

```
#Redirecting common scanner bots as well as malicious input to where they should be targeted
<IfModule mod_rewrite.c>
RewriteCond %{HTTP_USER_AGENT} ^w3af.sourceforge.net [NC,OR]
RewriteCond %{HTTP_USER_AGENT} dirbuster [NC,OR]
RewriteCond %{HTTP_USER_AGENT} nikto [NC,OR]
RewriteCond %{HTTP_USER_AGENT} sqlmap [NC,OR]
RewriteCond %{HTTP_USER_AGENT} fimap [NC,OR]
RewriteCond %{HTTP_USER_AGENT} nessus [NC,OR]
RewriteCond %{HTTP_USER_AGENT} whatweb [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Openvas [NC,OR]
RewriteCond %{HTTP_USER_AGENT} jbrofuzz [NC,OR]
RewriteCond %{HTTP_USER_AGENT} libwhisker [NC,OR]
RewriteCond %{HTTP_USER_AGENT} webshag [NC,OR]
RewriteCond %{HTTP_USER_AGENT} (havi|Netsparker|libwww-
perl|python|nikto|curl|scan|javal|winhttp|clshhttp|loader) [NC,OR]
RewriteCond %{HTTP_USER_AGENT} (<|>|'|"|\)|\| \| %0A| %0D| %27| %3C| %3E| %00) [NC,OR]
RewriteCond %{HTTP_USER_AGENT} (;|<|>|'|"|\)|\| \| %0A| %0D| %22| %27| %28| %3C| %3E| %00). *(libwww-
perl|python|nikto|curl|scan|javal|winhttp|HTTrack|clshhttp|archiver|loader|email|harvest|extra
[NC,OR]
RewriteCond %{HTTP:Acunetix-Product} ^WVS
RewriteCond %{REQUEST_URI} (<| %3C|([\^s]*s)+cript.*<| %3E) [NC,OR]
RewriteCond %{REQUEST_URI} (<| %3C|([\^e]*e)+mbed.*<| %3E) [NC,OR]
RewriteCond %{REQUEST_URI} (<| %3C|([\^o]*o)+bject.*<| %3E) [NC,OR]
RewriteCond %{REQUEST_URI} (<| %3C|([\^i]*i)+frame.*<| %3E) [NC,OR]
RewriteCond %{REQUEST_URI} base64_(en|de)code[^\[]*\([\^]*\)\) [NC,OR]
RewriteCond %{REQUEST_URI} (%0A| %0D| \\r| \\n) [NC,OR]
RewriteCond %{REQUEST_URI} union([\^a]*a)+1([\^s]*s)+elect [NC]
RewriteRule ^(.*)$ http://127.0.0.1 [R=301,L]
</IfModule>
```