Progress®
Kemp® LoadMaster®

Technical Notes OWASP Standard Rules

Generated on: 18 December 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 4

Chapter 2: OWASP Standard Rules 5

1

Introduction

Introduction

This document provides further details about the OWASP Core Rule Set (CRS) rules in the LoadMaster including a list of rule sets and associated ID numbers. All rule sets are enabled by default. Rule groups or individual rules within each ruleset can be enabled/disabled as required. To enable a rule or group of rules, select the relevant check box. If you have previously enabled/disabled rules in a ruleset within a Virtual Service – the rules retain their previous settings.

2

OWASP Standard Rules

OWASP Standard Rules

A list of the OWASP standard rule sets and associated ID numbers is shown in table below:

Rule Set Name	Rule Set Identifier	Associated Rules
Request Rules		
method-enforcement	911	911100
scanner-detection	913	913100, 913101, 913102, 913110, 913120
protocol-enforcement	920	920100, 920120, 920160, 920170, 920171, 920180, 920181, 920190, 920210, 920220, 920240, 920250, 920260, 920270, 920280, 920290, 920310, 920311, 920330, 920340, 920350, 920380, 920360, 920370, 920390, 920400, 920410, 920470, 920420, 920480, 920430, 920440, 920500, 920450, 920200, 920201, 920230, 920300, 920271, 920320, 920121, 920341, 920272, 920490, 920510, 920202, 920273, 920274,

Rule Set Name	Rule Set Identifier	Associated Rules
		920275, 920460
protocol-attack	921	921110, 921120, 921130, 921140, 921150, 921160, 921190, 921200, 921151, 921180
application-attack-lfi	930	930100, 930110, 930120, 930130
application-attack-rfi	931	931100, 931110, 931120, 931130
application-attack-rce	932	932100, 932105, 932110, 932115, 932120, 932130, 932140, 932150, 932160, 932170, 932171, 932180, 932200, 932106, 932190
application-attack-php	933	933100, 933110, 933120, 933130, 933140, 933500, 933150, 933160, 933170, 933180, 933210, 933151, 933131, 933161, 933111, 933190
application-attack-nodejs	934	934100
application-attack-xss	941	941100, 941110, 941120, 941130, 941140, 941160, 941170, 941180, 941190, 941200, 941210, 941220, 941230, 941240, 941250, 941260, 941270, 941280, 941290, 941300, 941310, 941350, 941360, 941370, 941101, 941150, 941330, 941340, 941380
application-attack-sqli	942	942100, 942140, 942160, 942170, 942190, 942220, 942230, 942240, 942250, 942270, 942280, 942290, 942320, 942350, 942360, 942500, 942110, 942120, 942130, 942150, 942180, 942200, 942210, 942260, 942300, 942310, 942330, 942340, 942361, 942370, 942380, 942390, 942400, 942410, 942470, 942480, 942430, 942440, 942450, 942510, 942251, 942490, 942420, 942431, 942460, 942101, 942511, 942421, 942432
application-attack-session-fixation	943	943100, 943110, 943120
application-attack-java	944	944100, 944110, 944120, 944130, 944200, 944210, 944240, 944250, 944300

Rule Set Name	Rule Set Identifier	Associated Rules
Response Rules		
data-leakages	950	950130, 950140, 950100
data-leakages-sql	951	951110, 951120, 951130, 951140, 951150, 951160, 951170, 951180, 951190, 951200, 951210, 951220, 951230, 951240, 951250, 951260
data-leakages-java	952	952100, 952110
data-leakages-php	953	953100, 953110, 953120
data-leakages-iis	954	954100, 954110, 954120, 954130
correlation	980	980100, 980110, 980120, 980130, 980140, 980150

All request rule sets are enabled by default. If you have the **Process HTTP Responses** option enabled you can also enable response rules. To get to the **Process HTTP Responses** option, go to **Virtual Services > View/Modify Services > Modify > WAF > Advanced Settings**.