Web Application Firewall

Certification Testing Report

Fortinet, Inc.
FortiWeb 1000E

ICSA Labs Web Application Firewall Certification Testing Criteria v.2.1

July 3, 2019

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

Table of Contents

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 30 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

The FortiWeb 1000E Web Application Firewall provides specialized, layered application threat protection for medium and large enterprises, application service providers, and SaaS providers. FortiWeb 1000E web application firewall protects your web-based applications and internet-facing data from attack and data loss. Using advanced techniques to provide bidirectional protection against malicious sources, application layer DoS attacks and sophisticated threats like SQL injection and Cross-site scripting.

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.

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

Hardware

During the recently completed ICSA Labs WAF test cycle, Fortinet provided and ICSA Labs tested the following model:

- FortiWeb 1000E

Software

Testing began and successfully completed with version 6.0.2 Build0056 (GA), 181113.

Documentation

To satisfy documentation requirements, Fortinet provided ICSA Labs with the following resources in order to assist in the installation, configuration, and administration of their WAF product:

- FortiOS Handbook- CLI Reference version 6.0.2
- FortiWeb Administration Guide version 6.0.0

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 Candidate WAF Product was configured in reverse web proxy mode for inbound connections. The Candidate WAF Product supports DNS forwarding for internal clients, but DNS forwarding was not enabled.

Additional configurations were performed to prepare for testing:

- For configuring the masking of sensitive log data: `WebGUI>Log & Report>Log Config>Sensitive Data Logging>"Create new">"Field Mask">"Field Name=password">"Field Value=.*">Click "OK"`
- For configuring the CSRF protection: `WebGUI>Web Protection>Advanced Protection>CSRF Protection>"Create New">Enter policy name>Select action "Alert & Deny">"Severity" high>Click OK. In the "Page List Table" click "Create New">Select "Simple String"> value of "Full URL"should be set to "/shop.php">Click OK. In the URL List table click "Create New">Select "Simple String"> click "Create New">Select "Simple String"> value should be set to "/buy.php". Click "OK"`

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 in terms of installation and administration 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 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.

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. In testing the WAF product was configured to store log data locally on the FortiWeb 1000E.

The following log example taken from the WebGUI interface is a client attempting and then being denied access a protected resource in the web application:

```
Nov 13 14:35:01 205.160.133.254 date=2018-11-13 time=14:30:45 log_id=20000008
msg_id=000000104048 device_id=FV-1KE4417900227 vd="root" timezone="(GMT-5:00)Eastern
Time(US & Canada)" type=attack pri=alert main_type="Signature Detection"
sub_type="Known Exploits" trigger_policy="" severity_level=High proto=tcp
service=http action=Alert_Deny policy="Musicstore" src=205.160.130.198 src_port=1541
dst=205.160.133.66 dst_port=80 http_method=get http_url="/siteinfo.php?=PHPE9568F35-
D428-11d2-A769-00AA001ACF42" http_host="musicstore.fortiweb1000e.prop:88"
http_agent="Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.19)
Gecko/2010031422 Firefox/3.0.19 ( .NET CLR 3.5.30729)"
http_session_id=3BDF3137TLKFD0TT2J2YVEH1FFXP5687 msg="URI triggered signature ID
090300047 of Signatures policy High Level Security" signature_subclass="Sensitive
Information Disclosure Dictionary 1" signature_id="090300047" signature_cve_id="N/A"
srccountry="United States" content_switch_name="none" server_pool_name="ICSA-
musicstore-pool" false_positive_mitigation=
```

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 and locally via a console connection. 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

Throughout testing, 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 30 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

Fortinet, Inc.

Fortinet's mission is to deliver the most innovative, highest performing network security platform to secure and simplify your IT infrastructure. We are a leading global provider of network security appliances for carriers, data centers, enterprises and distributed offices. Because of our custom ASICs, hardware systems, network software, management capabilities and security research, we have a large, rapidly growing customer base, including the majority of the Fortune Global 100. Our market position and solution effectiveness has been widely validated by industry analysts, independent testing labs, business organizations, and the media worldwide. Our broad product line of complementary solutions goes beyond Network Security to help secure the extended enterprise.

www.fortinet.com