Web Application Firewall

Certification Testing Report

Positive Technologies
PT Application Firewall

ICSA Labs Web Application Firewall Certification Testing Criteria v.2.1

February 23, 2018

Prepared by ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

Table of Contents

Executive Summary 1
- Introduction 1
- Product Overview 1
- Scope of Assessment 1
- Summary of Findings 1
- Continuous Deployment and Spot Checks 1
- Certification Maintenance 1

WAF Product Components 2
- Software 2
- Documentation 2

Installation and Configuration 2

Documentation 2
- Expectation 2
- Results 2

Functional and Vulnerability Testing 2
- Expectation 2
- Results 3

Testing the Additional Functions 3
- Results 4

Logging 4
- Expectation 4
- Results 4

Administration 5
- Expectation 5
- Results 5

Persistence 6
- Expectation 6
- Results 6

Criteria Violations and Resolutions 6
- Introduction 6
- Results 6

Authority 7

Positive Technologies – PT Application Firewall
WAF Certification Testing Report

Executive Summary

Introduction

The goal of ICSA Labs certification testing is to significantly increase user and enterprise trust in information security products and solutions. For more than 25 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product security, compliance and performance.

Product Overview

Positive Technologies Application Firewall (PT AF) is a comprehensive WAF solution that represents a modern response to the constantly evolving web threat landscape. It combines advanced technologies, including machine learning, real-time user behavior analytics, anomaly detection, and exclusive event correlations as well as proven approaches, including integration with Positive Technologies' AST solution PT Application Inspector and other security systems, to deliver targeted, proactive, and continuous protection against both known and unknown attacks. This includes the OWASP Top 10, automated and client-side attacks, and zero-days. PT AF also provides a high level of automation and adaptability to ensure quick and easy deployment and configuration as well as efficient day-to-day management with minimum human effort.

Scope of Assessment

In ICSA Labs Web Application Firewall (WAF) security certification testing, ICSA Labs determines through a mix of hands on and automated testing whether or not the security vendor's product properly implements security policy enforcement for the protection of HTTP and HTTPS web-based applications. Products are commonly tested against the ICSA Labs Web Application Firewall Certification Criteria. This WAF testing criteria standard was developed in conjunction with ongoing efforts in the WAF industry to provide security managers, application developers and others deploying web based applications with confidence in the products organizations use to secure vital web application services from attack and exploitation over the Internet.

At the customer's request ICSA Labs added additional tests beyond the baseline set of WAF testing criteria requirements. These additional test cases exercised special functionality built into PT AF including: malware detection, virtual patching, application level forensics, application layer DDoS, built-in vulnerability scanners, Content Security Policies, Robot protection, and both XML and JSON parsing.

Summary of Findings

ICSA Labs confirms that the tested WAF product met all of the WAF criteria elements during security testing and therefore retained ICSA Labs WAF Security Certification.

Continuous Deployment and Spot Checks

The tested product will remain continuously deployed at ICSA Labs for the length of the testing contract. If and as relevant new attacks and vulnerabilities are discovered, the deployed WAF model will be periodically checked that it is providing the requisite protection. In the event that the WAF product is found susceptible to new attacks or vulnerabilities during a check, ICSA Labs will work with the security product vendor to resolve the problems in order for the WAF product to maintain its ICSA Labs WAF Security Certification.

Certification Maintenance

This WAF product, like all WAFs and families of related WAF models that are granted ICSA Labs WAF Certification, will remain certified on this and future released versions of the product for the length of the testing contract, barring any criteria-related shortcomings discovered during a periodic spot check.

WAF Product Components

Software

Testing was successfully completed with version 3.6.3.

Documentation

To satisfy documentation requirements, Positive Technologies provided ICSA Labs with the following resources in order to assist in the installation, configuration, and administration of the Candidate WAF Product:

- The Application Access Control System Positive Technologies Application Firewall Administrator Guide
- The Application Access Control System Positive Technologies Application Firewall Quick Start Guide
- Positive Technologies Application Firewall Version 3.6.3 Administrator Guide

Installation and Configuration

Web Application Firewall products can be configured different ways; therefore, ICSA Labs typically faces many configuration related decisions before product installation as well as afterward. During testing, ICSA Labs attempted to exploit the WAF product and its protection of services, therefore configuration decisions were made to prevent such exploitation.

ICSA Labs installed and configured the product following the vendor's supplied documentation. For the purposes of this testing, ICSA Labs assumes that the WAF product would be deployed in a firewalled DMZ. Any special configuration or deviations from the documentation that were necessary to execute a test or meet a requirement are documented in this section.

The security vendor's WAF was configured as a reverse-proxy with routing enabled between two separate subnets.

Documentation

Expectation

The WAF product documentation should be accurate and applicable to the version tested while providing appropriate guidance for installation, administration and other related information.

Results

ICSA Labs determined that the WAF product documentation was adequate and accurate.

The WAF product met all documentation requirements. No violations were found in this area throughout testing.

Functional and Vulnerability Testing

Expectation

Once configured to enforce a security policy the security vendor's WAF product should properly permit and protect the services allowed by that policy while maintaining the integrity and confidentiality of the data. In this case, "properly" means that the service functions correctly. Confidentiality includes the masking of the internal application structure as well as information displayed to the user of the protected website.

During security testing, ICSA Labs used commercial, in-house, and freely available testing tools to attack and probe the WAF product. ICSA Labs used these tools to attempt to defeat or circumvent the security policy being enforced by the WAF product. In some cases the tools were used to exploit the product itself. The attacks include Denial-of-Service, buffer overflow, cross site scripting (XSS), cross site request forgery (CSRF), improper input validation, session mismanagement, information leakage, and other web application threats.

During security testing, ICSA Labs used commercial, in-house, and freely available testing tools to attack and probe the WAF product. ICSA Labs used these tools to attempt to defeat or circumvent the security policy being enforced by the WAF product. In some cases the tools were used to exploit the product itself. The attacks include Denial-of-Service, buffer overflow, cross site scripting (XSS), cross site request forgery (CSRF), improper input validation, session mismanagement, information leakage, and other web application threats.

Since there is overlap between functional and security vulnerability testing, the results of both phases of testing are presented here.

Results

The tested WAF product was not susceptible to the attacks targeting the product nor were the intended services being targeted. The security vendor’s WAF product allowed the applications to function as expected while maintaining the integrity and confidentiality of the data.

The WAF product met all functional and security vulnerability requirements. No violations were found in this area throughout testing.

Testing the Additional Functions

As mentioned in the Scope of Assessment section earlier in this report, the PT AF product was subjected to additional functional and security testing. This additional testing involved the testing of:

Application-Level Forensics
This level of forensics provides the capability for security incidents to be identified in detail from the analysis of a web server log.

Content Security Policy
The CSP functionality provides an additional layer of detection and mitigation for attacks such as cross-site scripting (XSS), data injection on the client side, etc.

Robot Protection
The rule engine checks if parameters match attack signatures to detect and mitigate a web robot attack by allowing the administrator to specify a number of useful conditions such as the Policy the rule is mapped to, actions to take in the event of a signature match, as well as what User-Agents are blocked.

Application layer DDoS
The DDoS protector provides functionality for the detection and mitigation of distributed denial of service attacks based on a multi-stage analysis of certain traffic patterns or thresholds.

Malware Detection
Malware detection capabilities are activated by enabling the ICAP protector and configuring the ICAP services. When this functionality is enabled, it is commonly used to integrate with external antivirus systems further extending the product’s ability to detect and mitigate malware.

XML, JSON, AMF Inspection

The XML, JSON, and AMF data formats are able to be examined properly for malicious payloads by the PT Application Firewall. The XML, JSON, and HTTP Protectors facilitate the examination of these data formats to determine the presence of malicious payload without executing the payload.

Blackbox Vulnerability Scanner

This feature allows for the vulnerability scanning of a web application that has not had a security policy built for it within PT Application Firewall. The scan output would facilitate a detailed understanding of the web applications current security posture. This, in turn, would allow for the patching, configuration hardening, and appropriately configured security policy with the PT Application Firewall.

DOM XSS Protection

This specific type of Cross-Site Scripting (XSS) attack occurs when a malicious payload is executed by modifying the DOM “environment” in the victim’s web browser used by the original client side script so that the client side code runs in an “unexpected” manner. The XSS protector feature detects and mitigates this, as well as other types, of XSS attacks.

Virtual Patching

Virtual Patching allows for the creation of patches in the form of rules based on a code analysis of the web application. This analysis of the web application code is done by a separate component such as P-Code or PT AI Desktop. These tools create an XML report that is uploaded to the PT Application firewall. The processing of this report results in the creation of the rule set that is applied to the policy.

Results

No shortcomings were found while testing of the additional product features; they were found to work as advertised.

Logging

Expectation

The WAF product is required to provide an extensive logging capability. In practice, this degree of logging may not be enabled at all times or by default; however, the capability must exist on tested WAF products in the event that detailed logging is needed by an organization.

ICSA Labs tested the logging functionality provided by the WAF product ensuring that it has the ability to capture and present the required system and network event information to audit security related events. ICSA Labs either configured the local logging mechanism or a remote logging mechanism such as syslog. For all logged events ICSA Labs verified that all required log data was recorded.

Results

The WAF Product has the ability to store logs on either the product itself or to send any logged data to a remote device.

The following is a log example of a failed XXE attack attempt. This example was taken from the attack panel on the bottom of the dashboard:

```
Field  Value
Actions
Log to DB (log), Block request (custom_response)
Policy
Musicstore-Sentry146
```

```
Events
Event tags: XML External Entities (attack)
Event: The XML document contains a reference to external entities
Severity: HIGH
Date
2018-02-12 14:20:09
Client
Username: Guest, Session:
1512aa333719d2c6cda08c9c7e477b293293c7833f8faa4e1896d57c88c03603df2e1b83020354d
504f5363e055beaca
Client: 205.160.140.156:2452
Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/28.0.1500.63 Safari/537.36
Client geolocation
Country United States, Region Wisconsin, City Milwaukee
Request
Client connects to 205.160.140.6:80 via HTTP
Method: POST
URI: //xmlrpc
Host: musicstore.ptsecurity.prop
Ticket ID
2018-02-12-19-20-09-38B9BDB41F01803F
Match
Protector: xml
Validator: xml.has_external_entities_reference, variable: REQUEST_RAW_BODY,
value: <?xml version="1.0"?>
 <!DOCTYPE foo [
 <!ELEMENT methodName ANY >
 <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
 <methodCall>
 <methodName>&xxe;</methodName>
 </methodCall>
 <...>
```

The WAF Product met all logging requirements. No violations were found in this area throughout testing.

Administration

Expectation

Web application firewall products often have more than a single method by which administration is possible. Whether the product can be administered remotely using vendor provided administration software, from a web browser based interface, via some non-networked connection such as a serial port, or some other means, authentication must be possible before access to administrative functions is granted. ICSA Labs tested not only that authentication mechanisms existed but also that they could not be bypassed. In addition ICSA Labs tested to determine whether remote administration traffic was encrypted and provided session controls.

Results

The WAF Product was remotely administered from the private network using the available web-based GUI via HTTPS. Attempts to bypass the authentication mechanism for all means of administration were unsuccessful. The remote administration session controls functioned as expected.

The security vendor’s WAF Product met all administration requirements. No violations were found in this area throughout testing.

Persistence

Expectation

Power outages, electrical storms, and inadvertent power losses should not cause the WAF product to lose valuable information such as the remote administration configuration, security policy being enforced, log data, time and date, and authentication data. This section documents the findings of ICSA Labs testing of the WAF product against the persistence requirements.

Results

When power was restored following a forced power outage, the WAF product continued to maintain its configuration, settings, and data while enforcing the appropriate, configured security policy.

The WAF product therefore met all persistence requirements. No violations were found in this area throughout testing.

Criteria Violations and Resolutions

Introduction

In the event that ICSA Labs uncovers criteria-related shortcomings while testing the WAF product, it is incumbent upon the security vendor to make repairs before testing can be completed and certification granted or retained. The section that follows documents any and all criteria violations found by ICSA Labs during testing.

Results

The WAF product met all of the ICSA Labs Web Application Firewall Certification Criteria requirements. No violations requiring correction were found during this test cycle.

Authority

This report is issued by the authority of the General Manager, ICSA Labs. Tests are done under normal operating conditions.

Sebastien Mazas, General Manager, ICSA Labs

ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For more than 20 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

www.icsalabs.com

Positive Technologies

Positive Technologies is a leading digital security firm with over 14 years of experience in 360º protection of critical IT systems against the most advanced cyberthreats. State-of-the-art solutions are developed at Positive Research, the company's flagship research center and one of the largest in Europe. Findings by Positive Research are used for updating the MaxPatrol knowledge base and for development of security solutions including PT Application Firewall, PT Application Inspector, and MaxPatrol SIEM. These products allow securing web applications, evaluating network protection, blocking attacks in real time, ensuring compliance with industry and national standards, and training security specialists.

www.ptsecurity.com