INDUSFACE™

APPTRANA PROTECTION

Rules Coverage Report:

Summary:

Most WAF solution fails, as application security is complex and creating rules inhouse is a time-Consuming job which requires expertise. Other Cloud security solutions that provide WAF generally go with cookie cutter solution. They provide certain generic rules and then provide customer means to write rules by themselves. It is up to the organizations to fine tune the rules to meet the application needs. Since default rules create false positives and fine-tuning rules becomes complex over time, organizations end up giving up on WAF compromising security for convenience.

We at Indusface approach the problem differently. We believe, security of the application starts with detection and AppTrana ensures that all the vulnerabilities are detected, and we also ensure it is protected by expert written rules. Our experts fine-tune the rules based on the application need to avoid false positives and ensure that your application remain secure round the clock.

The following checklist gives you overview of rule coverage provided by AppTrana' s different rules.

Advance Rules: Rules which are fine tuned for FPs and are put in block mode from day zero.

Premium Rules: Rules which are applied to site and moved to block mode after monitoring traffic for 14 days ensuring there are no FPs.

Custom Rules: Rules which are written for specific application needs in consultation with customer. Note that we can have more variants of WAF rules in place for each category and only generic category and types are captured in this document.

Summary:

S.no	Category	Severity	Rule Type	Rule Description
1	HTTP Method Restriction Policy	Critical	Premium	Non-supported HTTP request method (other than GET, POST & HEAD) detected.
2	HTTP Header Restriction Policy	Critical	Advance	Non-supported HTTP request headers detected.
3	Encoding Abuse Attacks Protection Policy	Critical	Advance	Encoding Abuse Attacks
4	Bot Protection Policy	Critical	Advance	Security scanner related HTTP header detected.
5	Bot Protection Policy	Critical	Premium	Automated program based User-Agent/HTTP header detected.
6	Blind SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected in HTTP request cookies and XML requests.
7	Blind SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected in HTTP request URI and arguments.
8	Blind SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected - 1.
9	Blind SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected - 2.
10	SQL Injection Protection Policy	Critical	Premium	SQL Injection attempt detected in HTTP request cookies and XML requests.
11	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected in HTTP request URI and arguments.
12	SQL Injection Protection Policy	Critical	Premium	SQL Injection attempt detected - 1.

13	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected in HTTP request cookies or in XML requests.
14	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected - 2.
15	Cross-Site Scripting Protection Policy	Critical	Advance	Cross-Site Scripting attack attempt detected in HTTP request Cookies and XML requests.
16	Cross-Site Scripting Protection Policy	Critical	Premium	Cross-Site Scripting attack attempt detected in HTTP request URI, Arguments and XML reuqests - 1.
17	File Injection Protection Policy	Critical	Advance	File injection attempt detected in HTTP request header and XML requests.
18	File Injection Protection Policy	Critical	Advance	File injection attempt detected in HTTP request URI and arguments.
19	SSI Injection Protection Policy	Critical	Advance	Server side Injection attempt detected in HTTP request URI or arguments.
20	SSI Injection Protection Policy	Critical	Advance	Server side Injection attempt detected in HTTP headers or XML file.
21	PHP Injection Protection Policy	Critical	Advance	PHP injection attempt detected in HTTP request URI and arguments.
22	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected - 3.
23	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected in HTTP request URI , arguments or HTTP Headers.
24	Bot Protection Policy	Error	Advance	Bad reputated IP detected.
25	Local File Inclusion Protection Policy	Critical	Advance	Local File Inclusion (LFI) attempt detected via file traversal character sequences.
26	Local File Inclusion Protection Policy	Critical	Premium	Local File Inclusion (LFI) attempt detected using path pointing from root directory.

27	Base64 Encoding Abuse Attacks Protection Policy	Critical	Advance	Base64-encoded payload detected in HTTP request.
28	Remote File Inclusion Protection Policy	Critical	Premium	Remote File Inclusion (RFI) attempt detected.
29	Blind SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected - 3.
30	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected in HTTP request URI , arguments or Cookie.
31	Blind SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected - 4.
32	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected - 4.
33	SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected in HTTP request URI , arguments or Cookie.
34	JavaScript Encoding Abuse Attacks Protection Policy	Critical	Advance	JavaScript encoding abuse detected - 1.
35	JavaScript Encoding Abuse Attacks Protection Policy	Critical	Advance	JavaScript encoding abuse detected - 2.
36	GNU Bash Remote Code Execution (CVE-2014-6271) Protection Policy	Critical	Advance	GNU Bash remote code execution (CVE-2014-6271) detected - 1.
37	SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected in HTTP request URI , arguments or Request Headers.

38	PHP Injection Protection Policy	Critical	Advance	PHP injection attempt detected in HTTP request header and XML requests.
39	GNU Bash Remote Code Execution (CVE-2014-6271) Protection Policy	Critical	Advance	GNU Bash remote code execution (CVE-2014-6271) detected - 2.
40	GNU Bash Remote Code Execution (CVE-2014-6271) Protection Policy	Critical	Advance	GNU Bash remote code execution (CVE-2014-6271) detected - 3.
41	GNU Bash Remote Code Execution (CVE-2014-6271) Protection Policy	Critical	Advance	GNU Bash remote code execution (CVE-2014-6271) detected - 4.
42	HTTP Response Splitting Protection Policy	Critical	Advance	HTTP response splitting attempt detected in HTTP request cookies - 1.
43	HTTP Response Splitting Protection Policy	Critical	Advance	HTTP response splitting attempt detected in HTTP request cookies - 2.
44	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected - 5.
45	OS Command Injection Protection Policy	Critical	Advance	System command injection attempt detected - 1.
46	OS Command Injection Protection Policy	Critical	Advance	System command injection attempt detected - 2.
47	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected - 6.
48	Local File Inclusion	Critical	Advance	Local File Inclusion (LFI) attempt detected via "\\\" character sequences.

	Protection Policy			
49	HTTProxy Protection Policy	Critical	Advance	HTTP Proxy request header detected.
50	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected in HTTP request URI , arguments ,HTTP Headers or XML file.
51	Cross-Site-Scripting	Critical	Premium	Cross-Site Scripting attack attempt detected in HTTP request URI, Arguments and XML reuqests - 2
52	Bot Protection Policy	Critical	Advance	Security scanner related URI detected.
53	Bot Protection Policy	Critical	Advance	Command Line Tool/Library related User-Agent/HTTP header (from internal database) detected.
54	Cross-Site Scripting Protection Policy	Critical	Premium	Cross-Site-Scripting
55	Apache Struts2 REST XStream RCE Vulnerability Protection Policy	Critical	Advance	Remote code execution attempt via suspicious Java class detected. User can execute system commands via processbuilder or runtime calls and an attacker can misuse these classes submitting improperly sanitized objects to run malicious system commands.
56	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected - 7.
57	Cross-Site Scripting Protection Policy	Critical	Advance	Cross-Site-Scripting
58	Generic Deserialization Defence for Java	High	Advance	Generic Deserialization attempt detected in Java.
59	Generic Deserialization Defence for Java	High	Advance	Generic Deserialization attempt detected in Java.
60	Generic Deserialization Defence for	High	Advance	Generic Deserialization attempt detected in Microsoft Products.

	Microsoft products			
61	Generic Deserialization Defence for Ruby on Rails	High	Advance	Generic Deserialization attempt detected in Ruby on Rails.
62	Generic Deserialization Defence for Ruby on Rails	High	Advance	Generic Deserialization attempt detected in Ruby on Rails.
63	XML External Entity (XXE) Injection Policy	High	Advance	XML External Entity (XXE) Injection attempt detected as local file inclusion.
64	Possible Apache Struts OGNL RCE Protection Policy	Critical	Advance	Possible Apache Struts OGNL Code Execution Policy
65	Apache Tomcat Remote Code Execution Vulnerability Protection Policy	Critical	Advance	Apache Tomcat Remote Code Execution (CVE-2019-0232) attack attempt detected.
66	Possible Malicious File Upload	Critical	Advance	File upload with malicious extensions detected
67	HTML5 ping DOS Protection Policy	Critical	Advance	DoS attack using Ping headers in HTML5 - 1.
68	HTML5 ping DOS Protection Policy	Critical	Advance	DoS attack using Ping headers in HTML5 - 2.
69	HTML5 ping DOS Protection Policy	Critical	Advance	DoS attack using Ping headers in HTML5 - 3.
70	IIS Remote Code Execution Protection Policy	Critical	Advance	Microsoft IIS HTTP.sys Remote Code Execution Exploit attempt (CVE-2014-6321)
71	Apache DOS Protection Policy	High	Advance	Attempt to exploit DOS on Apache Server Based on Range Header
72	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities

73	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
74	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
75	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
76	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
77	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
78	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
79	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
80	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
81	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
82	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
83	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
84	PHP Remote Code Execution	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities

	Protection Policy			
85	PHP Remote Code Execution Protection Policy	High	Premium	Attempt to detect possibility of Remote Code Execution based on php vulnerabilities
86	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to detect possibility of Remote Code Execution based on php vulnerabilities
87	Malicious File Upload Attacks: Blocking Large File upload Attempts	Critical	Advance	Malicious File Upload Attacks: Blocking Large File upload Attempts
88	CVE-2020-5902 F5 BIG-IP RCE	Critical	Advance	CVE-2020-5902 F5 BIG-IP Remote Code Execution
89	Bot Protection Policy	Critical	Advance	Malicious bot related User-Agent/HTTP header detected.
90	Bot Protection Policy	Critical	Advance	Website Security Scanner related User-Agent/HTTP header detected.
91	Bot Protection Policy	Critical	Advance	Website Crawler related User-Agent/HTTP header detected.
92	Bot Protection Policy	Critical	Advance	Website Scrappers related User-Agent/HTTP header detected.
93	ESI Injection Vulnerability	Critical	Advance	Rule to detect ESI Injection Vulnerability in request body or header or uri
94	Invalid Content-Length HTTP header	Critical	Advance	Invalid Content-Length HTTP header
95	HTTP Request Smuggling Attack	Critical	Advance	HTTP Request Smuggling Attack
96	Unicode Full/Half Width Abuse Attack Attempt	Critical	Advance	Unicode Full/Half Width Abuse Attack Attempt
97	URL file extension is restricted by policy	Critical	Advance	URL file extension is restricted by policy
98	Attempt to access a backup or working file	Critical	Advance	Attempt to access a backup or working file

99	Request with Header x-up-devcap-post-charset detected in combination with \'UP\' User-Agent prefix	Critical	Advance	Request with Header x-up-devcap-post-charset detected in combination with \'UP\' User-Agent prefix
100	HTTP Request Smuggling Attack	Critical	Advance	HTTP Request Smuggling Attack
101	HTTP Request Smuggling Attack	Critical	Advance	HTTP Request Smuggling Attack
102	HTTP Header Injection Attack via payload (CR/LF and header-name detected)	Critical	Advance	HTTP Header Injection Attack via payload (CR/LF and header-name detected)
103	HTTP Splitting (CR/LF in request filename detected)	Critical	Advance	HTTP Splitting (CR/LF in request filename detected)
104	Node.js-injection Attacks	Critical	Advance	Node.js Injection Attack
105	Apache Struts and Java Attacks	Critical	Advance	Remote Command Execution: Java process spawn (CVE-2017-9805)
106	Apache Struts and Java Attacks	Critical	Advance	Suspicious Java class detected
107	Apache Struts and Java Attacks	Critical	Advance	Base64 encoded string matched suspicious keyword
108	Remote File Inclusion Attacks	Critical	Advance	Possible Remote File Inclusion (RFI) Attack: Common RFI Vulnerable Parameter Name used w/URL Payload
109	PHP Injection Attack: PHP Open Tag Found	Critical	Advance	PHP Injection Attack: PHP Open Tag Found
110	PHP Injection Attack: Configuration Directive Found	Critical	Advance	PHP Injection Attack: Configuration Directive Found

111	PHP Injection Attack: Variables Found	Critical	Advance	PHP Injection Attack: Variables Found
112	PHP Injection Attack: I/O Stream Found	Critical	Advance	PHP Injection Attack: I/O Stream Found
113	PHP Injection Attack: Wrapper scheme detected	Critical	Advance	PHP Injection Attack: Wrapper scheme detected
114	PHP Injection Attack: High-Risk PHP Function Call Found	Critical	Advance	PHP Injection Attack: High-Risk PHP Function Call Found
115	PHP Injection Attack: Serialized Object Injection	Critical	Advance	PHP Injection Attack: Serialized Object Injection
116	PHP Injection Attack: Variable Function Call Found	Critical	Premium	PHP Injection Attack: Variable Function Call Found
117	Path Traversal Attack (/../)	Critical	Advance	Path Traversal Attack (/../)
118	Restricted File Access Attempt	Critical	Advance	Restricted File Access Attempt
119	OS File Access Attempt	Critical	Advance	OS File Access Attempt
120	Cross-site-scripting Attempt	Critical	Premium	Cross-site-scripting Attempt
121	NoScript XSS InjectionChecker: Attribute Injection	Critical	Premium	NoScript XSS InjectionChecker: Attribute Injection
122	IE XSS Filters - Attack Detected	Critical	Premium	IE XSS Filters - Attack Detected
123	IE XSS Filters - Attack Detected	Critical	Premium	IE XSS Filters - Attack Detected
124	JavaScript global variable found	Critical	Premium	JavaScript global variable found
125	Apache Struts Remote Code Execution Policy	Critical	Advance	Remote code execution attempt (CVE-2017-5638) using echo and expr commands in Apache Struts via content-type request

				header detected. The Jakarta Multipart parser in Apache Struts has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands.
126	Apache Struts Remote Code Execution Policy	Critical	Advance	Remote code execution attempt (CVE-2017-5638) using variations of grep commands in Apache Struts via content-type request header detected. The Jakarta Multipart parser in Apache Struts has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands.
127	Apache Struts Remote Code Execution Policy	Critical	Advance	Remote code execution attempt (CVE-2017-5638) using variations of grep commands in Apache Struts via content-type request header detected. The Jakarta Multipart parser in Apache Struts has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands.
128	Apache Struts Remote Code Execution Policy	Critical	Advance	Remote code execution attempt (CVE-2017-5638) using cc or wget commands in Apache Struts via content-type request header detected. The Jakarta Multipart parser in Apache Struts has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands.
129	Apache Struts Remote Code Execution Policy	Critical	Advance	Remote code execution attempt (CVE-2017-5638) using commands in Apache Struts via content-type request header detected. The Jakarta Multipart parser in Apache Struts has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands.
130	Apache Struts Remote Code Execution Policy	Critical	Advance	Remote code execution attempt (CVE-2017-5638) using linux system commands in Apache Struts via content-type request header detected. The Jakarta Multipart parser in Apache Struts has incorrect exception handling and error-message

				generation during file-upload attempts, which allows remote attackers to execute arbitrary commands.
131	Apache Struts Remote Code Execution Policy	Critical	Advance	Remote code execution attempt (CVE-2017-5638) using windows system commands in Apache Struts via content-type request header detected. The Jakarta Multipart parser in Apache Struts has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands.
132	Apache Struts Remote Code Execution Policy	Critical	Advance	Remote code execution attempt (CVE-2018-11776 and CVE-2017-5638) in Apache Struts via suspicious Java class detected. The vulnerability exists in the core of Apache Struts due to improper validation of user-provided untrusted inputs under certain configurations causing remote code execution.
133	Advanced SQL Injection Attacks	Critical	Advance	SQL Injection Attack: Common DB Names Detected
134	Advanced SQL Injection Attacks	Critical	Advance	Detects blind sqli tests using sleep() or benchmark() including Conditional Queries
135	Advanced SQL Injection Attacks	Critical	Advance	Postgres/MongoDB based SQLi Attempt Detected
136	Advanced SQL Injection Attacks	Critical	Advance	Detects MySQL and PostgreSQL stored procedure/function injections
137	Advanced SQL Injection Attacks	Critical	Advance	MySQL in-line comment detected
138	Advanced SQL Injection Attacks	Critical	Advance	Detects MySQL charset switch and MSSQL DoS attempts
139	Advanced SQL Injection Attacks	Critical	Advance	SQL Injection Attack
140	Advanced SQL Injection Attacks	Critical	Advance	SQL Injection Attack

141	Advanced SQL Injection Attacks	Critical	Advance	SQL Injection Attack
142	Malicious File Upload Attacks: Preventing all File Upload Attempts	Critical	Advance	Malicious File Upload Attacks: Preventing all File Upload Attempts
143	Malicious File Upload Attempt: Denying all Non-Document File upload Attempts	Critical	Advance	Malicious File Upload Attempt: Denying all Non-Document File upload Attempts
144	Malicious File Upload Attacks: Denying all Non-Media File upload Attempts	Critical	Advance	Malicious File Upload Attacks: Denying all Non-Media File upload Attempts
145	Malicious File Upload Attacks: Denying all Non-Document and Non-Media File upload Attempts	Critical	Advance	Malicious File Upload Attacks: Denying all Non-Document and Non-Media File upload Attempts
146	Advanced Command Injection Attacks	Critical	Advance	Remote Command Execution: Windows Command Injection
147	Advanced Command Injection Attacks	Critical	Advance	Remote Command Execution: Unix Command Injection
148	Advanced Command Injection Attacks	Critical	Advance	Remote Command Execution: Windows Command Injection
149	Advanced Command Injection Attacks	Critical	Advance	Remote Command Execution: Unix Shell Expression Found

150	HTTP Request Smuggling Attack	Critical	Advance	HTTP Request Smuggling identified with multiple Content-Length HTTP headers
151	HTTP Request Smuggling Attack	Critical	Advance	Unusual HTTP Protocol Format
152	HTTP Request Smuggling Attack	Critical	Advance	HTTP Request Smuggling Attack
153	HTTP Request Smuggling Attack	Critical	Advance	Advanced HTTP Request Smuggling Attack Identified
154	HTTP Request Smuggling Attack	Critical	Advance	Possible HTTP Request Smuggling Attack
155	JAVA SPRING RCE Attack	Critical	Advance	Restricted JAVA SPRING RCE Attack Detected for CVE-2022-22963.
156	MS Http.sys RCE vulnerability	Critical	Advance	Rule to block MS Http.sys RCE attacks
157	Apache Http Server Path Traversal Vulnerability	Critical	Advance	Rule to prevent path traversal attack
158	Apache Log4j Remote Code Execution Vulnerability	Critical	Advance	Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228) attack detected
159	Apache Log4j Remote Code Execution Vulnerability	Critical	Advance	Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228) attack detected
160	Apache Log4j Remote Code Execution Vulnerability	Critical	Advance	Restricted malicious requests with apache log4j DOS attack CVE-2021-45105
161	Apache Log4j Remote Code Execution Vulnerability	Critical	Advance	Restricts malicious requests with apache log4j CVE-2021-45046 DOS attack
162	Apache Log4j Remote Code Execution Vulnerability	Critical	Advance	Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228) attack detected
163	PHP Remote Code Execution	Critical	Advance	Attempt to detect possibility of Remote Code Execution based on php vulnerabilities

164	Path Traversal Coverage	Critical	Advance	Rule to cover encoded payloads (..2f..2f|2e2e2f|326532653266)
165	Cross Site Scripting Attack	Critical	Advance	This rule prevents Cross-Site-Scripting attacks by idThis rule prevents Cross-Site-Scripting attacks by identifying and preventing XSS payloads.entifying and preventing XSS payloads.
166	JSON SQL Injection Attack	Critical	Advance	JSON SQL Injection attempt detected in HTTP request URI and arguments.
167	ProxyNotShell (CVE-2022-40140 & CVE-2022-41082)	Critical	Advance	MS Exchange ProxyNotShell (CVE-2022-40140 & CVE-2022-41082) Attack Detected.
168	Advanced SQL Injection Attacks	Critical	Advance	This rule detects JSON based SQL injection.
169	Java Attacks	Critical	Advance	This rule detects Java class reflection usage to execute methods that allow OS commands execution.
170	Content Injection	Critical	Advance	HTML content injection within Request URL detected.
171	SQL Injection	Critical	Advance	SQL Injection attempt detected in HTTP request URI and arguments.
172	LDAP Injection	Critical	Advance	To identify LDAP injection attacks
173	Command Injection	Critical	Advance	To identify command injection attacks
174	Manage Engine Remote Code Execution	Critical	Advance	CVE-2022-47966 Manage Engine Remote Code Execution
175	Apache Struts and Java Attacks	Critical	Advance	Apache Struts and Java Attacks
176	MOVEit Transfer Vulnerability Policy	Critical	Advance	MOVEit Transfer Vulnerability Policy
177	MOVEit Transfer Vulnerability Policy	Critical	Advance	MOVEit Transfer Vulnerability Policy
178	MOVEit Transfer Vulnerability Policy	Critical	Advance	MOVEit Transfer Vulnerability Policy
179	MOVEit Transfer Vulnerability Policy	Critical	Advance	MOVEit Transfer Vulnerability Policy

180	MOVEit Transfer Vulnerability Policy	Critical	Advance	MOVEit Transfer Vulnerability Policy
181	MOVEit Transfer Vulnerability Policy	Critical	Advance	MOVEit Transfer Vulnerability Policy
182	Bot Attacks	Critical	Advance	Bot Attacks
183	Remote Unauthenticated API Access Vulnerability(CVE-2023-35078) policy	Critical	Advance	Remote Unauthenticated API Access Vulnerability(CVE-2023-35078)
184	Cross-Site-Scripting Attacks	Critical	Advance	This rule prevents SSTI Injection Attacks
185	Privilege Escalation in WooCommerce WordPress Vulnerability Policy	Critical	Advance	CVE-2023-28121 Privilege Escalation in WooCommerce Payments plugin for WordPress Vulnerability
186	PHP File Upload detection policy	Critical	Advance	PHP File Upload detection policy
187	Adobe Cold Fusion Vulnerability Policy	Critical	Advance	CVE-2023-29298 Adobe ColdFusion Access Control Bypass
188	Adobe Cold Fusion Vulnerability Policy	Critical	Advance	CVE-2023-38203 Adobe ColdFusion Deserialization Vulnerability
189	Cross-Site-Scripting Attack Policy	Critical	Advance	Cross-Site-Scripting attack detection.
190	Cross-Site-Scripting Attack Policy	Critical	Advance	Cross-Site Scripting attack attempt detected in Multiple targets.
191	Remote Code Execution (RCE) Detection Policy	Critical	Advance	Remote Code Execution (RCE) attack attempt detected in Multiple targets.
192	LDAP Injection Policy	Critical	Advance	LDAP Injection at arguments and XML
193	NoSQLI Injection Policy	Critical	Advance	NoSQLI Injection Detection

194	LFI Attack Policy	Critical	Advance	LFI attacks
195	PHP Injection Attacks Policy	Critical	Advance	PHP Injection attacks
196	Server Side Template Injection Policy	Critical	Advance	Server Side Template Injection detection
197	Server-Side Request Forgery (SSRF) Policy	Critical	Advance	Server-Side Request Forgery (SSRF) detection
198	GraphQL Policy	Critical	Advance	GraphQL detetction
199	CVE-2023-22515 - Broken Access Control Vulnerability in Confluence Data Center and Server Policy	Critical	Advance	Coverage for CVE-2023-22515 and CVE-2023-22518
200	SQL Injection Attacks	Critical	Advance	SQL Injection attempt detection
201	Remote Code Execution (RCE) Detection Policy	Critical	Advance	Remote Code Execution (RCE) Attack Detection at Cookie
202	Base64 Encoded Attack Detection Policy	Critical	Advance	Base64 Encoding Attack Detection
203	Base64 Encoded Attack Detection Policy	Critical	Advance	Base64 Encoding Detected
204	Apache OFBiz Auth bypass and Pre-Auth RCE Vulnerability (CVE-2023-49070 and CVE-2023-51467) policy	Critical	Advance	Apache OFBiz Auth bypass and Pre-Auth RCE Vulnerability (CVE-2023-49070 and CVE-2023-51467) detection
205	Apache Hadoop and Flink application Misconfiguration exploitation detection policy	Critical	Advance	Apache Hadoop and Flink application Misconfiguration exploitation detection policy

206	Server-Side Request Forgery leading to RCE in the SAML component of Ivanti(CVE-2024-21893 & CVE-2024-21887) detected	Critical	Advance	Server-Side Request Forgery leading to RCE in the SAML component of Ivanti(CVE-2024-21893 & CVE-2024-21887) detected
207	Auth bypass ScreenConnect CVE-2024-1708 and CVE-2024-1709 Policy	Critical	Advance	Auth bypass ScreenConnect CVE-2024-1708 and CVE-2024-1709 Detection
208	Base64 Encoded Attack Detection Policy	Critical	Advance	Malicious Base64 Encoding detected at useragent.
209	SQL Injection Attacks	Critical	Advance	SQL Injection detected at useragent.
210	Jet Brains Auth Bypass Policy	Critical	Advance	Jet Brains Auth Bypass Policy
211	CVE-2024-23897 Jenkins Code Execution Policy	Critical	Advance	Jenkins Remote Code Execution Policy CVE-2024-23897
212	Possible Unauthenticated Privilege Escalation (CVE 2024-2172) Policy	Critical	Advance	Possible Unauthenticated Privilege Escalation Detection
213	SQL Injection Attacks	Critical	Advance	SQL Injection Attack Detection at multiple targets
214	Advance Threat Detection Policy	Critical	Advance	Malicious command Injection Attack Detection at multiple targets
215	Advance Threat Detection Policy	Critical	Advance	Malicious Injection Attack Detection at Request Headers
216	Advance Threat Detection Policy	Critical	Advance	Obfuscated Injection Attack Detection at multiple targets
217	Advance Threat Detection Policy	Critical	Advance	Path traversal and sensitive file access attempt at Headers and Arguments
218	Advance Threat Detection Policy	Critical	Advance	SSRF attempt at Headers and Arguments

219	Advance Threat Detection Policy	Critical	Advance	Base64 encoded Malicious Injection Detection at multiple targets like URL, Headers, Body, ARGS etc.,
220	Advance Threat Detection Policy	Critical	Advance	Cross Site Scripting detection at Headers and arguments
221	Incorrect Authorization in Apache OFBiz (CVE-2024-38856)	Critical	Advance	CVE-2024-38856, CVE-2024-36104 and CVE-2024-32113 Incorrect Authorization vulnerability leading to RCE in Apache OFBiz
222	Incorrect Authorization in Apache OFBiz (CVE-2024-38856)	Critical	Advance	CVE-2024-38856, CVE-2024-36104 and CVE-2024-32113 Incorrect Authorization vulnerability leading to RCE in Apache OFBiz. Rule checks for encoded unicode characters sent from groovyprogram argument.
223	Advance Threat Detection Policy	Critical	Advance	Path traversal and sensitive file access attempt detected at URL
224	Advance Threat Detection Policy	Critical	Advance	SQL Injection attempt detected at Arguments
225	Advance Threat Detection Policy	Critical	Advance	Command Injection attempt detected at Arguments
226	Cross-Site Scripting Protection Policy	High	Advance	Cross-Site-Scripting attacks detected
227	VMWare Aria Remote Code Execution Policy	Critical	Advance	VMWare Aria Remote Code Execution Policy
228	Restrict Access to Suspicious Apache Tomcat Default Web Management Pages	Critical	Advance	Restrict Access to Suspicious Apache Tomcat Default Web Management Pages
229	Malware Policy	Critical	Advance	Malware Policy
230	Illegal Content-type Header Detection Policy	Critical	Advance	Multiple Content-type Header detection in a Request Header
231	WordPress URLs Protection Policy	Critical	Advance	WordPress User Enumeration Policy
232	WordPress URLs Protection Policy	Critical	Advance	WordPress User Enumeration-1 Policy

233	WordPress URLs Protection Policy	Critical	Advance	Wordpress Popup-Maker Injection Policy
234	WordPress URLs Protection Policy	Critical	Advance	WordPress Plugin Verison Disclosure Policy
235	WordPress URLs Protection Policy	Critical	Advance	WordPress Google Maps SQL Injection Policy
236	WordPress URLs Protection Policy	Critical	Advance	WordPress xmlrpc Blocking Policy
237	WordPress URLs Protection Policy	Critical	Advance	Detect attempts to use phpinfo or unauthorized file deletion through specific callback parameter
238	WordPress URLs Protection Policy	Critical	Advance	Prevent retrieval of user emails based on specific roles (administrator, subscriber)
239	WordPress URLs Protection Policy	Critical	Advance	External URL injection attempts within nested 'args' parameters
240	Malicious Pattern Detection-1	Critical	Advance	Malicious Injection Attack Detection at multiple targets

Apart from this, specific custom rules are written to address application specific needs. These rules are again created by Indusface security experts. Certain use cases that can be addressed are provided below, please note these are not comprehensive and should be used to judge the type of use cases that can be addressed through AppTrana.

Theft/DLP Protection:

Customers who need to protect sensitive information protected and ensure certain information do not leave the organization can request for response-based rule, which would monitor their response traffic and mask sensitive data. When these rules are enabled, sensitive information will be masked on the logs as well.

Note

Response based rules are highly intrusive and should be enabled judiciously as it may affect functioning of the application. *BAD IP Protection:*

Indusface provide IP protection that shows IP's which are malicious. customers can choose to monitor these malicious IP's either manually or have automated rule enabled that could block these IPs automatically. IPs with bad reputation is identified by using internal Global Threat Platform which identifies malicious IPs based on behaviour across all sites under Indusface Protection. Apart from this Global Threat Platform also gets periodic updates from Global 3rd party database which marks certain IP malicious.

Customer can also choose to have TOR IPs blocked through custom rule.

Protection Against Hidden Form Fields:

If customers have any hidden form fields and want to restrict requests which sends out of bound values for the field, then customer can request for custom rule which would be written by our security experts based on their need.

File Upload Violation:

Customers based on application need can request for custom rule written to avoid file uploads that does not meet the acceptable parameters.

Positive Security Rules:

Customer can choose to enable positive security model, in which some or all negative model rules would be disabled for the customer based on their need and positive security rules created which would take into accepted values for various fields like URLs, directories, cookies, headers, form/query parameters, File upload Extensions, allowed metacharacters etc and allow only values that meets the accepted parameters.

Honey Pot Bot Defender Rule:

We have enhanced our Bot defender rules which can now identify malicious bots through honeypots and block them. If a new malicious bot is identified when it attacks one of the protected sites, this information will be registered in our global threat intelligence database and attack from same botnet on any other sites under our protection will be blocked faster.

Behaviour Rules:

We have sophisticated anomaly scoring/ behaviour rules that changes the protection status of rules based on certain behaviour observed in the application. This can be done at application level or at a specific page level.

Tampering Protection Policies:

Customers can also enable tampering policies which would help them against cookie tampering/poisoning attacks. It also protects application from tampering like URL rewriting, encryption tampering, and so on. This rule can also be configured to protect against attacks to identify predictable resource location, unauthorized access, server reconnaissance.

HTTP Parameter Controlling Policies:

Solution protects HTTP Parameter pollution, tampering attacks, and policies can be written to protect against HTTP parameter pollution attack, restricting/controlling HTTP methods and validating header length, content length, Body length, Parameter length, body line length etc.

Enterprise Features:

AppTrana supports all enterprise use cases including- Support for Transformation Functions:

As part of core rules AppTrana supports transformation functions like URL Decoding, Null Byte string termination.

Customized Error Message:

Based on application requirement customer can request for rules to mask their server errors and show custom pages instead of default server errors.

Support for Custom Ports & Protocols:

By default, the rules are written for HTTP/HTTPS traffic and WAF listens on port 80/443. Customers can request for additional custom ports be opened based on their need and monitoring of additional protocols like SOAP, XML etc.

Support for IPv6:

Customer can enable IPv6 support for their sites by requesting it while onboarding. With this clients connecting to the application will be able to connect using IPv6 even if backend does not support IPv6.

Support for SIEM:

SIEM APIs are available that will enable customers to get real time attack logs from AppTrana that can be integrated with their SIEM tools for further analysis.

Support for 2FA & RBCA:

AppTrana provides support for Role based access control as well ensures access to AppTrana portal through 2FA support.