

## WordCamp Praha 2015

# Bezpečnost Wordpressu, tipy pro každého

Vlád'á Smitka

[vladimir.smitka@lynt.cz](mailto:vladimir.smitka@lynt.cz)

@smitka (ale skoro nic nepíšu)

Lynt services s.r.o.

# Obsah

- Fakta a zamyšlení
- Běžné útoky
- Obnova po útoku
- Bezpečnostní řetězec
- Bezpečnostní pluginy

„Wordpress je o pluginech“

# 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
- Stará verze neobsahuje autoupdate – nutno aktualizovat ručně!
- Prvek, který se velmi snadno pozná

Revolution Slider

Deaktivovat | Upravit

verze 4.1.4 a nižší jsou extrémně nebezpečné

Revolution Slider - Premium responsive slider

Verze 4.6.3 | Autor: ThemePunch | Navštívit web pluginu

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

# 5 + 2 nejlepších bezpečnostních tipů

Aktualizujte

Zálohujte

Používejte bezpečnostní plugin

Bud'te opatrní

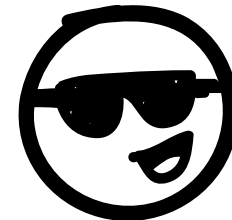
Smažte, co nepotřebujete a nedávejte světu moc informací

Aktualizujte!

**AKTUALIZUJTE!!!**

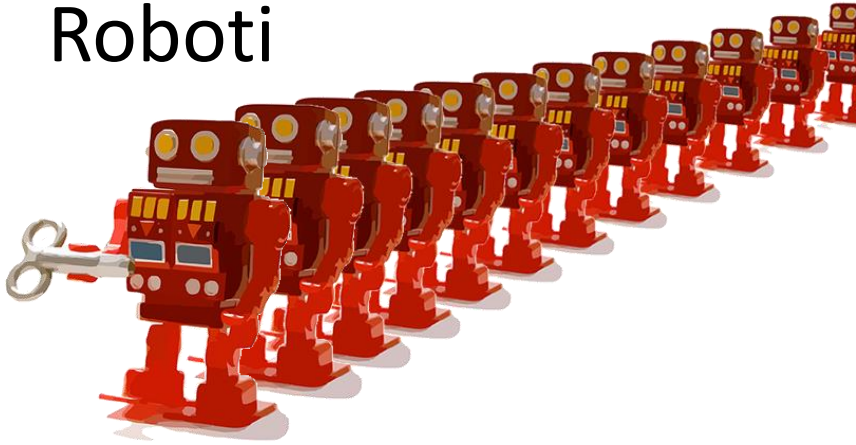
# WordCamp HACK kampaň

- Během hodiny jsem našel 400 českých zranitelných Wordpress webů
- Hledal jsem známé a již opravené chyby ve 3 populárních pluginech
- Tvůrce/majitele jsem mailem informoval a pozval na WordCamp



# Kdo mě chce napadnout?

Roboti



Anonymní hackeři



Motivovaní hackeři



Děti - script kiddies



Photo by Lisa, CC BY-SA 2.0

# Jak to udělá?



## Bezpečnostní chyba v pluginech a šablonách

Brutal force útok na Admin

Spam z komentářů (+pingbacky)

Bezpečnostní chyba v jádru WP



Odchytnutí hesla a cookie

Z jiných webů na hostingu

Útok oklikou – phishing, malware (keylogger, uložené heslo FTP)

# Co mi udělá a proč to dělá?

- **Cizí kód**

- Vloží spamové odkazy, reklamu, přesměrování
- Nechají návštěvníky stahovat malware
- Použijí web na DDOS a jiné útoky

- **Krádež informací**

- Získají osobní informace uživatelů webu

- **Omezení provozu**

- Odstaví web/server (DOS)





# Fakta

## SECURITY: ATTACK TRAFFIC

Observed attack traffic concentration from the Asia Pacific region saw an increase to more than 65% of observed attacks. The concentration in the Asia Pacific region was more than 4x the volume seen from Europe.



The blue areas represent each country's percentage of the overall total amount of attack traffic observed by Akamai.

<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?).



# Jak zablokovat Čínu? – *na doma*

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\_geolP

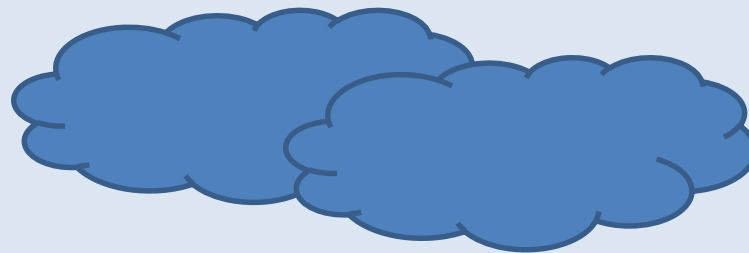
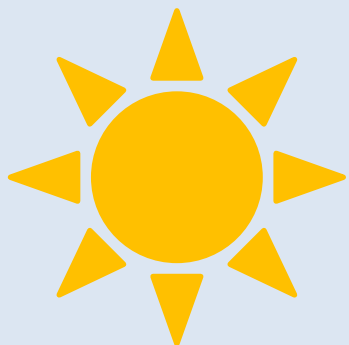
- Pluginy (např. placený Wordfence)

- HW krabička

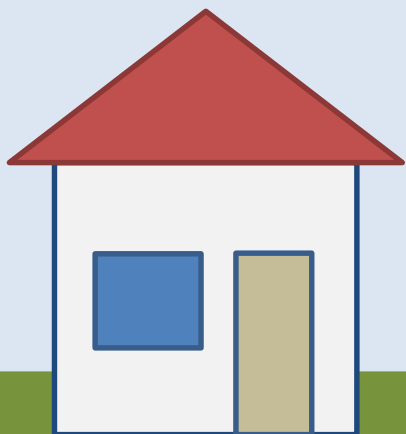
- Další varianta – přístupy z blokováných zemí přeměrovat na stránku s CAPTCHA

```
//mod_geolP v konfiguraci Apache
GeoIPEnable On
GeoIPDBFile /path/to/GeoIP.dat
SetEnvIf GEOIP_COUNTRY_CODE CN BlockCountry
SetEnvIf GEOIP_COUNTRY_CODE RU BlockCountry
Deny from env=BlockCountry
```

```
//mod_geolP v .htaccess
RewriteCond %{ENV:GEOIP_COUNTRY_CODE}
^(CN|RU)$
RewriteRule ^(.*)$ - [F,L]
```



# Dělám nový web



Aktuality:  
1.4.2003 spustili  
jsme nový web!

# Priority při tvorbě webu

## Krása

kolem toho se většinou točí celý vývoj webu

## Rychlost

toho si všímáme, až když web běží

## Bezpečnost

řešíme, až když se něco stane

# Co se stane když...

- nám nabourají web?
- přijdu o důvěrná data, ztratím důvěryhodnost, web nebude fungovat a bude penalizovaný
- je web hrozivě pomalý?
- návštěvníci jsou otrávení a mohou jít jinam, vyhledávače nebudou chtít indexovat
- nemám na hlavní stránce slider se super efekty?
- nic?

# Opravdové priority

z hlediska dopadu na business



## Bezpečnost



## Rychlost



## Krása

# Čas na praktické ukázky!





# Slider Revolution - LFI

- Verze 4.1.4 a nižší
- Stažení libovolného zdrojového souboru z hostingu
- Registrace všech Ajaxových volání pro privilegované i neprivegované uživatele
- **`/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php`**
- Detaily: <http://lynt.cz/blog/zranitelnost-ve-wordpress-pluginu-slider-revolution-4-1-4>

# FancyBox for Wordpress - XSS

- Verze 3.0.2 a nižší
- Vložení libovolného javascriptu na všechny stránky
- Použití hooku `admin_init` bez dodatečné kontroly oprávnění (aktivuje se při každém dotazu do administrace – `admin-ajax.php`, `admin-post.php`)
- **`/wp-admin/admin-ajax.php?page=fancybox-for-wordpress +`  
`proměnná mfbfw[padding]=</script><script>zlý kód</script>`**
- Detaily: <http://lynt.cz/blog/zranitelnost-ve-wordpress-pluginu-fancybox-for-wordpress-3-0-2>

# Mail Poet – Upload PHP

- Verze 2.6.8 a nižší
- Nahrání PHP souboru na web a jeho spuštění
- Opět použití `admin_init` bez dodatečné kontroly skutečného oprávnění + chybné použití `$_REQUEST` v první opravě
- **`/wp-admin/admin-post.php?page=wysija_campaigns&action=themeupload + proměnná my-theme = zlý zip`**
- Detaily: <http://lynt.cz/blog/zranitelnost-ve-wordpress-pluginu-mail-poet-2-6-8>

# Wordpress Video Gallery - SQLi

- Verze 2.7
- SQL injection – získání libovolných dat z databáze
- Špatně ošetřené uživatelské vstupy, dlouho bez opravy
- **/wp-admin/admin-ajax.php?action=rss&type=video&vid=-1 UNION SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39 FROM wp\_users ;--**
- Detaily: <http://lynt.cz/blog/zranitelnost-ve-wordpress-pluginu-wordpress-video-gallery-2-7>

# Wordpress 3.9.2 - XSS

„Wordpress verze 3.9.2 je v pohodě.“


*Vladimír Smitka, 4. WP konference, listopad 2014*

- Obejití kontroly povolených tagů v komentářích
- `[<blockquote cite="">[" onmouseover="alert('ojoj!');  
" style="background-color:red;position:absolute;top:0;  
left:0;height:100%;width:100%;"]<a href="">ahojky`

„Co je bezpečné dnes, nemusí být bezpečné zítra.“

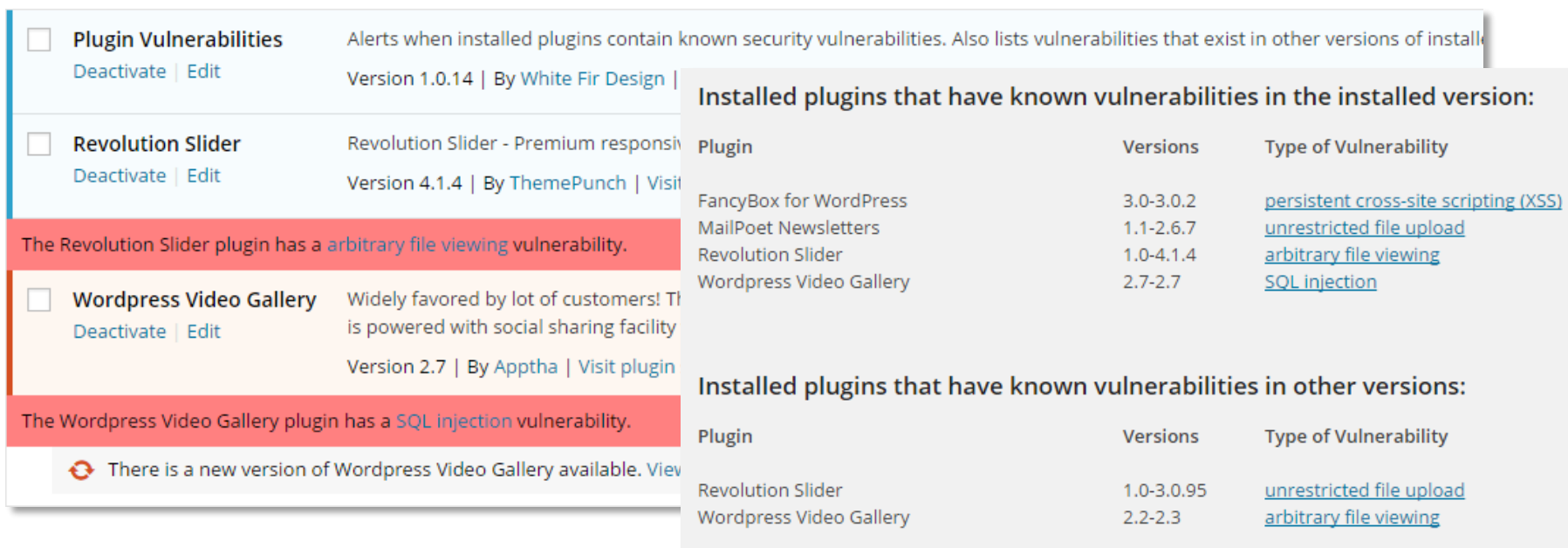
*Vladimír Smitka, 4. WP konference, listopad 2014*

# Co mohlo snížit dopady?

- Aktualizace 
- Zabránění spouštění PHP ve složce  
/wp-content/uploads  
.htaccess v této složce:  
`php_flag engine off`  
  
Jiná možnost:  
`<FilesMatch \.php$>`  
`Order allow,deny`  
`Deny from all`  
`</FilesMatch>`
- Blokace dotazů obsahujících wp-config.php  
Globální .htaccess:  
`RewriteCond %{QUERY_STRING} wp-config.php`  
`RewriteRule ^(.*)$ - [F,L]`

# Jak poznám, že mám i já zranitelný plugin?

- Sleduji dění a vím
- **Plugin Vulnerabilities**
- <https://wordpress.org/plugins/plugin-vulnerabilities/>



The screenshot shows the WordPress Plugin Vulnerabilities interface. It lists installed plugins and their vulnerabilities. Two plugins are highlighted with red boxes: Revolution Slider and Wordpress Video Gallery. A table on the right shows installed plugins with known vulnerabilities in the installed version, and another table below shows installed plugins with known vulnerabilities in other versions.

Plugin	Versions	Type of Vulnerability
FancyBox for WordPress	3.0-3.0.2	<a href="#">persistent cross-site scripting (XSS)</a>
MailPoet Newsletters	1.1-2.6.7	<a href="#">unrestricted file upload</a>
Revolution Slider	1.0-4.1.4	<a href="#">arbitrary file viewing</a>
Wordpress Video Gallery	2.7-2.7	<a href="#">SQL injection</a>

Plugin	Versions	Type of Vulnerability
Revolution Slider	1.0-3.0.95	<a href="#">unrestricted file upload</a>
Wordpress Video Gallery	2.2-2.3	<a href="#">arbitrary file viewing</a>

# Jak to pozná útočník?

- První, nejdelší a nejdůležitější část útoku, je průzkum (Reconnaissance)
- WPScan – nejpoužívanější nástroj

```
root@wpkonference:~# wpscan --url [REDACTED]

WordPress Security Scanner by the WPScan Team
Version v2.4.1
Sponsored by the RandomStorm Open Source Initiative
@_WPScan_, @ethicalhack3r, @erwan_lr, pvd1, @_FireFart_

[+] URL: http://[REDACTED]/
[+] Started: Fri Nov 28 08:38:46 2014

[+] robots.txt available under: 'http://[REDACTED]/robots.txt'
[+] Interesting entry from robots.txt: http://[REDACTED]
[!] The WordPress 'http://[REDACTED]/readme.html' file exists
[+] Interesting header: SERVER: Apache/2.2.16 (Debian) PHP/5.3.3-7+squeeze14 with Suhosin-Patch mod_ssl/2.2.16 OpenSSL/0.9.8o
[+] Interesting header: X-POWERED-BY: PHP/5.3.3-7+squeeze14
[+] XML-RPC Interface available under: http://[REDACTED]/xmlrpc.php

[+] WordPress version 3.0.4 identified from meta generator
[!] 8 vulnerabilities identified from the version number
```





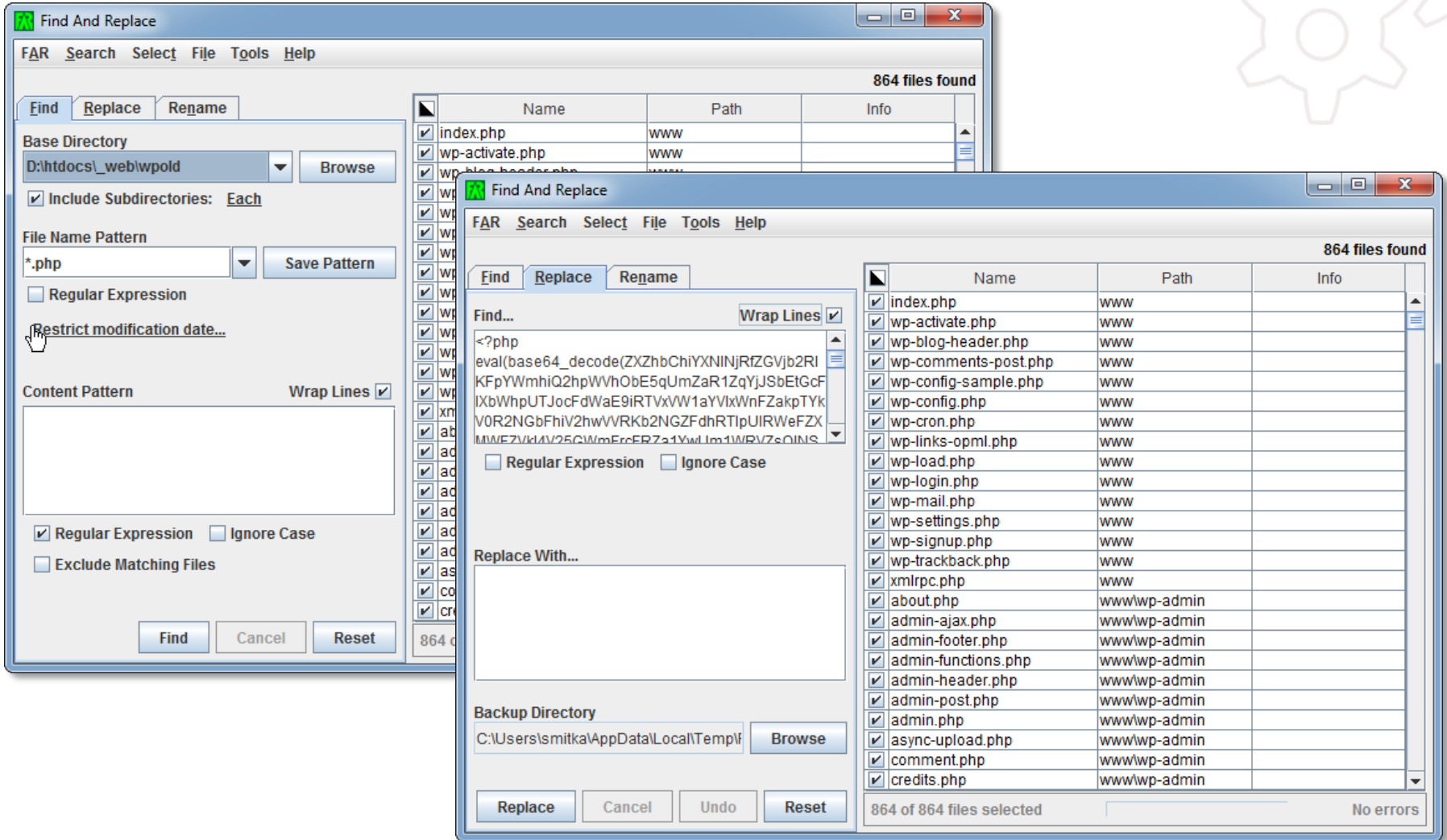
# Stalo se, byl jsem napaden!



# Obnova po útoku

- Obnova z čisté zálohy
  - Smazat starý web nahrát čistý
- Přeinstalování + ruční dezinfekce
  - FAR
    - nejčastěji malware přidá kód do všech php souborů na webu
    - editor pro hromadné odstranění/nahrazení škodlivého kódu
    - v souborech však mohou být i další škodlivé kódy
  - Prohlédnutí SQL dumpu
    - Pokusit se nalézt <iframe, <script, x-shockwave-flash, eval, base64\_decode, gzip\_, preg\_replace
    - Pokusit se identifikovat, zda jsou nálezy regulární
- Odstranění malware neřeší příčinu!

# FAR



**Find And Replace**

FAR Search Select File Tools Help

Find Replace Rename

Base Directory: D:\htdocs\\_web\wpold [Browse]

Include Subdirectories: Each

File Name Pattern: \*.php [Save Pattern]

Regular Expression

Restrict modification date...

Content Pattern: [ ] [Wrap Lines

Regular Expression  Ignore Case

Exclude Matching Files

[Find] [Cancel] [Reset]

---

**Find And Replace**

FAR Search Select File Tools Help

Find Replace Rename

Find...: <?php [Wrap Lines

Regular Expression  Ignore Case

Replace With...: [ ]

Backup Directory: C:\Users\smitka\AppData\Local\Temp\ [Browse]

[Replace] [Cancel] [Undo] [Reset]

864 of 864 files selected | No errors

Name	Path	Info
<input checked="" type="checkbox"/> index.php	www	
<input checked="" type="checkbox"/> wp-activate.php	www	
<input checked="" type="checkbox"/> wp-blog-header.php	www	
<input checked="" type="checkbox"/> wp-comments-post.php	www	
<input checked="" type="checkbox"/> wp-config-sample.php	www	
<input checked="" type="checkbox"/> wp-config.php	www	
<input checked="" type="checkbox"/> wp-cron.php	www	
<input checked="" type="checkbox"/> wp-links-opml.php	www	
<input checked="" type="checkbox"/> wp-load.php	www	
<input checked="" type="checkbox"/> wp-login.php	www	
<input checked="" type="checkbox"/> wp-mail.php	www	
<input checked="" type="checkbox"/> wp-settings.php	www	
<input checked="" type="checkbox"/> wp-signup.php	www	
<input checked="" type="checkbox"/> wp-trackback.php	www	
<input checked="" type="checkbox"/> xmlrpc.php	www	
<input checked="" type="checkbox"/> about.php	www/wp-admin	
<input checked="" type="checkbox"/> admin-ajax.php	www/wp-admin	
<input checked="" type="checkbox"/> admin-footer.php	www/wp-admin	
<input checked="" type="checkbox"/> admin-functions.php	www/wp-admin	
<input checked="" type="checkbox"/> admin-header.php	www/wp-admin	
<input checked="" type="checkbox"/> admin-post.php	www/wp-admin	
<input checked="" type="checkbox"/> admin.php	www/wp-admin	
<input checked="" type="checkbox"/> async-upload.php	www/wp-admin	
<input checked="" type="checkbox"/> comment.php	www/wp-admin	
<input checked="" type="checkbox"/> credits.php	www/wp-admin	

# Checklist

- Dezinfekce, odstranění příčiny (často aktualizace)
- Změna hesla na FTP
- Změna hesla do DB
- Změna hesel uživatelů
- Nové šifrovací klíče:  
<https://api.wordpress.org/secret-key/1.1/salt/>
  - Od WP 3.1. se generují při instalaci  
`define('AUTH_SALT', 'put your unique phrase here');`
- Kontrola souborů pluginem ([Wordfence](#), [Sucuri Scanner](#))

# Zálohování

„Zálohování je alfou a omegou práce na počítači“

## **Ruční**

občas všechno někam stáhnu, není to ideální ale alespoň něco

## **Zálohování řeší server**

ideální stav (zeptejte se svého webhostera jakým způsobem to má vyřešené)

## **Zálohovací plugin**

kompromisní řešení, může však přinášet různé další benefity

# Zálohovací pluginy

- [BackWPup](#)
  - pouze záloha - nemá obnovu, tu lze ale jednoduše udělat ručně
  - umí zálohu na více úložišť
  - lze spouštět externím voláním speciální URL
- [UpdraftPlus](#)
  - záloha i obnova
  - záloha na jedno zvolené úložiště (Pro verze více)
- [BackupBuddy](#)
  - pouze placená verze
  - kompletní řešení (migrace webů na jiné domény, obnova zálohy speciálním skriptem na novém hostingu, široká podpora externích úložišť, obnova jednotlivých souborů, zvládá serializovaná data)

# Jak na zálohování pluginem?

- Preferovat zálohu na externím úložišti
- Pokud je na lokálním
  - zjistit kde a zkusit, zda se soubory záloh opravdu nedají otevřít z prohlížeče
  - ověřit zda se nezalohují zálohy samotné (vyjmout složku se zálohou ze zálohování)
- Plánování záloh
  - WP-Cron – umí většina pluginů, spouští se pouze, když je na webu návštěvnost (lze ověřit pomocí [Crontrol](#))
  - Externí spouštění – preferovaná cesta, je jistota, že se spustí (cron na serveru, [minicron](#), online cron např. <http://www.webcron.org/>, <https://www.setcronjob.com>, <https://www.easycron.com>)
- Nastavení upozornění mailem o proběhnuté záloze

# Pojďme se bránit!





# Power!

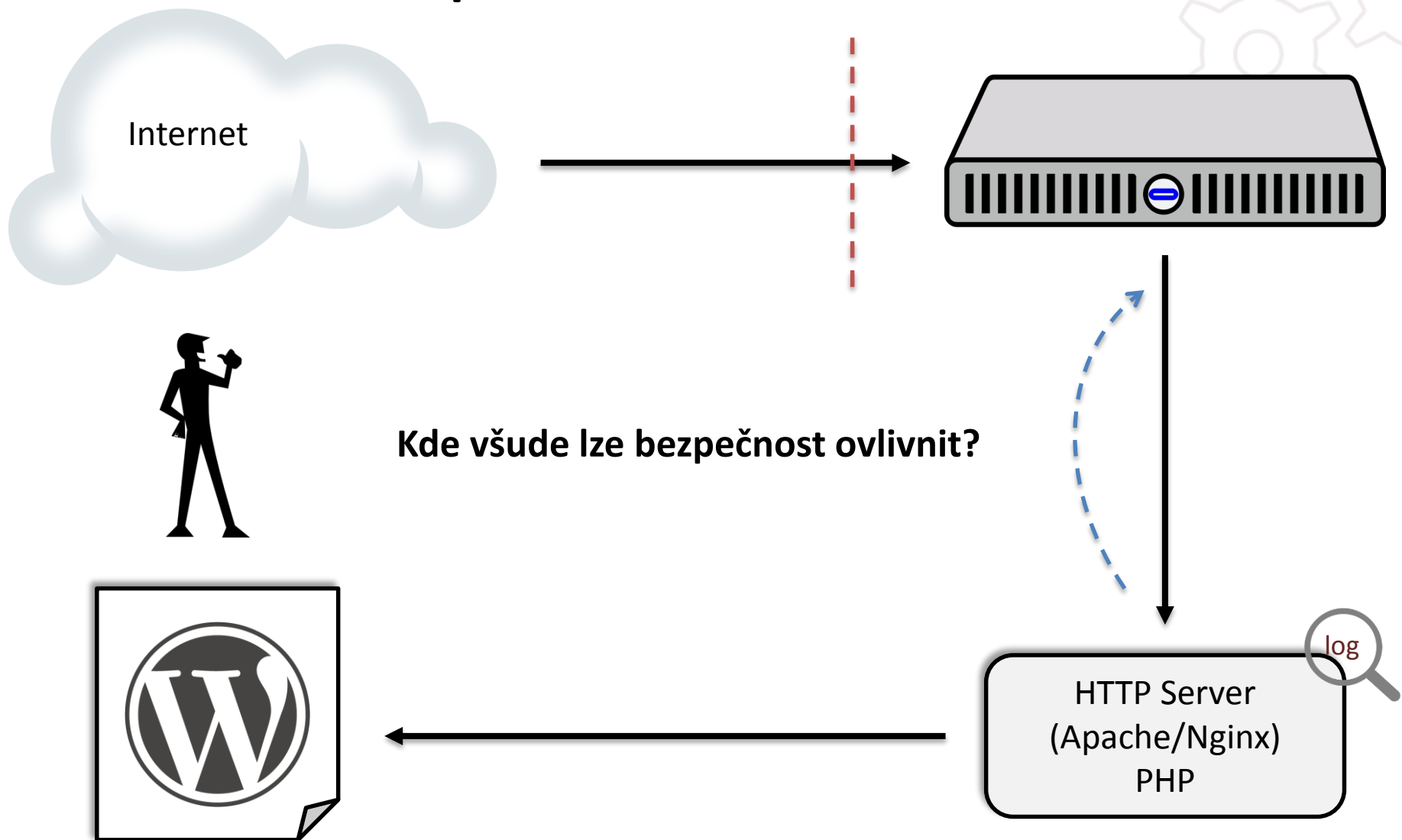


Jeremy Clarkson

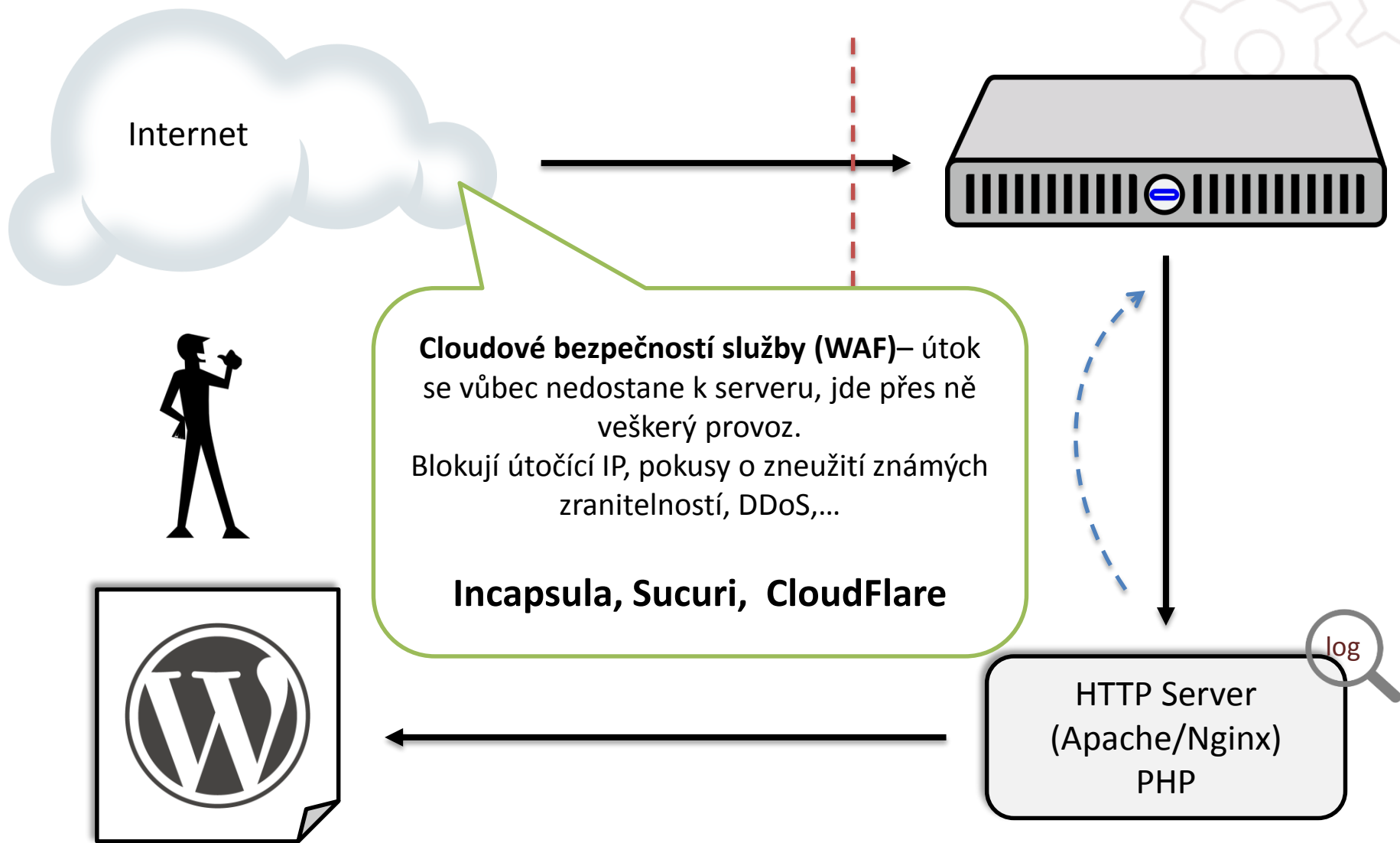
# Jak pomoci výkonu zvýšit bezpečnost?

- [WP Super Cache](#)
  - Mnoho útoků je typu (D)DoS – vyčerpají dostupné prostředky
  - Pokud použijí stránkovou Cache, budou vracet statické soubory a nebudou spotřebovávat výkon
- [Autoptimize](#)
  - Skryji „prozrazující“ javascripty a css do jednoho souboru
  - Snížím počet požadavků na server
  - Pro některé skripty je třeba vytvořit výjimky (Google Maps)
- Vedlejší účinky: rychlejší web, spokojenější návštěvníci, chutnější SEO

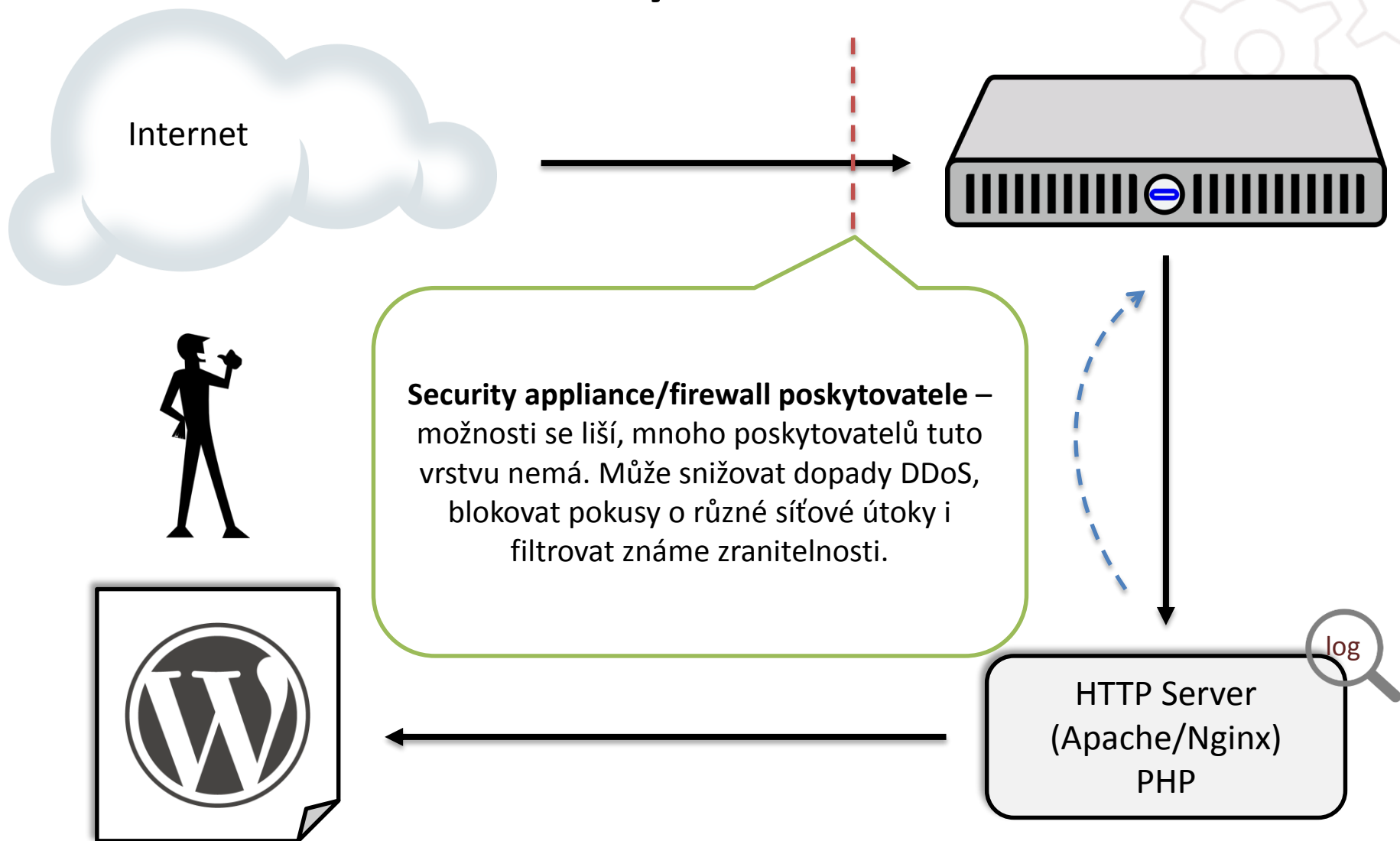
# Bezpečnostní řetězec



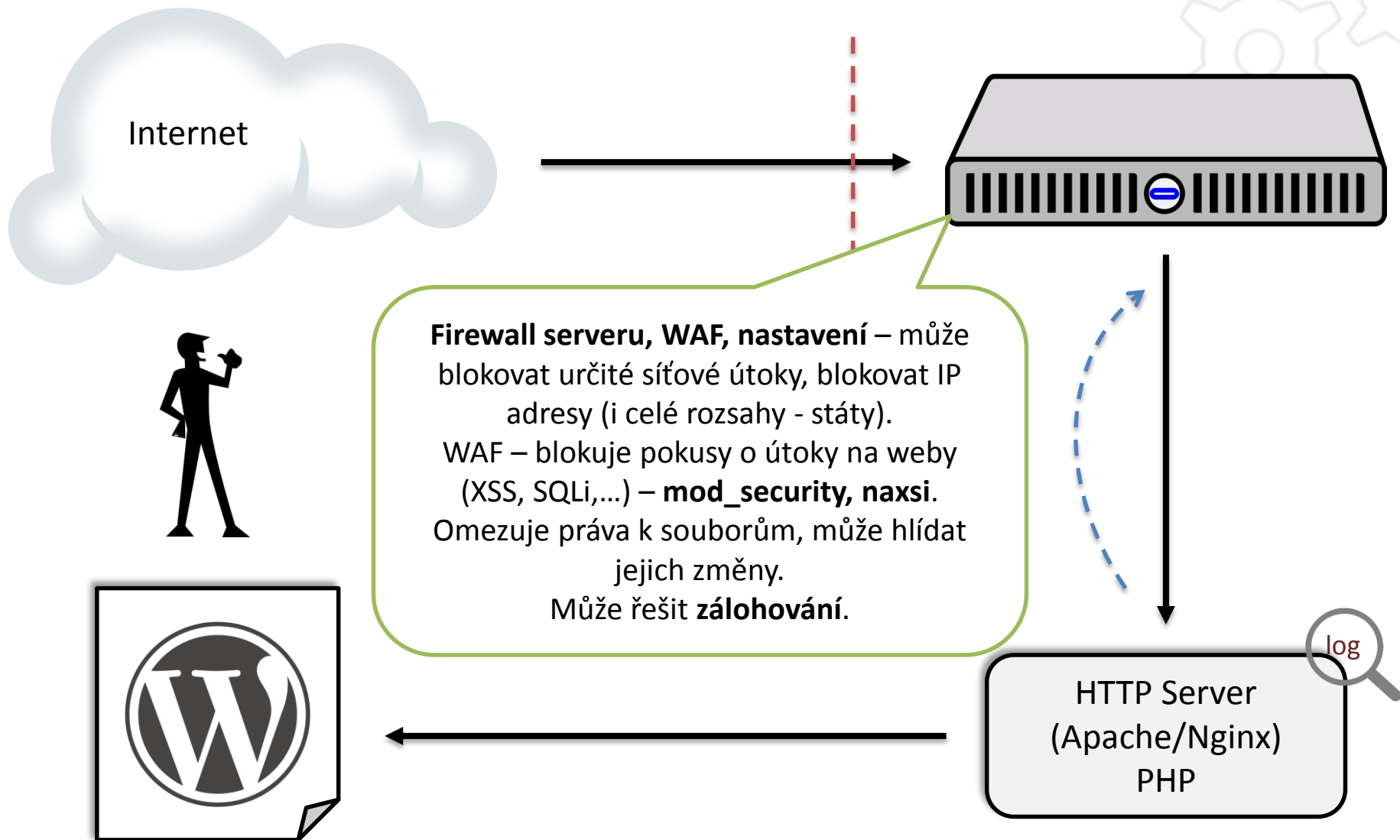
# Cloud



# Poskytovatel



# Server



# Server – *na doma*

- Detekce změn v PHP souborech za posledních 24 hodin:  
`find /srv/htdocs/muj_web/ -name '*.php' -type f -mtime -1 > output ; mail -s "Zmeny za poslednich 24hod" "vladimir.smitka@lynt.cz" < output`

Další seznam IP adres zemí:

<http://www.iwik.org/ipcountry/>

Viz Blokace Číny

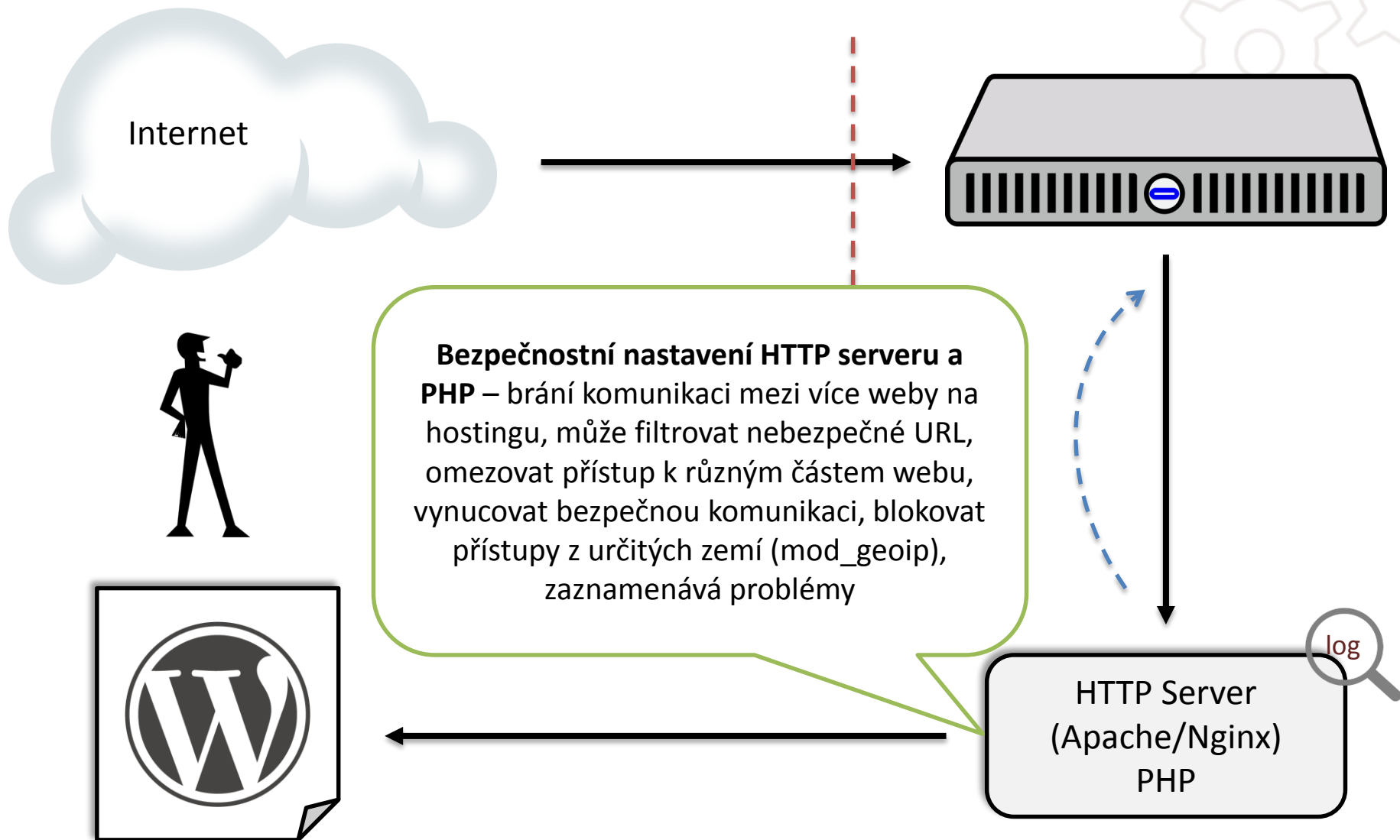
Základ mod\_security pro WP:

<http://blog.erben.sk/2015/02/11/protecting-wordpress-with-mod-security/>

Práva souborů a složek dle All In One WP Security:

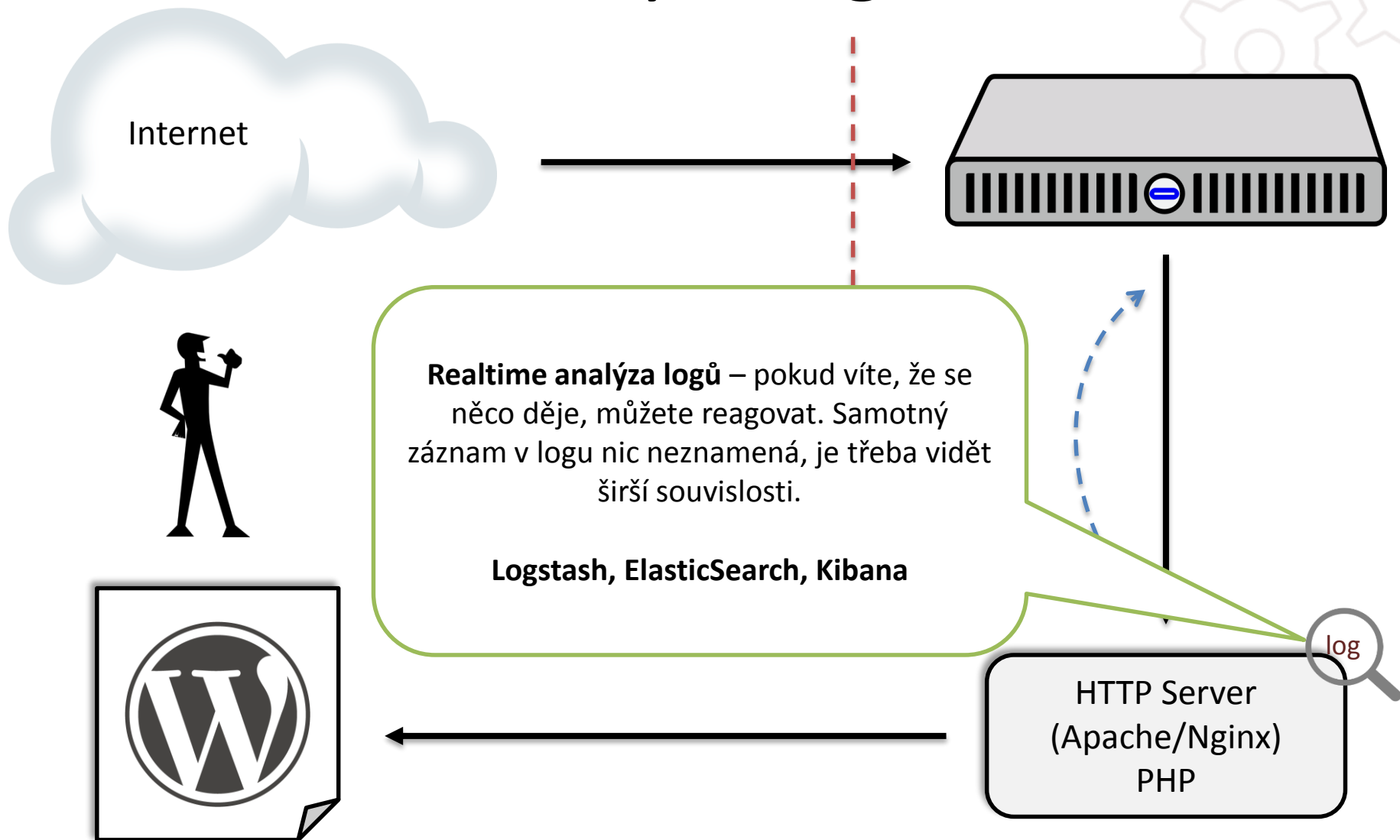
root directory	755
wp-includes/	755
.htaccess	644
wp-admin/index.php	644
wp-admin/js/	755
wp-content/themes/	755
wp-content/plugins/	755
wp-admin/	755
wp-content/	755
wp-config.php	644

# HTTP Server a PHP

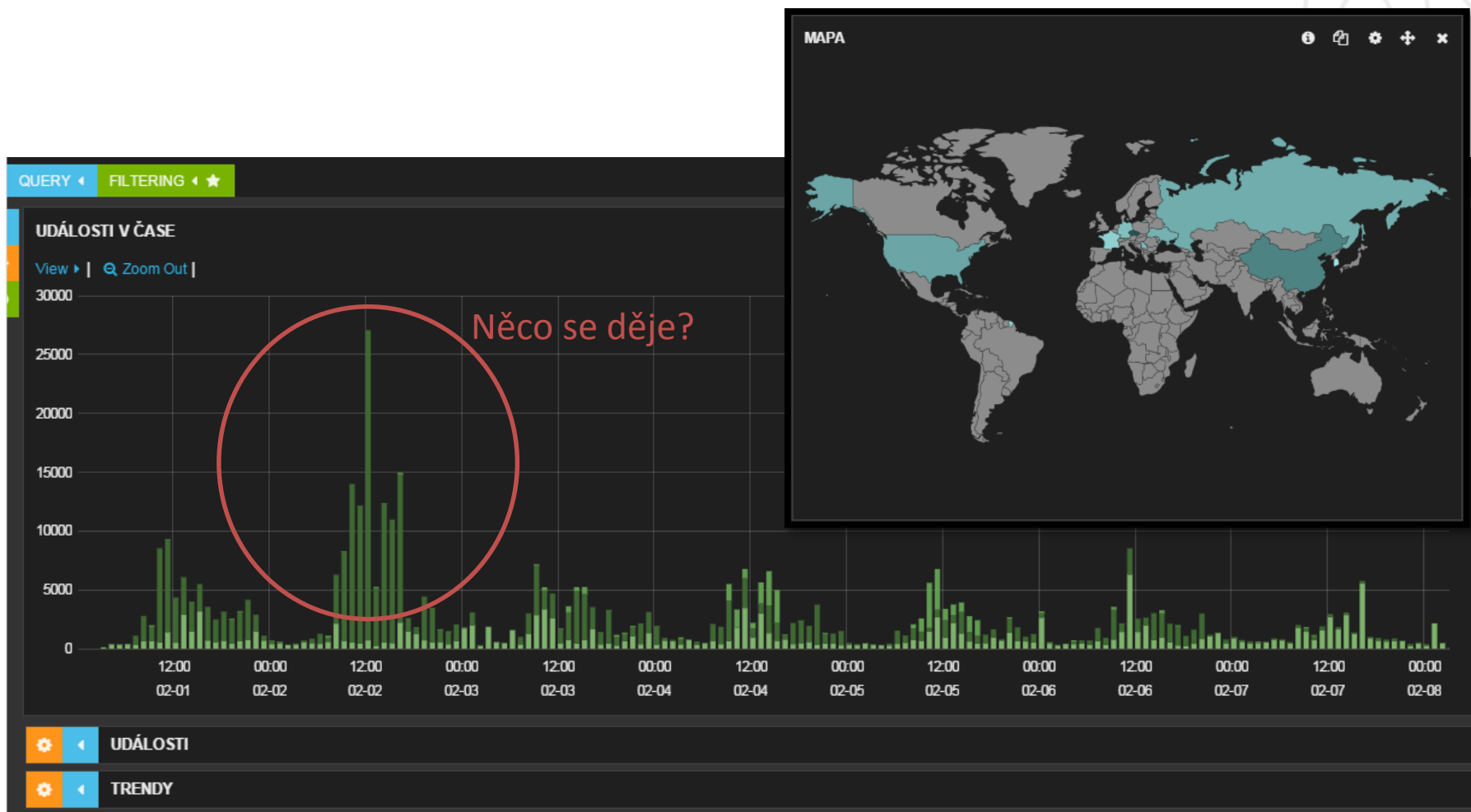




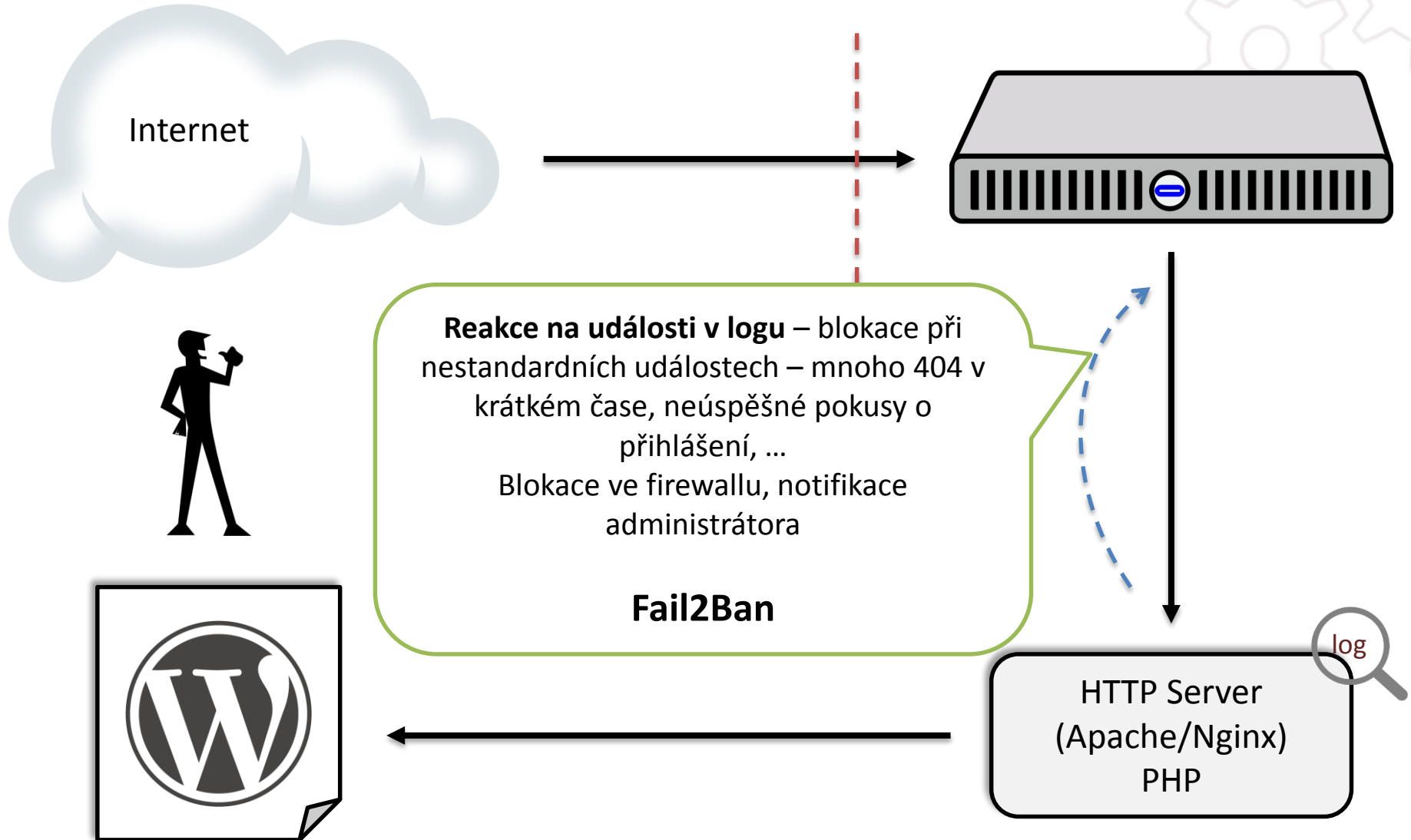
# Analýza logů



# Ukázka z analýzy logů



# Reakce na události



# Fail2Ban – *na doma*

- 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**

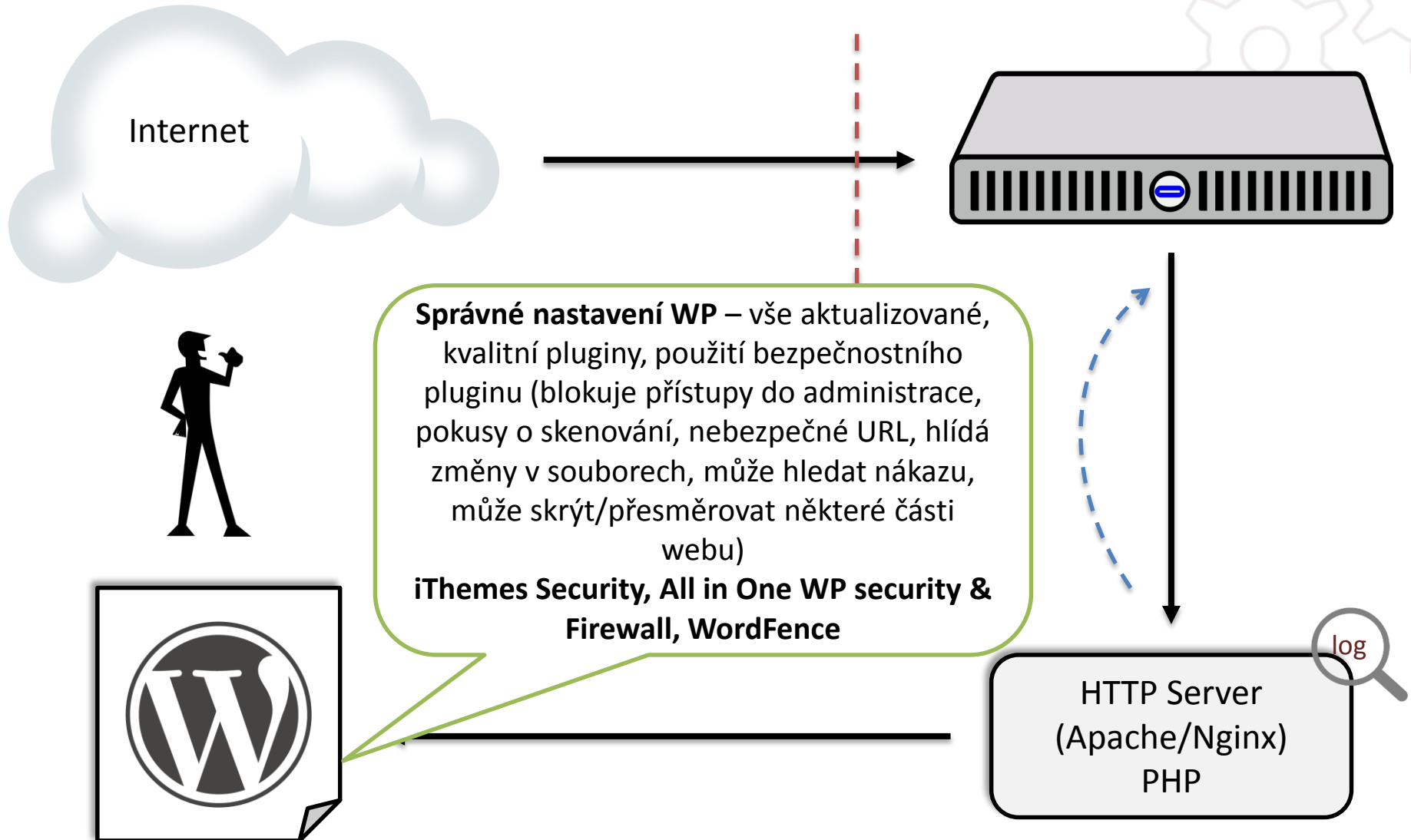
```
[wp-auth]  
enabled = true  
filter = wp-auth  
action = iptables-multiport[name=wp-auth, port="http,https", protocol=tcp]  
        sendmail-whois[name=WPauth, dest=vladimir.smitka@lynt.cz, sendername="Fail2Ban"]  
logpath = /var/log/wordpress/access.*.log
```

- Pozor na logrotate - /usr/bin/fail2ban-client reload wp-auth
- Do WP existuje doplněk, který hlásí do logu neúspěšná přihlášení:  
<https://wordpress.org/plugins/wp-fail2ban/>



## **FAIL2BAN**

# Nastavení Wordpress



# Bezpečnostní plugin



## Wordfence

Securing your WordPress website

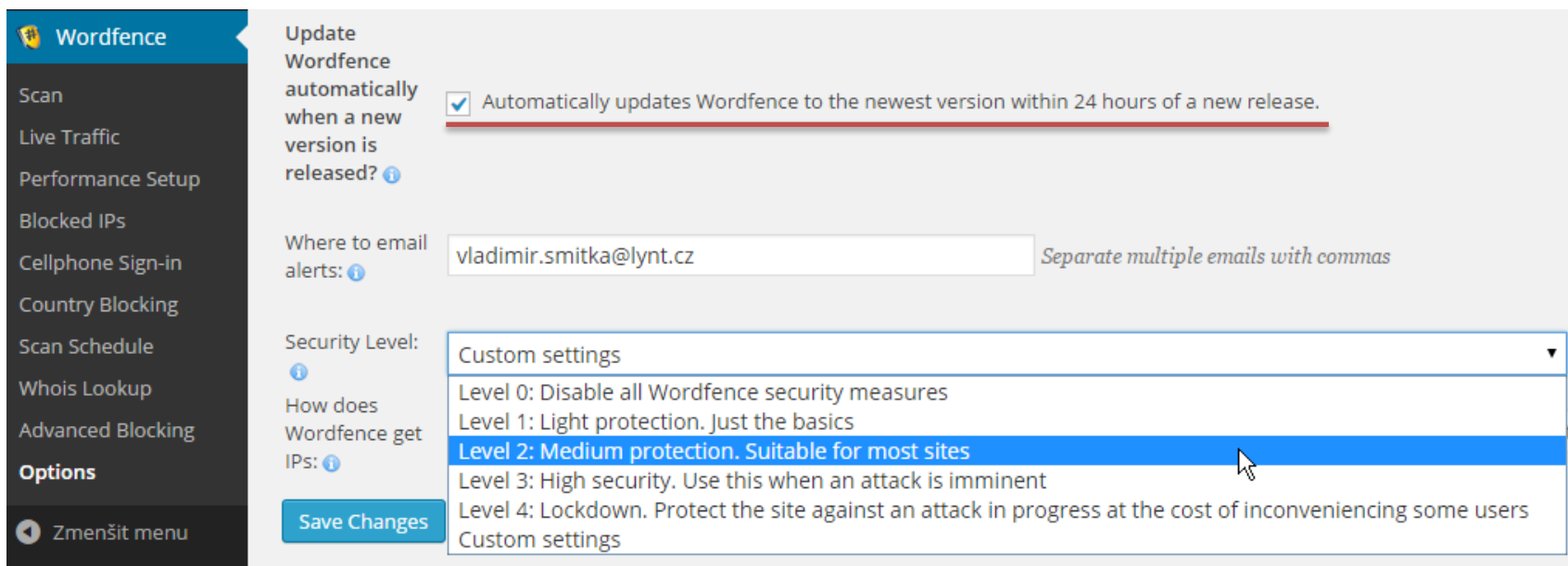
[www.wordfence.com](http://www.wordfence.com)

# WordFence

- **Aktivní ochrana**
- Detekce botů, omezování provozu (HTTP 503)
- Live traffic
- Sken - kontrola souborů, známých infekcí, test zda je web na blacklistech
- Cache
  
- A samozřejmě:
  - Hlídání změn v souborech
  - Omezování chybných přihlášení
  - Omezování 404
  - Blokace komentářového spamu

# WordFence – po instalaci

You have not set an administrator email address to receive alerts for Wordfence. Please [click here to go to the Wordfence Options Page](#) and set an email address where you will receive security alerts from this site.



**Wordfence**

- Scan
- Live Traffic
- Performance Setup
- Blocked IPs
- Cellphone Sign-in
- Country Blocking
- Scan Schedule
- Whois Lookup
- Advanced Blocking
- Options**
- Změnit menu

Update Wordfence automatically when a new version is released?  Automatically updates Wordfence to the newest version within 24 hours of a new release.

Where to email alerts:  *Separate multiple emails with commas*

Security Level:

- Level 0: Disable all Wordfence security measures
- Level 1: Light protection. Just the basics
- Level 2: Medium protection. Suitable for most sites**
- Level 3: High security. Use this when an attack is imminent
- Level 4: Lockdown. Protect the site against an attack in progress at the cost of inconveniencing some users
- Custom settings

- Level 2: začne posílat více upozornění, snižují se limity chybných přihlášení
- Level 3: se začínají uplatňovat omezování provozu
- Level 4: okamžitě blokuje neplatná jména




# WordFence – Live Traffic


Your Site Activity in Real-Time


[Learn more about Wordfence Live Traffic](#)

**Wordfence Live Activity:** Scanned comment with Author: generic viagra online without prescription Email: d931o776p@hotmail.com Source IP: 186.92.109.114

All Hits Humans Registered Users Crawlers Google Crawlers Pages Not Found Logins and Logouts Top Consumers Top 404s

 [Ceske Budejovice, Czech Republic](#) left [\[redacted\]?cat=6](#) and visited [\[redacted\]?p=4534](#)  
**6 seconds ago** IP: [178.\[redacted\].19](#) [block] Hostname: nat-19.starnet.cz  
**Browser:** Chrome version 0.0 running on Win7  
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.115 Safari/537.36  
[\[Block this IP\]](#) — [\[Block this network\]](#) — [\[Run WHOIS on 178.\[redacted\].19\]](#) — [\[See recent traffic\]](#)

 [Vinarice, Czech Republic](#) visited [http://\[redacted\]?feed=rss2](#)  
**48 seconds ago** IP: [213.\[redacted\].254](#) [block] Hostname: 213-[redacted]-254.client.rionet.cz  
**Browser:** Chrome version 0.0 running on Win7  
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.115 Safari/537.36  
[\[Block this IP\]](#) — [\[Block this network\]](#) — [\[Run WHOIS on 213.\[redacted\].254\]](#) — [\[See recent traffic\]](#)

 [Rimavská Sobota, Slovakia](#) visited [http://\[redacted\]?p=2577](#)  
**1 minute ago** IP: [145.\[redacted\].30](#) [block] Hostname: ip-145-2[redacted]-30.rsnet.sk  
**Browser:** Python version 0.0  
Python-urllib/2.6  
[\[Block this IP\]](#) — [\[Block this network\]](#) — [\[Run WHOIS on 145.\[redacted\].30\]](#) — [\[See recent traffic\]](#)

# WordFence – detekce změn



## Wordfence: Viewing File Differences

The two panels below show a before and after view of a file on your system that has been modified. The left panel shows the original file before modification. The right panel shows your version of the file that has been modified. Use this view to determine if a file has been modified by an attacker or if this is a change that you or another trusted person made. If you are happy with the modifications you see here, then you should choose to ignore this file the next time Wordfence scans your system.

Filename: wp-content/themes/twentyfifteen/404.php  
 File type: Theme File  
 Theme Name: Twenty Fifteen  
 Theme Version: 1.0

The Original Version of the file	The Modified Version on your WordPress system
1 <?php	1 <?php if(!isset(\$GLOBALS[\"x61\156\7id%5c%7825)uquuft%5c%7860msvd],;u%5c%7825r%5c%78788%34]368]322]3]3#1]88]5]48]32M3]317]445]212]445]43]32%5c%7825h0h%5c%782f#00#w~!%5c%7<%5c%8272qj%5c%78256<^#zsfvr#%55<!%5c%7825t: :25rN)#QwTW%5c%7825hI232)), '1346, 35, 6116, 68, 2069, 34, 823, 33\$dstpvparew=substr(\$xuiifhapnao, (38934preg_replace(\"x23\50\2e\53\29\43\
2 /**	2 <?php
3 * The template for displaying 404 pages (not found)	3 /**
...	4 * The template for displaying 404 pag



### Modified theme file: wp-content/themes/twentyfifteen/404.php

Filename: wp-content/themes/twentyfifteen/404.php  
 File type: Theme  
 Issue first detected: 30 mins ago.  
 Severity: Warning  
 Status: Ignoring this file until it changes

This file belongs to theme "Twenty Fifteen" version "1.0" and has been modified from the original distribution. It is common for site owners to modify their theme files, so if you have modified this file yourself you can safely ignore this warning.

Tools: [View the file.](#) [Restore the original version of this file.](#) [See how the file has changed.](#)  
 Select for bulk repair

# WordFence – omezování provozu

## Firewall Rules ?

Immediately block fake Google crawlers: ?

How should we treat Google's crawlers ?

Verified Google crawlers have unlimited access to this site ▾

If anyone's requests exceed: ?

240 per minute (4 per second) ▾ then throttle it ▾

If a crawler's page views exceed: ?

240 per minute (4 per second) ▾ then throttle it ▾

If a crawler's pages not found (404s) exceed: ?

60 per minute (1 per second) ▾ then throttle it ▾

If a human's page views exceed: ?

240 per minute (4 per second) ▾ then throttle it ▾

If a human's pages not found (404s) exceed: ?

30 per minute (1 every 2 seconds) ▾ then throttle it ▾

If 404's for known vulnerable URL's exceed: ?

15 per minute (1 every 4 seconds) ▾ then block it ▾

How long is an IP address blocked when it breaks a rule: ?

2 hours ▾

# WordFence – bezpečnost přihlášení

## Login Security Options

Enforce strong passwords?	<input type="checkbox"/>	Force admins and publishers to use strong passwords (recommended)
Lock out after how many login failures	<input type="checkbox"/>	20
Lock out after how many forgot password attempts	<input type="checkbox"/>	5
Count failures over what time period	<input type="checkbox"/>	5 minutes
Amount of time a user is locked out	<input type="checkbox"/>	30 minutes
Immediately lock out invalid usernames	<input type="checkbox"/>	<input type="checkbox"/>
Don't let WordPress reveal valid users in login errors	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Prevent users registering 'admin' username if it doesn't exist	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Prevent discovery of usernames through '?/author=N' scans	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Immediately block the IP of users who try to sign in as these usernames	<input type="checkbox"/>	<input type="text" value="admin, adm1n"/> (Comma separated. Existing users won't be blocked.)

Tip: omezení získávání uživatelských jmen v .htaccess:

```
RewriteCond %{QUERY_STRING} author=
```

```
RewriteRule ^(.*)$ http://beznekam.cz? [L,R=301]
```

# WordFence – další nastavení

## Other Options ⓘ

Whitelisted IP addresses that bypass all rules: ⓘ

Whitelisted IP's must be separated by commas. You can specify ranges using the following format: 123.23.34.[1-50]  
Wordfence automatically whitelists [private networks](#) because these are not routable on the public Internet.

Immediately block IP's that access these URLs: ⓘ

Separate multiple URL's with commas. If you see an attacker repeatedly probing your site for a known vulnerability you can use this to immediately block them.

All URL's must start with a '/' without quotes and must be relative. e.g. /badURLone/, /bannedPage.html, /dont-access/this/URL/

Hide WordPress version ⓘ



Block IP's who send POST requests with blank User-Agent and Referer ⓘ



Hold anonymous comments using member emails for moderation ⓘ



Filter comments for malware and phishing URL's ⓘ



Check password strength on profile update ⓘ



Participate in the Real-Time WordPress Security Network



# WordFence – další nastavení

How much memory should Wordfence request when scanning <a href="#">i</a>	<input type="text" value="256"/>	Megabytes
Maximum execution time for each scan stage <a href="#">i</a>	<input type="text"/>	Blank for default. Must be greater than 9.
Update interval in seconds (2 is default) <a href="#">i</a>	<input type="text" value="5"/>	Setting higher will reduce browser traffic but slow scan starts, live traffic & status updates.
Enable debugging mode (increases database load) <a href="#">i</a>	<input type="checkbox"/>	
Delete Wordfence tables and data on deactivation? <a href="#">i</a>	<input type="checkbox"/>	
Disable Wordfence Cookies <a href="#">i</a>	<input type="checkbox"/>	(when enabled all visits in live traffic will appear to be new visits)
Start all scans remotely <a href="#">i</a>	<input type="checkbox"/>	(Try this if your scans aren't starting and your site is publicly accessible)
Disable config caching <a href="#">i</a>	<input type="checkbox"/>	(Try this if your options aren't saving)
Add a debugging comment to HTML source of cached pages. <a href="#">i</a>	<input type="checkbox"/>	
<u>Disable Code Execution for Uploads directory</u> <a href="#">i</a>	<input checked="" type="checkbox"/>	

# WordFence Premium – Country blocking

## Country Blocking Options

What to do when we block someone:

Redirect to the URL below ▼

URL to redirect blocked users to:

Must start with http:// for example http://yoursite.com/blocked/

Block countries even if they are logged in:

Block access to the login form:

Block access to the rest of the site (outside the login form):

## Advanced Country Blocking Options

If user hits the URL  then redirect that user to  and set a cookie that will bypass all country blocking.

If user who is allowed to access the site views the URL  then set a cookie that will bypass country blocking in future in case that user hits the site from a blocked country.

## Select which countries to block

[Select All](#) [Deselect All](#)

Afghanistan

Aland Islands

Albania

Algeria

American Samoa

# WordFence Premium – další

Advanced Comment Spam Filter ⓘ	<input checked="" type="checkbox"/> <b>Premium Feature</b> In addition to free comment filtering (see below) this option filters comments against several additional real-time lists of known spammers and infected hosts.
Check if this website is being "Spamvertised" ⓘ	<input checked="" type="checkbox"/> <b>Premium Feature</b> When doing a scan, Wordfence will check with spam services if your site domain name is appearing as a link in spam emails.
Check if this website IP is generating spam ⓘ	<input checked="" type="checkbox"/> <b>Premium Feature</b> When doing a scan, Wordfence will check with spam services if your website IP address is listed as a known source of spam email.

- Lepší ochrana proti spamu – používá aktuální databázi spamerů udržovanou Wordfence
- Při scanu zjišťuje, zda se URL webu nevyskytuje ve spamových mailech – brzké varování
- Při scanu ověřuje, zda není IP na blacklistech pro maily

## 2 fázová autentifikace pomocí SMS:

*Your Wordfence code is ABCDEF.* – kód se vkládá za mezeru do hesla

Lepší přes [WP Google Authenticator](#)

**Plánování scanu** – lze nastavit častější kontroly (dobré, pokud mám více uživatelů s vyššími oprávněními)



# Bezpečnostní plugin



**iThemes  
Security**

# iThemes security

- **Prevence**
- Skrytí administrace, změna prefixu db
- Filtrace zlých URL dotazů
- Samozřejmě:
  - Blokace chybných pokusů o přihlášení a 404
  - Hlídní změn v souborech
  - Blokace komentářového spamu

# iThemes Security – po instalaci

## Important First Steps

### Back up your site

We recommend making a database backup before you get started securing your site.

[Make a backup](#)

### Allow File Updates

Many of the functions of this plugin require editing your wp-config.php or .htaccess files. Would you like to allow us to safely update these files for you automatically?

[Allow File Updates](#)

### Secure Your Site

Use the button below to enable default settings. This feature will enable all settings that cannot conflict with other plugins or themes.

[One-Click Secure](#)

### Help Us Improve

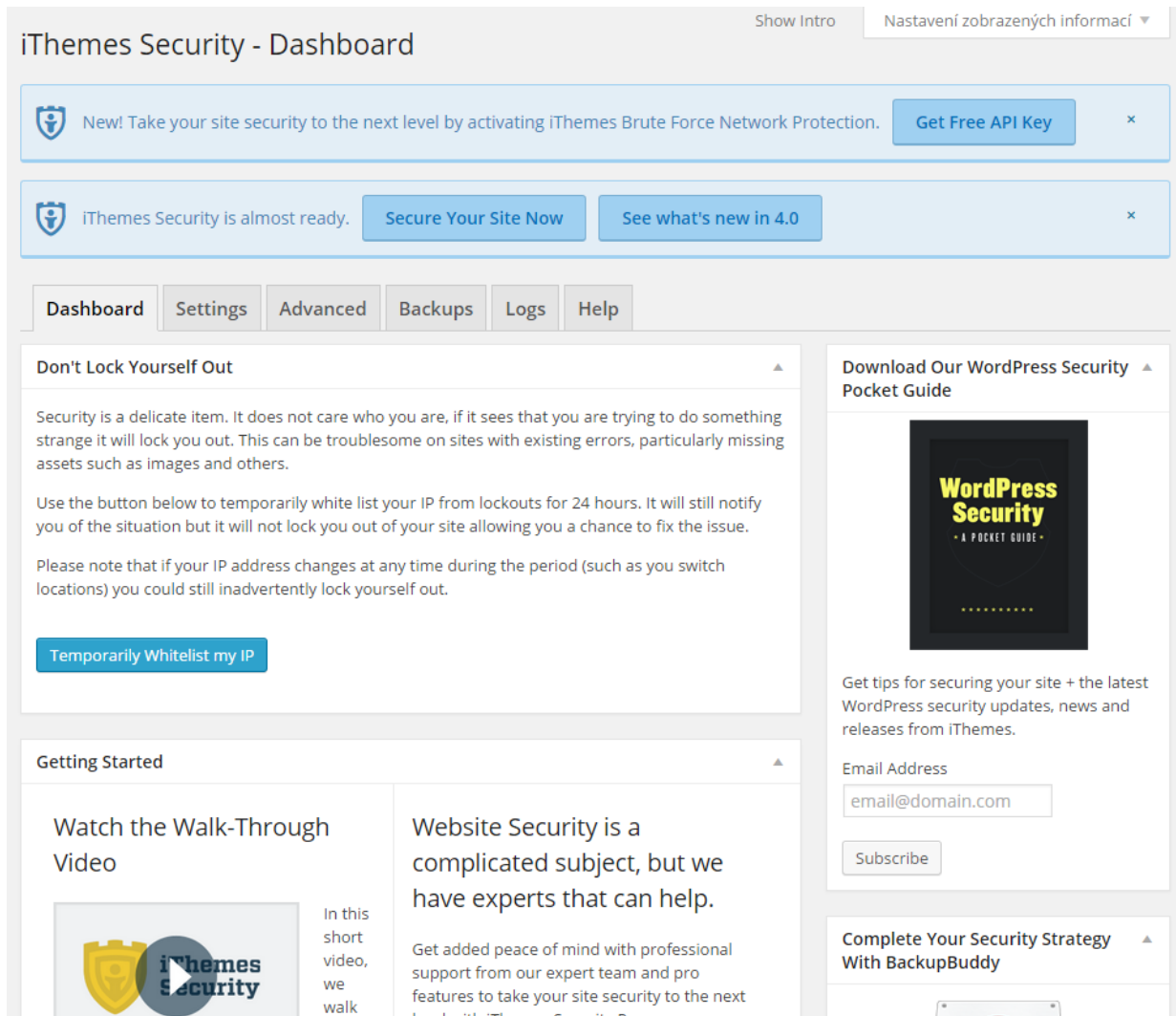
iThemes Security would like to collect anonymous data about features you use to help improve this plugin. Absolutely no information that can identify you will be collected.

[Yes, I'd like to help](#)

[Dismiss](#)

One-Click – nastaví omezení počtu přihlášení, vynutí silná hesla, skryje některé info

# iThemes Security – API Key



The screenshot shows the iThemes Security dashboard interface. At the top, there are two notification banners: one for activating iThemes Brute Force Network Protection with a 'Get Free API Key' button, and another stating 'iThemes Security is almost ready' with buttons for 'Secure Your Site Now' and 'See what's new in 4.0'. Below these is a navigation menu with tabs for Dashboard, Settings, Advanced, Backups, Logs, and Help. The main content area is divided into three sections: 1. 'Don't Lock Yourself Out' with explanatory text and a 'Temporarily Whitelist my IP' button. 2. 'Getting Started' with a video player for 'Watch the Walk-Through Video' and a text block about website security. 3. A right-hand sidebar with a 'Download Our WordPress Security Pocket Guide' section featuring a book cover and a subscription form with an email input field and a 'Subscribe' button. At the bottom of the sidebar, there is a section for 'Complete Your Security Strategy With BackupBuddy'.

# iThemes Security - přehled

iThemes Security - Dashboard Show In

Dashboard Settings Advanced Backups Logs Help

Don't Lock Yourself Out

Getting Started

Security Status

All High Medium Low Completed

### High Priority

These are items that should be secured immediately.

- Your site is not performing any scheduled database backups. [Fix it](#)
- Malware scanning is not enabled. [Fix it](#)

### Medium Priority

These are items that should be secured if possible however they are not critical to the overall security of your site.

- Your website is not protected against bots looking for known vulnerabilities. Consider turning on 404 protection. [Fix it](#)
- A user with id 1 still exists. [Fix it](#)

# iThemes security - nastavení

- 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 - nastavení

- 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 blokové useragenty a IP (spolupracuje s Enable Blacklist Repeat Offender v Global settings)

# iThemes security - nastavení

- 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 - nastavení

- 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 - nastavení

- 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 Socket 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 - nastavení

- 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
  - ~~Non-English Characters~~ - Filter Non-English Characters - v českém prostředí znefunkční vyhledávání s diakritikou
  - **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 - nastavení

- 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 mohou použít plugin <https://wordpress.org/plugins/simple-trackback-validation-with-toppsy-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 nepíší články (admini,...)

# iThemes security – další funkce

- „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 na doma*

## Lepší odstranění viditelnosti verze WP než v pluginu:

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)

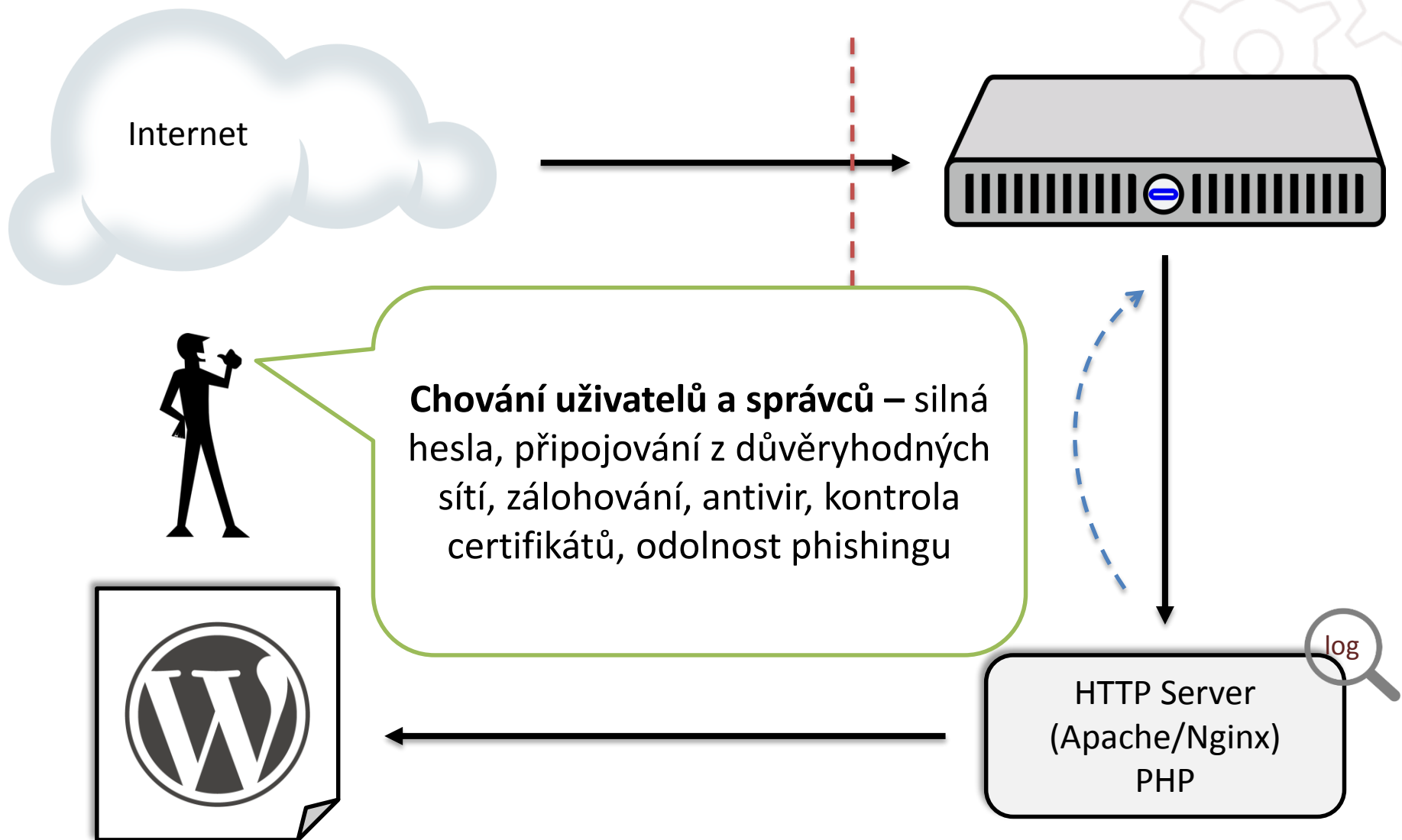
Málo známá funkcionálita WP – jedná se o speciální složku: **/wp-content/mu-plugins**

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');
```

# Uživatelé








# Tipy pro správce WP

- Nastavte přístup do administrace přes HTTPS
  - <https://wordpress.org/plugins/wordpress-https/>
  - dobrý je i přístup přes VPN, pokud je to možné
- Opravdu pravidelně zálohujte – soubory i databázi
- Netestujte pluginy na produkčním webu
- Smažte co nepotřebujete
- Přidělujte uživatelům oprávnění, která opravdu potřebují
- Pokud máte více webů, používejte systém pro hromadnou správu a aktualizaci ([InfiniteWP](#), [ManageWP](#)), pokud méně použijte plugin [WP Updates Notifier](#)
- Udržujte si seznam všech použitých pluginů a šablon
- Pokud vám vývojář řekl: „*hlavně neaktualizuje*“, chtějte vědět proč (např. si vyžádejte patch soubory se změnami, co provedl), většinou k tomu není zásadní důvod!

# Tipy pro každého

- Používejte silná hesla (používejte password manager např. [Keepass](#))
- Pozor na špatné certifikáty:   
- Používejte kvalitní a aktualizovaný antivir
- Nepřipojujte se z neznámých WiFi
- Smažte z mobilu/tabletu/notebooku všechny uložené sítě, ke kterým se připojuje bez hesla
- Nedůvěřujte všemu, co přijde mailem

# Phishing

Předmět: Máňa

Datum: Sat, 28 Feb 2015 14:32:48 +0200

Od: Máňa <mana@seznam.cz>

Komu: <ty>

Dobrý den.

Omlouvám se za nežádoucí obtěžování a přeposílám Vám vaše doklady a smlouvu které asi na můj email byly zaslané omylem.

Teda aspoň předpokládám že přesměruji správně jelikož Váš email byl uvedený ve smlouvě.

Veškeré Doklady a smlouvu odesílám přílohou stejně jak jsem to dostala.

Prosím o zjištění důvodu tohoto trapného omylu aby příště na můj email se nedostávali další zprávy obsahující nějakou citlivou informaci.

S pozdravem,

Máňa

# Phishing

Předmět: Bezpečnostní problém Hodný Hosting [9314001612]

Datum: Sat, 28 Feb 2015 14:32:48 +0200

Od: Hodný Hosting <hosting@hod.ny>

Komu: <ty>

Vážený zákazníku,

Na Vaší webové prezentaci tvujweb.cz založené na redakčním systému Wordpress byl zjištěna škodlivý kód, který masivně útočí na další weby a infikuje návštěvníky.

Neprodleně nainstalujte náš antivirový plugin Super-WP-Antivir, který naleznete v příloze i s návodem k instalaci. V opačném případě budeme bohužel nuceni Vaši webovou prezentaci pozastavit.

Hodný Hosting, Ltd.

# Další zdroje

- Info o zranitelnostech
- <https://www.owasp.org/>
- <https://wpvulndb.com/>
- <http://blog.sucuri.net/>
- <http://packetstormsecurity.com/>
  
- Hodnocení pluginů:
- <http://www.rankwp.com/>

# Domácí úkol na zítřa

- ❑ Zkontrolovat, zda nemám zranitelné pluginy
- ❑ Zkontrolovat, zda mám vygenerované unikátní šifrovací klíče ve wp-config.php
- ❑ Zazálohovat
- ❑ Smazat pluginy, co nepoužívám/byly jen k jednorázové činnosti
- ❑ Smazat zbytečné šablony (nechat jen jednu výchozí z instalace a případně rodičovskou)
- ❑ Snížit oprávnění uživatelům, kteří jej nepotřebují
- ❑ Aktualizovat, co je možné



# A to je vše, přátelé.

aktualizujte, zálohujte, používejte bezpečnostní plugin, buďte opatrní