

# Tartalomjegyzék

<b>Weboldalüzemeltetői praktikák</b> .....	1
<b>Átlag weboldal</b> .....	1
<b>Wordpress praktikák</b> .....	2
<b>Weboldalak betöltési sebességének növelése</b> .....	3



# Weboldalüzemeltetői praktikák

Itt próbáljuk összefoglalni azokat a - szerintünk - „best practices”, azaz jó gyakorlatot megvalósító beállításokat egy weboldal esetén. A javaslatok több esetben a web gyökérmappájában található .htaccess fájl érintik, ezért csak akkor fogjon hozzá, ha biztos a dolgában. Hibás beállítás esetén a weboldala elérhetetlenné válhat! Többnyire az oldal biztonságát vagy és/vagy az oldal betöltési sebességét növeli minden beállítás. A leírt beállítások nem új keletűek, de igyekszünk egy áttekinthető összefoglalót adni. A CMS rendszerek (Joomla, Wordpress, stb.) egyéb beállításaival és használatával itt nem foglalkozunk, mert azt már nagyon sok helyen leírták az interneten. A doimain.hu -t mindig cserélje ki a saját domainjére.

## Átlag weboldal

www átirányítása www nélküli oldalra, pl.: [www.mav-it.hu](http://www.mav-it.hu) ⇒ [mav-it.hu](http://mav-it.hu)

```
#### www => non-www ####
RewriteCond %{HTTP_HOST} ^www\.domain\.hu [NC]
RewriteRule ^(.*)$ https://domain.hu/$1 [L,R=301]
```

http: *oldal átirányítása https*: oldalra, ha erőltetni szeretnénk a titkosított adatforgalmat

```
#### http => https ####
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

Gzip oldaltömörítés bekapcsolása. Drasztikusan csökkentheti az oldal betöltési sebességét (a szerveren is telepítve kell lennie a modulnak!).

```
#### GZIP ####
<ifmodule mod_deflate.c>
AddOutputFilterByType DEFLATE text/text text/html text/plain text/xml
text/css application/x-javascript application/javascript
</ifmodule>
```

Hotlink védelem. Ez a kicsi kódcska sok sávszélességet spórolhat nekünk, illetve a webszerver üzemeltetőjének. Megakadályozza, hogy a weboldal fájljait más weboldalak is használják, ezáltal „ellopják” az Ön sávszélességét.

```
#### Hotlink protection ####
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^https://(.\+\.)?domain\.hu/ [NC]
RewriteRule \.(gif|jpg|jpeg|bmp|zip|rar|xml|png|css|pdf|js)$ - [F]
```

Az Apache alapértelmezésben (ha a könyvtár nem tartalmaz index.html vagy index.php fájlt) megmutatja a könyvtár tartalmát. Amennyiben ezt nem tartjuk kívánatosnak, akkor helyezzük ezl az alábbi kódpt a .htaccess fájlban:

## Options -Indexes

Az alábbi kód megakadályozza számos [exploit](#) becsempészését az URL-be.

```
# Szűrünk minden base64 kódolt tartalmat az URL-ben
RewriteCond %{QUERY_STRING} base64_encode[^(]*\[^\(\)\]* [OR]
#
# Szűrjük a <script></script> tageket az URL-ben
RewriteCond %{QUERY_STRING} (<|%3C)([^\s]*s)+cript.*(>|%3E) [NC,OR]
#
# Megakadályozzuk a PHP GLOBALS változók (át)írását
RewriteCond %{QUERY_STRING} GLOBALS(=|\\[|\\%[0-9A-Z]{0,2}) [OR]
#
# Megakadályozzuk a _REQUEST változó átírását
RewriteCond %{QUERY_STRING} _REQUEST(=|\\[|\\%[0-9A-Z]{0,2})
#
# a fenti feltételek esetén 403 Forbidden header-t ad vissza a böngészőnek
RewriteRule .* index.php [F]
```

## Wordpress praktikák

A wordpress egyik sebezhetősége, hogy a gyökérmappában található xmlrpc.php fájlon keresztül az adatbázishoz próbálnak hozzáférni akár brute force technikával. Ez a kis kód elérhetetlenné teszi ezt a fájlt (illetve átírányítja, és „no” szócskát láthatunk a fájl betöltésekor). (Természetesen ha használni akarjuk az RPC szolgáltatást akkor NE használjuk ezt a kódcskát!)

```
#### xmlrpc attack protection ####
Redirect 403 /xmlrpc.php
ErrorDocument 403 "no"
```

Vannak bizonyos könyvtárak, amikben nem szabad .php fájlokat futtatni. Ilyen pl a /wp-includes és a /wp-content/uploads könyvtárak. Ezekbe tegyük bele egy-egy üres .htaccess fájlt, és másoljuk bele az alábbi kódsort. Ezzel megakadályozzuk, hogy a rosszindulatú PHP kódot futtasson valaki ezekben a könyvtárakban.

```
<Files *.php>
deny from all
</Files>
```

Talán az egyik legkényesebb fájl a gyökérmappában lévő wp-config.php. Sok kényes adat között tartalmazza pl. az adatbázis hozzáférési adatait is. Ezt az alábbi kódcskát elhelyezve a gyökérmappában lévő .htaccess file-ban megakadályozzuk, hogy a kiszolgáló IP címétől eltérő IP címről elérjék a fájlt.

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```

## Weboldalak betöltési sebességének növelése

Az alábbi lista korántsem teljes, de igyekeztünk a legfontosabb tippeket összegyűjteni. Az alábbi beállítások / módosítások nagy részére a hosting szolgáltató együttműködése, támogatása kell. A weboldalunk sebességének mérésére számtalan eszköz létezik. Mi a <https://developers.google.com/speed/pagespeed/insights/> vagy a <https://gtmetrix.com/> oldalt szoktuk használni, de számtalan kiváló eszköz van erre.

#	Módosítás / opció	Online ellenőrzés	Elérhető sebességnövekedés
1.	Az első és legfontosabb, hogy olyan hosting szolgáltatót válassz, ahol a legfrissebb technológiákat használják. (Pl. SSD, stb.) Magyarország ebből a szempontból fejlett pozícióban van, a legtöbb szolgáltatónál jó helyen lesz az oldalad.	Egy szolgáltató minőségének objektív mérésére nincs online eszköz. :)	10-50%
2.	Ellenőrizzük, hogy a webkiszolgáló támogatja a HTTP/2 üzemét. Ha nem, kérjük a szolgáltatóunktól, hogy kapcsolja be. A HTTP/2 csak SSL titkosított oldalon működik!	<a href="https://tools.keycdn.com/http2-test">https://tools.keycdn.com/http2-test</a>	2-5%
3.	Kapcsolja be a gzip tömörítést. Ilyenkor a webservertől a weboldal bizonyos elemeit, így gyorsabban megkapja a böngésző, amely kicsomagolja és megjeleníti. Itt ellenőrizheti, hogy az Ön	<a href="https://www.giftofspeed.com/gzip-test/">https://www.giftofspeed.com/gzip-test/</a>	2-8% a tartalomtól függően

#	Módosítás / opció	Online ellenőrzés	Elérhető sebességnövekedés
4.	PHP alapú oldalnál (a CMS rendszerek túlnyomó többsége az) vannak gyorsítótárazási technikák, ilyen pl az Opcache, a memcache(d) és még néhány.	Ezt online nem lehet ellenőrizni. Amennyiben a szolgáltatója valamilyen adminisztrációs felületet a rendelkezésére bocsát (pl. cPanel), ott ellenőrizheti.	3-5%
5.	Tömörítsd / optimalizáld az oldaladon a képeket.	Sok ilyen online eszköz van, pl: <a href="https://imagecompressor.com/">https://imagecompressor.com/</a>	2-10% az oldal összetételétől függően.
6.	Tömörítsd / optimalizáld az oldaladon a javascript és CSS tartalmat. Előfordul, hogy a CMS rendszered is támogatja, de lehet, hogy manuálisan kell elvégezned. Az ilyen tömörítők eltávolítják a felesleget ezekből a fájlokból, és más technológiákkal is tömörebbé teszik. A JS fájlok betöltését késelted (ha lehet) defer vagy async attrinútomokkal.	JS fájlokra pl: <a href="https://javascript-minifier.com/">https://javascript-minifier.com/</a> CSS fájlokra pl: <a href="https://cssminifier.com/">https://cssminifier.com/</a>	2-10% az oldal összetételétől függően.

#	Módosítás / opció	Online ellenőrzés	Elérhető sebességnövekedés
7.	Ha fontos, hogy a világ minden pontjáról ugyanolyan gyorsan töltődjön be az oldal, akkor használj valamilyen CDN-t. Vannak CMS rendszerek amik ezt natívan támogatják, és bizonyos adminisztrációs rendszereken (pl. cPanel) is bekapcsolható. Ha az oldalad csak magyarországi látogatóknak szánod, akkor nem tapasztalsz különösebb változást CDN használatával.	<a href="https://www.cdnplanet.com/tools/cdnfinder/">https://www.cdnplanet.com/tools/cdnfinder/</a>	10-20% CDN-től függően.
8.	Használj minél magasabb verziószámú PHP-t! A frissebb verziók általában valamivel gyorsabbak mint az előzők, ezen felül a biztonságot is javítják. Ellenőrizd, hogy a szolgáltatóknál a legfrissebb PHP elérhető-e.	A legfrissebb verziót itt ellenőrizheted: <a href="https://www.php.net/supported-versions.php">https://www.php.net/supported-versions.php</a> Az éppen futó PHP megbízható detektálására online nincs mód.	5-25% attól függően, milyen elmaradásban vagy az aktuális verziótól.
9.	Ha lehet, kapcsoltsd be a szolgáltatóddal a Google-féle PageSpeed modult. Szárnyakat adhat a weboldalaidnak, de a beállítása komoly felkészülést igényel!	Online ellenőrzésre nincs lehetőség, de a <a href="https://www.modpagespeed.com/doc/config_filters">https://www.modpagespeed.com/doc/config_filters</a> oldalon mindent megtalálsz a beállításhoz.	akár 100-200% is lehet, beállításoktól függően.
10.	Ha lehet, konvertáld a képeket WebP vagy más korszerű formátuma png vagy jpg helyett.	Itt ellenőrizheted, hogy mely böngészők kompatibilisek a WebP formátummal: <a href="https://caniuse.com/webp">https://caniuse.com/webp</a>	0-50% a képek számától és méretétől függően.

From:  
<https://wiki.mav-it.hu/> - **Mav-IT Wiki**

Permanent link:  
<https://wiki.mav-it.hu/web>

Last update: **2020. December 23. 18:43**

