

```
# BULLETPROOF .47.1 MAINTENANCE .HTACCESS
```

```
RewriteEngine On  
RewriteBase /
```

```
# REQUEST METHODS FILTERED
```

```
RewriteEngine On  
RewriteCond %{REQUEST_METHOD} ^(HEAD|TRACE|DELETE|TRACK|DEBUG) [NC]  
RewriteRule ^(.*)$ - [F,L]
```

```
# TIMTHUMB FORBID RFI BY HOST NAME BUT ALLOW INTERNAL REQUESTS
```

```
RewriteCond %{QUERY_STRING} ^.*(http|https|ftp)(%3A|:)(%2F|/)(%2F|/)(w){0,3}?.?  
(blogger|picasa|blogspot|tsunami|petapolitiki|photobucket|imgurl|imageshack|wordpress\.com|img  
thegame).*$ [NC,OR]  
RewriteCond %{THE_REQUEST} ^.*(http|https|ftp)(%3A|:)(%2F|/)(%2F|/)(w){0,3}?.?  
(blogger|picasa|blogspot|tsunami|petapolitiki|photobucket|imgurl|imageshack|wordpress\.com|img  
thegame).*$ [NC]  
RewriteRule .* index.php [F,L]  
RewriteCond %{REQUEST_URI} (timthumb\.php|phpthumb\.php|thumb\.php|thumbs\.php) [NC]  
RewriteRule . - [S=1]
```

```
# BPSQSE BPS QUERY STRING EXPLOITS
```

```
RewriteCond %{HTTP_USER_AGENT} (<%0A| %0D| %27| %3C| %3E| %00) [NC,OR]  
RewriteCond %{HTTP_USER_AGENT} (libwww-  
perl|wget|python|nikto|curl|scan|java|winhttp|HTTrack|clsh|http|archiver|loader|email|harvest|  
RewriteCond %{THE_REQUEST} \?\ HTTP/ [NC,OR]  
RewriteCond %{THE_REQUEST} \/\ * \ HTTP/ [NC,OR]  
RewriteCond %{THE_REQUEST} etc/passwd [NC,OR]  
RewriteCond %{THE_REQUEST} cgi-bin [NC,OR]  
RewriteCond %{THE_REQUEST} (<%0A| %0D) [NC,OR]  
RewriteCond %{REQUEST_URI} owssvr\.dll [NC,OR]  
RewriteCond %{HTTP_REFERER} (<%0A| %0D| %27| %3C| %3E| %00) [NC,OR]  
RewriteCond %{HTTP_REFERER} \.opendirviewer\. [NC,OR]  
RewriteCond %{HTTP_REFERER} users\.skynet\.be.* [NC,OR]  
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=http:// [OR]  
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=(\.\.//?)+ [OR]  
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=/([a-z0-9_ ]//?)+ [NC,OR]  
RewriteCond %{QUERY_STRING} \=PHP[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{11} [NC,OR]  
RewriteCond %{QUERY_STRING} (\.\.//|\.\. ) [OR]  
RewriteCond %{QUERY_STRING} ftp\ : [NC,OR]  
RewriteCond %{QUERY_STRING} F44\ : [NC,OR]
```

