APPTRANA

Competency Matrix for OWASP Top 10

www.indusface.com

AppTrana is the industry's first truly integrated 'Total Application Security' solution that 'Detect, Protect & Monitor' your applications on a continuous basis. Our suite of products Includes- Web Application Scanning, Web Application Firewall with DDoS protection, and Mobile Application Scanning.

Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. They publish a ranking of the 10 most-critical web application security flaws, which are known as the OWASP Top 10. The OWASP Top 10 represents a broad consensus of the most-critical web application security flaws. It's a widely accepted methodology for evaluating web application security and build mitigation strategies for websites and web-based applications. It outlines the top 10 areas where web applications are susceptible to attacks, and where common vulnerabilities are found.

Last OWASP Top 10 was released on 2013 and new RC1 candidate was released on 2017. Final version is expected by Nov 2017

In the fight against cyber criminals, OWASP's Top 10 Vulnerabilities serve as an ideal place to start covering the bases. Though the coverage of AppTrana is well beyond OWASP top 10, this document talks only about OWASP Top 10 and how AppTrana can be used to protect your sites against OWASP Top 10 vulnerabilities.

How is AppTrana Different?

Most WAF solution fails, as application security is complex and creating rules in-house 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 AppTrana approach the problem differently. We believe, security of the application is best handled by experts and 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 to complete overview of tests done by AppTrana' s different offering and how you can be instantly protected through inbuilt WAF.

AppTrana's Coverage for OWASP Top 10

Glossery

Automates Scans	Automated scans done by Indusface Web Application Scanner
Premium Scans	Manual Penetration testing done by security experts
Advance Rules	Default Rules with zero false positive guarantee
Premium Rules	Experiential Rules that are put on block mode after false positive monitoring by experts
Custom Rules	Rules can be created by experts based on application need on request

OWASP Top 10 Vulnerabilities (2017)	Tests Recommended by OWASP	Detection Coverage		Protection Coverage		
		Premium Scans	Automated Scans	Premium Rules	Advance Rules	Custom Rules
A1 Injection						
	Test for SQL Injection	Yes	Yes	Yes	Yes	Yes
	Test for LDAP Injection	Yes	Yes			Yes
	Test for ORM Injection	Yes		Yes	Yes	Yes
	Test for XML Injection	Yes				Yes
	Test for SSI Injection	Yes		Yes	Yes	Yes
	Test for XPath Injection	Yes	Yes	Yes	Yes	Yes
	Test for IMAP/SMTP Injection	Yes				Partial*
	Test for Code Injection	Yes	Yes	Yes	Yes	Yes
	Test for Command Injection	Yes	Yes	Yes	Yes	Yes
	Test for Buffer Overflow	On Request				Yes
A2 Weak Authentication and Session Management						
	Test Role Definitions	Yes		Proper role definition must be done on application. Out of scope of WAF		
	Test User Registration Process	Yes		Registration process can only be improved in Application. WAF can be used to block on identity. Preventing malicious users registering multiple times		
	Test Account Provisioning Process	Yes		Process improvements needed. Out of scope of WAF		

	Test for Account Enumeration and Guessable User Account	Yes			Partial*
	Test for Weak or unenforced username policy	Yes			Yes
	Test for Credentials Transported over an Encrypted Channel	Yes	Yes	Encryption should be enforced at application. Out of scope of WAF	
	Test for default credentials	Yes		Strong password enforcement should happen at code level. Out of scope of WAF	
	Test for Weak lock out mechanism	Yes			Yes
	Test for Bypassing Authentication Schema	Yes		Strong authentication enforcement should happen at code level. Out of scope of WAF	
	Test for Vulnerable Remember Password	Yes			
	Test for Browser cache weakness	Yes			
	Test for Weak password policy	Yes			
	Test for Weak security question/answer	Yes			
	Test for weak password change or reset functionalities	Yes			
	Test for Weaker authentication in alternative channel	Yes			
	Test for Bypassing Authorization Schema	Yes			
	Test for Privilege escalation	Yes			Partial*
	Test for Session Management Schema	Yes			Partial*
	Test for cookies attributes	Yes	Yes		Yes
	Test for Session Fixation	Yes			Partial*
	Test for Exposed Session Variables	Yes	Yes		Partial*
	Test for logout functionality	Yes		Can be fixed only at the code level. Out of scope of WAF	
	Test Session Timeout	Yes			
	Test for Session puzzling	Yes			

A3 Cross Site Scripting						
	Test for Reflected Cross site scripting	Yes	Yes	Yes	Yes	Yes
	Test for Stored Cross site scripting	Yes	Yes	Yes	Yes	Yes
	Test for DOM-based Cross site scripting	Yes	Yes	Yes	Yes	Yes
	Test for JavaScript Execution	Yes		Yes	Yes	Yes
	Test for HTML Injection	Yes	Yes	Yes	Yes	Yes
	Test for Cross site flashing	Yes		Yes	Yes	Yes
	XSS Filter Evasion Cheat Sheet	Yes	Yes	Yes	Yes	Yes
A4 Broken Access Control						
	Test Directory traversal/file include	Yes	Yes	Yes	Yes	Yes
	Test for Insecure Direct Object References	Yes	Yes			Partial*
	Test for Local File Inclusion	Yes	Yes	Yes	Yes	Yes
	Test for Remote File Inclusion	Yes		Yes	Yes	Yes
	Test for Bypassing Authorization Schema	Yes		Authorization process can only be improved in Application. WAF can be used to block on identity, preventing malicious users gaining access to unauthorized resources		
	Test for Bypassing Authentication Schema	Yes				
A5 Security Misconfiguration						
	Fingerprint Web Server	Yes	Yes			Yes
	Fingerprint Web Application Framework	Yes	Yes			Yes
	Fingerprint Web Application	Yes	Yes			Yes
	Test Network/Infrastructure Configuration	No		Can be fixed only at Infra level. Out of Scope of WAF		
	Test Application Platform Configuration	No		Can be fixed only at Infra level. Out of Scope of WAF		

	Test File Extensions Handling for Sensitive Information	Yes				Partial*
	Review Old, Backup and Unreferenced Files for Sensitive Information	Yes				Partial*
	Enumerate Infrastructure and Application Admin Interfaces	Yes	Yes			Partial*
	Test HTTP Methods	Yes	Yes	Yes	Yes	Yes
	Test RIA cross domain policy	Yes	Yes	NA		Partial*
	Test for Error Code	Yes	Yes			Yes
	Test for Stack Traces	Yes	Yes			Yes
A6 Sensitive Data Exposure						
	Test for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection	Yes	Yes	Stronger Encryption can be enforced only in Application level. Out of scope of WAF. WAF can be used to block users based on identity, so that malicious users do not take advantage of vulnerability		
	Test for Padding Oracle	Yes	Yes			
	Test for Sensitive information sent via unencrypted channels	Yes	Yes			
	Test HTTP Strict Transport Security	Yes				
	Test for Credentials Transported over an Encrypted Channel	Yes	Yes			
A7 Insufficient Attack protection						
	Validation is done via attack vectors to verify if application server has deployed any WAF/IPS/IDS or not.	Yes	NA	With WAF this vulnerability cannot exist. So Protected		
A8 Cross - Site Request Forgery						
	Test for CSRF	Yes				Yes
A9 - Using components with Unknown Vulnerabilities						
	Enumerate Applications on Webserver	Yes				Partial*
A10 - Under protected APIs						
	Enumerate Applications on Webserver	Yes				Partial*
	REST Security Cheat Sheet	Yes				Partial*

* Vulnerabilities are application specific and capability of virtual patching through custom rules is limited. Custom rules will be created by experts on request if vulnerability is detected. This will reduce the risk exposure but will not eliminate it.