

Web Application Firewall (WAF) – Hands-On Learning | TryHackMe

Excited to share that I've completed a TryHackMe lab focused on Web Application Firewalls (WAF)

A Web Application Firewall (WAF) is a critical security layer that protects web applications by monitoring, filtering, and blocking malicious HTTP/HTTPS traffic. It acts as a shield between users and web apps, defending against common web-based attacks.

Key Concepts I Explored:-

What a WAF is and how it works

How WAFs detect and block attacks using:

Signature-based rules

Behavioral analysis

Anomaly detection

Understanding false positives & false negatives

How attackers attempt to bypass WAF protections

Hands-On Skills Gained:-

Analyzing blocked requests and WAF responses

Testing payloads for SQL Injection & XSS

Learning how improper WAF rules can be bypassed

Gaining a defender's mindset while thinking like an attacker

Why This Matters:-

WAFs play a crucial role in real-world web security, especially in defending applications against OWASP Top 10 attacks. This lab helped me understand how attackers adapt and why defense-in-depth is essential.



You did it! 🎉 WAF: Introduction complete!

Points earned
112

Completed tasks
8

Streak
1

Scroll down to review your progress