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**	**RuleType**	**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	Encoding Abuse Attacks Protection Policy	High	Hidden	Encoding Abuse Attacks
5	Bot Protection Policy	Critical	Advance	Security scanner related HTTP header detected.
6	Bot Protection Policy	Critical	Premium	Automated program based User-Agent/HTTP header detected.
7	Blind SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected in HTTP request cookies and XML requests.
8	Blind SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected in HTTP request URI and arguments.
9	SQL Injection	High	Disabled	SQL Injection
10	SQL Injection	High	Disabled	SQL Injection
11	Blind SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected - 1.
12	Blind SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected - 2.
13	SQL Injection Protection Policy	Critical	Premium	SQL Injection attempt detected in HTTP request cookies and XML requests.
14	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected in HTTP request URI and arguments.
15	SQL Injection Protection Policy	Critical	Premium	SQL Injection attempt detected - 1.
16	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected in HTTP request cookies or in XML requests.

17	SQL Injection	High	Disabled	SQL Injection
18	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected - 2.
19	Cross-Site Scripting Protection Policy	Critical	Advance	Cross-Site Scripting attack attempt detected in HTTP request Cookies and XML requests.
20	Cross-Site Scripting Protection Policy	Critical	Premium	Cross-Site Scripting attack attempt detected in HTTP request URI, Arguments and XML reuqests - 1.
21	File Injection Protection Policy	Critical	Advance	File injection attempt detected in HTTP request header and XML requests.
22	File Injection	High	Disabled	File Injection
23	File Injection Protection Policy	Critical	Advance	File injection attempt detected in HTTP request URI and arguments.
24	OS Command Injection	Critical	Hidden	OS Command Injection
25	SSI Injection Protection Policy	Critical	Advance	Server side Injection attempt detected in HTTP request URI or arguments.
26	SSI Injection Protection Policy	Critical	Advance	Server side Injection attempt detected in HTTP headers or XML file.
27	PHP Injection	Critical	Hidden	PHP Injection
28	PHP Injection Protection Policy	Critical	Advance	PHP injection attempt detected in HTTP request URI and arguments.
29	Blind SQL Injection Protection Policy	High	Hidden	Blind SQL Injection
30	Blind SQL Injection Protection Policy	High	Hidden	Blind SQL Injection
31	SQL Injection Protection Policy	High	Hidden	SQL Injection
32	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected - 3.
33	SQL Injection Protection Policy	High	Hidden	SQL Injection
34	Cross-Site Scripting Protection Policy	High	Hidden	XSS

35	File Injection Protection Policy	High	Hidden	Remote File Access Attempt
36	OS Command Injection Protection Policy	Critical	Hidden	System Command Injection
37	PHP Injection Protection Policy	Critical	Hidden	PHP Injection
38	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected in HTTP request URI , arguments or HTTP Headers.
39	Cross-Site Scripting Protection Policy	High	Hidden	XSS
40	Cross-Site Scripting Protection Policy	Critical	Premium	Cross-Site-Scripting
41	Bot Protection Policy	Error	Advance	Bad reputated IP detected.
42	SQL Injection	High	Hidden	SQL Injection
43	Local File Inclusion Protection Policy	Critical	Advance	Local File Inclusion (LFI) attempt detected via file traversal character sequences.
44	Local File Inclusion Protection Policy	Critical	Premium	Local File Inclusion (LFI) attempt detected using path pointing from root directory.
45	Base64 Encoding Abuse Attacks Protection Policy	Critical	Advance	Base64-encoded payload detected in HTTP request.
46	Remote File Inclusion Protection Policy	Critical	Premium	Remote File Inclusion (RFI) attempt detected.
47	Blind SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected - 3.
48	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected in HTTP request URI , arguments or Cookie.
49	Blind SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected - 4.
50	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected - 4.
51	SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected in HTTP request URI , arguments or Cookie.

52	JavaScript Encoding Abuse Attacks Protection Policy	Critical	Advance	JavaScript encoding abuse detected - 1.
53	JavaScript Encoding Abuse Attacks Protection Policy	Critical	Advance	JavaScript encoding abuse detected - 2.
54	GNU Bash Remote Code Execution (CVE-2014-6271) Protection Policy	Critical	Advance	GNU Bash remote code execution (CVE-2014-6271) detected - 1.
55	SQL Injection Protection Policy	Critical	Advance	Blind SQL Injection attempt detected in HTTP request URI , arguments or Request Headers.
56	PHP Injection Protection Policy	Critical	Advance	PHP injection attempt detected in HTTP request header and XML requests.
57	GNU Bash Remote Code Execution (CVE-2014-6271) Protection Policy	Critical	Advance	GNU Bash remote code execution (CVE-2014-6271) detected - 2.
58	GNU Bash Remote Code Execution (CVE-2014-6271) Protection Policy	Critical	Advance	GNU Bash remote code execution (CVE-2014-6271) detected - 3.
59	GNU Bash Remote Code Execution (CVE-2014-6271) Protection Policy	Critical	Advance	GNU Bash remote code execution (CVE-2014-6271) detected - 4.
60	HTTP Response Splitting Protection Policy	Critical	Advance	HTTP response splitting attempt detected in HTTP request cookies - 1.
61	HTTP Response Splitting Protection Policy	Critical	Advance	HTTP response splitting attempt detected in HTTP request cookies - 2.
62	Legitimate File Request whitelist	Notice	Hidden	Whitelisting known file types.
63	Legitimate File Request whitelist	Notice	Hidden	Whitelisting known file types.
64	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected - 5.

65	OS Command Injection Protection Policy	Critical	Advance	System command injection attempt detected - 1.
66	OS Command Injection Protection Policy	Critical	Advance	System command injection attempt detected - 2.
67	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected - 6.
68	Local File Inclusion Protection Policy	Critical	Advance	Local File Inclusion (LFI) attempt detected via "\\\" character sequences.
69	SearchEngine WhiteListing Policy	Notice	Hidden	SearchEngine White-Listing Policy
70	Basic DoS/DDoS Threshold Based IP Restriction Policy (Non-Redis)	Notice	Disabled	IP Threshold Limiting Policy
71	Basic DoS/DDoS Threshold Based IP Restriction Policy (Non-Redis)	Notice	Disabled	IP Threshold Limiting Policy
72	Basic DoS/DDoS Threshold Based IP Restriction Policy (Non-Redis)	Notice	Disabled	IP Threshold Limiting Policy
73	HTTProxy Protection Policy	Critical	Advance	HTTP Proxy request header detected.
74	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected in HTTP request URI , arguments ,HTTP Headers or XML file.
75	Cross-Site Scripting Protection Policy	High	Hidden	Cross-Site-Scripting
76	Cross-Site Scripting	High	Disabled	Cross-Site Scripting
77	OS Command Injection Protection Policy	Critical	Hidden	Command Injection
78	Cross-Site-Scripting	Critical	Advance	Cross-Site Scripting attack attempt detected in HTTP request URI, Arguments and XML reuqests - 2
79	Cross-Site Scripting Protection Policy	High	Hidden	Cross-Site-Scripting

80	Bot Protection Policy	Critical	Advance	Security scanner related URI detected.
81	Bot Protection Policy	Critical	Advance	Command Line Tool/Library related User-Agent/HTTP header (from internal database) detected.
82	OS Command Injection Protection Policy	Critical	Hidden	Command Injection
83	Cross-Site Scripting Protection Policy	Critical	Premium	Cross-Site-Scripting
84	OS Command Injection Protection Policy	Critical	Hidden	System Command Injection
85	OS Command Injection Protection Policy	Critical	Hidden	System Command Injection
86	Basic DoS/DDoS Threshold Based IP Restriction Policy (Non-Redis)	Notice	Disabled	IP Threshold Limiting Policy
87	Remote File Inclusion Protection Policy	High	Disabled	NEW CRS 6.4
88	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.
89	SQL Injection Protection Policy	Critical	Advance	SQL Injection attempt detected - 7.
90	Apache Struts2 REST XStream RCE Vulnerability Protection Policy	Critical	Hidden	Apache Struts2 REST XStream RCE Vulnerability
91	Apache Struts2 REST XStream RCE Vulnerability Protection Policy	Critical	Hidden	Apache Struts2 REST XStream RCE Vulnerability
92	Custom CRS Version Check Policy	Notice	Hidden	Custom CRS Version Check Policy
93	Cross-Site Scripting Protection Policy	High	Hidden	Cross-Site-Scripting

94	Cross-Site Scripting	High	Hidden	Cross-Site Scripting
95	Cross-Site Scripting Protection Policy	Critical	Advance	Cross-Site-Scripting
96	Cross-Site Scripting Protection Policy	High	Hidden	Cross-Site-Scripting
97	Cross-Site Scripting Protection Policy	High	Hidden	Cross-Site-Scripting
98	Generic Deserialization Defence for Java	High	Hidden	Generic Deserialization attempt detected in Java.
99	Generic Deserialization Defence for Java	High	Hidden	Generic Deserialization attempt detected in Java.
100	Generic Deserialization Defence for Java	High	Advance	Generic Deserialization attempt detected in Java.
101	Generic Deserialization Defence for Java	High	Hidden	Generic Deserialization attempt detected in Java.
102	Generic Deserialization Defence for Java	High	Advance	Generic Deserialization attempt detected in Java.
103	Generic Deserialization Defence for Microsoft products	High	Advance	Generic Deserialization attempt detected in Microsoft Products.
104	Generic Deserialization Defence for Microsoft products	High	Disabled	Generic Deserialization attempt detected in Microsoft Products.
105	Generic Deserialization Defence for Ruby on Rails	High	Advance	Generic Deserialization attempt detected in Ruby on Rails.
106	Generic Deserialization Defence for Ruby on Rails	High	Advance	Generic Deserialization attempt detected in Ruby on Rails.
107	XML External Entity (XXE) Injection Policy	High	Hidden	XML External Entity (XXE) Injection attempt detected as local file inclusion.
108	XML External Entity (XXE) Injection Policy	High	Hidden	XML External Entity (XXE) Injection attempt detected as local file inclusion.
109	XML External Entity (XXE) Injection Policy	High	Advance	XML External Entity (XXE) Injection attempt detected as local file inclusion.

110	Possible Apache Struts OGNL RCE Protection Policy	Critical	Advance	Possible Apache Struts OGNL Code Execution Policy
111	Apache Tomcat Remote Code Execution Vulnerability Protection Policy	Critical	Advance	Apache Tomcat Remote Code Execution (CVE-2019-0232) attack attempt detected.
112	Possible Malicious File Upload	Critical	Advance	File upload with malicious extensions detected
113	HTML5 ping DOS Protection Policy	Critical	Advance	DoS attack using Ping headers in HTML5 - 1.
114	HTML5 ping DOS Protection Policy	Critical	Advance	DoS attack using Ping headers in HTML5 - 2.
115	HTML5 ping DOS Protection Policy	Critical	Advance	DoS attack using Ping headers in HTML5 - 3.
116	IIS Remote Code Execution Protection Policy	Critical	Advance	Microsoft IIS HTTP.sys Remote Code Execution Exploit attempt (CVE-2014-6321)
117	Apache DOS Protection Policy	High	Advance	Attempt to exploit DOS on Apache Server Based on Range Header
118	HTTP Policy Violation	Notice	Disabled	HTTP Policy Violation
119	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
120	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
121	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
122	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
123	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities

124	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
125	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
126	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
127	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
128	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
129	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
130	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
131	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities
132	PHP Remote Code Execution Protection Policy	High	Premium	Attempt to detect possibility of Remote Code Execution based on php vulnerabilities
133	PHP Remote Code Execution Protection Policy	High	Advance	Attempt to detect possibility of Remote Code Execution based on php vulnerabilities
134	Cross-Site Scripting	High	Hidden	Cross-Site Scripting
135	Malicious File Upload Attacks: Blocking Large File upload Attempts	Critical	Advance	Malicious File Upload Attacks: Blocking Large File upload Attempts
136	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Advanced DoS/DDoS Policy with Cookie Injection
137	Blacklisting IPs	Critical	Auto-generated	Blacklisting IPs

138	Whitelisting IPs	Critical	Auto-generated	Auto-generated
139	Whitelisting URIs	Notice	Auto-generated	Auto-generated
140	Cookie Injection Policy	Notice	Hidden	Cookie Injection Policy
141	IP Reputation Based Restriction Policy	Notice	Disabled	Access from Bad reputed IP detected (When config set to LOW, Threat Score >=10, Days Since Activity <=15)
142	IP Reputation Based Restriction Policy	High	Disabled	Access from Bad reputed IP detected (Based on cache)
143	IP Reputation Based Restriction Policy	Notice	Disabled	Access from Bad reputed IP detected (When config set to LOW, Threat Score >=10, Days Since Activity <=15)
144	IP Reputation Based Restriction Policy	Notice	Disabled	Access from Bad reputed IP detected (When config set to LOW, Threat Score >=10, Days Since Activity <=15)
145	IP Reputation Based Restriction Policy	Notice	Disabled	Access from Bad reputed IP detected (When config set to LOW, Threat Score >=10, Days Since Activity <=15)
146	IP Reputation Based Restriction Policy	High	Disabled	Access from Bad reputed IP detected (When config set to LOW, Threat Score >=10, Days Since Activity <=15)
147	IP Reputation Based Restriction Policy	High	Disabled	Access from Bad reputed IP detected (When config set to MED, Threat Score >=25, Days Since Activity <=5)
148	IP Reputation Based Restriction Policy	High	Disabled	Access from Bad reputed IP detected (When config set to HIGH, Threat Score >=40, Days Since Activity <=3)
149	IP Reputation Based Restriction Policy	Notice	Disabled	Access from Bad reputed IP detected (When config set to LOW, Threat Score >=10, Days Since Activity <=15)
150	Browser Integrity Check Policy	Critical	Disabled	Rule to block non-standard requests
151	Browser Integrity Check Policy	Critical	Disabled	Rule to block non-standard requests
152	Browser Integrity Check Policy	Critical	Disabled	Rule to block non-standard requests

153	Browser Integrity Check Policy	Critical	Disabled	Rule to block non-standard requests
154	Basic DoS/DDoS IP Threshold Based Policy v2.0	High	Disabled	Whitelist well known file ext for DDOS
155	Basic DoS/DDoS IP Threshold Based Policy v2.0	High	Disabled	Internal Tracking Rule
156	Basic DoS/DDoS IP Threshold Based Policy v2.0	High	Disabled	Basic DDOS 2.0
157	Basic DoS/DDoS IP Threshold Based Policy v2.0	High	Disabled	Basic DDOS 2.0
158	Basic DoS/DDoS IP Threshold Based Policy v2.0	High	Disabled	Basic DDOS 2.0
159	Basic DoS/DDoS IP Threshold Based Policy v2.0	High	Disabled	Basic DDOS 2.0
160	Basic DoS/DDoS IP Threshold Based Policy v2.0	High	Disabled	Basic DDOS 2.0
161	Basic DoS/DDoS IP Threshold Based Policy v2.0	Critical	Disabled	DoS/DDoS detected based on specified IP threshold value - 2.
162	Basic DoS/DDoS IP Threshold Based Policy v2.0	High	Disabled	Basic DDOS 2.0
163	Basic DoS/DDoS IP Threshold Based Policy v2.0	High	Disabled	Basic DDOS 2.0
164	Basic DoS/DDoS IP Threshold Based Policy v2.0	Critical	Disabled	DoS/DDoS detected based on specified IP threshold value - 1.
165	Basic DoS/DDoS IP Threshold Based Policy v2.0	Critical	Disabled	Basic DDOS 2.0

166	Basic DoS/DDoS IP Threshold Based Policy v2.0	High	Disabled	Basic DDOS 2.0
167	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
168	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
169	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
170	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
171	Cookie Injection Policy	Notice	Hidden	Cookie Injection Policy
172	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
173	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
174	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
175	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
176	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
177	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
178	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0

179	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
180	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Critical	Disabled	DoS/DDoS detected based on specified user threshold value - 1
181	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
182	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
183	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Critical	Disabled	DoS/DDoS detected based on specified user threshold value - 2
184	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Critical	Disabled	Advanced DDOS 2.0
185	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
186	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
187	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
188	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
189	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
190	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Critical	Disabled	DoS/DDoS detected based on specified IP threshold value - 1.
191	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0

192	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
193	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Critical	Disabled	DoS/DDoS detected based on specified IP threshold value - 2.
194	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Critical	Disabled	Advanced DDOS 2.0
195	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
196	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
197	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
198	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
199	Cookie Injection Policy	Notice	Hidden	Cookie Injection Policy
200	Cookie Injection Policy	Notice	Hidden	Cookie Injection Policy
201	Cookie Injection Policy	Notice	Hidden	Cookie Injection Policy
202	Cookie Tampering Detection Policy	Notice	Disabled	Cookie Tampering Detection Policy
203	Cookie Tampering Detection Policy	Notice	Disabled	Cookie Tampering Detection Policy
204	Cookie Tampering Detection Policy	Notice	Disabled	Cookie Tampering Detection Policy
205	Cookie Tampering Detection Policy	Notice	Disabled	Cookie Tampering Detection Policy
206	Cookie Tampering Detection Policy	Critical	Disabled	Detected user cookie tampering violation - 2.
207	Cookie Tampering Detection Policy	Notice	Disabled	Cookie Tampering Detection Policy

208	Cookie Tampering Detection Policy	Notice	Disabled	Cookie Tampering Detection Policy
209	Cookie Tampering Detection Policy	Notice	Disabled	Cookie Tampering Detection Policy
210	Cookie Tampering Detection Policy	Critical	Disabled	Detected user cookie tampering violation - 1.
211	Cookie Tampering Detection Policy	Notice	Disabled	Cookie Tampering Detection Policy
212	Cookie Tampering Detection Policy	Notice	Disabled	Cookie Tampering Detection Policy
213	Cookie Tampering Detection Policy	Critical	Disabled	Blocked due to too much cookie tampering detected by an IP
214	Cookie Tampering Detection Policy	Notice	Disabled	Cookie Tampering Detection Policy
215	Proxyshell RCE CVE-2021-34473	Critical	Advance	Proxyshell RCE (CVE-2021-34473)
216	CVE-2020-5902 F5 BIG-IP RCE	Critical	Advance	CVE-2020-5902 F5 BIG-IP Remote Code Execution
217	Confluence Server OGNL injection - CVE-2021-26084	Critical	Advance	Confluence Server OGNL injection - CVE-2021-26084
218	JSON Data Whitelisting Policy	Info	Advance	JSON Data Whitelisting Policy
219	Cookie Injection Policy	Notice	Hidden	Cookie Injection Policy
220	Cookie Injection Policy	Notice	Hidden	Cookie Injection Policy
221	Cookie Injection Policy	Notice	Hidden	Cookie Injection Policy
222	Cookie Injection Policy	Notice	Hidden	Cookie Injection Policy
223	Cookie Injection Policy	Notice	Hidden	Cookie Injection Policy
224	Cookie Tampering Detection Policy	Critical	Disabled	Violation detected for allowed number of cookies for an IP - 2.
225	Cookie Tampering Detection Policy	Notice	Disabled	Cookie Tampering Detection Policy
226	Cookie Tampering Detection Policy	Critical	Disabled	Violation detected for allowed number of cookies for an IP - 1.

227	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
228	Basic DoS/DDoS IP Threshold Based Policy v2.0	High	Disabled	Basic DoS/DDoS IP Threshold Based Policy v2.0
229	Cookie Injection Policy	Notice	Hidden	Cookie Injection Policy
230	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
231	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Notice	Disabled	Advanced DDOS 2.0
232	Cookie Injection Policy	Notice	Hidden	Cookie Injection Policy
233	XML Processing Analysis Policy	Notice	Hidden	These rules will enable XML Processing when content-type is XML.
234	XML Processing Analysis Policy	Notice	Hidden	These rules will enable XML Processing when content-type is XML.
235	XML Processing Analysis Policy	Notice	Hidden	These rules will enable XML Processing when content-type is XML.
236	XML Processing Analysis Policy	Notice	Hidden	These rules will enable XML Processing when content-type is XML.
237	Bot Protection Policy	Critical	Advance	Malicious bot related User-Agent/HTTP header detected.
238	Bot Protection Policy	Critical	Advance	Website Security Scanner related User-Agent/HTTP header detected.
239	Bot Protection Policy	Critical	Advance	Website Crawler related User-Agent/HTTP header detected.
240	Bot Protection Policy	Critical	Advance	Website Scrappers related User-Agent/HTTP header detected.
241	TOR exit node blacklist	Critical	Disabled	TOR exit node blacklist
242	Slow HTTP DOS Block Policy	Critical	Advance	Rule to block slow dos attacks
243	Slow HTTP DOS Block Policy	Critical	Advance	Rule to block slow dos attacks

244	ESI Injection Vulnerability	Critical	Advance	Rule to detect ESI Injection Vulnerability in request body or header or uri
245	Catch_All_Replay_Requests_Policy	Info	Advance	To catch and block all replay requests which are not blocked by any of the rules in config.
246	Global SessMap Cookie	Alert	Hidden	Global SessMap Cookie
247	LRN PHPSESSID Cookie	Alert	Hidden	LRN PHPSESSID Cookie
248	Global Env Vars Bot-API (Segmentation Fault Error Fix)	Alert	Hidden	Global Env Vars Bot-API (Segmentation Fault Error Fix)
249	Invalid Content-Length HTTP header	Critical	Advance	Invalid Content-Length HTTP header
250	HTTP Request Smuggling Attack	Critical	Advance	HTTP Request Smuggling Attack
251	Unicode Full/Half Width Abuse Attack Attempt	Critical	Advance	Unicode Full/Half Width Abuse Attack Attempt
252	Invalid character in request (null character)	Critical	Hidden	Invalid character in request (null character)
253	URL file extension is restricted by policy	Critical	Advance	URL file extension is restricted by policy
254	Attempt to access a backup or working file	Critical	Advance	Attempt to access a backup or working file
255	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
256	HTTP Request Smuggling Attack	Critical	Advance	HTTP Request Smuggling Attack
257	HTTP Request Smuggling Attack	Critical	Advance	HTTP Request Smuggling Attack
258	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)

259	HTTP Splitting (CR/LF in request filename detected)	Critical	Advance	HTTP Splitting (CR/LF in request filename detected)
260	Node.js-injection Attacks	Critical	Advance	Node.js Injection Attack
261	Apache Struts and Java Attacks	Critical	Advance	Remote Command Execution: Java process spawn (CVE-2017-9805)
262	Apache Struts and Java Attacks	Critical	Advance	Remote Command Execution: Java serialization (CVE-2015-5842)
263	Apache Struts and Java Attacks	Critical	Advance	Suspicious Java class detected
264	Apache Struts and Java Attacks	Critical	Advance	Base64 encoded string matched suspicious keyword
265	Remote File Inclusion Attacks	Critical	Advance	Possible Remote File Inclusion (RFI) Attack: Common RFI Vulnerable Parameter Name used w/URL Payload
266	PHP Injection Attack: PHP Open Tag Found	Critical	Advance	PHP Injection Attack: PHP Open Tag Found
267	PHP Injection Attack: Configuration Directive Found	Critical	Advance	PHP Injection Attack: Configuration Directive Found
268	PHP Injection Attack: Variables Found	Critical	Advance	PHP Injection Attack: Variables Found
269	PHP Injection Attack: I/O Stream Found	Critical	Advance	PHP Injection Attack: I/O Stream Found
270	PHP Injection Attack: Wrapper scheme detected	Critical	Advance	PHP Injection Attack: Wrapper scheme detected
271	PHP Injection Attack: High-Risk PHP Function Call Found	Critical	Advance	PHP Injection Attack: High-Risk PHP Function Call Found
272	PHP Injection Attack: Serialized Object Injection	Critical	Advance	PHP Injection Attack: Serialized Object Injection
273	PHP Injection Attack: Variable Function Call Found	Critical	Advance	PHP Injection Attack: Variable Function Call Found

274	PHP Injection Attack: Variable Function Call Found	Critical	Premium	PHP Injection Attack: Variable Function Call Found
275	Path Traversal Attack (/../)	Critical	Advance	Path Traversal Attack (/../)
276	Restricted File Access Attempt	Critical	Advance	Restricted File Access Attempt
277	OS File Access Attempt	Critical	Advance	OS File Access Attempt
278	XSS Javascript Injection Attempt	Critical	Hidden	XSS Javascript Injection Attempt
279	Cross-site-scripting Attempt	Critical	Premium	Cross-site-scripting Attempt
280	NoScript XSS InjectionChecker: HTML Injection	Critical	Premium	NoScript XSS InjectionChecker: HTML Injection
281	NoScript XSS InjectionChecker: Attribute Injection	Critical	Premium	NoScript XSS InjectionChecker: Attribute Injection
282	IE XSS Filters - Attack Detected	Critical	Premium	IE XSS Filters - Attack Detected
283	IE XSS Filters - Attack Detected	Critical	Premium	IE XSS Filters - Attack Detected
284	JavaScript global variable found	Critical	Premium	JavaScript global variable found
285	AngularJS client side template injection detected	Critical	Premium	AngularJS client side template injection detected
286	Malicious File Upload Attacks	High	Disabled	Possible Malicious file-upload
287	Malicious File Upload Attacks	High	Disabled	Possible Malicious file-upload
288	Malicious File Upload Attacks	High	Advance	Filename exceeds 255 Character limit
289	Malicious File Upload Attacks	Critical	Advance	Invalid filename upload attempt
290	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.
291	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.
292	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.
293	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.
294	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.
295	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.
296	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.
297	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.
298	Advanced SQL Injection Attacks	Critical	Advance	SQL Injection Attack: Common DB Names Detected
299	Advanced SQL Injection Attacks	Critical	Advance	Detects blind sqli tests using sleep() or benchmark() including Conditional Queries
300	Advanced SQL Injection Attacks	Critical	Advance	Postgres/MongoDB based SQLi Attempt Detected
301	Advanced SQL Injection Attacks	Critical	Advance	Detects MySQL and PostgreSQL stored procedure/function injections
302	Advanced SQL Injection Attacks	Critical	Advance	MySQL in-line comment detected

303	Advanced SQL Injection Attacks	Critical	Advance	Detects MySQL charset switch and MSSQL DoS attempts
304	Advanced SQL Injection Attacks	Critical	Advance	SQL Injection Attack: Common DB Names Detected
305	Advanced SQL Injection Attacks	Critical	Advance	Detects basic SQL authentication bypass attempts
306	Advanced SQL Injection Attacks	Critical	Advance	Detects MySQL comment-/space-obfuscated injections and backtick termination
307	Advanced SQL Injection Attacks	Critical	Advance	Detects basic SQL authentication bypass attempts
308	Advanced SQL Injection Attacks	Critical	Advance	Detects basic SQL authentication bypass attempts
309	Advanced SQL Injection Attacks	Critical	Advance	Detects chained SQL injection attempts
310	Advanced SQL Injection Attacks	Critical	Advance	Detects classic SQL injection probings
311	Advanced SQL Injection Attacks	Critical	Advance	Detects basic SQL authentication bypass attempts
312	Advanced SQL Injection Attacks	Critical	Advance	Detects classic SQL injection probings
313	Advanced SQL Injection Attacks	Critical	Advance	SQL Injection Attack
314	Advanced SQL Injection Attacks	Critical	Advance	SQL Injection Attack
315	Advanced SQL Injection Attacks	Critical	Advance	SQL Injection Attack
316	Malicious File Upload Attacks: Preventing all File Upload Attempts	Critical	Advance	Malicious File Upload Attacks: Preventing all File Upload Attempts
317	Malicious File Upload Attempt: Denying all Non-Document File upload Attempts	Critical	Advance	Malicious File Upload Attempt: Denying all Non-Document File upload Attempts
318	Malicious File Upload Attacks: Denying all	Critical	Advance	Malicious File Upload Attacks: Denying all Non-Media File upload Attempts

	Non-Media File upload Attempts			
319	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
320	Advanced Command Injection Attacks	Critical	Advance	Remote Command Execution: Windows Command Injection
321	Advanced Command Injection Attacks	Critical	Advance	Remote Command Execution: Unix Command Injection
322	Advanced Command Injection Attacks	Critical	Advance	Remote Command Execution: Windows Command Injection
323	Advanced Command Injection Attacks	Critical	Advance	Remote Command Execution: Windows Command Injection
324	Advanced Command Injection Attacks	Critical	Advance	Remote Command Execution: Unix Shell Expression Found
325	Double Extension Remote Code Execution Attack	Critical	Advance	Malicious File Upload: Remote code execution-SA-CORE-2020-012 Attack Identified
326	HTTP Request Smuggling Attack	Critical	Advance	HTTP Request Smuggling identified with multiple Content-Length HTTP headers
327	HTTP Request Smuggling Attack	Critical	Advance	Unusual HTTP Protocol Format
328	HTTP Request Smuggling Attack	Critical	Advance	HTTP Request Smuggling Attack
329	HTTP Request Smuggling Attack	Critical	Advance	Advanced HTTP Request Smuggling Attack Identified
330	HTTP Request Smuggling Attack	Critical	Advance	Possible HTTP Request Smuggling Attack
331	Advanced Cookie Tampering Detection Policy	Critical	Advance	Advanced Cookie Tampering Detection Policy
332	Advanced Cookie Tampering Detection Policy	Critical	Advance	Policy to Block IP due to number of cookies generated more than allowed

333	Advanced Cookie Tampering Detection Policy	Critical	Advance	Setting var to track cookie counts by IP
334	Advanced Cookie Tampering Detection Policy	Critical	Advance	Blocks requests if for specific IP cookies are generated more than expected count.
335	Advanced Cookie Tampering Detection Policy	Critical	Advance	Sliding IP blocking time
336	Advanced Cookie Tampering Detection Policy	Critical	Advance	This policy will Block an IP due to too much Cookie generation behind the NATed IP
337	Advanced Cookie Tampering Detection Policy	Critical	Advance	Management rule to support Cookie Tampering rule framework.
338	Advanced Cookie Tampering Detection Policy	Critical	Advance	Management rule to support Cookie Tampering rule framework.
339	Advanced Cookie Tampering Detection Policy	Critical	Advance	Management rule to support Cookie Tampering rule framework.
340	Advanced Cookie Tampering Detection Policy	Critical	Advance	Management rule to support Cookie Tampering rule framework.
341	Advanced Cookie Tampering Detection Policy	Critical	Advance	Blocking Session in case of Cookie Validation failures.
342	Advanced Cookie Tampering Detection Policy	Critical	Advance	Management rule to support Cookie Tampering rule framework.
343	Advanced Cookie Tampering Detection Policy	Critical	Advance	Management rule to support Cookie Tampering rule framework.
344	Advanced Cookie Tampering Detection Policy	Critical	Advance	Management rule to support Cookie Tampering rule framework.
345	Advanced Cookie Tampering Detection Policy	Critical	Advance	Management rule to support Cookie Tampering rule framework.

346	Advanced Cookie Tampering Detection Policy	Critical	Disabled	Advanced Cookie Tampering Detection Policy
347	Spring Framework WebappClassLoader Code Execution Vulnerability CVE-2010-1622	High	Advance	Restricted SPRING RCE Attack Detected for CVE-2010-1622.
348	JAVA SPRING RCE Attack	Critical	Advance	Restricted JAVA SPRING RCE Attack Detected for CVE-2022-22963.
349	Microsoft Exchange Server Remote Code Execution	Critical	Advance	Remote code execution attempt (CVE-2021-26855) in Microsoft Exchange Server can be exploited via sending arbitrary http requests with configured headers.
350	MS Http.sys RCE vulnerability	Critical	Advance	Rule to block MS Http.sys RCE attacks
351	Apache Http Server Path Traversal Vulnerability	Critical	Advance	Rule to prevent path traversal attack
352	Microsoft Exchange .NET Deserialization RCE Vulnerability	Critical	Advance	Restrict malicious requests exploiting CVE-2021-42321
353	Apache Log4j Remote Code Execution Vulnerability	Critical	Advance	Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228) attack detected
354	Apache Log4j Remote Code Execution Vulnerability	Critical	Advance	Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228) attack detected
355	Apache Log4j Remote Code Execution Vulnerability	Critical	Advance	Restricted malicious requests with apache log4j DOS attack CVE-2021-45105
356	Apache Log4j Remote Code Execution Vulnerability	Critical	Advance	Restricts malicious requests with apache log4j CVE-2021-45046 DOS attack
357	Apache Log4j Remote Code Execution Vulnerability	Critical	Advance	Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228) attack detected

358	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Behavioral DoS/DDoS IP Logging
359	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Behavioral DoS/DDoS IP Logging
360	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Behavioral DoS/DDoS IP Logging
361	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Behavioral DoS/DDoS IP-Session Logging
362	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Behavioral DoS/DDoS IP-Session Blocking
363	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Behavioral DoS/DDoS Host-Level Logging
364	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Behavioral DoS/DDoS Host-Level Blocking
365	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Behavioral DoS/DDoS URI Blocking
366	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Behavioral DoS/DDoS URI Logging
367	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Behavioral DoS/DDoS URI-Session Blocking
368	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Behavioral DoS/DDoS URI-Session Blocking
369	Behavioral Bot Attacks Policy	Critical	Auto-generated	Behavioral Bot Attacks Policy
370	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Behavioral DoS/DDoS IP Logging
371	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	API Behavioral DoS/DDoS Rate Limit Blocking Policy
372	Behavioral DoS/DDoS Rate Limiting Policy	Critical	Auto-generated	Behavioral DoS/DDoS IP Logging
373	Blacklisting Countries	High	Auto-generated	Blacklisting Countries
374	Whitelisting Scanner IPs	Info	In-line Header Rule	IP Blacklist URI/IP Whitelist Headers
375	Whitelisting Scanner IPs	Info	In-line Header Rule	IP Blacklist URI/IP Whitelist Headers

376	Whitelisting indus.html	Info	In-line Header Rule	IP Blacklist URI/IP Whitelist Headers
377	CRS-6.4-hotfix-v1 Policy	Notice	Advance	CRS-6.4-hotfix-v1 Policy
378	PHP Remote Code Execution	Critical	Advance	Attempt to detect possibility of Remote Code Execution based on php vulnerabilities
379	Cookie Injection Policy	Notice	Advance	Generating New Cookie for Older one
380	Cross-Site-Scripting Attacks	Critical	Advance	This rule prevents Cross-Site-Scripting attacks by identifying and preventing XSS payloads.
381	Path Traversal Coverage	Critical	Advance	Rule to cover encoded payloads (..2f..2f|2e2e2f|326532653266)
382	Atlassian Backdoor Attack CVE-2022-26138	Critical	Advance	Atlassian Backdoor Attack CVE-2022-26138 Coverage
383	Spring Framework WebappClassLoader Code Execution Vulnerability	Critical	Advance	Restricted SPRING RCE Attack Detected for CVE-2010-1622 in Request Body
384	Encoding Abuse Attacks - NULL Code Injection	Critical	Advance	Encoding Abuse Attacks
385	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.
386	JSON SQL Injection Attack	Critical	Advance	JSON SQL Injection attempt detected in HTTP request URI and arguments.
387	ProxyNotShell (CVE-2022-40140 & CVE-2022-41082)	Critical	Advance	MS Exchange ProxyNotShell (CVE-2022-40140 & CVE-2022-41082) Attack Detected.
388	ProxyNotShell (CVE-2022-40140 & CVE-2022-41082)	Critical	Advance	MS Exchange OWASSRF Attack Detected
389	Whitelisting Scanner IPs	Info	In-line Header Rule	IP Blacklist URI/IP Whitelist Headers

390	Whitelisting Scanner IPs	Info	In-line Header Rule	IP Blacklist URI/IP Whitelist Headers
391	Whitelisting Scanner IPs	Info	In-line Header Rule	IP Blacklist URI/IP Whitelist Headers
392	Whitelisting Scanner IPs	Info	In-line Header Rule	IP Blacklist URI/IP Whitelist Headers
393	Whitelist NAT IPs for /indus.html	Info	Global-Config Rule	Whitelist NAT IPs for /indus.html
394	Allow GET request for URI /.well-known/acme-challenge	Info	Global-Config Rule	Allow GET request for URI /.well-known/acme-challenge
395	Whitelisting NAT IPs for autobypass health check	Info	Global-Config Rule	Whitelisting NAT IPs for autobypass health check
396	Whitelisting IPs	Info	Global-Config Rule	Whitelisting IPs
397	Advanced SQL Injection Attacks	Critical	Advance	This rule detects JSON based SQL injection.
398	Java Attacks	Critical	Advance	This rule detects Java class reflection usage to execute methods that allow OS commands execution.
399	Content Injection	Critical	Advance	HTML content injection within Request URL detected.
400	SQL Injection	Critical	Advance	SQL Injection attempt detected in HTTP request URI and arguments.
401	LDAP Injection	Critical	Advance	To identify LDAP injection attacks
402	Command Injection	Critical	Advance	To identify command injection attacks
403	Manage Engine Remote Code Execution	Critical	Advance	CVE-2022-47966 Manage Engine Remote Code Execution
404	Apache Struts and Java Attacks	Critical	Advance	Apache Struts and Java Attacks

405	VMWare Aria Remote Code Execution Policy	Critical	Advance	VMWare Aria Remote Code Execution Policy
406	VMWare Aria Remote Code Execution Policy	Critical	Advance	VMWare Aria Remote Code Execution Policy
407	MOVEit Transfer Vulnerability Policy	Critical	Advance	MOVEit Transfer Vulnerability Policy
408	MOVEit Transfer Vulnerability Policy	Critical	Advance	MOVEit Transfer Vulnerability Policy
409	MOVEit Transfer Vulnerability Policy	Critical	Advance	MOVEit Transfer Vulnerability Policy
410	MOVEit Transfer Vulnerability Policy	Critical	Advance	MOVEit Transfer Vulnerability Policy
411	MOVEit Transfer Vulnerability Policy	Critical	Advance	MOVEit Transfer Vulnerability Policy
412	MOVEit Transfer Vulnerability Policy	Critical	Advance	MOVEit Transfer Vulnerability Policy
413	Bot Attacks	Critical	Advance	Bot Attacks

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.