ISAPIRewrite or Mod_Rewrite Rules

Posted At : August 8, 2008 4:29 PM | Posted By : Mark Kruger
Related Categories: Coldfusion Security

For those of you interested in stopping the SQLi attack before it even hits your ColdFusion server, you might try these rewrite rules are from the CF-Linux email list (run by House of Fusion). They were provided by list member Mike Chytracek and forwarded to me by Linux CFG Ryan Stille. These rules are for for use with Helicon's ISAPI Rewrite filter, but with very little tweaking these rules aught to work for Apache Mod_rewrite as well.

```
# Helicon ISAPI_Rewrite configuration file

# Version 3.1.0.54


RewriteEngine On

RewriteCompatibility2 On

RepeatLimit 20

RewriteBase

# unsupported directive: [ISAPI_Rewrite]


# CacheClockRate 300


RewriteRule ^.*DECLARE%20.*$ http://www.cybercrime.gov/ [NC]

RewriteRule ^.*NVARCHAR.*$ http://www.cybercrime.gov/ [NC]

RewriteRule ^.*sp_password.*$ http://www.cybercrime.gov/
[NC]
RewriteRule ^.*%20xp_.*$ http://www.cybercrime.gov/ [NC]

RewriteRule ^.*EXEC\(@.*$ http://www.cybercrime.gov/ [NC]

RewriteRule ^.*%20@.*$ http://www.cybercrime.gov/ [NC]


RewriteRule ^METHOD$ OPTIONS
```

Please note that these rules will actually redirect the request to the governments cybercrime website. That's going to freak a few folks out if you end up with any fals positives :)