Why Security Component

Web Application Firewall (WAF) for the Follower Cities

Why use security component

1. Stop attacks from happening in the first place with WAF heuristics rule engine.

2. Receive customizable alerts from WAF via email so you can act on threats.

3. Make attacks visible, have situational awareness.

Internet is attacking all the time mercilessly. Normally you do not know this, until something stops working or you experience some other problem.

When not to use security component

1. If you don't want to know about attacks.
2. Act only when something is already wrong and fix when system is already down.

Problem

Internet is attacking all the time mercilessly.

Normally you do not know this, until something stops working or you experience some other problem.

Details and architecture

A web application firewall (WAF) protects applications against sophisticated Layer 7 attacks that might otherwise lead to loss of sensitive data, system hijack by attackers, and downtime.

A WAF protects applications by actively monitoring and filtering traffic. It looks for common attack types such as SQL injection, cross-site scripting (XSS), file inclusions, and other types of active intrusion. It is like a shield sitting right in front of your web server to keep out potentially harmful attacks.
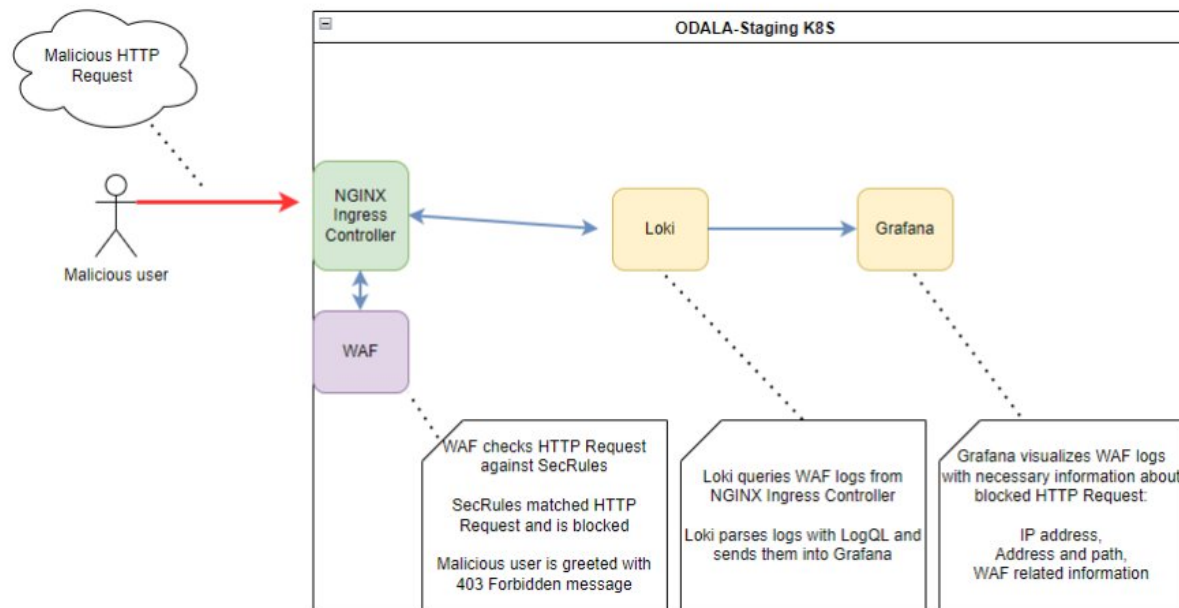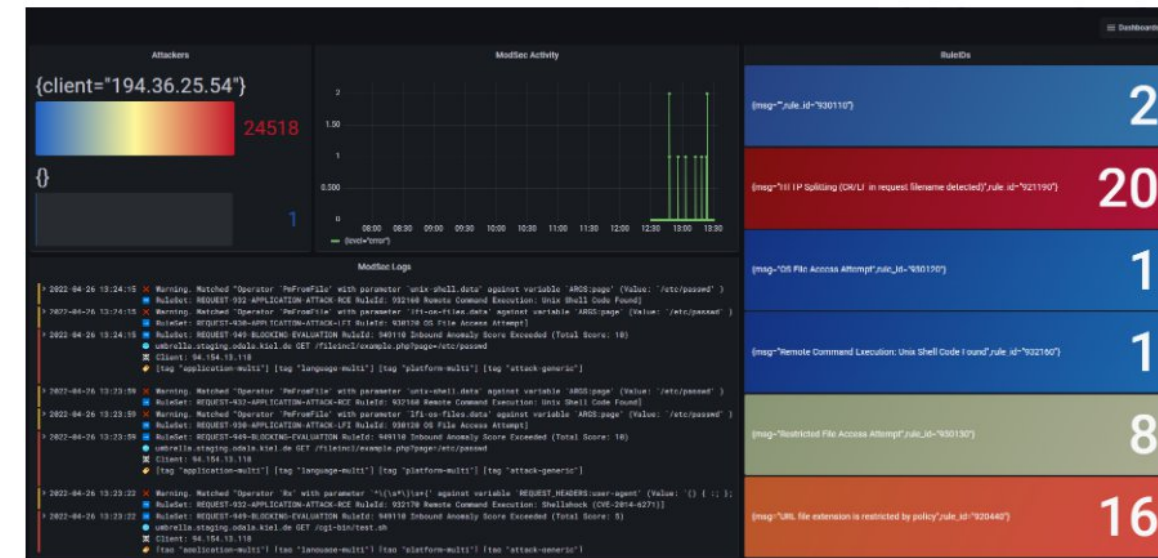
Security Dashboard contains useful graphs that visualizes ModSecurity logs.
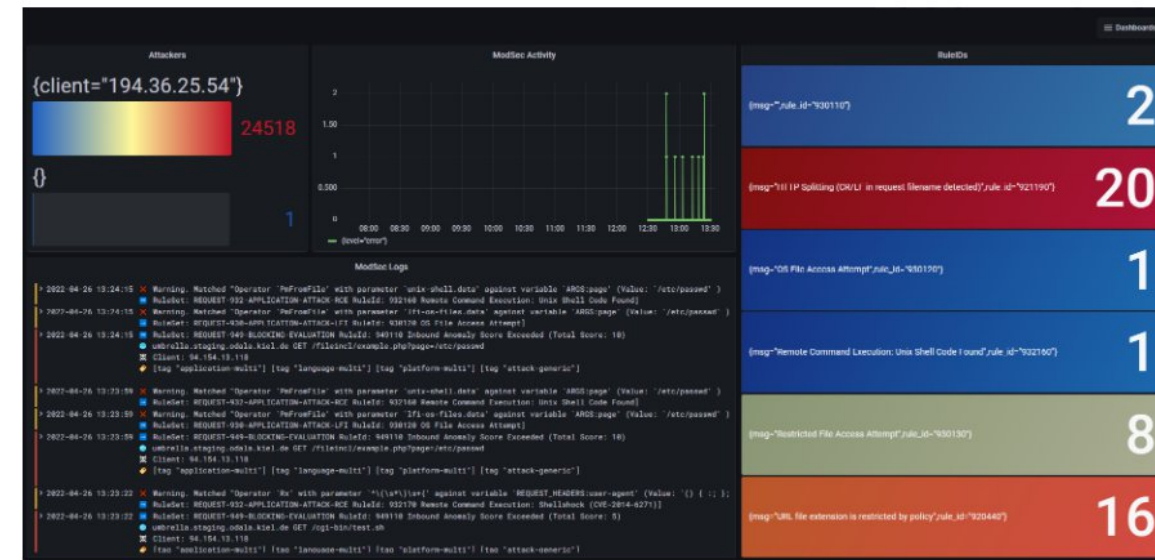
Use case Kiel

ODALA received attacks from IP: 194.36.25.54

Service provider with the IP was contacted promptly by the city of Kiel.

Attacks stopped.

Easy security!

Security Dashboard contains useful graphs that visualizes ModSecurity logs.

Sources & Glossary

https://www.nginx.com/resources/glossary/what-is-a-waf/

https://pixabay.com/vectors/firewall-antivirus-status-security-154670/

https://tenor.com/view/this-is-fine-gif-24177057

https://gitlab.publiccode.solutions/odala/odala-documentation/-/tree/main/waf

WAF – Web Application Firewall

ODALA – Open DAta LAke