Webservery

Základní bezpečnostní pravidla pro Wordpress a Joomla

Oblíbené redakční systémy Wordpress a Joomla jsou velmi častým cílem útočníků pro svojí rozšířenost.
Vhodným nastavením a dodržováním několika zásad se dá řadě těchto útoků předejít.

Základem je udržovat redakční systém vždy v nejaktuálnější dostupné verzi. Povědomí o nově nalezených bezpečnostních trhlinách se rychle šíří a zanedlouho pátrá celá řada automatizovaných skriptů a botů, aby je objevila a využila jich.

Wordpress i Joomla obsahují mechanismus pro jejich automatickou aktualizaci. Jeho povolení je však nutno zvážit, problematická aktualizace může webovou aplikaci i znefunkčnit.

Důležité je věnovat pozornost i instalovaným pluginům a šablonám. Je třeba udržovat jejich verze aktuální, instalovat pouze ty důvěryhodné a rozšířené, pokud možno z důvěryhodných zdrojů, naopak u těch zastaralých s ukončeným vývojem se poohlédnout po aktualizovaných alternativách.

Dalším bodem jsou správná práva na adresářích a souborech.
Pro Wordpress i Joomlu platí, že práva adresářích by měla být 755, na souborech pak 644.

Dále je vhodné u Wordpresu nastavit práva 600 pro soubor wp-config.php, u Joomly 444 pro configuration.php.
Nikdy nikde nenastavujte práva 777!

Obecné zásady

Nepoužívat pro účty běžná jména jako 'Admin' nebo 'Administrator'. Při bruteforce útoku budou vyzkoušena jako první.

Používejte pro uživatelské účty bezpečná hesla. Takové heslo by nemělo obsahovat žádné běžně používané slovo a zároveň by mělo obsahovat malá a velká písmena, číslice a speciální znaky.

Zabezpečení pomocí .htaccess

Omezení dostupnosti přihlašovací stránky pouze na vybrané IP adresy

Pro Wordpress je zapotřebí přidat do souboru .htaccess v jeho kořenovém adresáři následující obsah (pokud neexistuje, vytvořit jej):

```
<Files wp-login.php>
        Order deny,allow
        Deny from all
    Allow from 12.34.56.78
```

Allow from 98.76.54.32
</Files>

Pro Joomlu je nutno vytvořit soubor .htaccess v adresáři /administrator s následujícím obsahem:

Order deny,allow
Deny from all
Allow from 12.34.56.78
Allow from 98.76.54.32

Zakázání spouštění PHP v určitých adresářích
Adresáře určený pro upload souborů, obvykle obrázků, nejsou určeny pro umístění PHP skriptů. Pokud se tam nějaký objeví, byl obvykle zapsán útočníkem. Z hlediska bezpečnosti je lepší v těchto adresářích provádění PHP skriptů rovnou zakázat.

Stačí vytvořit soubor .htaccess o následujícím obsahu a následně jej umístit v požadovaném adresáři:

php_flag engine off

<Files *.php>
Order allow,deny
Deny from all
</Files>

V případě Wordpressu jde o tyto adresáře:

/wp-includes
/wp-content/uploads

V případě Joomly:
/images

Unikátní ID: #1014
Autor: Technicka podpora
Aktualizováno: 2016-05-01 22:36