SecureIQlab®

Cloud Web Application Firewall (WAF) CyberRisk Validation Report – Wallarm Web Application and API Protection (WAAP)

Product Version: 4.2.1-1

Published: November 8, 2022

Revision 1.1   12/6/2022
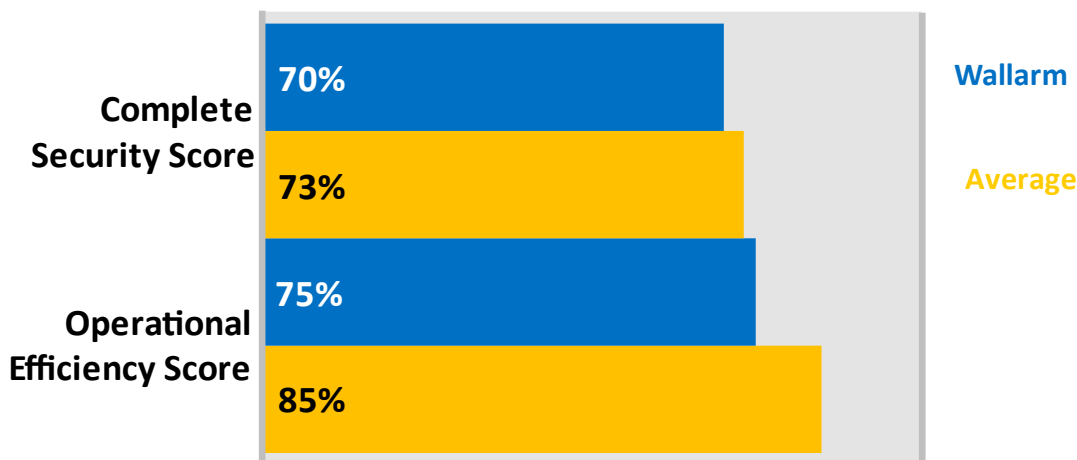
Report Contents:

1   INTRODUCTION

Figure 1. Overall Validation Results for Wallarm Web Application and API protection (WAAP)

SecureIQLab completed testing for 14[1] of the leading enterprise class cloud web application firewall (WAF) products to determine their security efficacy and operational efficiency. Testing was conducted in accordance with the standards of the Anti-Malware Testing Standards Organization[2] (AMTSO). The test used version 2.0 of the SecureIQLab Cloud WAF CyberRisk Validation Methodology (AMTSO Test ID: AMTSO-LS1-TP054).

This report discusses the test results for the Amazon Machine Image (AMI) deployed Wallarm Web Application and API protection (WAAP) version 4.2.1-1. Test results for group minimums, averages and maximum results are also provided in certain categories for additional insight. Because thousands of attacks were simulated during the test, test results have necessarily been simplified and presented for review in a summary format. Figure 1 provides a summary of the product's overall validation results.

Bring Your Own Device (BYOD) and the remote workforce have dissolved the network perimeter and expanded the enterprise attack surface. Cost savings and operational simplicity drive organizations to adopt cloud-native and cloud-driven application architectures. These cloud-native and cloud-driven application architectures include API-driven, multi-tenant and multiuser applications.

The ubiquitous adoption of the cloud is not without challenges. Web application-based vulnerabilities are among the top breach vectors[3] and threats to our cloud and hybrid environments are on the rise. Cloud-based web application firewalls (WAFs) are designed to protect web applications without interrupting business continuity in the cloud-first world. This test of cloud WAFs is intended to evaluate these products' effectiveness in mitigating these challenges.

In this cloud WAF test we measured effectiveness by subjecting products under test to a battery of diverse attacks. We secured cloud applications with the cloud WAFs we were testing. The cloud applications we secured

---

[1] Testing was attempted on a total of 17 cloud WAF solutions. See appendix section 6.6 for details.

[2] https://www.amtso.org/

[3] https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/summary-of-findings/

       SecureIQlab

included simple Ecommerce applications, multiuser web applications and applications with known vulnerabilities. These cloud applications were then used as attack targets. This allowed us to obtain empirically validated data based upon industry frameworks and regulations such as the OWASP Top 10[4], MITRE ATT&CK and PCI DSS 4.0[5].

This report covers testing for just 1 of the 14 products. An overview comparative report generally covering all 14 products is also available. Additionally, reports are available for the other 13 products tested.

In addition to cloud WAFs, SecureIQLab has also identified the following critical technologies for cloud security:

- Advanced Cloud Firewall (ACFW)
- Application Programming Interface (API) Security
- Extended Detection and Response (XDR)
- Internet of Things (IoT) Security
- Security Service Edge (SSE) and Secure Access Service Edge (SASE)

Because these technologies are critical for cloud security, SecureIQLab will test, evaluate and publish its findings about products in the above categories in upcoming tests.

SecureIQLab is a cloud security testing lab that was founded in 2019 and works with enterprises, governments, and security vendors to bridge the applied intelligence gap that exists between market analysis and technology research. SecureIQLab provides services to operationalize security and define metrics to help organizations improve their return on security investments and lower risk.

The Anti-Malware Testing Standards Organization (AMTSO) is an international non-profit association that focuses on addressing the industry need for improvement in the objectivity, quality, and relevance of cybersecurity testing methodologies. SecureIQLab is a member of AMTSO.

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. "Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web."[6] It publishes the OWASP Top 10 Report. SecureIQLab has no affiliation with OWASP. Wallarm Inc. was founded in 2014 and is a rising vendor in the WAF market. The Wallarm WAAP product was selected for inclusion in this test because it meets the SecureIQLab WAF validation methodology selection criteria.[7]

---

[4] Open Web Application Security Project®.
[5] Payment Card Industry Data Security Standards.
[6] https://owasp.org/
[7] New market entrants and interested participating vendors with breakthrough technology offerings.

2   TESTING PARAMETERS AND RESULTS

Cloud-based web application firewalls (WAFs) should accurately detect, prevent, and log attack attempts while avoiding false positives. The majority of the attacks conducted against the cloud WAF product under test were tactics and techniques identified by OWASP for the exploitation of applications. SecureIQLab believes that attack tactics and techniques should be blocked, not just those with malicious payloads. For example, replacing the payload of "evil.com" with "hello world" doesn't change the fact that an attack technique was missed in some cases in order to avoid potential false positives. SecureIQLab's testing demonstrates the efficacy of the Wallarm WAAP in this area.

Tests were performed utilizing black-box and gray-box testing. Black-box testing assumes that the internal code structure of the product being tested is unknown to the tester. For this testing approach, testers are not required to know a system's implementation details. Gray-box testing assumes that part of the product's internal code structure is known to the tester.

Default configurations and rule sets were used for the majority of the products in this test. However, any "Detect Only" mode settings that were part of default configurations were modified to "Block" mode, with default rulesets used as applicable.

Tuning a WAF can be complex. Tuning was based on industry and marketplace expectations that these solutions will require minimal to no tuning during provisioning, deployment, and management phases, which translates to lower operational expenses and increased revenue for the targeted audience, i.e., SMBs, managed service providers (MSPs), and managed security service providers (MSSPs).

Further, any required tuning was performed (1) according to vendor recommendations publicly available on the Wallarm's website and (2) according to relevant documentation available on Wallarm's documentation site to align with the customer experience during the deployment and management of the product. (Enterprises are advised to exercise due diligence during this process to avoid impacting business.)

WAF-protected applications were used during testing by performing standard user transactions that included form submissions, comment writing, ecommerce transactions, and other transactions. See Appendix Section 6 for additional information on the configurations utilized during this test.

More detailed information about our testing methods is contained in version 2.0 of the SecureIQLab Cloud WAF CyberRisk Validation Methodology (AMTSO Test ID: AMTSO-LS1-TP054).
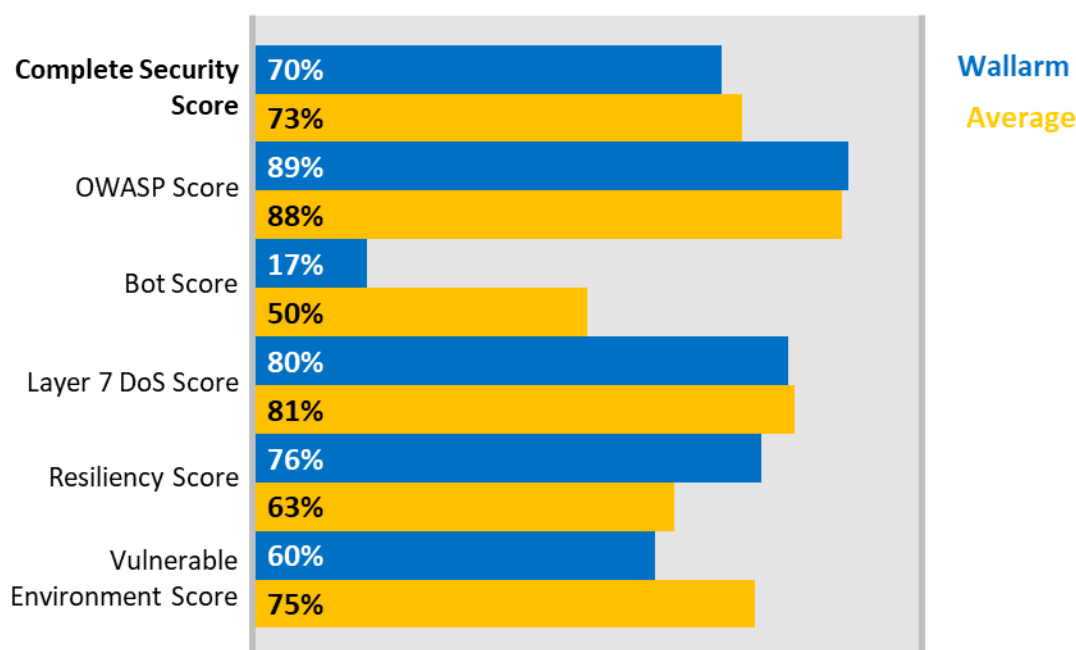
3   SECURITY EFFICACY

Figure 2. Security Validation Results for Wallarm Web Application and API protection (WAAP)

Figure 2 above provides an overview of the SecureIQLab findings during the security validation of the Wallarm Web Application and API protection (WAAP) version 4.2.1-1. The *Complete Security Score* depicts the average of all five security categories tested, minus any duplicated data in the *OWASP Score*. Equation 1 below depicts the *Complete Security Score* calculation. In this equation, the *Deduped OWASP Score* is the *OWASP Score*, from section 3.1, with the A02, A04, A06, and A09 vulnerability results excluded to avoid duplicating data.

$$
\begin{array}{c}
Complete\ Security \\
Score
\end{array} = \frac{\left(\begin{array}{ccccccccc} Deduped \\ OWASP\ Score \end{array} + \begin{array}{c} Bot\ Attack \\ Score \end{array} + \begin{array}{c} Layer\ 7\ DoS \\ Score \end{array} + \begin{array}{c} Resiliency \\ Score \end{array} + \begin{array}{c} Vulnerable \\ Environment \\ Score \end{array} \right)}{5}
$$

Equation 1. Calculation of Complete Security Score

Every cloud WAF evaluated in this test was subjected to fourteen different categories of more than 400 real world-based operational scenarios targeting small-to-medium businesses and enterprises alike. Over 9100 attacks were used encompassing these scenarios and categories. The depth and scope of the testing performed by SecureIQLab carries on our tradition of innovation and improvement. SecureIQLab will continue to add attack libraries and other relevant operational metrics in future iterations of this test.

3.1   OWASP SCORE

The Open Web Application Security Project (OWASP) is a non-profit foundation dedicated to improving web application security[8]. The OWASP Top 10[9] Report is assembled by security experts from across the globe and describes the most critical web application vulnerabilities. This year's testing is based on the OWASP Top 10 2021.

---

[8] SecureIQLab is not affiliated with OWASP.
[9] https://owasp.org/www-project-top-ten/

The Wallarm WAAP was tested against nine of the OWASP Top 10 vulnerabilities. The OWASP A08:2021 – Software and Data Integrity Failures vulnerability was not included in testing because it relates to coding and infrastructure practices that are outside the scope of WAF security.

For detailed explanations of each of these attacks, please reference the OWASP Top 10. Table 1 below provides the results from these tests.

OWASP	Test Case	# Attacks	# Blocked	%Blocked or Score	Test Minimum	Test Average	Test Maximum
A01 Broken Access Control	CSRF	4	0	0%	0%	16%	100%
	Path Traversal	3977	3872	97%	48%	92%	100%
A02 Cryptographic Failures	Feature to implement SSL certificates	NA	NA	100%	100%	100%	100%
A03 Injection	CRLF	103	14	14%	0%	28%	100%
	Cross Site Scripting	2691	2227	83%	3%	87%	100%
	Host Header Injection	10	3	30%	0%	47%	100%
	HTML injection	5	0	0%	0%	40%	100%
	LDAP injection	46	46	100%	15%	94%	100%
	OS injection	324	310	96%	23%	71%	97%
	SQL Injection	1549	1080	70%	31%	70%	97%
	SSTI	123	123	100%	4%	67%	100%
	Xpath	16	2	13%	0%	47%	88%
A04 Insecure Design	Web scraping bot	1	0	0%	0%	86%	100%
A05 Security Misconfiguration	Unrestricted File Upload	36	24	67%	0%	75%	100%
	XXE	122	84	69%	0%	41%	100%
A06 Vulnerable and Outdated Components	Web Application CVEs	20	12	60%	55%	74%	90%
A07 Identification and Authentication Failures	Credential Stuffing Brute force attack	1	0	0%	0%	36%	100%
A09 Security Logging and Monitoring Failures	Logging, monitoring and provided by WAF	NA	NA	80%	60%	80%	93%
A10 Server-Side Request Forgery (SSRF)	SSRF	15	4	27%	0%	50%	100%
OWASP Score				**89%**	**75%**	**88%**	**96%**

Table 1. OWASP Vulnerability Testing

Category averages are determined by equally weighting the test case averages within each category. As an example, Equation 2 below provides the formula for calculating the average for the *A01 Broken Access Control* vulnerabilities category.

$$\begin{array}{c} A01\ Broken \\ Access\ Control \end{array} = \frac{\left(\begin{array}{c} \%\ Path\ Traversal \\ Attacks\ Blocked \end{array} + \begin{array}{c} \%\ CSRF \\ Attacks\ Blocked \end{array} \right)}{2}$$

Equation 2. Formula for calculating the average for A01 Broken Access Control vulnerabilities OWASP category

The *OWASP Score* is derived from averaging *A02 Cryptographic Failures Score* with *A09 Security Logging and Monitoring Failures Score*, and the combined total block/the combined total attacks for *A01 Broken Access Control, A03 Injection, A04 Insecure Design, A05 Security Misconfiguration, A06 Vulnerable and Outdated Components, A07 Identification and Authentication Failures, and A10 Server-Side Request Forgery (SSRF)*. Equation 3 provides the formula for the calculation of the *OWASP Score*.

$$\begin{array}{c} OWASP \\ Score \end{array} = \frac{\begin{array}{c} A02 \\ Score \end{array} + \begin{array}{c} A09 \\ Score \end{array} + \dfrac{\left(\begin{array}{c} Total\ A01 \\ Attacks \\ Blocked \end{array} + \begin{array}{c} Total\ A03 \\ Attacks \\ Blocked \end{array} + \begin{array}{c} Total\ A04 \\ Attacks \\ Blocked \end{array} + \begin{array}{c} Total\ A05 \\ Attacks \\ Blocked \end{array} + \begin{array}{c} Total\ A06 \\ Attacks \\ Blocked \end{array} + \begin{array}{c} Total\ A07 \\ Attacks \\ Blocked \end{array} + \begin{array}{c} Total\ A10 \\ Attacks \\ Blocked \end{array} \right) \times 100\%}{\left(\begin{array}{c} Total\ A01 \\ Attacks \end{array} + \begin{array}{c} Total\ A03 \\ Attacks \end{array} + \begin{array}{c} Total\ A04 \\ Attacks \end{array} + \begin{array}{c} Total\ A05 \\ Attacks \end{array} + \begin{array}{c} Total\ A06 \\ Attacks \end{array} + \begin{array}{c} Total\ A07 \\ Attacks \end{array} + \begin{array}{c} Total\ A10 \\ Attacks \end{array} \right)}}{3}$$

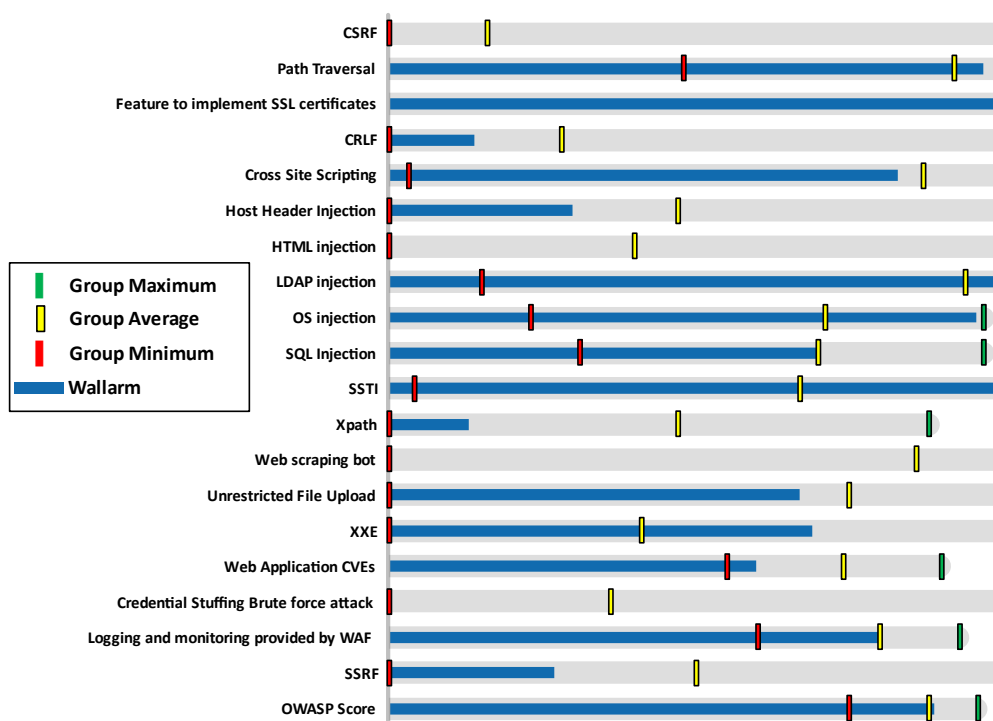*Equation 3. Calculation of OWASP Score*

SecureIQlab

Figure 3. OWASP Score Visual

The *OWASP Score* visual, Figure 3, shows how the results for the Wallarm WAAP version 4.2.1-1 (**blue bar**) compares to the minimum score from the test group (**red line**), the average score from the test group (**yellow line**) and the maximum score from the test group (**green line**). The **gray** vertical left and right lines mark 0% and 100% respectively.

Please see appendix section 6.7 for information regarding mapping the OWASP test cases to the MITRE ATT&CK Enterprise Framework.[10]

3.2   BOT ATTACKS

For purposes of this test, a bot is defined as an automated tool that is used by a remote attacker to carry out automated attacks. The bot tool can exist on the attacker's computer or a compromised endpoint. Wallarm's WAAP was tested against seven types of bot attacks. These attacks were initiated from Asian and North American locations to determine whether the geolocation of an attack source impacts the product's security effectiveness. Results show that geolocation does not impact the product's security effectiveness. Six different bot attacks were used while testing. The results and these attacks are mapped in Table 2 to the MITRE ATT&CK framework, as far as possible. The *Bot Score* is calculated by averaging the seven contributing scores. The maximum *Bot Attack Score* for the tested vendors was 100%. The minimum *Bot Attack Score* for the tested vendors was 17%.

---

[10]SecureIQLab is not affiliated with The MITRE Corporation.

Bot Attacks	ATT&CK® Enterprise Techniques			Wallarm	Test Group
	MITRE Tactic	MITRE Technique	Sub-techniques	Test Results	Average Results
Broken Link Checker	Reconnaissance ID: TA0043	Search Victim-Owned Websites ID: T1594	NA	Bypass	36%
L7 DOS with TOR network	Impact ID:TA0040	Endpoint Denial of Service ID: T1499	Application or System Exploitation T1499.004	Blocked	86%
Login Bruteforce	Credential Access ID: TA006	Brute Force ID: T1110	Password Spraying ID: T1110.003	Bypass	50%
User Agent Manipulation	Reconnaissance ID: TA0043	Gather Victim Host Information ID: T1592	Client Configurations ID: T1592.004	Bypass	43%
Web Scraping	Reconnaissance ID: TA0043	Search Open Websites/Domains ID: T1593 Gather Victim Org Information ID: T1591	Search Engines ID: T1593.002 Identify Business Tempo ID: T1591.003	Bypass	50%
Website crawler	Reconnaissance ID: TA0043	Search Open Websites/Domains ID: T1593 Gather Victim Org Information ID: T1591 Active Scanning ID: T1595	Search Engines ID: T1593.002 Identify Business Tempo ID: T1591.003 Wordlist Scanning ID: T1595.003	Bypass	36%
Bot Score				17%	50%

Table 2. Bot Attack Results with Attacks Mapped to MITRE ATT&CK

3.3   LAYER 7 DOS ATTACKS

Layer 7 Denial-of-Service (DoS) attacks are more difficult to detect than other DoS layer attacks because they use a valid TCP connection. Test cases for such attacks are also more infrastructure friendly than Distributed Denial-of-Service (DDoS) attacks and thus avoid the issues that DDoS attacks may trigger with cloud service providers. Below, Table 3 presents the results of testing the Wallarm WAAP version 4.2.1-1 against five Layer 7 DoS attacks and maps these attacks to the MITRE ATT&CK framework, as far as possible. The product's *Layer 7 DoS Score* was determined by taking the average of its scores against the five attacks. The highest *Layer 7 DoS Score* of the group of tested vendors in this category was 100% and the lowest rating was 40%.

Layer 7 DoS	Wallarm	Test Group
	Test Results	Average Results
DoS Attack	Bypass	64%
Slow DoS Attack	Blocked	93%
Slow DoS Attack	Blocked	93%
Slow DoS Attack	Blocked	79%
Slow DoS Attack	Blocked	79%
Layer 7 DoS Score	80%	81%

Table 3. Layer 7 DoS Validation

Table 4 shows how the attacks used in the resiliency test cases map to the MITRE ATT&CK framework.

ATT&CK® Enterprise Techniques		
MITRE Tactic	MITRE Technique	Sub-techniques
Impact ID:TA0040	Endpoint Denial of Service ID: T1499	Application or System Exploitation T1499.004

Table 4. Layer 7 DoS Attacks Mapped to MITRE ATT&CK

3.4   RESILIENCY SCORE

Security products must demonstrate resiliency. Failure to do so will have significant consequences. The prevailing definition of operational resilience is provided by the Department of Defense (DoD), and states it is: "The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions."[11]

To test its operational resilience, The Wallarm WAAP version 4.2.1-1 was tested against 71 total test cases using 25 unique evasive methods were employed to determine whether it could successfully block attacks that would otherwise go unseen. A higher resiliency score indicates a product is more capable of withstanding and absorbing different variations of attacks while a lower resiliency score indicates a product is less likely to detect different variations of attacks.

Table 5 below provides the test cases used on the Wallarm WAAP and maps these attacks to the MITRE ATT&CK framework, as far as possible. The *Resiliency Score* is the percentage of attacks blocked out of the total 71 attacks. The maximum *Resiliency Score* for the tested vendors was 90%. The minimum *Resiliency Score* for the tested vendors was 17%.

🕵 Resiliency	Wallarm	Test Group
	Test Results	Average Results
Cross Site Scripting	80%	84%
HTML Injection	14%	39%
OS Command Injection	93%	50%
SQL Injection	71%	62%
Unrestricted File Uploads	80%	79%
XXE	100%	47%
Resiliency Score	**76%**	**63%**

Table 5. Resiliency Validation Results

Table 6 shows how the attacks used in the resiliency test cases map to the MITRE ATT&CK framework.

ATT&CK® Enterprise Techniques	
MITRE Tactic	**MITRE Technique**
Defense Evasion ID: TA0005	Obfuscated Files or Information ID: T1027

Table 6. Resiliency Attacks Mapped to MITRE ATT&CK

3.5   WEB APPLICATION PROTECTION

A cloud-based WAF should protect vulnerable web applications. While the proliferation of web application frameworks has made deployment and maintenance of web applications simpler, it has also made it challenging to update these frameworks without affecting the functionality of the web applications. Businesses, MSPs and MSSPs by extension, can ill afford downtime and may delay updates to avoid breaking applications. Consequently, applications

---

[11] https://csrc.nist.gov/glossary/term/operational_resilience

can remain vulnerable to various known vulnerabilities and exploits. This makes it easier for cybercriminals and script kiddies to compromise these applications.

The Wallarm WAAP version 4.2.1-1 was tested against known exploits on 20 different vulnerable applications. See Table 7 below for the full results. The Vulnerable Environment Score is percentage of attacks blocked out of the 20 attacks. The highest Vulnerable Environment Score of the group of tested vendors in this category was 90% and the lowest rating was 55%.

Vulnerable Environment	Wallarm	Test Group
	Test Results	Average Results
Apisix	0%	79%
Confluence	100%	100%
Django	100%	50%
Flink	100%	68%
Ghostscript	0%	29%
Grafana	100%	100%
Log4J	100%	100%
Metabase	100%	93%
OpenTSDB	0%	71%
PhpMyAdmin	100%	100%
Rails	200%	79%
Shiro	0%	50%
Solr	100%	100%
Struts2	100%	93%
Uwsgi	100%	100%
Vulnerable Environment Score	**60%**	**75%**

Table 7. Vulnerable Web Environment Results

Table 8 shows how the attacks used in the vulnerable environment test cases map to the MITRE ATT&CK framework.

ATT&CK® Enterprise Techniques	
MITRE Tactic	**MITRE Technique**
Inital access ID: TA0001	Exploit Public-Facing Application ID: T1190

Table 8. Vulnerable Environment Attacks Mapped to MITRE

3.6   WAF VULNERABILITY ASSESSMENT

Security solutions, regardless of their deployment method, should not increase the attack surface of the environments that they are designed to protect. Additionally, privileges often granted to security solutions, should not be exploitable by threat actors. In another groundbreaking test, SecureIQLab has assessed the security of the cloud WAF product itself.

The Wallarm WAAP version 4.2.1-1 was tested against 9 vulnerability assessment techniques that are commonly used to assess the hardness of applications. Table 9 provides the details of our findings and maps key areas of these attacks to the MITRE ATT&CK framework where possible. All WAFs assessed passed the WAF Vulnerability Assessment.

WAF Vulnerability Assesment	ATT&CK®			Wallarm Results	Group Average
IDOR - Insecure Direct Object Reference	Reconnaisance ID: TA0043	Gather Victim Host Information: Software ID: T1592	Software DI: T1592.002	Blocked	Blocked
Cross Site Scripting	Initial Access ID: TA0001	Drive-by Compromise ID: T1189	NA	Blocked	Blocked
Server Side Request Forgery	Credential Access ID: TA0006	Forge Web Credentials ID: T1606	NA	Blocked	Blocked
Privilege Escalation	Privilege Escalation ID: TA0004	Valid Accounts ID:T1078	NA	Blocked	Blocked
Hard Coded Values (URLs, IDs, Passwords etc)	NA	NA	NA	Blocked	Blocked
Back Button Enabled	NA	NA	NA	Blocked	Blocked
Insecure Session Management	Privilege Escalation ID: TA0004	NA	NA	Blocked	Blocked
Sensitive Data Exposure	Reconnaisance ID: TA0043	Active scanning ID: T1595	Vulnerability Scanning ID: T1595.002	Blocked	Blocked
Weak SSL Ciphers	NA	NA	NA	Blocked	Blocked
WAF Vulnerability Assesment Score				Pass	Pass

Table 9. Wallarm WAAP Vulnerability Assessment
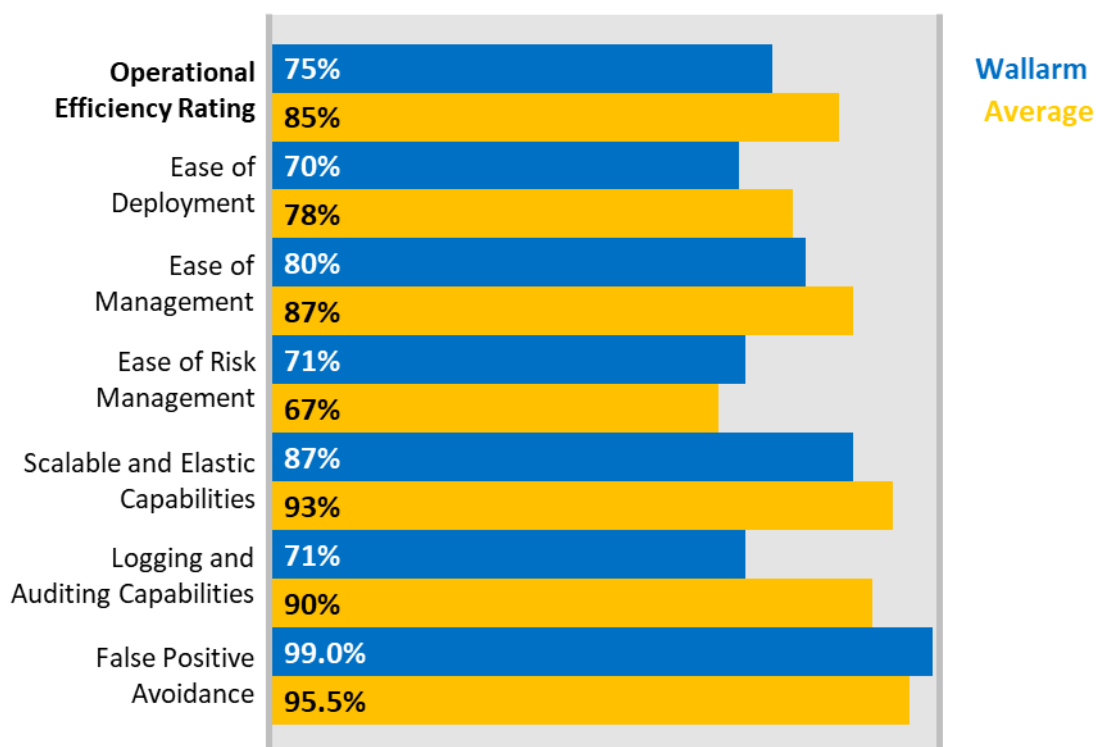
4   OPERATIONAL EFFICIENCY

Figure 4. Validation of Operational Efficiency for Wallarm Web Application and API protection (WAAP)

Cloud-based WAF technology allows for the creation of customized security, which benefits organizations in the following ways:

- Ease of deployment and integration
- Less complex to manage
- Ease of risk management

- Scalable and elastic
- Monitoring, logging, and control capabilities
- Allows business-related transactions

The Wallarm WAAP version 4.2.1-1 was validated in each of these areas of operational efficiency. Figure 4, above, displays the product's high-level results.

Category scores were calculated by aggregating earned points and then dividing this number by the total number of possible points to find a percentage. Points (integers 0 – 3) are earned for each feature within a category as follows:

- 🟩 High or Yes (Green) = 3 Points
- 🟨 Med (Yellow) = 2 Points
- 🟧 Low (Orange) = 1 Point
- 🟥 NA/No (Red) = 0 Points

The *Operational Efficiency Rating* was calculated by adding together the total points for each category, then dividing this number by the maximum potential points (114) and multiplying that number by 100%. Equation 4 states the *Operational Efficiency Score* calculation.

$$\begin{array}{c} Operational \\ Efficiency \\ Rating \end{array} = \frac{\left(\begin{array}{ccccc} Ease\ of & Ease\ of & Ease\ of\ Risk & Scalable & Logging\ and \\ Deployment\ + & Management\ + & Management\ + & and\ Elastic\ + & Auditing \\ Points & Points & Points & Points & Points \end{array} \right)}{114\ points} \times 100\%$$

Equation 4. Operational Efficiency Rating Calculation

The mode for each feature validated is used to calculate the test group feature results. Group test averages were then calculated by adding the modes for each feature and then dividing this number by the total number of possible points to find a percentage.

4.1   EASE OF DEPLOYMENT

Cloud WAFs typically take less than an hour to a few days to set up and seldom require installation of custom software or hardware.

Cloud WAFs should integrate with other security tools, Security Information and Event Management (SIEM) systems, and data repositories. This typically allows both tasks and alerts to be automated. Typical integrations include DevOps tools like Slack and Jira and can include automated additions to policies as threats are detected.

SecureIQLab validated the ease of deployment and integration for the Wallarm WAAP version 4.2.1-1. The overall simplicity of the deployment was low. A minimal understanding of AWS resources is a prerequisite for deployment. Findings for deployment and ease of integration are in Table 10 below.

Ease of Deployment	Wallarm	Test Group
	Validation Results	**Average Results**
Simplicity of Provisioning	Low	Med
Ease of Setting Up WAF Service	Med	Med
Ease of Certificate Creations and Management	Med	Med
Application Load Balancing and Monitoring	Med	High
Deployment Autonomy/Customer Support Experience	High	High
Integration with Multi-Cloud WAF	Yes	Yes
Plug and Play Integration with On-prem Firewall	No	No
Plug and Play Integration for SIEM/S3 Bucket	Yes	Yes
Plug and Play Integration for API Gateway	Yes	Yes
Rating	**70%**	**78%**

Table 10. Deployment and Ease of Integration Findings

Earning 19 of the possible 27 points gave Wallarm a 70% *Ease of Deployment Rating*. The highest rating of the group of tested vendors in this category was 100% and the lowest rating was 56%.

4.2   EASE OF MANAGEMENT

Cloud WAFs market the promise that they are more easily managed than on-premise solutions. They are less complex and more easily managed because they receive automated updates, automatically deal with spikes in traffic (as discussed below) and work out of the box.

Cloud WAFs are less complex because the cloud WAF provider manages the security details and automatically allocates the resources needed. The cloud WAF provider typically has already tuned the security software. Users typically have a single management console to monitor.

Users can typically create additional policies that allow identity-based access and network segmentation. Because the cloud WAF provider automatically applies policy modifications wherever the cloud WAF is deployed, policy modification is generally simple and rapid. Results from SecureIQLab's experience while managing Wallarm's WAAP version 4.2.1-1 are in Table 11, below.

Ease of Management	Wallarm	Test Group
	Validation Results	**Average Results**
Simplicity of Tuning WAF	Med	High
Intuitiveness Security Policy	High	High
Ease of Managing Security Policy	High	High
Customization of Dashboard	Med	High
Capability of Asset Management	Low	Low
Facilitation of PCI Compliance	Med	Med
Facilitation of Data Sovereignty (GDPR)	High	High
WAF Update Automation	Med	Med
Simplicity of Managing Web ACL	High	High
Single Sign On Support	Yes	Yes
Rating	**80%**	**87%**

Table 11. Ease of Management Rating

Earning 24 of the possible 30 points gave Wallarm an 80% *Ease of Management Rating.* The highest rating of the group of tested vendors in this category was 97% and the lowest rating was 63%.

4.3   EASE OF RISK MANAGEMENT

Today's enterprises typically incorporate an Enterprise Risk Management (ERM) program, and Ease of Risk Management is an integral category within such program. In the context of cybersecurity solutions, such as a Cloud WAF, deployed within an enterprise, it is imperative that organizations measure some of the Key Performance Indicators (KPI's) associated with risk management while deploying, managing, and operating such solutions.

These KPI's should then be aggregated such that significant cyber threats form a big picture of the enterprise's risks. Risk management should align with format and measurement scales that can be compared to other types of operational risks.

Table 12 provides Wallarm's *Ease of Risk Management Rating*. The higher the *Ease of Risk Management Rating*, the easier it is to manage security threats and business continuity risks. This in turn lowers the solution's operational overhead and hidden costs of ownership.

Ease of Risk Management	Wallarm	Test Group
	Validation Results	Average Results
Business Continuity Management	Low	Low
Risk Assessment & Mitigation	High	High
Security Metrics Reporting	High	Med
Threat Analytics Dashboard	Med	Med
Alert and Rule Management	NA	High
Automated Alert and Rule Management	High	High
Incident Management	High	High
Rating	**71%**	**67%**

Table 12. Ease of Risk Management Rating

Earning 15 of the possible 21 points gave Wallarm a 71% *Ease of Risk Management Rating*. The highest rating of the group of tested vendors in this category was 95% and the lowest rating was 57%.

4.4   SCALABLE AND ELASTIC

Cloud WAFs should help the customer avoid sizing issues planning by providing for automated flexible scaling. Scaling typically occurs in response to changing traffic load patterns. Providers typically allow customers to choose options that balance optimal performance and optimizing costs. Table 13 highlights SecureIQLab's findings in this area.

Scalable and Elastic Capabilities	Wallarm	Test Group
	Validation Results	Average Results
Load Balancing and Failover Capability	Low	Med
Auto-Scaling Capability	Yes	Yes
Manual Scaling Capability	Yes	Yes
Designed for Static and Dynamic Sites	Yes	Yes
Multi-tenancy Support	Yes	Yes
Rating	**87%**	**93%**

Table 13. Scalable and Elastic Validation

Earning 13 of the possible 15 points gave Wallarm an 87% *Scalable and Elastic Compatibilities Rating*. The highest rating of the group of tested vendors in this category was 100% and the lowest rating was 67%.

4.5   LOGGING, MONITORING, AND AUDITING

Robust logging capabilities are required for incident response, auditing, and many compliance and regulatory purposes. Cloud WAFs need to provide enough visibility into web traffic and sufficient control capabilities for security teams to spot issues and resolve them. Additionally, Cloud WAFs need to have a means to integrate logged data with other storage devices for redundancy. Below, Table 14 covers our logging, compliance and auditing findings.

Logging and Auditing Capabilities	Wallarm	Test Group
	Validation Results	Average Results
Log Configuration Simplicity	High	High
Log Storage Capability	High	High
Web Request Inspection	Med	Med
Application Monitoring	Med	Med
Infrastructure Monitoring	NA	High
Auditing Capability	Med	High
Multi-Factor Authentication	Yes	Yes
Rating	**71%**	**90%**

Table 14. Log and Audit details

Earning 15 of the possible 21 points gave Wallarm a 71% *Logging and Capabilities Rating.* The highest rating of the group of tested vendors in this category was 95% and the lowest rating was 57%.

4.6   FALSE POSITIVE AVOIDANCE

WAFs need to allow business-related transactions while blocking malicious activity. The false positive rate is important because false positives interfere with the operation of the business. Policies need to be adjusted to minimize false positives. False Positives increase alerts for already stretched thin security teams and contribute to alert fatigue. Properly tuned security devices will not detect benign traffic as malicious. Over 300 different false positive test cases were used to validate that the product under test (PUT) would not block simulated consumer purchases. These test cases simulated users that would browse the web application normally while being protected by the cloud WAF. Blocking legitimate user activity constitutes a false positive, increases the operational burden for the enterprise and would require additional tuning to correct. The results for the *False Positive Avoidance* testing are found below in Table 15. Wallarm's *False Positive Avoidance Score* is the percentage of the total allowed legitimate activity test cases to the total possible 308 test cases. The Wallarm WAAP version 4.2.1-1 allowed 305 out of 308 test cases for a score of 99.0%. False positives decrease operational efficiency. The higher the *False Positive Avoidance Score*, the less impact on the operational efficiency.

False Positives	Wallarm	Test Group
	Test Results	Average Results
False Positive Avoidance Score	99.0%	95.5%

Table 15. False Psitive Avoidance Results

The highest *False Positive Avoidance Score* of the group of tested vendors in this category was 100.0% and the lowest score was 81.2%. The *False Positive Avoidance Score* will be used in the calculation of the *Return on Security Investment (ROSI)* in the 2022 comparative report.

5   DIFFERENTIATORS

SecureIQLab testers and analysts researched the products under test and worked to determine key differentiators for the Wallarm WAAP version 4.2.1-1, from other cloud WAFs. Information in this section is sourced from hands on experience, customer feedback and from vendor subject matter experts.

- "So many deployment options"" - SecureIQLab tester. Deployable in AWS, GCP, Azure, IBM Cloud, private, hybrid and multi-cloud, Kubernetes or on a service mesh, and zero-trust environments.
- Many integration options...e.g., incident management systems, data storage, analytics, or SIEM and SOAR solutions.
- Vulnerability scanner and vulnerability management functions built into the Wallarm console.
- Web accessible console, independent of deployment model.

6   APPENDIX
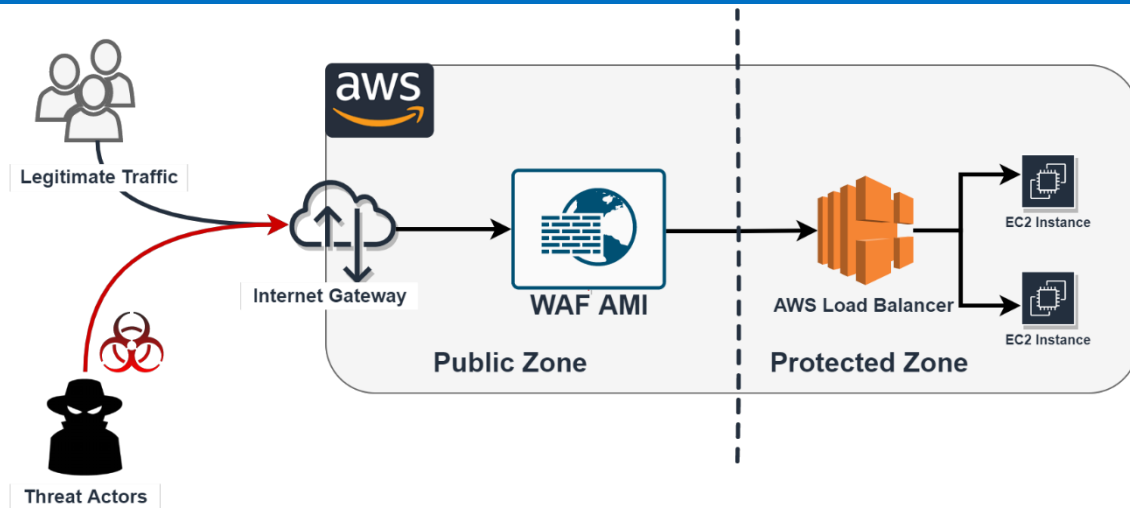
6.1   CLOUD WAF TEST DEPLOYMENT

Figure 5. WAF deployment diagram

The cloud WAF was deployed with default policy with an elastic load balancer to protect the web-applications on AWS, see Figure 5. All web-application transactions were inspected by the cloud WAF. In doing so, the cloud WAF was expected to provide protections against threats that were originated by the malicious actors while allowing authorized users to access the web application resources.

During deployment, our engineers noted the time it took to deploy with out of the box controls and the complexity of the deployment. Also noted was whether our engineering team was required to contact the WAF vendor's support team to successfully complete the WAF deployment. See Table 10 for deployment findings.

6.2   TEST EXECUTION

SecureIQLab performed security validation using crafted attacks that are relevant to today's cloud application hosted on cloud and cloud native applications. SecureIQLab carefully curated such attacks via research generated by our own red team as well as the attacks that are prevalent in the wild. Open-source tool kits were also utilized while performing this assessment.

Before the testing was conducted, SecureIQLab validated that the cloud WAF solution was in an operational state by verifying the following:

- Connection Validation:
  - o Before any test was conducted, SecureIQLab ensured that the Cloud WAF could be accessed by the administrator and was passing normal application traffic. This was to ensure that any dynamic content such as IP blacklist protection could be updated on regular basis by the cloud WAF.
- Logging:
  - o SecureIQLab asserts that logging is a critical and a crucial component while running a cloud WAF. SecureIQLab verified that the cloud WAF being tested had sufficient administrative as well as attack logging to ensure Security Analysts could troubleshoot and fix issues as required.
- Updates:
  - o Protocol updates in the form of rules, signatures and reputations were applied as they became generally available. SecureIQLab made best efforts to apply these updates to products prior to their evaluation.

The above processes were repeated wherever applicable throughout the test. Once the deployment of Wallarm WAAP solution and baseline testing were completed, the security validation testing began.

The first phase of attack was to gather information and perform reconnaissance against the application. The was done to gather as much information as possible to be utilized when penetrating the target during the vulnerability assessment and exploitation phases. SecureIQLab performed vulnerability analysis using automated tools such as Burpsuite and Nessus in addition to performing manual analysis. The main objective of vulnerability analysis is to discover flaws in the systems and applications which can be leveraged by an attacker. These flaws ranged anywhere from host and service misconfiguration to insecure application design. Vulnerability Analysis was based on:

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

Once information gathering and reconnaissance was completed, we began exploitation as the next phase in this process. Penetration testing was critical in the evaluation of cloud WAF technologies.

Once exploited, "post-exploitation" was undertaken. 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—which allowed SecureIQLab, in this case, to establish a new source of attack from the new vantage point in the system—to gain additional access to systems or network resources. We demonstrate the risk presented by exploitable systems and what post-exploitation may likely occur with web applications.

Additionally, 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 which might otherwise get blocked by the Cloud WAF. More details on these techniques are covered in the Resiliency section.

The testing demonstrates 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.

6.3   ATTACK TYPES

The SecureIQLab threat and attack suite contains attacks (including mutations of the same underlying attacks) and proprietary exploits harvested through our test harness or crafted by our threat research team. SecureIQLab has a number of complex web applications which have also been constructed to include known vulnerabilities and coding errors. Groups of exploits are carefully selected from this library to test based on the intended attack. Each exploit has been validated to impact the target vulnerable host(s) by compromising the asset, which can range from being the web server, the web application or sites.

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.

6.4   WALLARM WAAP VERSION 4.2.1-1 CONFIGURATION

The Wallarm WAAP version 4.2.1-1 was deployed and configured according to the instructions found in *Quick start with Wallarm API Security*[12].

6.5   WALLARM WAAP VERSION 4.2.1-1 FIREWALL RULES:

The Wallarm WAAP version 4.2.1-1 was configured per the WAF's default configurations.

---

[12] https://www.wallarm.com/support

6.6 VENDOR PARTICIPATION

Table 16 lists the test status for each of the 17 vendors that SecureIQLab attempted to evaluate in this test iteration.

Vendor	Test Status
Akamai	Testing Completed
AWS	Testing Completed
Microsoft	Testing Completed
Barracuda	Testing Completed
Citrix	Evaluation terminated due to product issues[13]
Cloudflare	Testing Completed
F5	Testing Completed
Fastly	Evaluation terminated by vendor[13]
Fortinet	Testing Completed
Google	Testing Completed
Imperva	Testing Completed
Oracle	Testing Completed
Prophaze	Testing Completed
Radware	Evaluation terminated by vendor[13]
StackPath	Testing Completed
Sucuri	Testing Completed
Wallarm	Testing Completed

Table 16. Vendor Test Status

[13] Contact SecureIQLab for details

6.7   MITRE MAPPED OWASP ATTACKS

Table 17 maps attacks used in the test from the OWASP to the MITRE ATT&CK Enterprise Framework.

OWASP	ATT&CK		
	Tactic	Technique	Sub-technique
CRLF Injection	Discovery ID: TA0007		
XSS	Initial Access ID: TA0001	Drive-by Compromise ID: T1189	
CSRF	Credential Access ID: TA0006	Forge Web Credentials ID: T1606	
Host Header Injection	Execution ID: TA002	User Execution ID: T1204	Malicious Link ID: T1204.001
HTML Injection	Execution ID: TA002	User Execution ID: T1204	Malicious Link ID: T1204.001
LDAP Injection	Discovery ID: TA0007	Domain Trust Discovery ID: T1482	
OS Command Injection	Defense Evasion ID: TA005 Execution ID: TA0002	Indirect Command Execution ID: T1202 Command and Scripting Interpreter ID: T1059	Unix Shell ID: T1059.004
Path Traversal	Discovery ID: TA0007	File and Directory Discovery ID: T1083	
SSTI	Defense Evasion ID: TA005	Template Injection ID: T1221	
SQL Injection	Initial Access ID: TA0001	Exploit Public-Facing Application ID: T1190	
SSRF	Credential Access ID: TA0006	Forge Web Credentials ID: T1606	
Unrestricted File Upload	Defense Evasion ID: TA005	Masquerading ID: T1036	
XXE	Execution ID: TA002	User Execution ID: T1204	Malicious Link ID: T1204.001
Xpath	Initial Access ID: TA0001	Drive-by Compromise ID: T1189	

Table 17. OWASP ATTACKS TO MITRE ATT&CK

6.8   DEDUPED OWASP SCORE CALCULATION

Equation 5 demonstrates the calculation of the *Deduped OWASP Score*.

$$\text{Deduped OWASP Score} = \frac{\left(\dfrac{\text{Total A01 Attacks Blocked}} + \dfrac{\text{Total A03 Attacks Blocked}} + \dfrac{\text{Total A05 Attacks Blocked}} + \dfrac{\text{Total A10 Attacks Blocked}} \right) \times 100\%}{\left(\text{Total A01 Attacks} + \text{Total A03 Attacks} + \text{Total A05 Attacks} + \text{Total A10 Attacks} \right)}$$

Equation 5. Deduped OWASP Score Calculation

         SecureIQlab

7	CONTACT INFORMATION

SecureIQLab, LLC.
6001 W. Parmer Lane Ste 370, #970
Austin, TX 78704 USA

+1.512.575.3457

www.secureiqlab.com
info@secureiqlab.com

8	COPYRIGHT AND DISCLAIMER

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

SecureIQLab (November 2022)

1.1 Corrected typos and added section 6.8 Deduped OWASP Score Calculation.