SecureIQLab™

Bridging the enterprise cloud security gap

# Cloud Web Application Firewall (WAF) CyberRisk Validation Methodology

**Version:** 2.0

**Last Revision:** 9 June 2022

**Language:** English

www.secureiqlab.com

AMTSO Standard Compliance Statement

This Test has been designed to comply with the Anti-Malware Testing Standards Organization, Inc. ("AMTSO") Testing Protocol Standard for the Testing of Anti-Malware Solutions, Version [1.3] (the "Standard"). This Test Plan has been prepared using the AMTSO Test Plan Template and Usage Directions, Version [2.4]. SecureIQLab is solely responsible for the content of this Test Plan.

# Contents:

# 1 INTRODUCTION

## 1.1 THE NEED FOR WEB APPLICATION FIREWALLS (WAFS)

Attackers have moved up the stack. They are no longer simply attacking the web server and its underlying operating systems; they are attacking the web applications running on the web server that are front-ending critical corporate data. Such applications are often incredibly complex and difficult to secure effectively, and simple coding errors can render them open to remote exploits.

To counter such attacks, enterprises must in turn evolve their network defenses to provide a different kind of protection. Web application firewalls (WAF) exist to prevent web servers and their applications from being exploited.

The Web Application Firewall remains the most frequently used security control to protect web applications (84%). The global web application firewall market size was valued at $3.9 billion in 2020, and is projected to reach $25.6 billion by 2030, growing at a Compound Annual Growth Rate (CAGR) of 20.88% from 2021 to 2030. (Allied Market Research 2022).

**Cloud-based WAF on the rise:**

- Certain government and industry regulations, such as PCI DSS, require WAF deployment for compliance.
- 95.1% of the enterprise based WAF controls are deployed in the cloud today.
- Enterprises report 49% of their workloads are in public cloud with plans to expand workloads in cloud by 6% in the next twelve months. (Flexera 2022)
- 69.2% of the enterprises manage their own cloud based WAF controls and 25% are managed by their Cloud providers. Only 6.2% of the WAF based cloud deployments are managed by a 3rd party/Managed Security Service Provider (MSSP).
- Main challenges to WAFs are cost and performance. (Mordor Intelligence 2021)
- With the DC traffic primarily constituting HTTPS (75.9%) and HTTP (64.5%) based traffic, WAFs are expected to play a critical role in protecting applications.

## 1.2 CLOUD WAF BENEFITS:

Cloud WAF technology allows for the creation of customized security and benefits organizations in the following ways:

**Less complex to manage than on-premise WAF solutions**

**Ease of integration with existing security solutions**

**Scalable and elastic**

**Fast deployment and easy to set up**

**Protect web applications against external and internal attacks**

**Able to monitor and control access to web applications**

**Allows all transactions except those that contain threat/attack (Negative Security Model)**

**Able to collect access logs for compliance/auditing and analytics**

## 1.3 Proposed Cloud WAF Deployment Models:

Cloud WAF deployment models are:

- IaaS deployment as a software appliance or virtual machine
- Software as a Service (SaaS)
- Reverse Proxy
- Offered as pay-as-you-go service

## 1.4 Statement of Intent:

The purpose of this cloud web application firewall (WAF) security test is to provide empirically validated data based upon industry guidelines, such as OWASP, to assist in securing cloud applications. SecureIQLab believes that the test will lead to better, more secure cloud WAF products.

## 1.5 Testing Goals Include:

Testing goals include the following:

- Publicly publish results that improve transparency and accountability with the security community
- Highlight key technology differentiators
- Inspire innovation
- Refine forward looking technology

## 1.6 Cloud WAF Features to be Evaluated

### 1.6.1 Performance, Availability and Reliability:

The WAF performance, availability, and reliability features that to be validated are the following:

- Automatic content compression
- Load balancing web requests
- WAF is delivered through application load balancer as well as through Content Deliver Network (CDN) like Amazon Cloud Front
- PCI DSS Compliance
- Compliance management module

### 1.6.2 Security Features

The following are the list of cloud web application firewall security features that to be validated:

- Protection against attacks that can be mapped to OWASP 2021 Top 10.
- Protection against multi-layered application-based attacks.
- Geolocation attack protection from Layer 7 DDOS, SQL injection, Cross-site scripting and Zero-day web application attacks.
- Protection against encrypted attacks.

- Protection against account takeover attacks.
- Advanced attacks
    - Testing for performance versus advanced attacks will include testing for protection against Bots that usually do not get detected by traditional security controls. These attacks use open-source tool kits, simulate users, and have the ability to remain undetected using techniques such as DNS tunneling. Available in the wild, these bots have been used in account take over, content scraping, fraudulent transactions, and payments.
- Protection against tool-based attacks.
- Protection against product attack surface.

## 1.7 Cloud WAF Vendor Participation Selection Criteria

We select vendors based on three following criteria:

1. Market Leaders – Either in terms of revenue generated, customer numbers globally, or strong channel play
2. Analyst and Enterprise challengers – Small-mid-large enterprise security professional surveys, direct 1:1 inquiries and engagement with enterprises, organizations, MSP's, MSSP's and Gartner MQ, buyers guide, Forrester Wave, and IDC reports
3. New market entrants and interested participating vendors with breakthrough technology offerings

There are no known conflicts of interest that exist.

## 1.8 Scope:

The scope of this iteration of the test will be limited to cloud WAF that are available in the cloud marketplace, SaaS offerings, or standalone cloud offerings. Any physical WAF is out of the scope of this methodology.

**Considered vendors at the time of this publication:**

| Vendor | Product Name | Process Used |
|---|---|---|
| Cisco | ACE XML Gateway | Test to be evaluated utilizing Blackbox Security and Greybox Security Tasks |
| Alert Logic | Alert Logic | |
| Radware | AppWall | |
| Microsoft | Azure WAF | |
| Barracuda Networks | Barracuda | |
| F5 Networks | BIG-IP Local Traffic Manager | |
| Google | Cloud Armor | |
| AWS | AWS WAF | |
| Cloudflare Inc. | Cloudflare | |
| Distil Networks | Distil | |
| Fastly | Fastly | |
| Fortinet | FortiWeb | |
| Imperva | Incapsula | |
| Indusface | AppTrana WAF | |
| Akamai | Kona SiteDefender | |

| | |
|---|---|
| Oracle | Oracle Cloud |
| Citrix Systems | NetScaler AppFirewall |
| NSFocus Global Inc. | NSFocus |
| Palo Alto Networks | Palo Alto Next Gen Firewall |
| Sophos | UTM Web Protection |
| StackPath | StackPath |
| Sucuri | Sucuri WAF |
| SonicWall | SonicWall WAF |
| Prophaze | Cloud WAF |
| Wallarm | Wallarm Cloud WAF |

## 1.9 FUNDING AGREEMENT:

This is a non-commissioned test funded by SecureIQLab.

## 1.10 OPT-OUT POLICY

**Opt-Out: Opt-out will only be considered for the following reasons:**

1. The product, solution (or) technology is found to be outside of scope in the context of the methodology as determined by SecureIQLab.
2. Any technology, product or a solution that is NOT generally available nor ready for deployment.
3. Publishing the test would not serve the public interests as deemed by SecureIQLab.

Opt-out requests must be provided in writing. Emailed opt-ops must be sent to info@secureiqlab.com. Mailed opt-outs must be sent to:

SecureIQLab
6001 W. Parmer Lane
Ste 370 #970
Austin, TX 78727

Mailed opt-outs are effective by the date received, not the date posted. We do not accept opt-outs through phone, voice, social media or similar.

***The opt-out must contain the name, title, email and phone number of the individual authorized to request an opt-out on behalf of the vendor. To be considered a completed opt-out, the request must state under which of the reasons above the request should be considered and provide details to support the request***. All vendors have a limited right to opt-out for the designated reasons listed above. The opt out period begins at the *Test Commencement* and continues through the end of the *Dispute Phase [Section 2.2]*. Vendors will be contacted by SecureIQLab within 3 business days of receiving the opt-out request to discuss feasibility. If a vendor successfully opts out before the end of the *Configuration Phase*, the vendor will be listed as 'Participant, not tested '. If a vendor successfully opts out after testing has been performed for their product, their product will be marked in the results 'Participant tested, not published '.

# 2 General Evaluation Approach

The aim of this section is to verify that the cloud web application firewall (WAF) referred here as the product under test (PUT) is capable of detecting, preventing, and logging attack attempts accurately, while remaining resistant to false positives.

The PUT will be configured either by walking through the applications, e-commerce, and other sites as relevant (automatically, or manually) or by creating rulesets and a security policy manually. The appropriate deployment model will be chosen per vendor recommendations where available, and the WAF will be deployed to protect against attacks that target the potential assets beings protected.

## 2.1 Cloud WAF Security Effectiveness Validation

SecureIQLab will evaluate the security effectiveness of the cloud WAF using the following approaches:

Blackbox Security Testing
Greybox Security Testing

Each of the categories above will consist of the following validation tasks:

### 2.1.1 Information Gathering and PUT Reconnaissance

Information gathering and reconnaissance will be performed against the application to gather as much information as possible to be utilized when penetrating the target during the vulnerability assessment and exploitation phases. SecureIQLab will perform vulnerability analysis using automated tools such as Burpsuite and Nessus and perform manual analysis. The main objective of vulnerability analysis is to discover flaws in systems and applications that can be leveraged by an attacker. These flaws can range anywhere from host and service misconfigurations to insecure application design. Vulnerability analysis will be based on:

- ActiveScan: Active scan involves direct interaction with the component being tested for security vulnerabilities.
- PassiveScan: Passive scan involves meta-data analysis and traffic monitoring.

### 2.1.2 Exploitation

Once information gathering and reconnaissance is over, we will begin exploitation as the next phase in this process. Exploitation involves leveraging the vulnerability information gathering through reconnaissance to gain a foothold within the targeted environment.

### 2.1.3 Post Exploitation

The term “post-exploitation” refers to the actions taken after the initial compromise of a system or device. It often describes the methodical approach of using privilege escalation or pivoting techniques. This allows the tester to gain additional access to systems or network resources by attacking from a new vantage point within the system. We will demonstrate the risk presented by exploitable systems and what post-exploitation may likely occur with web applications.

### 2.1.4 DEFENSE EVASION TESTING

Defense evasion is an important tool in an attacker's arsenal. This allows old methods and techniques to be repurposed to evade protection against attacks that might otherwise get blocked by the cloud WAF. SecureIQLab will focus defense evasion testing in the following areas.

1. **Pre-processor Attacks: These attacks involve the decision on whether a request will be processed further. We will perform the pre-processor attack by identifying possible application inputs and end points.**
2. **Normalization: We will perform the normalization task by tweaking the different end points, for example, a compress whitespace attack where we convert of whitespace characters to spaces.**
3. **Validate Input with Payload: Check user input against policies. We will perform fuzzing and prepare payloads in an attempt to bypass the security rules set by the cloud WAF.**

## 2.2 CLOUD WAF TEST LIFE CYCLE

The Cloud WAF test plan is within scope if the project remains within four weeks of the below timeline. This methodology is open to feedback and updates until it is finalized on 23 June 2022.

SecureIQLab will execute the test in six phases:

1. **Phase1: Reconnaissance**

   We will start the initial validation with basic and advance level reconnaissance.

2. **Phase 2: Attacking the pre-processor**

   As a part of the input validation, we will perform pre-processor attack by trying to skip input validation.

3. **Phase 3: Attempting an impedance mismatch.**

   We will attempt to make the WAF interpret a request differently than the backend in an effort to not be detected.

4. **Phase 4: Bypassing the rule set.**

   We will prepare a payload that will not be blocked and can bypass the WAF's rule set.

5. **Phase 5: Identifying the vulnerabilities.**

   We will perform the security testing based on the guidelines around the OWASP Security Testing guidelines along with customized testing.

6. **Phase 6: Post Assessment Phase**

   We will review, assess, and document the discovered vulnerabilities and the issues, and will tabulate the scorecard and prepare the final report.

SecureIQLab will execute the project in six phases that are listed in table format below:

| *Schedule Summary for Test Project* | | | |
|---|---|---|---|
| **Index** | **Test Activity** | **Date Range** | **Dependencies** |
| ***1*** | *Test Commencement* | *24 Jun 2022* | *Vendor voluntary participation (or) procurement of vendor Software* |
| ***2*** | *Confirm Vendor Configuration Feedback* | *1 July 2022 – 19 August 2022* | *All required vendors installed and testing commences without any problems* |
| ***3*** | *Milestone 1 – Preliminary Results* | *22 July 2022 – 2 September 2022* | *Vendor confirmation and validation* |
| ***4*** | *Milestone 2 – Test Scorecard First Edition – End of Testing Period* | *2 September 2022 – 16 September 2022* | *Based on preliminary result disputes and resolution* |
| ***5*** | *Feedback and Dispute Resolution Time – Retests as Needed* | *16 September 2022 – 29 September 2022* | *Based on report feedback and final dispute resolution.* |
| ***6*** | *Milestone 3 – Issue Final Report – End Date for Test* | *30 September 2022* | *Based on retesting or testing period extended* |

## 2.3 Risk and Risk Management:

No additional risks are known at this time.

## 2.4 Proposed Attack Types

Testing will demonstrate the effectiveness of the PUT to protect vulnerable assets from targeted threats and exploitation. This asset/target and threat-based approach forms the basis from which PUT security effectiveness is measured.

Attack types and test configuration: The SecureIQLab threat and attack suite contains attacks (including mutations of the same underlying attacks) and proprietary exploits either harvested through our test harness or crafted by our threat research team. Crafted exploits are intended to simulate attacks in the wild. Groups of exploits are carefully selected from the attack library to test based on the intended attack. Each exploit has been validated to impact the target vulnerable host(s) by compromising either the asset which can vary from a web server, web application or sites.

Cloud WAFs will defend a number of complex web applications that have also been constructed to include known vulnerabilities and coding errors.

SecureIQLab includes attacks that have a definite outcome i.e., an attacker establishing a reverse connection, file uploads or proof of concept (PoC) attacks are all part of the test set. This ensures that the WAF under test's ability is stressed for outcome-based tests.

The level of compromise can vary between instigating a Denial of Service (DoS) condition, providing administrator/root access to the host server, allowing malicious users to amend system parameters or application data before submission, browse and/or retrieve files stored on the host server, escalating user privileges and so on.

## 2.5 Attack Relevance:

SecureIQLab will use and craft attacks that are relevant to today's cloud applications hosted on cloud and cloud native applications. SecureIQLab carefully curates such attacks via research generated by our own Red-team as well as the attacks that are prevalent in the wild. Open-source tools kits will also be utilized while performing this assessment.

## 2.6 Geo-Limitations:

While performing web application attacks, SecureIQLab will make every effort to use only attacks that are not geo-location centric when necessary. SecureIQLab will ensure that attacks also originate from as wide a range of IP addresses as possible.

## 2.7 Distribution of Test Data:

Upon the completion of the six phases of this validation project, the resulting data will be organized into individual test reports and one comparative report. These results will then be publicly available to download at https://secureiqlab.com/publications/.

Vendors are offered an optional partnership. This optional partnership is based on testing results with potential publication to provide insight and alignment with their specific security offerings. This optional partnership is intended to be useful for vendor marketing. If there is a fee agreement in exchange for services rendered, vendors are given the option to progress forward with published results following AMTSO standards.

# 3 Control Procedures

Before any test is conducted, SecureIQLab ensures that the cloud WAF under test has been validated in the following areas:

Connection Validation:

- The WAF must be accessible by the administrator.
- The WAF must pass normal application traffic.

Logging:

- Verify that logs are being generated and recorded. Test subjects will not have access to test logs. Participating vendors are granted access to test logs through time of publication.

Updates:

- Protocol updates in the form of rules, signatures and reputations will be applied as it becomes generally available. SecureIQLab will make a best effort to apply these updates to the products prior to the evaluation.

## 4 DEPENDENCIES

Participant and test subject vendors suggested actions:

Participating vendors are invited to be actively involved in the testing process. This process includes:

Setup

- Default configuration
- Tuned configuration as an Add-on service. SecureIQLab expects Cloud WAF to provide protection out of the box without any tuning. Any tuning required for products that don't have feature to provide protection out of the box will be an add-on or extra service. Vendors are advised to do due diligence beforehand by contacting SecureIQLab prior to the setup to leverage this add-on.

Testing

- Score card feedback for the cloud WAF products.

## 5 SCORING AND DISPUTE PROCESS

For all web-attacks blocked by the cloud WAF under test, SecureIQLab will give the block credit to the cloud WAF under test. Multiple packet capture tools will ensure test result accuracy.

If any inconsistencies exist between our packet capture tools and the vendor's packet capture tool, SecureIQLab will default to the vendor packet capture as long as it provides sufficient evidence beyond reproach. No credit will be given for missed attacks and there is no negative scoring for attacks missed by the cloud WAF. The outcome of the attacks combined with the logging of the attacks will be used for scoring purposes.

Industry norms and best practices will be followed if there are any disputes on the nature of the attacks used during the testing window.

SecureIQLab will make best efforts to resolve disputes regarding scoring. Any changes to scoring resulting from successful disputes will be applied to all vendor results, and not just to the disputing vendor.

All cloud WAF vendors who participate in this test, and are not only test subjects, will receive their score. This will include a breakdown of security efficacy and operational efficiency scores. This data set will be shared individually with the cloud WAF vendors and SecureIQLab will work closely with cloud WAF vendors to go over the metrics as well as relevant metadata where warranted. Furthermore, SecureIQLab will not share web-attacks that are missed during the testing window to third parties unless required by law. SecureIQLab will provide vendors up to two weeks for the dispute resolution on the nature of attacks. Any security vulnerabilities that are uncovered during the testing windows related to the cloud WAF under test will be shared based upon responsible disclosure policy which provides vendors up to 20 days to fix the vulnerability. Vulnerability details will be disclosed to the broader public when a fix is available or is in the interest of the general public.

SecureIQLab will not entertain disputes or changes to scoring after the Comparative and Individual Test reports

have been published.

# 6 ATTESTATIONS

I understand and agree that I am submitting this Test Plan, and the following Attestations, on behalf of the entity listed below, and I represent and warrant that I have authority to bind such entity to these Attestations. All references to "I" or "me" or similar language refer to such entity. I represent and warrant that the following Attestations are true, to the best of my knowledge and belief, and each of the following commitments will be upheld to the best of my ability.

I will provide public notification on the AMTSO website covering my obligation for notification of a Public Test, regardless of whether a potential Participant is in actual receipt of such notification prior to the Commencement Date of a Test.

All products included in this Test will be analyzed fairly and equally.

I will disclose any anticipated or known imbalance or inequity in the Test design to all Participants in the Test.

Although I may charge for participation in a Test, I will not charge any additional fees for a vendor to be a test subject under the Standards.

I will disclose any material conflicts of interest or other information that could materially impact the reliability of the Test.

I will disclose how the Test was funded.

I hereby affirm, to the best of my knowledge and belief that this Test Plan complies with the AMTSO Testing Standards, as of the date hereof.

Signature: /s/ David Ellis
Name: David Ellis
Test Lab: SecureIQLab
AMTSO Test ID: AMTSO-LS1-TP054

# 7 APPENDIX:

## 7.1 DOCUMENT REVISIONS:

| Version | Section | Revision overview |
|---|---|---|
| V2.0 | 1.62 | Protection against product attack surface. |
| V2.0 | 1.8 | Removed AWS compatibility requirement. |
| V2.0 | 3 | Added SecureIQLab will share logs with participating vendors. |

| | | |
|---|---|---|
| V2.0 | 4 | Added Tuning as add-on for testing. |

## 7.2 EXAMPLE ATTACK TYPES:

- **URL Parameter Manipulation**
  - Altering URL data to gain potentially protected information or access protected areas of a website.
- **Form/Hidden Field Manipulation**
  - Constructing POST requests to access protected information or protected areas of a website, or to manipulate "fixed" data directly (such as pricing information).
- **Cookie/Session Poisoning**
  - Manipulation of cookie or session variables to access protected information/areas of a website.
- **Cross-Site Scripting (XSS)**
  - The process of manipulating user input in such a way that, when rendered in the context of a webpage, it will be interpreted by the browser as code.
- **Directory traversal**
  - The URL to access areas of the web server that should not otherwise be accessible
- **SQL Injection**
  - Manipulating user input in such a way that, when processed by the database server, it will be interpreted as code, potentially providing direct access to private data.
- **Padding Oracle attacks**
  - Altering a block-cypher cryptographic hash in such a way as to decrypt encrypted information.
- **Cross-Site Request Forgery (CSRF)**
  - The process of executing a request on behalf of a user without their knowledge, using a trusted session between a vulnerable website and the user's browser.
- **Unmodified Exploit Validation**
  - A number of common exploits are executed across the PUT to ensure that they are detected in their unmodified state. These will be chosen from a suite of older/common basic exploits for which SecureIQLab is certain that all vendors will have signatures/rules.
- **URL Obfuscation and Normalization**
  - Random URL encoding techniques are employed to transform simple URLs, which are often used in pattern- matching signatures, to apparently meaningless strings of escape sequences and expanded path characters using one or any combination of techniques such as:
    - Escape encoding using various character sets
    - Microsoft %u encoding
    - Path character transformations and expansions
    - Null-byte string termination
    - HTML entities
    - Base64
    - Path references

- Padding
- Delimiters

These techniques are combined in various ways for each URL tested, ranging from minimal transformation, to extreme (every character transformed). All transformed URLs are verified to ensure they still function as expected after transformation.

## 8 COPYRIGHT AND DISCLAIMER



For more information about SecureIQLab and the testing methodologies, please visit our website.

SecureIQLab (April 2022)