



SKUDONET WAF VS Cloudflare WAF SaaS

Performance and Cost Comparison of Web Application Firewalls

WAF **security level** and comparison

This report presents a **direct performance comparison** between SKUDONET's Web Application Firewall (WAF) and a Cloudflare WAF solution.

Using **gotestwaf**, a specialized security testing tool, we simulate real-world attacks to measure each WAF's ability to block threats and secure web applications.

What is **gotestwaf**, and How Does It Work?

gotestwaf is an advanced testing tool designed to simulate various types of web and API attacks. By mimicking common threats like SQL injections, cross-site scripting (XSS), and remote file inclusion (RFI), it evaluates the effectiveness of a WAF in real-time.

After testing, gotestwaf assigns a security rating **based on the WAF's ability to detect and block** these attacks, **offering a clear, measurable comparison of security performance.**

ENVIRONMENT

Description of the Tests Overview



ENVIRONMENT

Description of the Tests Overview

Client (Testing Tool)

Tool Used: *gotestwaf*

Purpose: An API and WAF attack simulator used to test the effectiveness of each WAF solution against common threats.

Backend Environment

Simple web server with a “Hello World!” setup.

Controlled environment to simulate attacks and measure each WAF’s response.

WAF Endpoints Tested

Both endpoints were configured with the respective WAF module to observe **performance under similar conditions.**

ENVIRONMENT

What This Report Checks

API and WEB Protection Level

This test measures each WAF's ability to protect API endpoints and web applications against simulated attacks.

Simulation Tool (gotestwaf)

Evaluates WAFs by simulating various API and web-based attacks, assigning a security rating based on the number of blocked attacks.

Tested WAF Configurations

SKUDONET: WAF module fully enabled.

Cloud WAF SaaS Leader: Pro plan with default security configurations.

ENVIRONMENT

Types of Simulated Attacks

SQL Injection (SQLi): Manipulates database queries to extract or alter sensitive data.

Cross-Site Scripting (XSS): Injects malicious scripts into webpages viewed by users.

Remote File Inclusion (RFI): Loads external files with harmful code into the application.

Remote Code Execution (RCE): Executes code remotely on the server to gain control.

Local File Inclusion (LFI): Accesses sensitive local files on the server.

Session Fixation: Hijacks a user's session to gain unauthorized access.

Data Leakages (SQL, PHP, JAVA, etc.): Exposes sensitive data like credentials or personal information.

ENVIRONMENT

Tested WAF Configurations

SKUDONET

WAF default Configuration

Method enforcement	application attack SQLi
scanner detection	application attack Session fixation
protocol enforcement	application attack JAVA
protocol attack	data leakages
application attack LFI	data leakages SQL
application attack RFI	data leakages JAVA
application attack RCE	data leakages PHP
application attack PHP	data Leakages IIS
application attack Generic	web Shells protection
application attack XSS	

Cloudflare

Business Plan Activated with WAF

OWASP core Ruleset
Leaked Credential checks
Managed Rulesets

Up to 310 Cloud Rules
100 WAF Rules

TEST RESULTS

Performance Comparison



TEST RESULTS

Performance Comparison

Cloudflare Business gotestwaf result

Endpoint <https://skudo-networks.com> is configured with Cloud WAF SaaS Leader

Overall grade:

F

56.1 / 100

Project name : generic

URL : <http://waf.skudo-networks.com/>

Testing Date : 12 November 2024

GoTestWAF version : unknown

Test cases fingerprint : c4d9cb74807fac06bcf62e636f6d4e60

Used arguments : --url <http://waf.skudo-networks.com/>

SKUDONET gotestwaf result

Endpoint <https://skudo-networks.com> is configured with SKUDONET WAF module

Overall grade:

A

94.9 / 100

Project name : generic

URL : <https://skudo-networks.com/>

Testing Date : 14 October 2024

GoTestWAF version : unknown

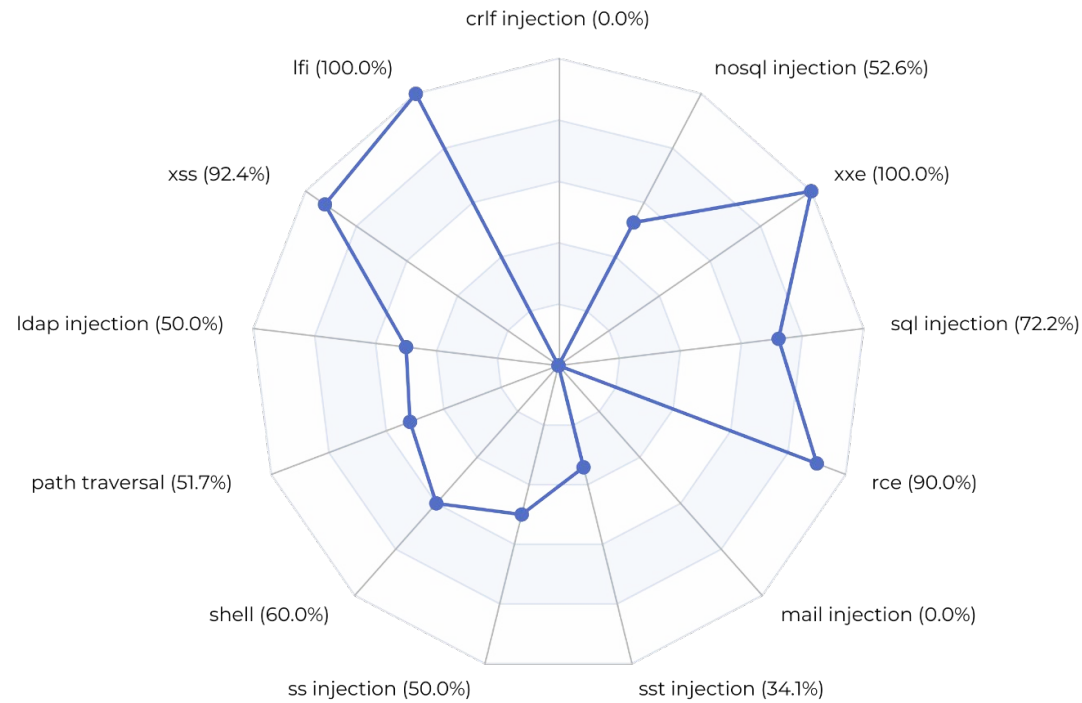
Test cases fingerprint : c4d9cb74807fac06bcf62e636f6d4e60

Used arguments : --url <https://skudo-networks.com/>

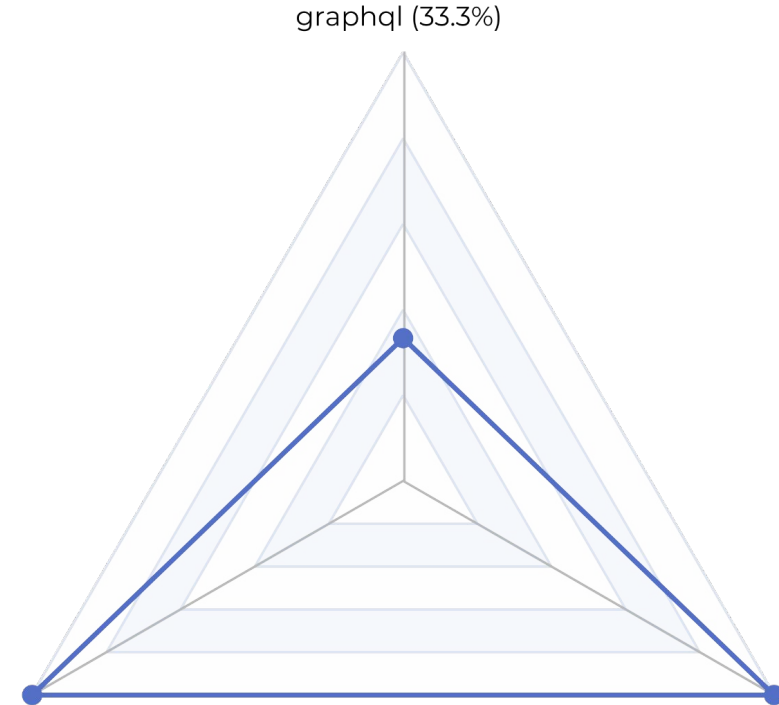
TEST RESULTS

Cloudflare Business Gotestwaf Results

Application Security



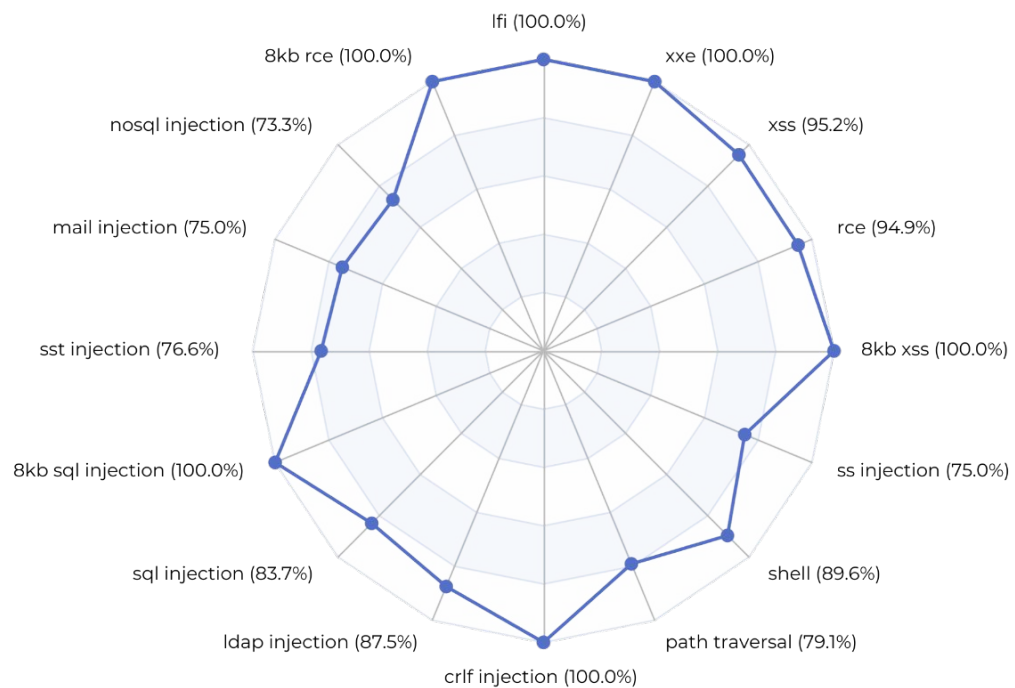
API Security



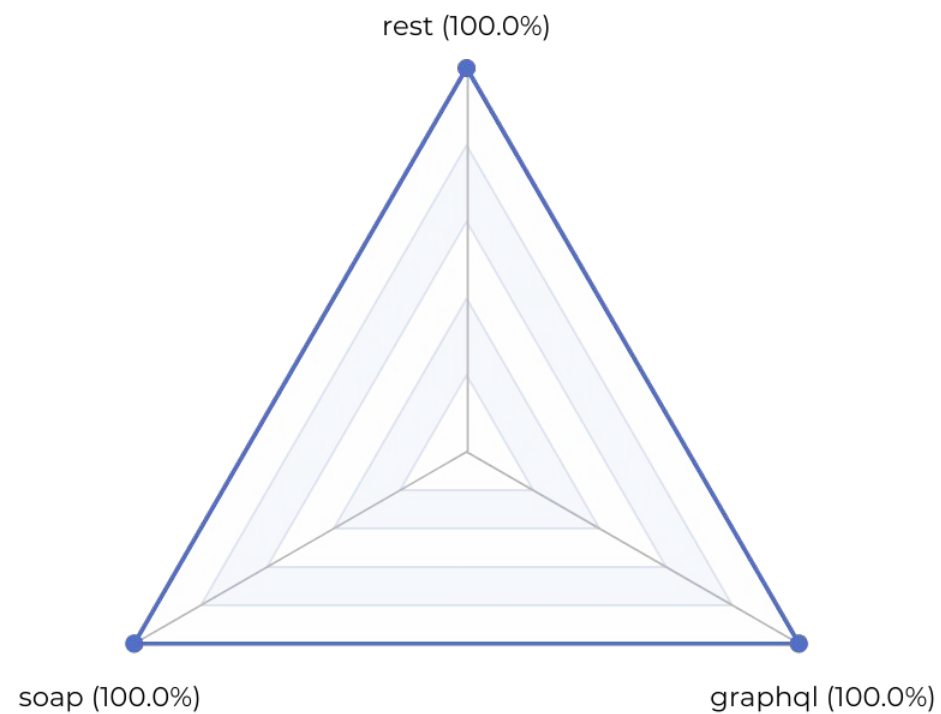
TEST RESULTS

SKUDONET Gotestwaf Results

Application Security



API Security



TEST RESULTS

Performance Comparison

94.9/100

**Security level for
SKUDONET v10 WAF**



- Grade A as protection level 94.9/100
- 100% protection on xss, sqli, crlt, xxe, rce and lfi attacks.
- 100% protection in APIs REST, Graphql and SOAP.

56.1/100

**Security level for
Cloudflare Business WAF**



- Grade F protection level 56.1/100
- 100% protection on lfi and xxe.
- 33% protection in APIs Graphql, no protection for SOAP and REST APIs.

COST COMPARISON

Price Analysis



SKUDONET

8x5 Plan

€950

/node per year

- **Unlimited SKUDONET security rules.**
- **8x5 Support:** Software updates, unlimited cases, and technical support via email.
- SKUDONET for SaaS: **unlimited free host names.**
- **Include DDoS protection** for the network layer (L3)

Cloudflare

Business Plan

€2400

/node per year

- Security **Cloud rules:** up to **310 rules.**
- **Business Support:** incidents, chat, and community forums.
- Cloud for SaaS: **<100 free host names.**
- **Does not include DDoS protection** for the network layer (L3)



“An Application Delivery Controller made secure and easy to manage, ready to work in any Environment with capabilities compared with the market leader, a simple license model makes SKUDONET an alternative for Load Balancing and Cyber Security”



Thank You

Contact us:

info@skudonet.com

+34 954 10 35 02

skudonet.com