requestclassifier.ini

The blocks and settings of requestclassifier.ini.

Source file: `doc/eng-us/examples/ini-settings/requestclassifier/README.md` Last changed 2026-11-04
https://doc.exponential.earth/learninminutes/exphelp/viewer/examples/ini-settings/requestclassifier/README.md

The shipped settings of `settings/requestclassifier.ini`: 7 blocks, 22 settings.

> The request classifier: tells a probe (/wp-login.php, /.env, /backup.zip), a path traversal (../), an injection
> (union select, {{7*7}}, <script>), a known attack tool and a burst of not-found answers from an ordinary request,
> and writes one line for each such request to var/log/security.log instead of 404.log, notice.log or error.log.
> Guide: doc/eng-us/features/6.0/request-logs.md
>
> Do not edit this file: override it in settings/override/requestclassifier.ini.append.php, in a siteaccess's
> requestclassifier.ini.append.php or in an extension's settings.
>
> Classification only. Nothing is blocked, slowed down or answered differently because of a verdict: the request
> gets the answer it would get anyway, and its log line goes to security.log. Blocking and rate limiting are left
> to listeners (Listeners[] below) and to the web server in front (request-shield under Velocity refuses some
> probes before PHP runs, so those never reach this classifier).
>
> Cost: no database. The patterns of a rule set are compiled into one regular expression, cached per version of
> these settings in var/<site>/cache/requestclassifier/ (safe to delete; made again on the next request). Only a
> 404 or 410 answer touches the not-found counter.
>
> A line in security.log (the address masked as site.ini [RequestLogSettings] MaskIP says, the query values with
> secrets and e-mail addresses masked, the user agent as a short hash and its first 60 characters):
> [Oct 17 2026 09:00:00] [203.0.x.x] probe/wp-login confidence=high 404 GET /wp-login.php siteaccess=site namespace=/wp-login.php ua=3f2a9c1b "curl/8.5.0"
> probe/wp-login <category>/<rule>: the category of the rule set and the rule that matched
> confidence=high low | medium | high, how sure the rule is
> 404 GET /wp-login.php the final HTTP status (- when unknown), the method and the URI
> namespace= the path below the siteaccess: /admin/wp-login.php and /site/wp-login.php are both
> /wp-login.php, so a rule sees the same path under every siteaccess

Block	Settings
ClassifierSettings	5
ThresholdSettings	3

Block	Settings
RuleSet-probes	4
RuleSet-traversal	3
RuleSet-injection	3
RuleSet-scanner	3
RuleSet-threshold	1

- All examples

Generated by `./console exp:help:examples` from `settings/requestclassifier.ini`. Do not edit this page: change the source and generate again (how). Free documentation: GFDL 1.3 or later.

Exponential Copyright © 1998-2026 Exponential Foundation and 7x
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".
This documentation is free documentation, licensed under the GNU Free Documentation License 1.3 or later:
https://www.gnu.org/licenses/fdl-1.3.html.