ICSA Labs
Web Application Firewall Certification Testing Report
Web Application Firewall - Version 2.1 (Corrected)

Radware Inc.

AppWall

V5.6.4.1

May 30, 2013

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

WAFX–RADWAREINC-2013-0530-01

Executive Summary

Introduction

Not every product can achieve ICSA Labs Web Application Firewall Certification. Only those products that meet the criteria after undergoing rigorous testing by network security experts at ICSA Labs earn this distinction.

The criteria against which vendor-submitted products are tested is an industry-accepted standard to which a consortium of web application firewall vendors, end users, and the ICSA Labs staff contributed. This standard has evolved over the years into its present iteration – version 2.1 (Corrected) of *The Web Application Firewall Certification Criteria.*

The setting for testing is the Network Security Lab at ICSA Labs. During and following initial testing, products remain continuously deployed within this lab environment, which closely approximates the real Internet to ensure more realistic web application firewall testing. Products are available for and regularly subjected to supplemental testing as new attack techniques emerge and vulnerabilities become known.

Successful web application firewall product testing culminates in the writing of a report that documents the results of each phase of testing. It also documents the product components submitted by the vendor, the configuration of the product as tested, and any patches or updates generated during testing.

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.

ICSA Labs manages and facilitates technology consortia that focus on emerging, well-defined technologies. The consortia provide for information exchanges among industry leading developers, and for the development of product testing and certification programs and standards. For more information about ICSA Labs, please visit www.icsalabs.com.

Product Overview

Radware's AppWall® is a Web Application Firewall (WAF) appliance that secures Web applications and enables PCI compliance by mitigating web application security threats and vulnerabilities. It prevents data theft and manipulation of sensitive corporate and customer information.

Scope of Assessment

The goal of ICSA Labs' Web Application Firewall testing and certification program is to evaluate and certify products that implement security policy enforcement for the protection of HTTP and HTTPS Web-based applications. In conjunction with ongoing efforts in the industry to classify and categorize application security issues and mitigate potential vulnerabilities, the Web Application Firewall certification criteria was developed to provide security managers, application developers and others deploying web based applications with confidence in the products that secure vital application services from exploitation or attack.

Summary of Findings

The Candidate Web Application Firewall Product met all the criteria elements in Version 2.1 (Corrected) of *The Web Application Firewall Certification Criteria* and therefore has attained ICSA Labs Web Application Firewall Certification. As mentioned above, the Candidate Web Application Firewall Product will remain continuously deployed at ICSA Labs for the length of the testing contract. In the event that the

Candidate Web Application Firewall Product is found to no longer meet the criteria during a check, the Network Security Lab team will work with the vendor to resolve the problems in order for the Candidate Web Application Firewall Product to maintain its ICSA Labs Web Application Firewall Certification.

A detailed overview of any issues found, and their resolutions, is located in the WAF Testing as well as the Criteria Violations and Resolutions section of this report

Certification Maintenance

The AppWall, like all products and product groups that are granted ICSA Labs Web Application Firewall Certification, will remain certified on this and future released versions of the product for the length of the testing contract. Future versions continue to be certified since the product is continuously deployed in the Network Security Lab and subjected to periodic spot-checks on the most current product version.

Two circumstances will cause the AppWall to have its ICSA Labs Web Application Firewall Certification revoked:

1. Radware withdraws from the ICSA Labs Web Application Firewall Certification Program.
2. The product fails a periodic spot-check or full test cycle and Radware subsequently fails to provide an adequate fix within a prescribed length of time.

Candidate Web Application Firewall Product Components

Introduction

To comply with the requirements stated in version 2.1 (Corrected) of *The Web Application Firewall Certification Criteria*, vendors must submit all necessary product hardware, software, and documentation. Collectively, the set of components delivered to ICSA Labs for testing comprises the product under test, called the "Candidate Web Application Firewall Product". This section of the report describes each component of the Candidate Web Application Firewall Product submitted for testing in the Network Security Lab at ICSA Labs.

Hardware

Radware submitted an AppWall for testing. The Appwall was a 1U rackmount appliance with six 10/100/1000 Copper Ethernet ports, two GE SFP Fiber ports, one management console port and one USB port.

Software

The AppWall was delivered with version 5.6.3.1_86 of the firmware installed during the course of testing, the software was upgraded to 5.6.4.1.

The AppWall required a license key, which was obtained from Radware.

Documentation

To satisfy documentation requirements, Radware provided the Network Security Lab team with the following electronic documents in order to assist in the installation, configuration and administration of the AppWall:

- *AppWall Management Application User Guide*
- *AppWall Release Notes*, Version 5.6.4, April 24, 2013
- http://kb.radware.com/questions/3175
- http://kb.radware.com/questions/3193

Web Application Firewall Certification Criteria

The Candidate Web Application Firewall Product was tested against version 2.1 (Corrected) of *The Web Application Firewall Certification Criteria:*

- *https://www.icsalabs.com/sites/default/files/WAF_Corrected_Criteria_V2.1.pdf*

Web Application Firewall Configuration

Introduction

ICSA Labs installs the product submitted for testing to simulate a realistic deployment of the Candidate Web Application Firewall Product in a typical end user environment. Since products submitted for testing can often be configured many different ways, analysts frequently confront many configuration-related decisions both before and after installing the Candidate Web Application Firewall Product. For the purposes of these tests, analysts attempted to install and configure the Candidate Web Application Firewall Product as a typical end user would and according to its intended use. Analysts use the provided documentation to assist with all configuration decisions. If multiple configurations were used for testing, they are detailed below with the findings.

Test Description

The Network Security Lab team deployed the AppWall on a testbed designed to represent a real-world deployment of a web application firewall. The AppWall was deployed in a simulated DMZ, and was be protected from a simulated Internet by an ICSA Labs Certified Network Firewall

Network Security Lab analysts ran a sophisticated suite of web attacks, penetration tests, and scans against a set of web sites protected by the AppWall to verify web application firewall functionality as defined in *The Web Application Firewall Certification Criteria*. ICSA Labs analysts also ran tests to verify proper operation of product administration and general functionality as dictated by the criteria above.

Product Configuration

Using the AppWall's Management Application, analysts did the following to configure the product:

- Created a new HTTP tunnel by right-clicking Tunnels -> HTTP -> Add.
- The tunnel was configured to have the listening the address be the public facing IP address which resolved to the protected webserver and the forwarding address was set to the IP address of the protected webserver itself. The hostname was added here as well.
- Under Security Policies, a new web application was created. The tunnel created in the previous step was added here.
- Under this web application, the [Any Host] settings for User Tracking and Authentication were enabled.
- Under Security Policies -> Hosts -> <Any Host>, CSRF was set to active, along with Directory Listing and URL Rewrite. Under the musicstore sub-directory, all actions were set to inherit.
- Under Auto Policy Generation, the auto Policy Generation was enabled to learn the protected website. After this completed, the application paths filter settings were all set to Manual and Active.
- Under Filters -> Parameters, some methods required fine tuning to enforce proper method usage.
- Filters were arranged such that logging was set highest in order to capture all requests before they were acted upon by the AppWall engine.

Documentation

Introduction

The Network Security Lab team evaluated the documentation provided with the Candidate Web Application Firewall Product to verify that the vendor supplies adequate documentation to assist an end user with the installation, configuration, maintenance, and administration of the Candidate Web Application Firewall Product. Throughout testing, the Network Security Lab team use the documentation provided and evaluate it for accuracy, completeness, and usefulness.

Findings

All documentation used during testing was found to meet the criteria.

Functional Testing

Introduction

Once configured to enforce a security policy the Candidate Web Application Firewall Product is tested to validate that through testing that its security policy cannot be circumvented. The Candidate Web Application Firewall Product, while enforcing its security policy, must allow permitted services to function (HTTP, HTTPS, SSL) as designed while maintaining the integrity and confidentiality of the data. This includes the masking of internal application structure as well as information displayed to the user of the protected website.

During Functional Security Testing the Network Security Lab team evaluates the Candidate Web Application Firewall Product to verify that it is also not susceptible to commonly known vulnerabilities or exploits. This includes attacks targeting buffer overflow, cross site scripting (XSS), cross site request forgery (CSRF), improper input validation session mismanagement and information leakage.

Findings

The Network Security Lab team confirmed that the AppWall properly permitted the services tested while correctly enforcing the security policy.

Vulnerability Testing

Introduction

During Vulnerability Testing he Network Security Lab team verifies that no unauthorized control of any of the Candidate Web Application Firewall Product administrative functions can be obtained. Also, the Candidate Web Application Firewall Product must demonstrate through testing that it is not vulnerable to any publicly know exploits or vulnerabilities as well as not introducing any vulnerabilities while enforcing its security policy. Finally, the Candidate Web Application Firewall Product must be able to mitigate as well as not be rendered inoperable by any trivial Denial of Service attack. The Network Security Lab team uses commercial, in-house, and freely available testing tools to attack and probe the Candidate Web Application Firewall Product.

During vulnerability testing it is assumed that the Candidate Web Application Firewall Product resides behind an ICSA Labs Certified Firewall (network firewall). Therefore, the scope of this requirement is limited to valid network traffic destined for the Candidate Web Application Firewall Product or the servers it is protecting, for example, services such as HTTP, HTTPS, and Remote Administration.

Findings

After Radware addressed the issues reported by the Network Security Lab team the AppWall was re-tested. The product properly permitted the minimum set of common services inbound and outbound per

the Corporate module of the criteria. Furthermore, during re-testing of the AppWall, it was not susceptible to attacks launched inbound and outbound to and through the product, including trivial Denial-Of-Service attacks.

Logging

Introduction

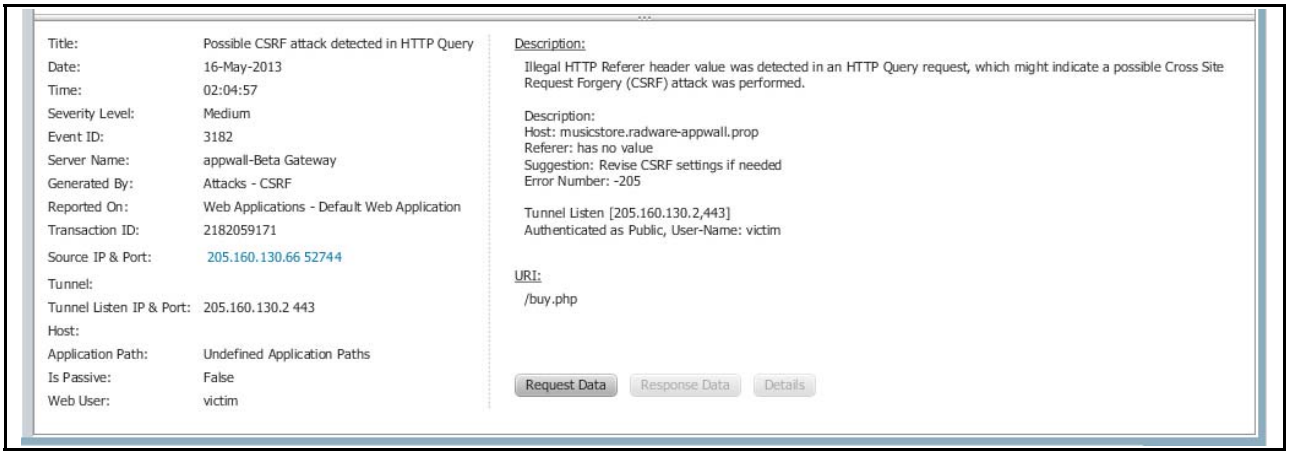
Version 2.1 (Corrected) of *The Web Application Firewall Certification Criteria* requires that the Candidate Web Application Firewall Product provide an extensive logging capability. In practice, this degree of logging may not be enabled at all times or by default. The Network Security Lab team evaluates each Candidate Web Application Firewall Product to verify that it has the ability to capture, and present the required system and network event information to enable an administrator to audit security related events. Additionally, it is not required that the Candidate Web Application Firewall Product be capable of storing the logs locally. However, if stored remotely additional testing is conducted. For all logged events the Network Security Lab team verifies that all necessary log data is recorded.

Findings

The following log examples were collected during testing. The first is an example of a configuration change (time modified), the second is an example of a non-malicious request collected from the AppWall's logging filter, and the third is an example of a blocked attack collected from the AppWall's Management Application Web GUI. During the course of testing, Radware submitted firmware upgrades to address issues found in testing. See the Criteria Violations and Resolutions section for more information.

May 8 00:26:00 appwall-Beta Date Modified from Wed May 8 00:25:59 GMT 2013 to Wed May 8 00:26:00 GMT 2013 (date-set)

##205.160.130.66 40614##5-7-2013 23:15:5##
GET /shop.php?sort=genre&&genre=Punk HTTP/1.1
Host: musicstore.radware-appwall.prop
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9) Gecko/2008070309 CentOS/3.0-2.el5.centos Firefox/3.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://musicstore.radware-appwall.prop/shop.php?sort=genre
Cookie: store_cookie=DD129729254;
Session_ID=0,Public,258,258,victim,1367968497,205.160.130.66,75d20cd5ac3220757daec57d98da3efd,3b5737eb4b657363682076686dea30a1,;
K_V_D_store_cookie=kjbmdfkfnapbfgdlagpkphiapjejnkmlojoegpbiiamcpjmpoffdafhdhnkijhbnmcfdffpgaicc
Accept-Encoding: identity



Administration

Introduction

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 via some other means, authentication must be possible before access to administrative functions is gained. The Network Security Lab team tests not only that authentication mechanisms exist but also that they cannot be bypassed for all required administrative interfaces.

Findings

The AppWall was administered through a Web GUI, although an SSH interface exists as well. Within the Web GUI interface, the Management Application can be run to administer the product's security engine. Initially, this was done through a separate application, but during the course of testing, this was integrated into the Web GUI. Initially, the AppWall did not meet all Administrative requirements. See the Criteria Violations and Resolutions section for more information.

Persistence

Introduction

Power outages, electrical storms, and inadvertent power losses should not cause the Candidate Web Application Firewall Product to lose valuable information such as the security policy being enforced, log data, authentication data, and system clock information. Further, the security policy being enforced following the restoration of power should be the same as the security policy being enforced prior to the loss of power. This section documents the findings of the Network Security Lab team while testing the Candidate Web Application Firewall Product against the persistence requirements.

Findings

During testing, no issues were found related to persistence.

Criteria Violations and Resolutions

Section Introduction

In the event that the Network Security Lab team uncover criteria violations while testing the Candidate Web Application Firewall Product, the vendor must make repairs before testing can be completed and

certification granted. The section that follows documents any and all criteria violations discovered during testing. Additionally any steps that must be taken by an administrator to ensure that the product meets the criteria are documented below.

Results

- Logged events did not contain all elements specified in the criteria. This was corrected by updating the firmware to 5.6.4.1.

- Sensitive data fields were not masked in all areas. This was corrected by updating the firmware to 5.6.4.1.

- Not all administrative interfaces correctly enforced authentication. This was corrected by updating the firmware to 5.6.4.1.

Testing Information

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

Lab Report Date

May 30, 2013

Please visit *www.icsalabs.com* for the most current information about this and other products

Test Location

ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050

Product Developer's Headquarters

Radware Inc.
575 Corporate Drive
Mahwah, NJ 07430
USA

The certification test methods used to produce this report are accredited and meet the requirements of ISO/IEC 17025 as verified by the ANSI-ASQ National Accreditation Board/ACLASS. Refer to certificate and scope of accreditation number AT – 1423.