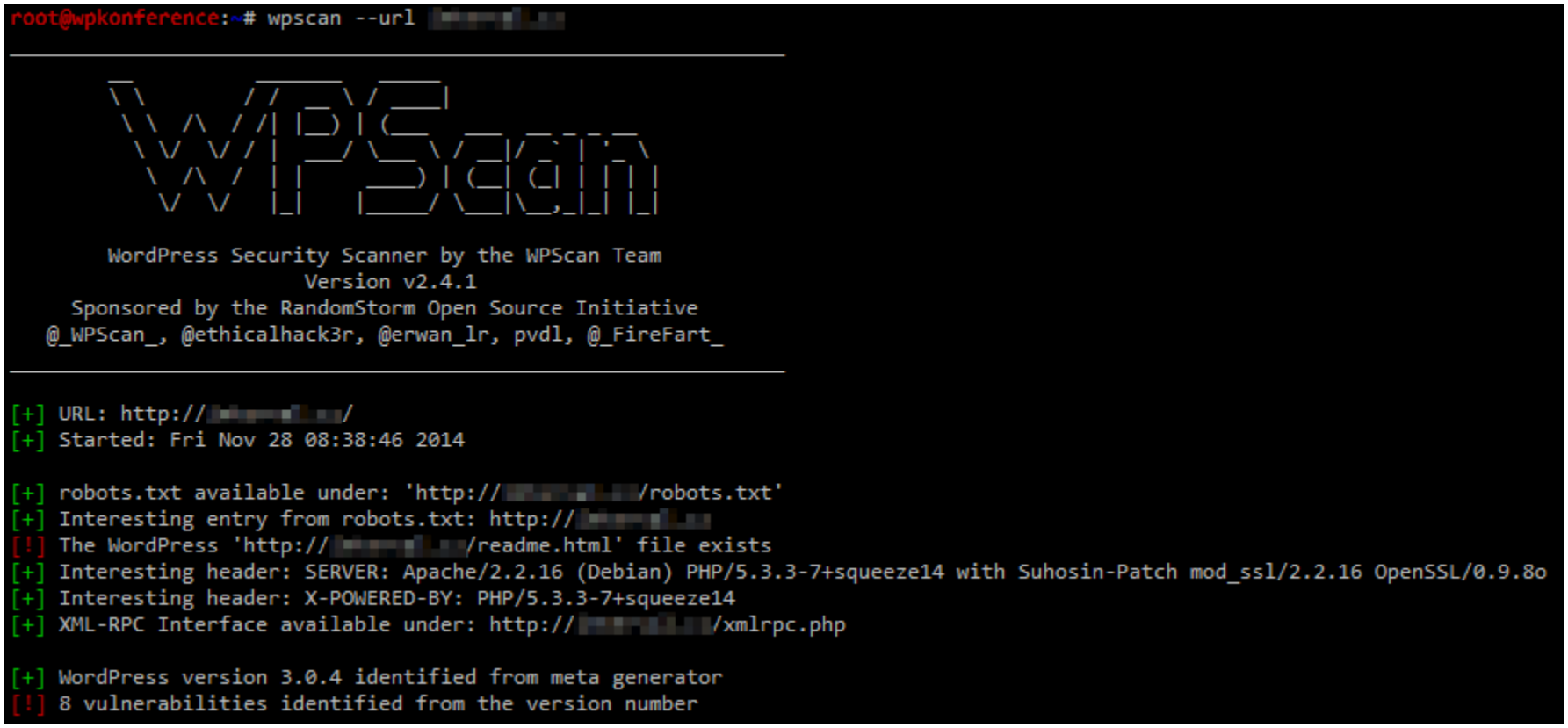
Získání dat uživatelů

Získání wp-config.php

Nahrání vlastního PHP kódu

Průzkum / Reconnaissance

- Počáteční fáze útoku – nejdůležitější a často nejdelší
- Při útoku na WP se nejčastěji používá nástroj WPscan



WPscan

-Do 'non-intrusive' checks ...

ruby ./wpscan.rb --url www.example.com

-Do wordlist password brute force on enumerated users using 50 threads ...

ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --threads 50

-Do wordlist password brute force on the 'admin' username only ...

ruby ./wpscan.rb --url www.example.com --wordlist darkc0de.lst --username admin

-Enumerate installed plugins ...

ruby ./wpscan.rb --url www.example.com --enumerate p

-Enumerate installed themes ...

ruby ./wpscan.rb --url www.example.com --enumerate t

-Enumerate users ...

ruby ./wpscan.rb --url www.example.com --enumerate u

-Enumerate installed timthumbs ...

ruby ./wpscan.rb --url www.example.com --enumerate tt

-Use a HTTP proxy ...

ruby ./wpscan.rb --url www.example.com --proxy 127.0.0.1:8118

-Use a SOCKS5 proxy ... (cURL >= v7.21.7 needed)

ruby ./wpscan.rb --url www.example.com --proxy socks5://127.0.0.1:9000

SQL injection

Příklad nebezpečného dotazu:
SELECT * FROM users WHERE (jmeno="{$_GET["jmeno"]}") AND (heslo="{$_GET["heslo"]}")

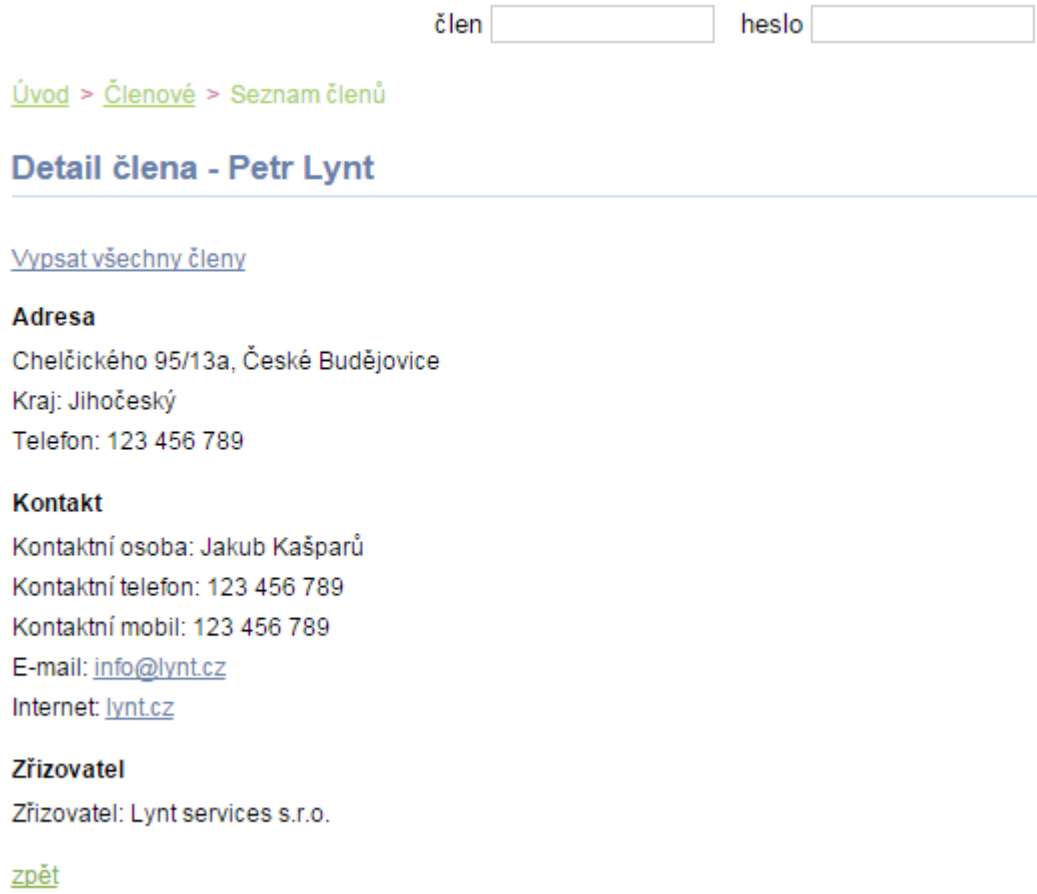
http://mojeapka.xy/prihlasit.php?jmeno=admin")#
SELECT * FROM users WHERE (jmeno="admin")#") AND (heslo="")
znak # značí komentář – zakomentuje zbytek dotazu => příkaz se nedostane k ověření hesla

http://mojeapka.xy/prihlasit.php?jmeno=admin&heslo=" OR "1"="1
SELECT * FROM users WHERE (jmeno="admin") AND (heslo="" OR "1"="1")
hledá uživatele se jménem admin a ověřuje, zda jeho heslo odpovídá zadanému, nebo zda 1=1 => splněno vždy ☺

mysql_real_escape_string() – pro řetězce
inval() – pro čísla
MySQL prepared statements

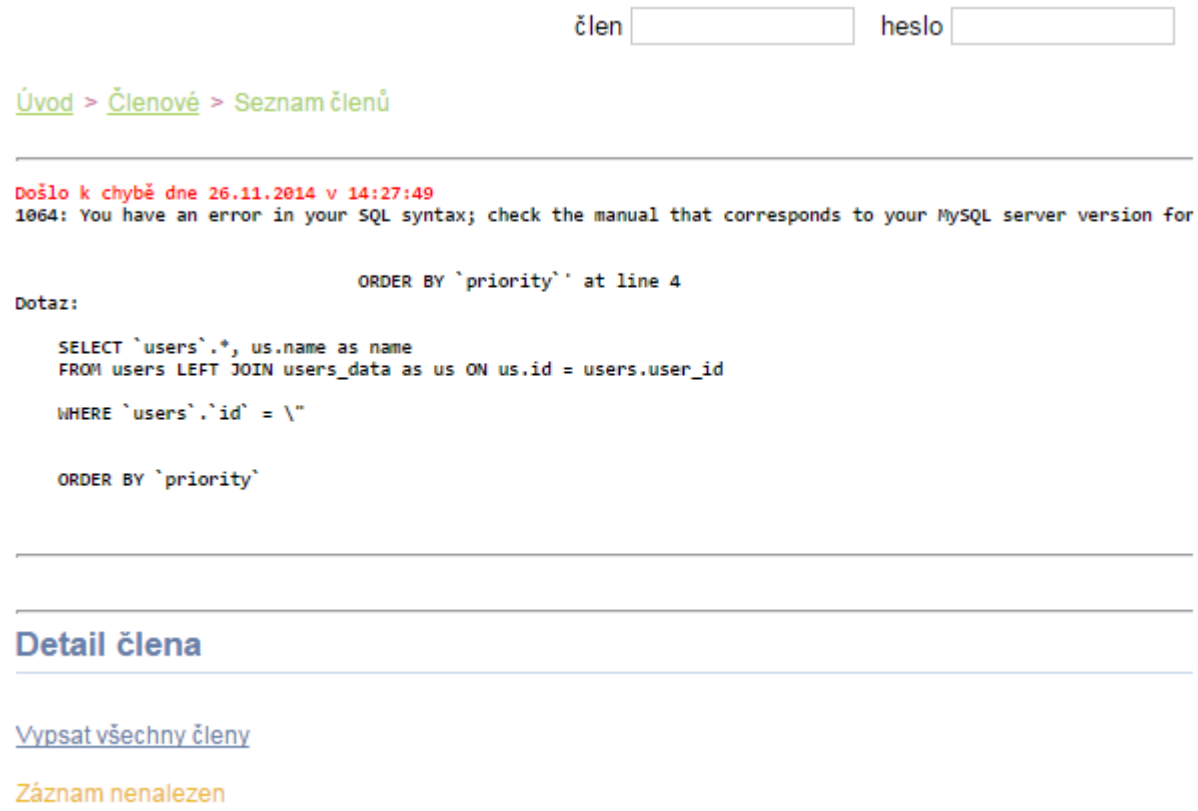
SQL injection

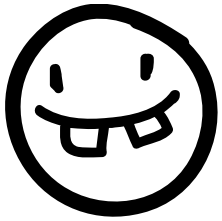
/clenove/seznam/&id=666



SQL injection

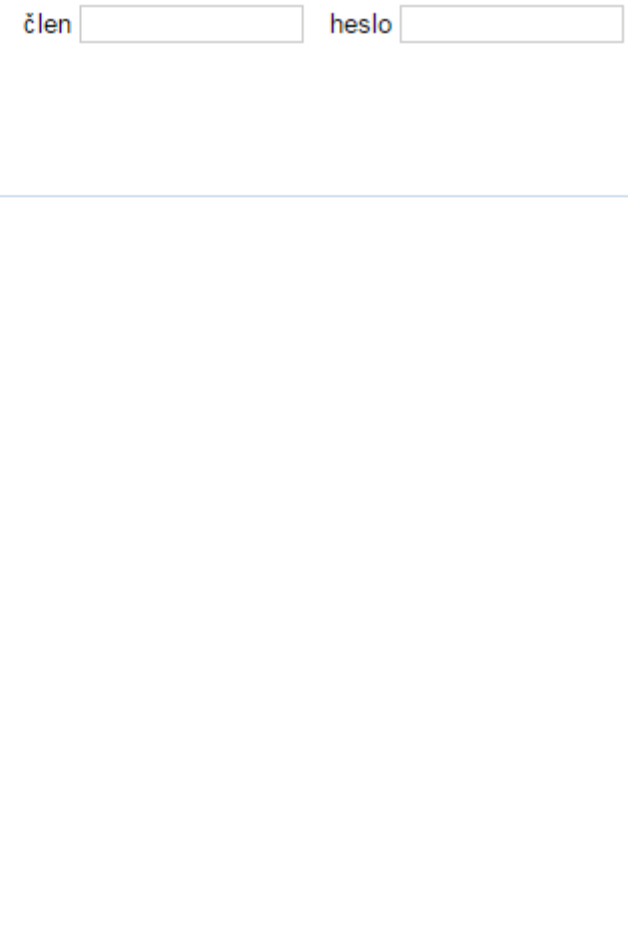
/clenove/seznam/&id="





SQL injection

/clenove/seznam/&id=0 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27 from users



SQL injection

/clenove/seznam/&id=0 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,name,pass,20,21,22,23,24,25,26,27 from users where id=666

člen heslo

Úvod > Členové > Seznam členů

Detail člena - 25

Vypsat všechny členy

Adresa

Adresa: 7, 10, 8, okres 9
Kraj: Praha
Telefon: 12

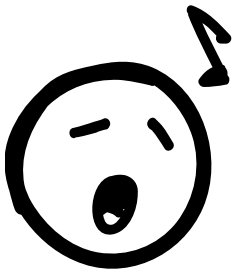
Kontakt

Kontaktní osoba: 13
Kontaktní telefon: 14
Kontaktní mobil: 15
E-mail: 16
Internet: 23

Zřizovatel

Zřizovatel: lyntik
Adresa: 955db0b81ef1989b4a4dfeae8061a9a6

zpět



Nevýhoda opensource řešení:
Útočník dopředu zná strukturu databáze – jména tabulek, počty a jména sloupců

Proto je dobré změnit prefix databáze.

Blind SQL injection

- Někdy se výsledek dotazu nikam nevypisuje, ani mi nezajistí přístup
- Pomocí UNION SELECT se lze ptát databáze na otázky s odpovědí ANO/NE

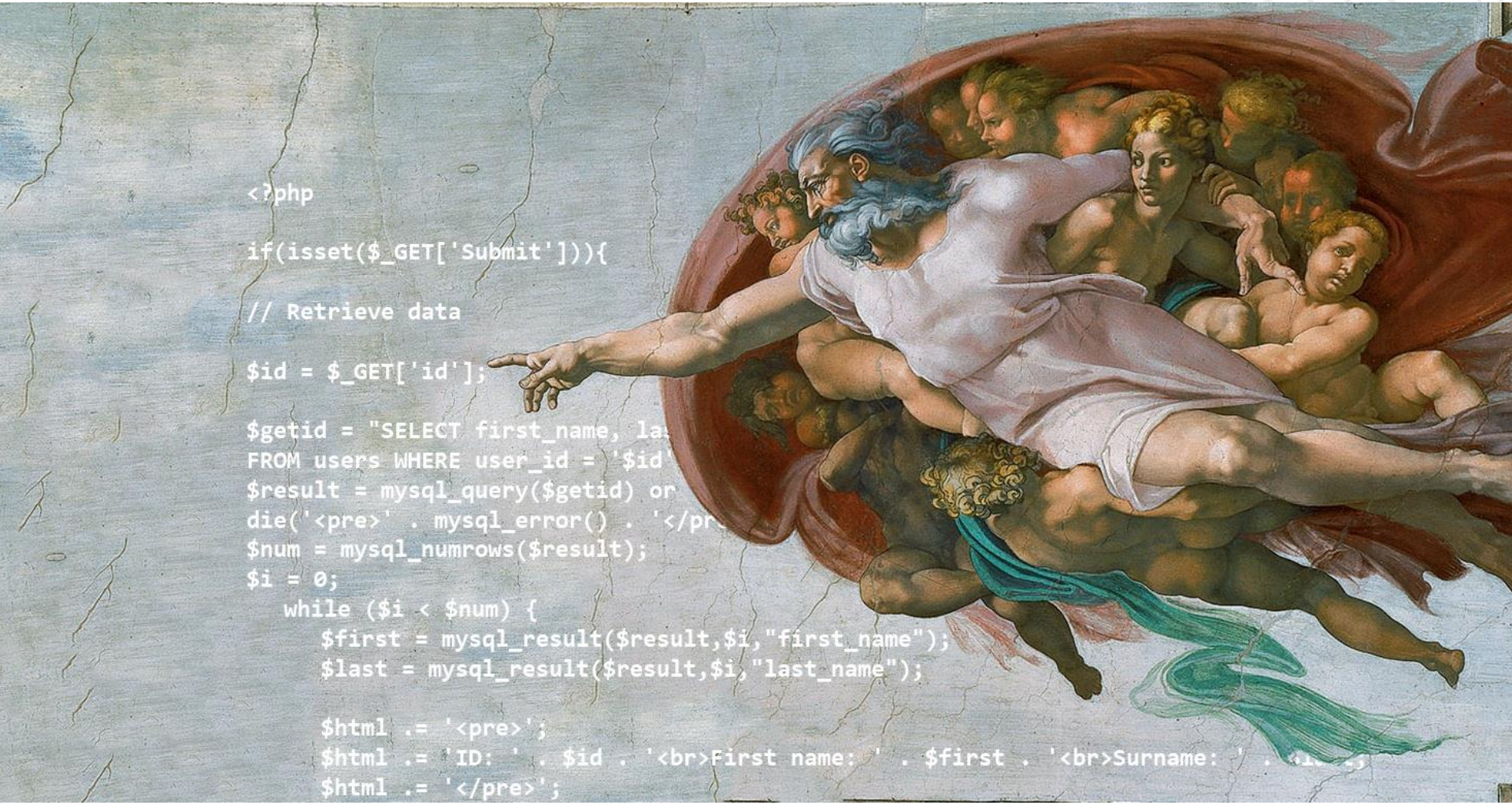
- Content based:
  /clenove/seznam/&id=666 AND 1=1 => stránka s výsledkem
  /clenove/seznam/&id=666 AND 1=2 => stránka bez výsledků

- Time based:
  SELECT IF(1=1, BENCHMARK(1000000,MD5('lynt')),NULL) FROM tabulka

- Je první písmenko hesla „A“?

- Automatizace nástrojem SQLmap

„SQL injection je umění“



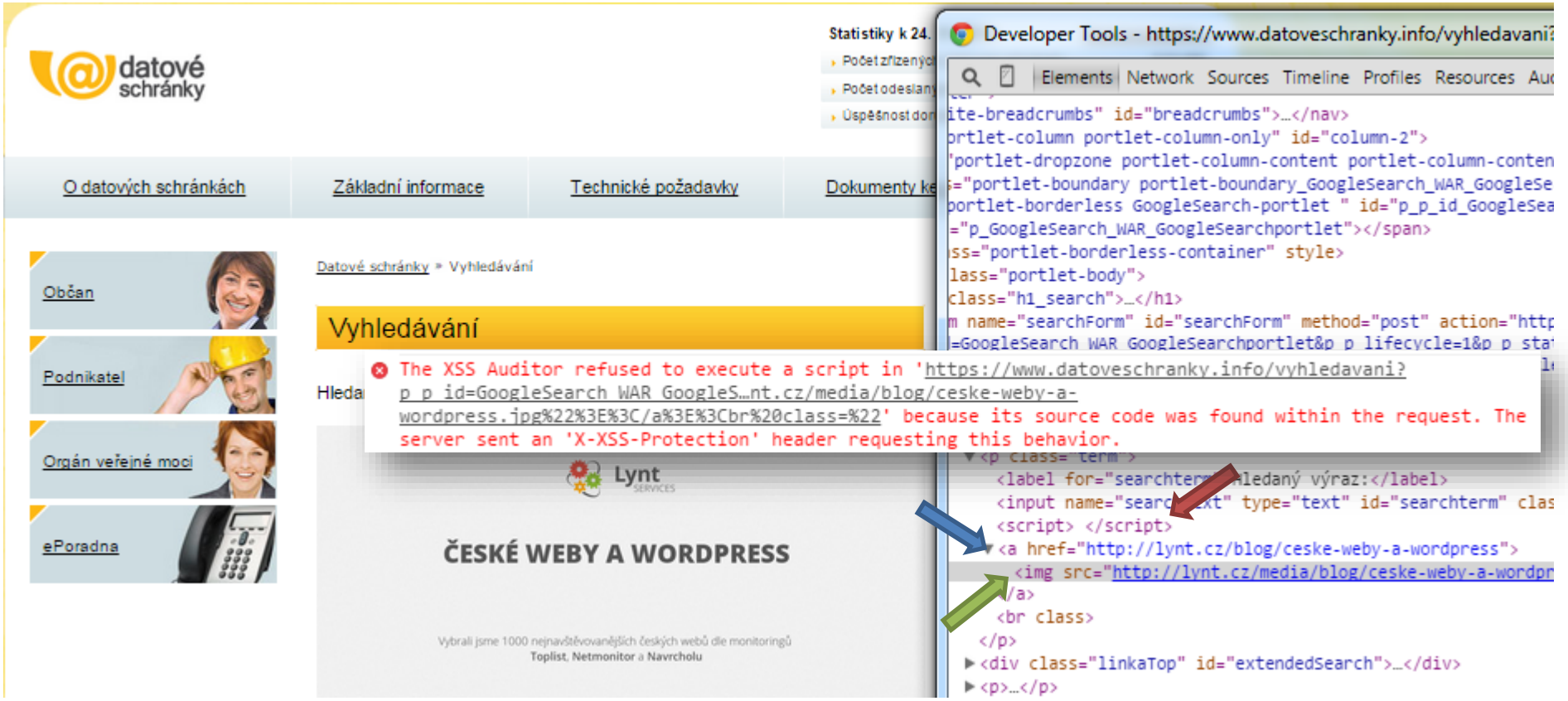
XSS

- Podaří se mi do stránky vložit nějaký svůj kód – nejčastěji javascript
- Persistentní (např. v komentářích) vs. dočasný (pomocí URL parametrů) – ty však mohu dále propagovat
- V moderních prohlížečích mohu použít HTTP hlavičku X-XSS-protection

- https://www.owasp.org/index.php/List_of_useful_HTTP_headers

XSS

https://www.datoveschranky.info/vyhledavani?p_p_id=GoogleSearch_WAR_GoogleSearchportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_GoogleSearch_WAR_GoogleSearchportlet_javax.portlet.action=searchForm&searchtext=%22%3E%3Cscript%3Ealert(%22hack%22)%3E%3C/script%3E%3Ca%20href=%22http://lynt.cz/blog/ceske-weby-a-wordpress%22%3E%3Cimg%20src=%22http://lynt.cz/media/blog/ceske-weby-a-wordpress.jpg%22%3E%3C/a%3E%3Cbr%20class=%22



Bezpečnostní plugin

iThemes security

- Global Settings
  - **Write to Files** - Allow iThemes Security to write to wp-config.php and .htaccess – pokud nepovolím, mohu příslušné sekce nakopírovat z dashboardu pluginu
  - **Lockout White List** – vhodné zadat svou IP
  - **Log Type** - Database Only (malé weby, log je pak dostupný na záložce Logs), File Only (velké weby, vhodné také pro zpracování fail2ban)
  - **Path to Log Files** - cesta k logům při File Only, pokud je možnost přístupu mimo složku webu, tak je umístit mimo, pokud ne, lze nechat výchozí (lépe ale jméno složky změnit)
- 404 detection
  - **Enable 404 detection** – zablokuje násilné skenování

Červené = dle mého názoru nejdůležitější nastavení

iThemes security

- Away Mode - možno nastavit dostupnost administrace např. jen na pracovní dobu...
- Banned Users
  - **Default Blacklist** - Enable HackRepair.com's blacklist feature - možno povolit - přidá známé útočící useragenty do .htaccess
  - **Enable ban Users** - můžeme si dodefinovat vlastní blokované useragenty a IP (spolupracuje s Enable Blacklist Repeat Offender v Global settings)

iThemes security

- Brute Force Protection
  - **Get your iThemes Brute Force Protection API Key** - iThemes získá přístup k globálnímu blacklistu útočících IP adres na iThemes.com
  - **Enable iThemes Brute Force Network Protection** – povolí ochranu dle globálního blacklistu
  - **Enable local brute force protection** - blokuje hádání hesel do administrace – tvoří vlastní blacklist (blokace jsou uloženy v tabulce _itsec_lockouts)
  - **Automatically ban "admin" user** - Immediately ban a host that attempts to login using the "admin" username - pokud mám přejmenovaného admina, tak to může být dobrá nástraha ☺ - jakmile se někdo pokusí přihlásit jako uživatel admin, je okamžitě zablokován

iThemes security

- Database Backups
  - **Backup Method** - Email Only (bude posílat zálohu mailem), Save local only - pouze pokud mohu uložit zálohu mimo složku webu (Backup Location)
  - **Schedule Database Backups** - Enable Scheduled Database Backups – automatické vytváření záloh/jinak pouze ručně na záložce Backups
  - Zálohuje pouze DB. Raději bych použil jiné zálohovací řešení mimo WP i se soubory.

- File Change Detection
  - **File Change Detection** - Enable File Change detection
  - **Split File Scanning** - Split file checking into chunks – vhodné pokud mám méně RAM - generuje ale více emailů
  - **Files and Folders List** - pokud používáme cachovací plugin, tak je vhodné zde jeho složku vyjmout

- Hide Login Area
  - **Hide Backend**- Enable the hide backend feature – přesměruje /wp-admin na jinou adresu
  - **Login Slug** – nová adresa administrace - např. admin5547, nebo česky administrace
  - **Enable Theme Compatibility** - Enable theme compatibility – zapnout, pokud přesměrování administrace způsobí nefunkčnost některých šablon a pluginů
  - Přesměrování administrace je dobré dělat až v druhé vlně ladění - neprovádět více změn naráz

iThemes security

- Malware Scanning
  - **Enable Malware scanning** - po vložení API klíče z VirusTotal.com může nechat jednorázově otestovat homepage, zda se nenachází na cca 60 blacklistech (Sucuri SiteCheck, Google Safebrowsing,...)
- Secure Soceket Layers (SSL)
  - nastavení pro vynucení SSL přístupu do administrace - vhodné nejprve otestovat, zda je administrace přes https správně dostupná
- Strong Passwords
  - **Strong Passwords** - Enable strong password enforcement - Vynutí používání silných hesel (původní slabá hesla zůstávají)
  - **Select Role for Strong Passwords** - pro jaké role vyžadujete silná hesla (minimálně Šéfredaktor – může vkládat JS do komentářů, ale klidně už od Návštěvníka)

iThemes security

- System Tweaks
  - **System Files** - protect System Files - zakáže přístup z internetu přímo k důležitým souborům a k souborům, které prozrazují informace
  - **Suspicious Query Strings** - Filter Suspicious Query Strings in the URL - může zabránit jednoduchým SQL injections (pozor, chyba u nginx – viz další slidy)
  - **Long URL Strings** - Filter Long URL Strings - blokuje příliš dlouhé URL (nad 255 znaků), dále také blokuje URL obsahující funkce eval a base64 a union select (podobnou funkci plní samostatný plugin Block Bad Queries (BBQ))
    + je dobré přidat blokaci query obsahující wp-config.php
  - **File Writing Permissions** – nastaví práva pro .htaccess a wp-config.php – lepší si to nastavit sám a podrobněji
  - **Uploads** - Disable PHP in Uploads – zakáže PHP ve složce s uploady

iThemes security

- System Tweaks
  - **Generator Meta Tag** + **Display Random Version** - pokusí se zamaskovat verzi WP, jde to udělat lépe – viz další slidy
  - **Windows Live Writer Header** & **EditURI Header** – hlavičky pro integraci s dalšími službami a aplikacemi – jsou potřeba jen zřídka
  - **Comment Spam** - kontroluje, zda byl komentář vložen z našeho webu (případně z wordpress.com) + blokuje komentáře od botů, kteří nemají vyplněn user-agent
  - **File Editor** – vypne editor šablon a pluginů ve WP (lze to jednoduše udělat v wp-config)
  - **XML-RPC** - při "Completely Disable XMLRPC" zakáže veškeré XML-RPC požadavky, např. trackbacky (pro bezpečné použití trackbacků mohu použít plugin https://wordpress.org/plugins/simple-trackback-validation-with-topsy-blocker/)
  - **Login Error Messages** - přestane ukazovat hlášky o chybném přihlášení
  - **Force Unique Nickname** - nutí uživatele zvolit jiný nickname než je jeho přihlašovací jméno (není tak přímo vidět uživatelský účet)
  - **Disable Extra User Archives** - skryje uživatele, kteří nepíšou články (admini,...)

iThemes security

- „Pokročilé funkce“ – Advanced
  - **Admin user** – umožňuje přejmenovat uživatele admin na jiné, hůře odhadnutelné jméno
    - Lepší je vytvořit nového uživatele s admin právy, přihlásit se na něj a původního admina smazat (WP nabídne převedení jeho příspěvků na jiného uživatele)
  - **Change content directory** – přejmenování složky wp-content, může přinést problémy a brání pouze některým automatizovaným útokům (správnou složku lze jednoduše vyčíst z kódu stránky)
  - **Change database prefix** – pokud se nechal při instalaci default wp_, tak je možné ho zde změnit
    - Automatizovaný nástroj, ručně je to složitější

iThemes security - poznámky

- Suspicious Query Strings v nginx:

```
set $susquery 0;
if ($args ~* "wp-config.php") { set $susquery 1; } #navíc blokace při pokusu stažení wp-config.php
if ($args ~* "\.\./") { set $susquery 1; }
if ($args ~* "\.(bash|git|hg|log|svn|swp|cvs)") { set $susquery 1; }
if ($args ~* "etc/passwd") { set $susquery 1; }
if ($args ~* "boot.ini") { set $susquery 1; }
if ($args ~* "ftp:") { set $susquery 1; }
if ($args ~* "http:") { set $susquery 1; }
if ($args ~* "https:") { set $susquery 1; }
if ($args ~* "(<|%3C).*script.*(>|%3E)") { set $susquery 1; }
if ($args ~* "mosConfig_[a-zA-Z_]{1,21}(=|%3D)") { set $susquery 1; }
if ($args ~* "base64_encode") { set $susquery 1; }
if ($args ~* "(%24&x)") { set $susquery 1; }
if ($args ~* "(&#x22;|&#x27;|&#x3C;|&#x3E;|&#x5C;|&#x7B;|&#x7C;|%24&x)"){ set $susquery 1; }
if ($args ~* "(127.0)") { set $susquery 1; }
if ($args ~* "(globals|encode|localhost|loopback)") { set $susquery 1; }
if ($args ~* "(request|insert|concat|union|declare)") { set $susquery 1; }
if ($args !~ "^loggedout=true"){ set $susquery 0; } # <= špatná logika, má zde být ~*
if ($args !~ "^action=jetpack-sso"){ set $susquery 0; } # <= špatná logika, má zde být ~*
if ($args !~ "^action=rp"){ set $susquery 0; } # <= špatná logika, má zde být ~*
if ($http_cookie !~ "^.*wordpress_logged_in_.*$"){ set $susquery 0; } # <= špatná logika, má zde být ~*
if ($http_referer !~ "^http://maps.googleapis.com(.*)$"){ set $susquery 0; } # <= špatná logika, má zde být ~*
if ($susquery = 1) { return 403; }
```

Přidání blokace wp-config.php do .htaccess:
RewriteCond %{QUERY_STRING} wp-config.php [NC,OR]

iThemes security - poznámky

- Lepší odstranění viditelnosti verze WP:

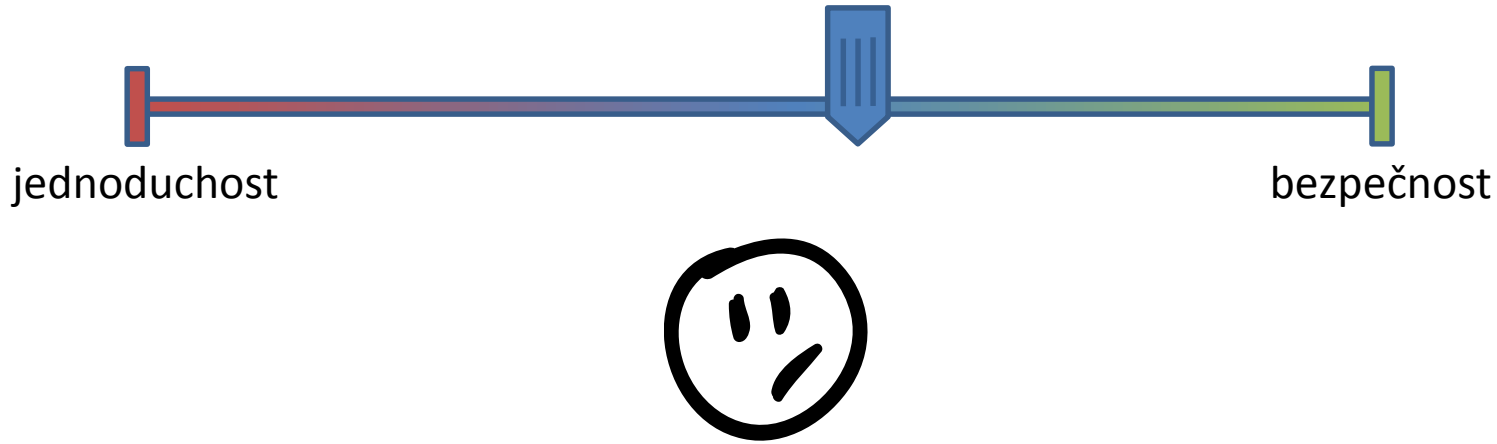
Do functions.php nebo plugin do mu-plugins:

```
function remove_wp_version()
{ return ; }
add_filter('the_generator', remove_wp_version');
```

Odbočka – MU-plugins (Must Use Plugins)
Málo známá funkcionalita WP – jedná se o speciální složku: **/wp-content/mu-plugins**
Skripty/pluginy v této složce jsou automaticky spouštěny a nelze je v administraci deaktivovat.
Hodí se to pro různá bezpečnostní nastavení, např. pokud chceme automatické updaty pluginů a šablon pomocí filtrů – mnoho autorů je dává do wp-config/functions.php – správně mají být zde.

```
add_filter( 'auto_update_plugin', '__return_true' );
add_filter( 'auto_update_theme', '__return_true' );
```

Použití bezpečnostního pluginu



FAIL2BAN

Fail2ban – pomocník na straně serveru

- Některé funkce bezpečnostního pluginu můžeme posunout o úroveň níže
- Např. detekci brutal force analýzou logů nebo 404 (může být dobré nelogovat statické soubory):

- **filter.d/wp-auth.conf**

```
# WordPress brute force auth filter: /etc/fail2ban/filter.d/wp-auth.conf:
#
# Block IPs trying to auth wp wordpress
#
# Matches e.g.
# 178.63.72.184 - - [16/Oct/2014:11:40:50 +0200] "POST /wp-login.php HTTP/1.0" 200 1531 "-" "-"
[Definition]
failregex = ^<HOST> .* "POST /wp-login.php
```

- **jail.conf**

```
[wp-auth]
enabled = true
filter = wp-auth
action = iptables-multiport[name=wp-auth, port="http,https", protocol=tcp]
         sendmail-whois[name=WPauth, dest=vladimir.smitka@lynt.cz, sendername="Fail2Ban"]
logpath = /var/log/wordpress/access.*.log
```

- Pozor na logrotate - /usr/bin/fail2ban-client reload wp-auth

Fail2ban – další triky

- Reverzní sociální inženýrství
- Fail2ban může hlídat logy na předem připravené nástrahy

- Nástraha v robots.txt

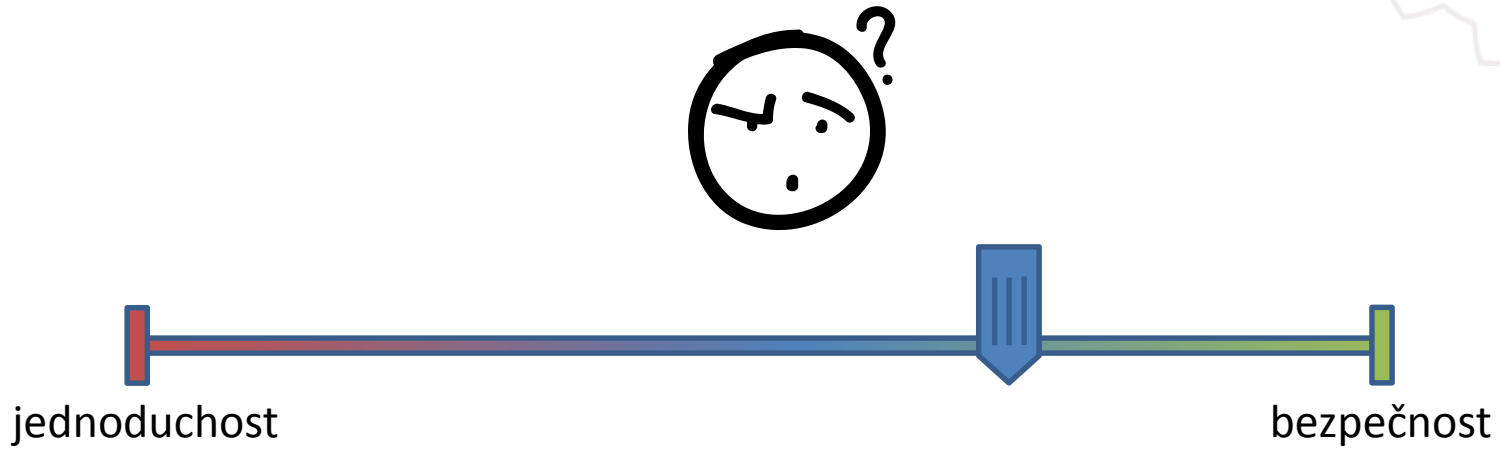
```
User-agent: *
Disallow: /db-10-8-2014.sql #zaloha stareho WP3.6
Allow: /
```

- Webserver na zvláštním portu

```
Listen 8080
```

- Při pokusu o přístup k danému souboru nebo na daný port zablokujeme IP adresu
- Zkušený hacker nikdy nebude používat svou adresu, ale alespoň se dozvíme, že se někdo chytřejší k nám snaží nabourat

Být v obraze - analýza logů



+ vhodné spojit s upozorňováním na dostupné updaty:
https://wordpress.org/plugins/wp-updates-notifier/
http://infinitewp.com/ (hromadná správa WP webů)


POLICE
WAF
POLICE
POLICE

Web Application Firewall

- Pro Apache: mod_security (ověřený, stabilní, mnoho možností, poměrně pomalý)
- Pro nginx: naxsi (stále ve vývoji, velmi výkonný, je třeba dlouho ladit whitelist)

Jako služba:

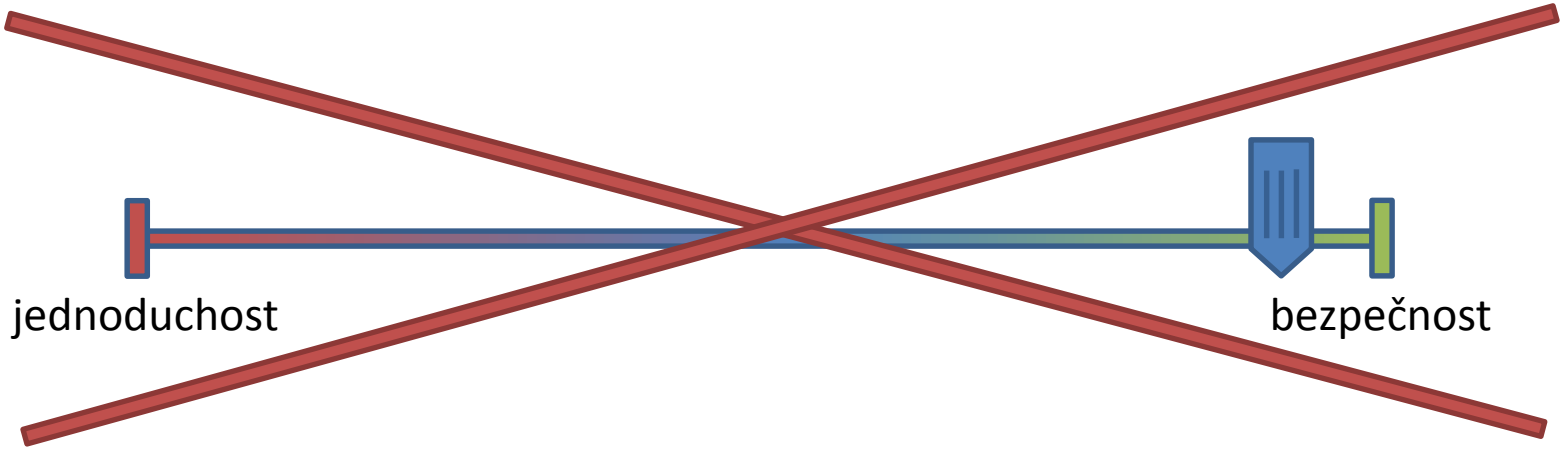
Sucuri – zaměření na bezpečnost, nejbližší node ve Francii

Incapsula – zaměření na bezpečnosti i výkon, node ve Frankfurtu

CloudFlare – hlavně CDN – zaměření na výkon, používá mod_security, node v Praze

Použití WAF

Dokonale zabezpečený web stále může narazit na své uživatele



- Phishing
- Malware v PC
- Připojování z neznámých sítí

Další zajímavé zdroje

Vizualizace útoků:
http://www.stateoftheinternet.com/trends-visualizations-security-real-time-global-ddos-attack-sources-types-and-targets.html
http://www.digitalattackmap.com/

Databáze zranitelností, kterou využívá WPscan:
https://wpvulndb.com/

Další bezpečnostní pluginy:
https://wordpress.org/plugins/wordfence/
https://wordpress.org/plugins/all-in-one-wp-security-and-firewall/

Má minulá přednáška:
http://edu.lynt.cz/course/jak-si-ne-nechat-hacknout-wordpress-stranky

A to je vše, přátelé.

aktualizujte, zálohujte, používejte bezpečnostní plugin, buďte opatrní