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 provides 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	Basic DoS/DDoS IP Threshold Based Policy v2.0	Critical	Advance	DoS/DDoS detected based on specified IP threshold value - 1.
2	Basic DoS/DDoS IP Threshold Based Policy v2.0	Critical	Advance	DoS/DDoS detected based on specified IP threshold value - 2.
3	Cross-Site Scripting	Critical	Premium	Cross-Site Scripting attack attempt detected in HTTP request URI, Arguments and XML requests - 1.
4	Cross-Site Scripting	Critical	Advance	Cross-Site Scripting attack attempt detected in HTTP request Cookies and XML requests.
5	Cross-Site Scripting	Critical	Premium	Cross-Site Scripting attack attempt detected in HTTP request URI, Arguments and XML requests - 2.
6	HTTP Policy Violation	Medium	Premium	Non-supported HTTP request method (other than GET, POST & HEAD) detected.
7	HTTP Policy Violation	Low	Advance	Non-supported HTTP request headers detected.
8	SQL Injection	Critical	Advance	SQL Injection attempt detected in HTTP request URI and arguments.
9	SQL Injection	Critical	Premium	SQL Injection attempt detected in HTTP request cookies and XML requests.
10	SQL Injection	Critical	Premium	SQL Injection attempt detected - 1.
11	SQL Injection	Critical	Advance	SQL Injection attempt detected - 2.
12	SQL Injection	Critical	Advance	SQL Injection attempt detected - 3.
13	SQL Injection	Critical	Advance	SQL Injection attempt detected in HTTP request cookies or in XML requests.
14	SQL Injection	Critical	Advance	SQL Injection attempt detected in HTTP request URI, arguments, or HTTP Headers
15	SQL Injection	Critical	Advance	Blind SQL Injection attempt detected in HTTP request URI and arguments.
16	SQL Injection	Critical	Advance	Blind SQL Injection attempt detected in HTTP request cookies and XML requests.
17	SQL Injection	Critical	Advance	Blind SQL Injection attempt detected - 1.
18	SQL Injection	Critical	Advance	Blind SQL Injection attempt detected - 2.
19	SQL Injection	Critical	Advance	Blind SQL Injection attempt detected - 3.
20	SQL Injection	Critical	Advance	Blind SQL Injection attempt detected - 4.
21	SQL Injection	Critical	Advance	Blind SQL Injection attempt detected in HTTP request URI, arguments, or Cookie.
22	SQL Injection	Critical	Advance	Blind SQL Injection attempt detected in HTTP request URI, arguments, or Cookie.
23	SQL Injection	Critical	Advance	SQL Injection attempt detected in HTTP request URI, arguments, or Cookie.
24	SQL Injection	Critical	Advance	SQL Injection attempt detected - 5.
25	SQL Injection	Critical	Advance	SQL Injection attempt detected - 4.
26	SQL Injection	Critical	Advance	SQL Injection attempt detected – 6

27	SQL Injection	Critical	Advance	SQL Injection attempt detected - 7.
28	SQL Injection	Critical	Advance	Blind SQL Injection attempt detected in HTTP request URI, arguments, or Request Headers.
29	SQL Injection	Critical	Advance	SQL Injection attempt detected in HTTP request URI, arguments, HTTP Headers or XML file.
30	SSI Injection	Critical	Advance	Server- side Injection attempt detected in HTTP request URI or arguments.
31	SSI Injection	Critical	Advance	Server- side Injection attempt detected in HTTP headers or XML file.
32	Bot Protection	High	Premium	Automated program-based User-Agent/HTTP header detected.
33	Bot Protection	High	Premium	Security scanner related User-Agent detected.
34	Bot Protection	High	Advance	Security scanner related User-Agent detected.
35	Bot Protection	High	Advance	Security scanner related HTTP header detected.
36	Bot Protection	High	Advance	Security scanner Nessus based URI detected.
37	Bot Protection	High	Advance	Website Crawler related User-Agent/HTTP header detected.
38	Bot Protection	High	Advance	Website Crawler related User-Agent/HTTP header (from internal database) detected.
39	Bot Protection	High	Advance	Security scanner related User-Agent/HTTP header (from internal database) detected - 2.
40	Bot Protection	High	Advance	Security scanner related User-Agent/HTTP header (from internal database) detected - 1.
41	Bot Protection	High	Advance	Security scanner related URI detected.
42	Bot Protection	High	Advance	Command Line Tool/Library related User-Agent/HTTP header (from internal database) detected.
43	Bot Protection	High	Advance	Bad bots related User-Agent/HTTP header (from internal database) detected.
44	Cross-Site Scripting	Critical	Premium	Cross-Site Scripting attack attempt detected in HTTP request URI, Arguments and XML requests - 1.
45	File Injection	High	Advance	File injection attempt detected in HTTP request URI and arguments.
46	File Injection	High	Advance	File injection attempt detected in HTTP request header and XML requests.
47	OS Command Injection	Critical	Advance	System command injection attempt detected - 1.
48	OS Command Injection	Critical	Advance	System command injection attempt detected - 2.
49	PHP Injection	High	Advance	PHP injection attempt detected in HTTP request URI and arguments.
50	PHP Injection	High	Advance	PHP injection attempt detected in HTTP request header and XML requests.
51	Bot Protection	High	Advance	Bad reputated IP detected.
52	File Inclusion	High	Advance	Local File Inclusion (LFI) attempt detected via file traversal character sequences.
53	File Inclusion	High	Advance	Local File Inclusion (LFI) attempt detected via "\\\" character sequences.

54	File Inclusion	High	Premium	Local File Inclusion (LFI) attempt detected using path pointing from root directory.
55	Abuse of Functionality	Medium	Advance	Base64-encoded payload detected in HTTP request
56	File Inclusion	Medium	Premium	Remote File Inclusion (RFI) attempt detected.
57	Abuse of Functionality	Medium	Advance	JavaScript encoding abuse detected - 1.
58	Abuse of Functionality	Medium	Advance	JavaScript encoding abuse detected - 2.
59	Remote Code Execution	High	Advance	GNU Bash remote code execution (CVE-2014-6271) detected - 1.
60	Remote Code Execution	High	Advance	GNU Bash remote code execution (CVE-2014-6271) detected - 2.
61	Remote Code Execution	High	Advance	GNU Bash remote code execution (CVE-2014-6271) detected - 3.
62	Remote Code Execution	High	Advance	GNU Bash remote code execution (CVE-2014-6271) detected - 4.
63	HTTP Response Splitting	Medium	Advance	HTTP response splitting attempt detected in HTTP request cookies – 1
64	HTTP Response Splitting	Medium	Advance	HTTP response splitting attempt detected in HTTP request cookies - 2.
65	HTTP Proxy Protection	Medium	Advance	HTTP Proxy request header detected.
66	Apache Struts Remote Code Execution	High	Advance	Remote code execution attempt via suspicious Java class detected. User can execute system commands via process builder or runtime calls and an attacker can misuse these classes submitting improperly sanitized objects to run malicious system commands.
67	Apache Struts Remote Code Execution	High	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.
68	Apache Tomcat Remote Code Execution	Medium	Advance	Apache Tomcat Remote Code Execution (CVE-2019-0232) attack attempt detected.
69	DOS Protection	Critical	Advance	DoS attack using Ping headers in HTML5 - 1.
70	DOS Protection	Critical	Advance	DoS attack using Ping headers in HTML5 - 2.
71	DOS Protection	Critical	Advance	DoS attack using Ping headers in HTML5 - 3.
72	File Upload	High	Premium	File upload with malicious extensions detected.
73	IIS Remote Code Execution	High	Advance	Microsoft IIS HTTP.sys Remote Code Execution Exploit attempt (CVE2014-6321).
74	Apache Struts Remote Code Execution	High	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.
75	Apache Struts Remote Code Execution	High	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.
76	Apache Struts Remote Code Execution	High	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.
77	Apache Struts Remote Code Execution	High	Advance	Remote code execution attempt (CVE-2017-5638) using cc or get 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.
78	Apache Struts Remote Code Execution	High	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.
79	Apache Struts Remote Code Execution	High	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.
80	Apache Struts Remote Code Execution	High	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.

81	PHP Remote Code Execution	High	Advance	Attempt to exploit Remote Code Execution based on php vulnerabilities.
82	PHP Remote Code Execution	High	Premium	Attempt to detect possibility of Remote Code Execution based on php vulnerabilities.
83	PHP Remote Code Execution	High	Advance	Attempt to detect possibility of Remote Code Execution based on php vulnerabilities.
84	Apache DOS Protection	High	Advance	Attempt to exploit DOS on Apache Server Based on Range Header
85	IP Reputation	High	Advance	Access from Bad reputed IP detected (Based on cache).
86	IP Reputation	High	Advance	Access from Bad reputed IP detected (When config set to LOW, Threat Score >=10, Days Since Activity<=15).
87	IP Reputation	High	Advance	Access from Bad reputed IP detected (When config set to MED, Threat Score >=25, Days Since Activity<=5).
88	IP Reputation	High	Advance	Access from Bad reputed IP detected (When config set to HIGH, Threat Score >=40, Days Since Activity<=3).
89	XML External Entity	High	Advance	XML External Entity (XXE) Injection attempt detected as local file inclusion. Generic Deserialization Defence for Java High Advance Generic D
90	Generic Deserialization Defence for Java	High	Advance	Generic Deserialization attempt detected in Java.
91	Generic Deserialization Defence for Microsoft products	High	Advance	Generic Deserialization attempt detected in Microsoft Products.
92	Generic Deserialization Defence for Ruby on Rails	High	Advance	Generic Deserialization attempt detected in Ruby on Rails.
93	Node.js-injection Attacks	Critical	Advance	Node.js Injection Attack
94	Apache Struts and Java Attacks	Critical	Advance	Remote Command Execution: Java process spawn (CVE-2017-9805).
95	Apache Struts and Java Attacks	Critical	Advance	Remote Command Execution: Java serialization (CVE-2015-5842).
96	Apache Struts and Java Attacks	Critical	Advance	Suspicious Java class detected
97	Apache Struts and Java Attacks	Critical	Advance	Base64 encoded string matched suspicious keyword.
98	Remote File Inclusion Attacks	Critical	Advance	Possible Remote File Inclusion (RFI) Attack: Common RFI Vulnerable Parameter Name used w/URL Payload
99	PHP Injection Attacks	Critical	Advance	PHP Injection Attack: PHP Open Tag Found

100	PHP Injection Attacks	Critical	Advance	PHP Injection Attack: Configuration Directive Found
101	PHP Injection Attacks	Critical	Advance	PHP Injection Attack: Variables Found
102	PHP Injection Attacks	Critical	Advance	e PHP Injection Attack: I/O Stream Found
103	PHP Injection Attacks	Critical	Advance	PHP Injection Attack: Wrapper scheme detected
104	PHP Injection Attacks	Critical	Advance	PHP Injection Attack: High-Risk PHP Function Call Found
105	PHP Injection Attacks	Critical	Advance	PHP Injection Attack: Serialized Object Injection
106	PHP Injection Attacks	Critical	Advance	PHP Injection Attack: Variable Function Call Found
107	PHP Injection Attacks	Critical	Premium	PHP Injection Attack: Variable Function Call Found
108	Path Traversal Attack	Critical	Advance	Path Traversal Attack (/../)
109	Path Traversal Attack	Critical	Premium	OS File Access Attempt
110	Path Traversal Attack	Critical	Advance	Restricted File Access Attempt
111	HTTP Protocol Attack Prevention	Critical	Advance	HTTP Request Smuggling Attack
112	HTTP Protocol Attack Prevention	Critical	Advance	HTTP Header Injection Attack via payload (CR/LF and header-name detected)
113	HTTP Protocol Attack Prevention	Critical	Advance	HTTP Splitting (CR/LF in request filename detected)
114	HTTP Protocol Enforcement	Critical	Advance	Invalid Content-Length HTTP header
115	HTTP Protocol Enforcement	Critical	Advance	HTTP Request Smuggling Attack
116	HTTP Protocol Enforcement	Critical	Advance	Unicode Full/Half Width Abuse Attack Attempt
117	HTTP Protocol Enforcement	Critical	Advance	Invalid character in request (null character)
118	HTTP Protocol Enforcement	Critical	Advance	URL file extension is restricted by policy
119	HTTP Protocol Enforcement	Critical	Advance	Attempt to access a backup or working file
120	HTTP Protocol Enforcement	Critical	Advance	Request with Header x-up-devcap-post-charset detected in combination with \'UP\' User-Agent prefix
121	Cross-Site Scripting Attacks	Critical	Premium	XSS Javascript Injection Attempt
122	Cross-Site Scripting Attacks	Critical	Premium	Cross-site-scripting Attempt
123	Cross-Site Scripting Attacks	Critical	Premium	No Script XSS Injection Checker: HTML Injection
124	Cross-Site Scripting Attacks	Critical	Premium	No Script XSS Injection Checker: Attribute Injection

125	Cross-Site Scripting Attacks	Critical	Premium	IE XSS Filters - Attack Detected
126	Cross-Site Scripting Attacks	Critical	Premium	JavaScript global variable found
127	Cross-Site Scripting Attacks	Critical	Premium	AngularJS client-side template injection detected.
128	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Critical	Advance	DoS/DDoS detected based on specified user threshold value – 1
129	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Critical	Advance	DoS/DDoS detected based on specified user threshold value – 2
130	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Critical	Advance	DoS/DDoS detected based on specified IP threshold value - 1.
131	Advanced DoS/DDoS Policy with Cookie Injection v2.0	Critical	Advance	DoS/DDoS detected based on specified IP threshold value - 2.
132	Cookie Tampering Detection Policy	Critical	Advance	Violation detected for allowed number of cookies for an IP - 2.
133	Cookie Tampering Detection Policy	Critical	Advance	Violation detected for allowed number of cookies for an IP - 1.
134	Cookie Tampering Detection Policy	Critical	Advance	Blocked due to too much cookie tampering detected by an IP.
135	Cookie Tampering Detection Policy	Critical	Advance	Detected user cookie tampering violation - 2.
136	Cookie Tampering Detection Policy	Critical	Advance	Detected user cookie tampering violation - 1.
137	TOR exit node blacklist	High	Premium	The rule will block Tor Exit Node Ips
138	Advanced SQL Injection Attacks	Critical	Advance	SQL Injection Attack: Common DB Names Detected
139	Advanced SQL Injection Attacks	Critical	Advance	Detects blind sqli tests using sleep() or benchmark() including Conditional Queries
140	Advanced SQL Injection Attacks	Critical	Advance	Postgres/MongoDB based SQLi Attempt Detected
141	Advanced SQL Injection Attacks	Critical	Advance	Detects MySQL and PostgreSQL stored procedure/function injections
142	Advanced SQL Injection Attacks	Critical	Advance	MySQL in-line comment detected
143	Advanced SQL Injection Attacks	Critical	Advance	Detects MySQL charset switch and MSSQL DoS attempts
144	Advanced SQL Injection Attacks	Critical	Advance	SQL Injection Attack: Common DB Names Detected
145	Advanced SQL Injection Attacks	Critical	Advance	Detects basic SQL authentication bypass attempts

146	Advanced SQL Injection Attacks	Critical	Advance	Detects MySQL comment-/space-obfuscated injections and backtick
147	Advanced SQL Injection Attacks	Critical	Advance	Detects basic SQL authentication bypass attempts
148	Advanced SQL Injection Attacks	Critical	Advance	Detects chained SQL injection attempts
149	Advanced SQL Injection Attacks	Critical	Advance	Detects classic SQL injection probings.
150	Advanced SQL Injection Attacks	Critical	Advance	Detects basic SQL authentication bypass attempts
151	Advanced SQL Injection Attacks	Critical	Advance	Detects classic SQL injection probings.
152	Advanced SQL Injection Attacks	Critical	Advance	SQL Injection Attack.
153	Advance Command Injection	Critical	Advance	Remote Command Execution: Windows Command Injection.
154	Advance Command Injection	Critical	Advance	Remote Command Execution: Unix Command Injection.
155	Advance Command Injection	Critical	Advance	Remote Command Execution: Unix Shell Expression Found.
156	Bot Protection	High	Advance	Website Security Scanner related User-Agent/HTTP header detected.
157	Bot Protection	High	Advance	Website Scrappers related User-Agent/HTTP header detected.
158	Malicious File Upload Attacks	Critical	Advance	Blocking Large File upload Attempts
159	Malicious File Upload Attacks	Critical	Advance	Denying all Non-Document and Non-Media File upload Attempts
160	Malicious File Upload Attacks	Critical	Advance	Denying all Non-Media File upload Attempts
161	Malicious File Upload Attacks	Critical	Advance	Blocking All file Uploads
162	Malicious File Upload Attacks	Critical	Advance	Blocking Upload of Non-Document Files
163	TOR exit node blacklist	Critical	Advance	TOR exit node blacklist
164	Double Extension Remote Code Execution Attack	Critical	Advance	Remote code execution-SA-CORE-2020-012 Attack Identified
165	Slow HTTP Dos Attack	Critical	Advance	Rule to block slow dos attacks
166	HTTP Request Smuggling Attack	Critical	Advance	HTTP Request Smuggling identified with multiple Content-Length HTTP headers
167	HTTP Request Smuggling Attack	Critical	Advance	Unusual HTTP Protocol Format
168	HTTP Request Smuggling Attack	Critical	Advance	HTTP Request Smuggling Attack

169	HTTP Request Smuggling Attack	Critical	Advance	Advanced HTTP Request Smuggling Attack Identified
170	HTTP Request Smuggling Attack	Critical	Advance	Possible HTTP Request Smuggling Attack
171	Microsoft Exchange Server Remote Code Execution	Critical	Advance	Microsoft Exchange Server Remote Code Execution Policy

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 IP's automatically. IP's with bad reputation is identified by using internal Global Threat Platform which identifies malicious IP's 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 IP's 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 API's 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.