Ingyenes, mégis hatékony WP védelmek

Milyen lehetőségeink vannak a WordPress honlapunk védelmére

Rólam

Rottenbacher Tamás

- WordPress Magyarország csapatához tartozom 2016 óta és a Nyílt Web Alapítvány egyik alapítója vagyok.
- 2006 óta foglalkozok honlapkészítéssel, 2008 óta SEO-val és WordPress fejlesztéssel, 2010 óta WordPress oldalak üzemeltetésével, jó ideje saját vállalkozásban.
- 2018 óta több szerverrel rendelkezem (Cloud VPS-el már).
- Több hazai WP-s projektet vezetek, ami a közösséget támogatja, például TrustedWP.hu alapító, szerkesztő vagy a WordPress Budapest MeetUp előadásorozat egyik szervezője, előadója vagyok.

RotiSoft

TrustedWP

WordPress Magyarország

Nyílt Web Alapítvány

WordPress Budapest Meetup

Szükséges a WordPress-t “védeni”?

- A válasz nem olyan egyszerű, de rövid válasz: Nem szükséges, de ajánlott.

Miért?

Maga a WordPress nagyon biztonságos. A támadások legtöbb esetben plugin vagy felhasználói hibákat használnak ki.

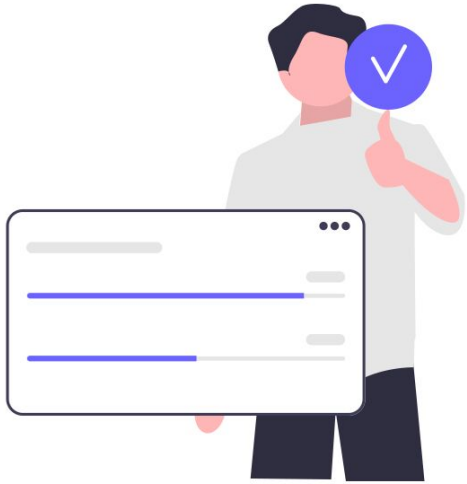
Mi tartozhat ide? Például: Kikerült jelszó, nem megfelelő (óccó) hosting, elmulasztott frissítések, rosszul megírt bővítmények

Ezek ellen nem jó

- Biztonsági bővítmények használata (például Wordfence, SolidWP -iThemes Security), mivel megfelelő beállítás nélkül alig érnek valamit, jéghegy csúcsát jelzik csak + lassítanak
- Jelszavak osztogatása
- “Most működik, nem kell hozzányúlni” gondolatmenet és vallási alapú “védelem” vagy szerencse
- Régi, nem védett eszközök használata

Ezek ellen a védekezés

- Hivatalos, megbízható, aktívan támogatott bővítmények és sablon használata
- Saját eszközeink (asztali gép, telefon) védelme (pl. víruskeresőkkel)
- Jelszavak megfelelő kezelése, védelme
- Rendszeres frissítések, ellenőrzésekkel (pl. inkognitó ablakban keresés és megtekintés, Search Console bekötés)
- Szakemberek bevonása, megbízása

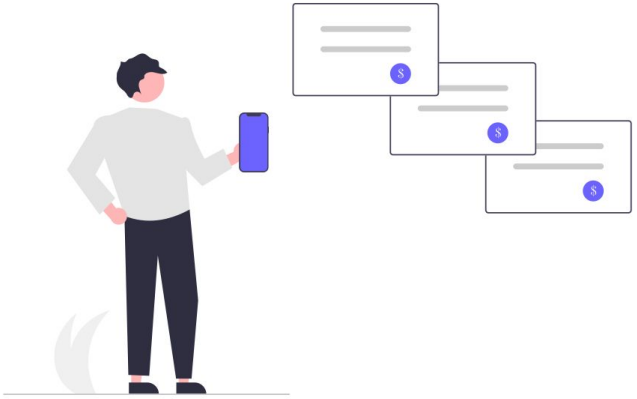



SZAKEMBERRE BÍZNI
BAJBAN AZONNALI SEGÍTSÉGET KÉRNI PÁNIKOLVA
imgflip.com

TIPP:
Rendszeresen ellenőrizzük mely felhasználóknak milyen szerepköre van!

1. Lokális
2. WP-ben
3. Tárhely
4. Szerver
5. Domain

(pre server)



Lokális védelem

A lokális védelem alatt értendő, hogy milyen olyan eszköz aminél a hozzáférések megjelenhetnek, legyen naprakész (frissítve legyen) és legyen rajta szintén naprakész adatbázissal víruskereső, védelem.

Hab a tortán ha jelszókezelőt használunk. (Személyes ajánlásom: RoboForm)

Ne használjunk ingyenes, nyitott WIFI hálózatot sehol vagy magasabb szintű védelemmel csak.

Ne txt/word fájlba tároljuk a jelszavakat, minél kevesebb helyre mentsük el azokat. A kockás füzet még mindig biztonságosabb ha csak otthon van!

WP szinten

Felhasználóként

- Biztonsági mentés és frissítés, frissítés
- Felhasználók rendszeres ellenőrzése akik az adminhoz hozzáférnek (aki feliratkozó vagy vásárló szerepkörnél magasabb)

Fejlesztőként

- A htaccess szabályok és PHP snipet-ek hozzáadása
- Kódok WP Codex-ben foglaltak szerinti alkalmazása (például data validation, szerepkör ellenőrzés, esc_html output)

Sose bízz ügyfélben, felhasználóban!

Fejlesztőként minden felhasználók által megadott adatot validáljunk, mielőtt mentjük! Lehet hiba, de lehet szándékos is, erre fel kell készülni!

Minden bővítmény, sablon vagy funkció készítéskor az összes adatot ellenőrizzük minden esetben, pl. az inject alapú kártékony kódok ellen.

A naplózás, log pedig segít megtalálni a probléma forrását.

Ha egy admin jelszavával belép a támadó, akkor se a WP, se a fejlesztő nem fogja tudni kivédeni*.

Megoldás: Jogosultság korlátozása és log, napló készítése és pl. 404-es napló alapján egyéni védelmek készítése

Tárhely szinten

Felhasználóként

- Fájl jogosultságok ellenőrzése (CHMOD, legtöbb tárhelyadminban van)
- Olyan szolgáltató választása, mely rendszeresen frissíti a szoftveres környezetet
- Mappatartalom listázás kikapcsolása

Fejlesztőként

- Tárhely beállításainak finomhangolása

Szerver szinten

Felhasználóként

- Jó szolgáltató választása (occó vagy szomszéd Ferike megoldja legyen mindig gyanús...)

Fejlesztőként

- Szerver szoftveres környezetének rendszeres frissítése, sebezhetőségek nyomonkövetése (aktualitás fontossága)
- Apache/Nginx naplózás és figyelés
- Egyéni szabályok (pl. fájlok módosításának tiltása a frissítéseken kívül)

Pre szerver szinten

Mi is az a pre-szerver szint?

A legtöbb rosszindulatú támadás megfogható és meggátolható már azelőtt, hogy az elérné a szervert, illetve azon a honlapunkat. Ez lehet akár egy szakosodott domain névszerver szolgáltató (például Cloudflare) vagy terhelés elosztó, zárt cloud hálózat.

Felhasználó tud így védekezni?

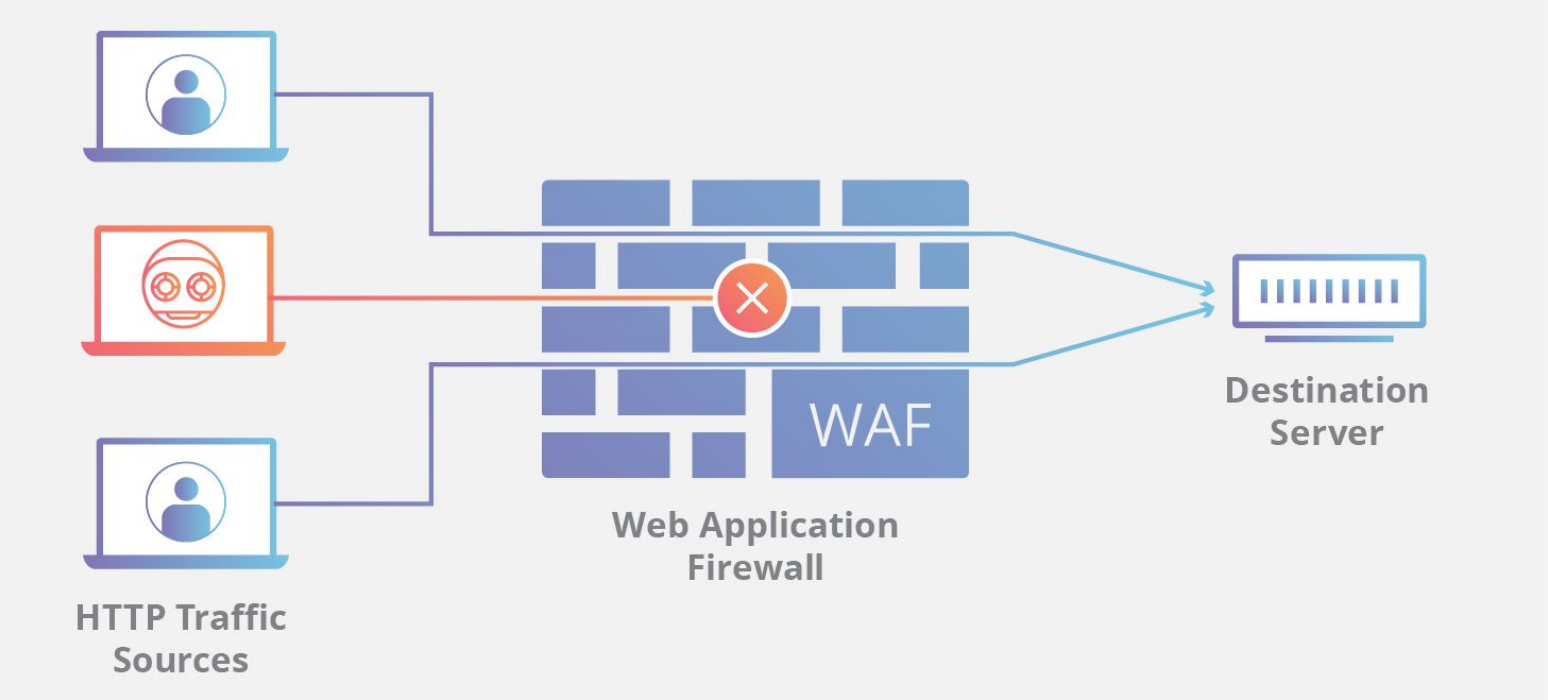
Köszönhetően az egyre elérhetőbb leírásoknak és pl. Cloudflare szolgáltatásának köszönhetően felhasználók is védekezhetnek így!

Beszéljünk a Cloudflare-ről

Hogyan működik?

- A CF minden adatot, lakérést megvizsgál ami a szerverünk felé halad
- Hatalmas adatbázisból dolgozik, így könnyebben talál viselkedésmintákat
- Képes a kártékony, rosszindulatú bot-okat megállítani
- Gyorsít honlapunkon, miközben véd (CDN és szerver kisebb terhelése)

Cloudflare WAF



A Cloudflare (ingyenes) védvonala: WAF, avagy tűzfal

Lehetőségek jéghegyének csúcsai:

- Korlátozhatjuk url-ek elérését
  - Kitilthatunk országokat
  - Egyéni védelmet adhatunk (pl. WordPress wp-login.php fájlának és wp-admin lekéréseknek, így nem kell admin és belépés url-t cserélni)
- Több szintű védelmet állíthatunk be (blokkolástól és automatikus tiltástól kezdve captcha-ig vagy JS tesztig, kivételeket kezelhetünk, pl. bankok ip tartományát whitelist-elhetjük)
- Injection alapú támadások kivédése (url alapú lekérések szűrésével)

Edit rule

Custom rules

Rule name (required)

wp-ved-wpmeetup-minta

Give your rule a descriptive name.

Field	Operator	Value	
URI Path	contains	/wp-admin/	And
		e.g. /content	
And			
URI Path	does not conta...	/wp-admin/admin-ajax.php	And
		e.g. /content	
Or			
URI Path	contains	/xmlrpc.php	And
		e.g. /content	
Or			
URI Path	contains	/wp-login.php	And
		e.g. /content	
And			
URI Full	does not conta...	logout	And Or
		e.g. https://example.com/contact?page=1234	

Oct 18, 2024 10:54:00 PM	Interactive Challenge	Singapore	152.42.251.162	Custom rules

Matched service

Export event JSON

Service	Custom rules	Ruleset	default …8bac1d66
Action taken	Interactive Challenge	Rule	wp-ved …2bb6843e

Request details

Ray ID	8d4b6bca1dc67983	HTTP Version	HTTP/1.1
IP address	152.42.251.162	Method	GET
ASN	AS14061 DIGITALOCEAN-ASN	Host	wpmeetup.hu
Country	Singapore	Path	//xmlrpc.php
User agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36	Query string	?rsd

Oct 18, 2024 8:02:10 PM	Interactive Challenge	Ireland		138.91.59.210	Custom rules

Matched service

Export event JSON

Service	Custom rules	Ruleset	*Unavailable* …8bac1d66
Action taken	Interactive Challenge	Rule	*Unavailable* …2bb6843e

Request details

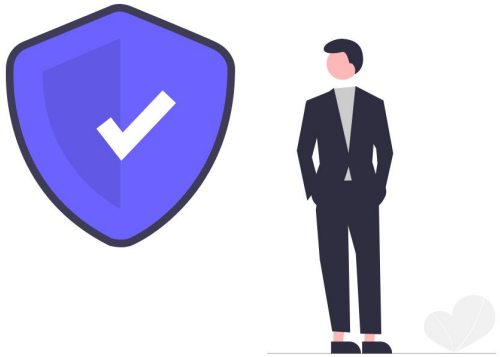
Ray ID	8d4a7018385cbe3b	HTTP Version	HTTP/1.1
IP address	138.91.59.210	Method	GET
ASN	AS8075 MICROSOFT-CORP-MSN-AS-BLOCK	Host	wpmeetup.hu
Country	Ireland	Path	/wp-login.php
User agent	*Empty user agent*	Query string	*Empty query string*

Tanácsok Cloudflare WAF alkalmazáshoz

Gondoljuk át, hogy mely url-eket védünk. Például teljes honlapunkra ne állítsunk be captcha szűrőt, mert akkor keresőrobotokat is megfogja. Illetve webáruházakban (például WooCommerce Fiókom oldalra) sem érdemes, mert elriaszthatja a látogatót. Ott inkább WP szinten használjunk catpcha-t.

DEV/stagging oldalt levédhetünk teljesen és különösképpen a keresőrobotokat, hogy ne legyen duplikáció.

+1 Tipp: A Cloudflare esetén a Cookie-khoz hozzá kell adni a CF-et is, mivel látogató azonosításhoz van olyan módszere, melyhez cookie-t használ. (Személyes adatot nem tárol benne.)



A Cloudflare WAF magasabb szinten

Több lehetőséget használhatunk:

- Korlátozhatjuk url-ek elérését akár cookie vagy IP alapon (fix IP-vel lehessen például az admint és belépést elérni)
- Azonosító alapján egyéni átirányítás hozzáadása
- JSON és API lekérések megszűrése és limitálása (pl. bank, SEO eszköz IP tartományára)

Ez csak pár fontos példa a több száz funkcióból.

Ha ingyenes, mivel fizetünk a CF-nek?

Az itt említett alap WAF beállítások ingyenes fiókkal is elérhetőek.

Az “ingyenes” jelző alatt értsük: Nem anyagiakkal fizetünk a szolgáltatásért. A Cloudflare a mi honlapunk forgalmi adatait is felhasználja a saját védelmének tanításához. (Nem személyes, hanem csak forgalmi adatokat.)

Fizetős csomagok részletesebb beállítási és többlet funkciókat biztosítanak.

Mi ellen nem védekezhetünk

Mindig vannak olyan esetek, amikor olyan helyzet áll elő, hogy minden törekvés ellenére megtörténik a baj. Ilyenre is fel kell készülni!

Lehet például Zero day vulnerability. (Hiába frissítünk, hiába védekezünk egyéni szabályokkal.) Illetve ha komoly, profi támadóval van dolgunk.

“Megoldás”

Mindig legyen biztonsági mentésünk!!!44!4!!NÉGY!!!

Minél fontosabbak (és minél gyorsabban bővülnek) a mentett adatok, annál gyakrabban készüljön mentés, lehetőleg több helyre, automatizáltan!

Hivatkozások

- **Véleményem a biztonsági bővítményekről és ennek az okai:**
  https://rotisoft.hu/blog/wordpress-biztonsagi-bovitmenyekrol-velemeny-cikk/
- **WordPress védelmének növelése:**
  https://rotisoft.hu/blog/wordpress-oldal-biztonsag/
- **WordPress szerepkörök, jogosultságokról:**
  https://rotisoft.hu/blog/wordpress-szerepkorok-jogosultsagok/
- **Biztonsági mentés készítés:**
  https://hu.wordpress.org/wordpress-biztonsagi-mentes-backup/
  https://rotisoft.hu/blog/wordpress-biztonsagi-mentes/
- **Cloudflare WAF:**
  https://developers.cloudflare.com/waf/get-started/

Köszönöm a figyelmet!

Kérdésekre az utolsó előadást követően vagy email-ben szívesen válaszolok!

Rottenbacher Tamás

www.rotisoft.hu

tamas@rotisoft.hu

+3630 387 39 69