Savjeti za maksimalnu zaštitu WordPress *open source* CMS-a (2.0)

Većina vlasnika hakiranih web stranica uvijek se pita: „Zašto baš ja, zašto su mene hakirali? Koji od konkurenata mi je to mogao napraviti?" Vjerojatnost da su Vas konkurenti ili netko drugi namjerno hakirali toliko je mala da ju je bespotrebno uzimati kao jedan od mogućih razloga. Kao vlasnik web stranice izrađene u *open source* CMS-u, samo ste jedan od milijuna drugih koji se nalazi na meti hakera. Znači li to da *open source* CMS koji koristim nije kvalitetan ili da ga moram prestati koristiti? Nipošto!

Osim što je jednostavno i brzo napraviti web stranicu u WordPressu, WordPress imaj vrlo jak izgrađeni *community* te širok spektar već gotovih različitih dodataka (dizajnerski predlošci, pluginovi, ekstenzije i sl). Vašem WordPressu možete dodati nove funkcionalnosti bez potrebe za naprednim programiranjem ili ovisiti o nečijem raspoloživom vremenu. Također, savjete i odgovore na većinu Vaša pitanja vezanih uz njega naći ćete kroz različite forume.

Međutim, ono o čemu obavezno i uvijek morate voditi računa kod korištenja bilo kojeg *open source* CMS-a, pa tako i WordPressa, to je da morate redovito održavati svoju stranicu, što uključuje praćenje postoje li nove sigurnosne zakrpe WordPressa te njihovo redovito ažuriranje. U nastavku slijede naši savjeti za maksimalnu zaštitu Vašeg Wordpressa.

1. KORISNIČKO IME I LOZINKA

Zlatno pravilo koje treba primijeniti na svakoj web stranici ili aplikaciji koja ima *backend* sučelje je da se ne koristi *username* „admin", „root" i slično. Naime, 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. PRIKAZIVANJE VERZIJE WORDPRESSA I OZNAKA VEZANIH UZ WORDPRESS

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. Oznaku verzije Wordpressa uklonite tako da pod „functions.php“ od same teme upotrijebite funkciju: **remove_action('wp_head', 'wp_generator');**.

WordPress svoju verziju još prikazuje i na *rss fileu*, tako da oznaku verzije Wordpressa 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 oznake „WordPress“, „Powered by WordPress“ ili slični pojmovi, koji upućuju na to da je stranica rađena u Wordpress-u, ne prikazuju na Vašoj stranici. Takve oznake se obično nalaze u samoj temi u datoteci **footer.php**, ali se mogu nalaziti i na drugim mjestima.

3. PREFIX TABLICA

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. TIMTHUMB SKRIPTA

Većina modernijih tema koristi tzv. *Timthumb* skriptu 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 je li ga potrebno ažurirati.

5. KORISNI PLUGINOVI

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. ISKLJUČIVANJE INDEXES

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. PROMJENA LOZINKI

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. AŽURIRANJE CMS-A, TEMA I PLUGINOVA

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.

9. UKLANJANJE TEMA KOJE NE KORISTITE

Sve teme koje ne koristite obrišite, uključujući i WordPressove defaultne teme. Svaka tema koja postoji, a ne koristi se, nosi određeni rizik za postojanje sigurnosne rupe.

10. OBAVEZNO NAPRAVITE SVE KORAKE OD 1. DO 9.

Slijedeći ove upute zaštitit ćete svoju 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).

Iznimno je važno da slijedite i napravite **SVE NAVEDENE KORAKE**, u suprotnom Vaš WordPress neće biti zaštićen na temeljnoj razini i postojat će velika vjerojatnost neovlaštenog upada na Vašu stranicu.

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).