Savjeti za maksimalnu zaštitu Wordpress CMS-a

1. Zlatno pravilo koje treba primijeniti na svakoj web stranici ili aplikaciji koja ima backend sučelje jest da se ne koristi username „admin“, „root“ i slično, s obzirom na to da, kada su u pitanju brute force napadi i upiti prema stranici, napadači najčešće koriste takva korisnička imena s raznim kombinacijama lozinki, čime se povećava vjerojatnost kompromitiranja pristupnih podataka. Umjesto korisničkog imena „admin“ ili „root“, obavezno koristite neko vlastito. Lozinka također mora biti kompliciranija. Kada je odabirete ili mijenjate unutar Wordpress sučelja, pobrinite se da indikator jačine lozinke bude na „strong“. Jedna od uspješnijih metoda da se riješite brute force napada te mogućnosti da Vam se preotmu podatci za prijavu, jest da postavite Wordpress plugin pod nazivom „Login lockdown“ koji će na temelju neuspješnih prijava privremeno onemogućiti daljnje prijave. Instalirajte ga i konfigurirajte po želji. Probajte ga konfigurirati zajedno s nekim od captcha plugina. Ako želite još i dodatnu zaštitu nad administracijskom prijavom, zaštitite wp-admin folder putem .htaccess (u cPanel sučelju pogledajte dio „Password protected directories“).

2. Hakeri i početnici koji vole isprobavati hakiranje, vrlo rado koriste sigurnosne rupe pojedinih verzija Wordpress CMS-a. Hakeri znaju točne ranjivosti određene Wordpress verzije, čije su informacije dostupne javnosti. Nažalost, sam Wordpress u source kodu koji se generira na stranici prikazuje Wordpress verziju čime napadaču može jasno dati do znanja koju ranjivost ima. Uklonite ga tako da pod „functions.php“ od same teme upotrijebite funkciju: remove_action('wp_head', 'wp_generator');. Wordpress svoju verziju još prikazuje i na rss file-u, tako da ga trebate i tamo ukloniti upotrebom funkcije: function wpbeginner_remove_version() { return ''; } add_filter('the_generator', 'wpbeginner_remove_version'); Nakon ovih radnji pobrinite se i provjerite da se „Wordpress“, „powered by wordpress“ ili slični pojmovi koji upućuju na to da je stranica rađena u Wordpress-u, ne prikazuju na Vašoj stranici. Takve stvari se obično nalaze u samoj temi u datoteci footer.php, ali se može nalaziti i drugdje.

3. Ako je prefix Vaših tablica u Wordpressu ostao wp_ , trebali biste ga promijeniti u neku drugu kombinaciju slova, jer će hakeri prilikom napada prvenstveno pokušati s wp_ prefiksom.

4. Većina modernijih tema koristi tzv. Timthumb scriptu koja je odličan alat i brine se za automatski resize i crop slika, ali je nažalost otkrivena velika sigurnosna rupa na prijašnjim verzijama, ostavljajući mogućnosti napadaču da na Vaš hosting paket bez problema naseli i izvrši malicioznu skriptu. Instalirajte i pokrenite plugin „Timthumb vulnerability scanner“ koji će provjeriti imate li timthumb, te da li ga je potrebno ažurirati.

5. Od ostalih pluginova koji se preporučuju da ih instalirate i podesite mogu se izdvojiti:

- Exploit scanner (skenira i pregledava Vaše datoteke u Wordpressu te javlja o mogućim zarazama. Velika većina njih je lažno pozitivna te je potrebno određeno znanje Javascripta i PHP-a kako bi se ustanovilo je li zaista lažno pozitivna ili nije);
- Wordfence security (štiti Vaš Wordpress na određenoj razini);
- BulletProof Security (štiti od XSS napada, RFI, CRLF, CSRF, base64, code i SQL injectiona);
- Vip Scanner.

6. Ako su kojim slučajem na Vašem hosting paketu uključeni Indexes (izlistavanje datoteka i mapa), obavezno ih ugasite na način da u htaccess datoteku dodate liniju koda „Options –Indexes“.

7. Ako ste se dosad već susreli s hakerskim napadima i ako niste promijenili šifre svoje baze, ftp računa ili security keysa unutar wp-config.php, vrijeme je da to učinite.

8. Redovito ažurirajte svoj Wordpress CMS, temu i sve pluginove. Moguće je da će se možda updateom Wordpressa ili teme ponovno pojaviti readme.html ili ponovno prikazivati verzija Wordpress CMS-a pa to provjerite i po potrebi ponovite točku 2.

Slijedeći ove upute zaštitit ćete Vašu stranicu do određene razine, a ostatak ovisi o pluginovima koje koristite (provjeravajte imaju li sigurnosne rupe) te o klijentskom računalu koje pristupa administraciji (provjeravajte računalo, redovito ga čistite od virusa, malicioznih programa i slično, jer pomoću takvih programa Vaši podatci za prijavu mogu biti kompromitirani). I na kraju, važno je i samo ponašanje korisnika. Stoga pazite na svoje pristupne podatke te ne nasjedajte na phishing poruke ili slične poruke u kojima se od Vas traži da ostavljate pristupne podatke (bilo za mail, hosting, banku i slično).