Understanding WAF Violations and NGINX Integration

What is a WAF Violation?

A WAF violation occurs when a request is flagged as malicious based on security policies.

Detection Mechanisms

WAFs use rule-based, signature-based, and anomaly-based detection methods.

Common Violation Scenarios

Includes SQL injection, XSS, CSRF, path traversal, and DoS attacks.

Actions Taken

Requests may be blocked, logged, rate-limited, or redirected.

NGINX and WAFs

NGINX can be extended with WAF modules like ModSecurity and NGINX App Protect.

Logging in NGINX

WAF logs contain details about blocked requests, aiding security analysis.

Conclusion

WAFs integrated with NGINX enhance web security by mitigating attacks and enforcing policies.