Modulo 2 - defesa e monitoramento

by: Danilo Gomes

Passos seguidos

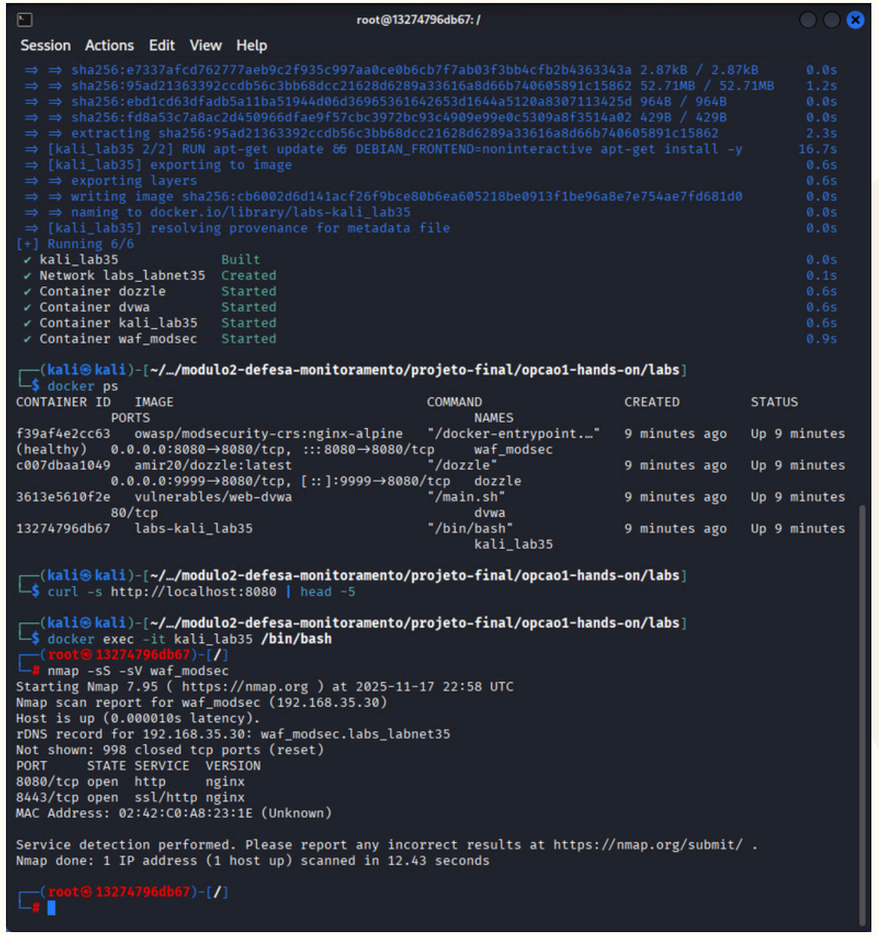
1. Introdução
2. Nmap
3. SQLI + XSS
4. SQLI + XSS 403
5. Duzzle XSS - SQLI
6. Conclusão

Introdução

Segurança em sistemas, infraestrutura, cloud e resposta a incidentes.

Nmap

é para analisar a rede, e verificar quantas maquinas estão conectadas na rede... Retornou 1 maquina conectada



SQLi+ XSS

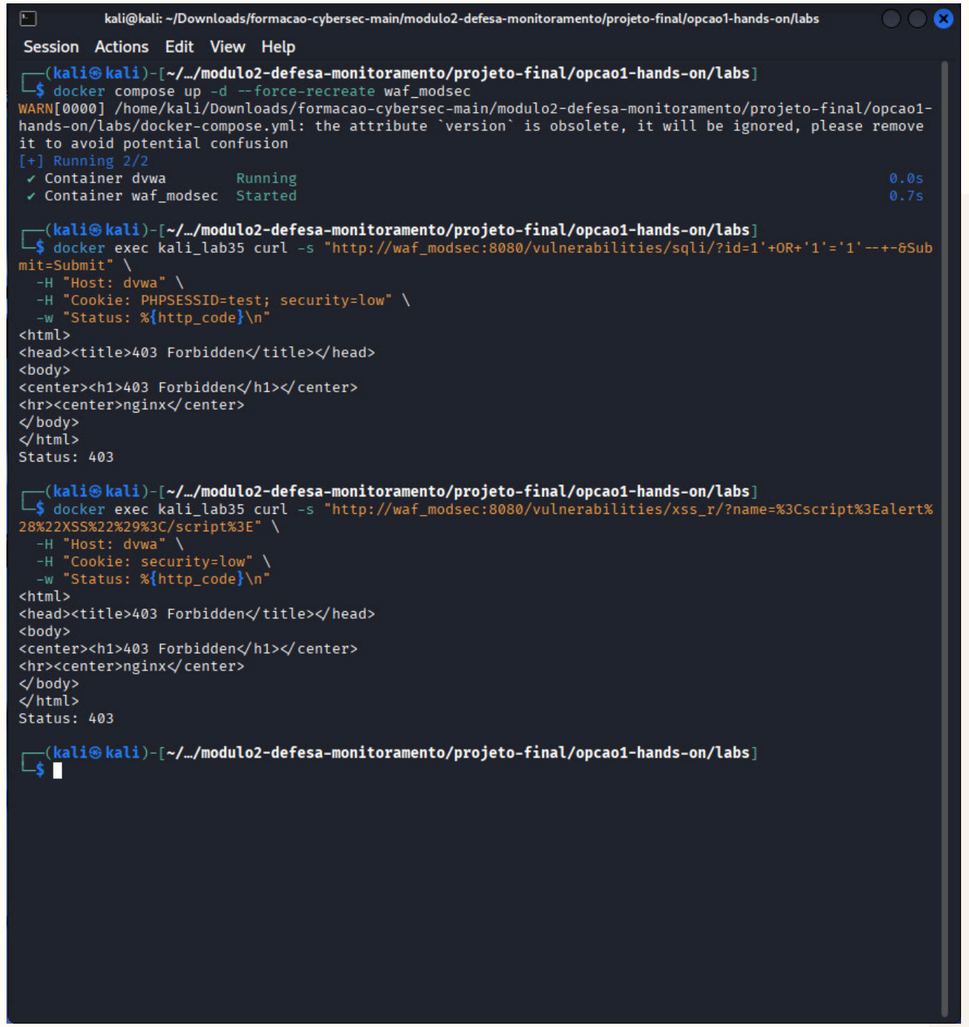
1. verifica, se esta ocorrendo algum ataque. depois aparece o status no log do duzzle.

2. Foi feito um teste de ataque, mas não foi bloqueado por isso retornou o status 302

SQLi + XSS 403

1. verifica, se ainda está ocorrendo algum ataque. foi feito a verificação no status do log do duzzle.

2. Foi feito um teste de ataque novamente, porém retorna o status 403 dessa vez, que significa que o ataque foi bloqueado.



Duzzle xss / sqli

resultado1

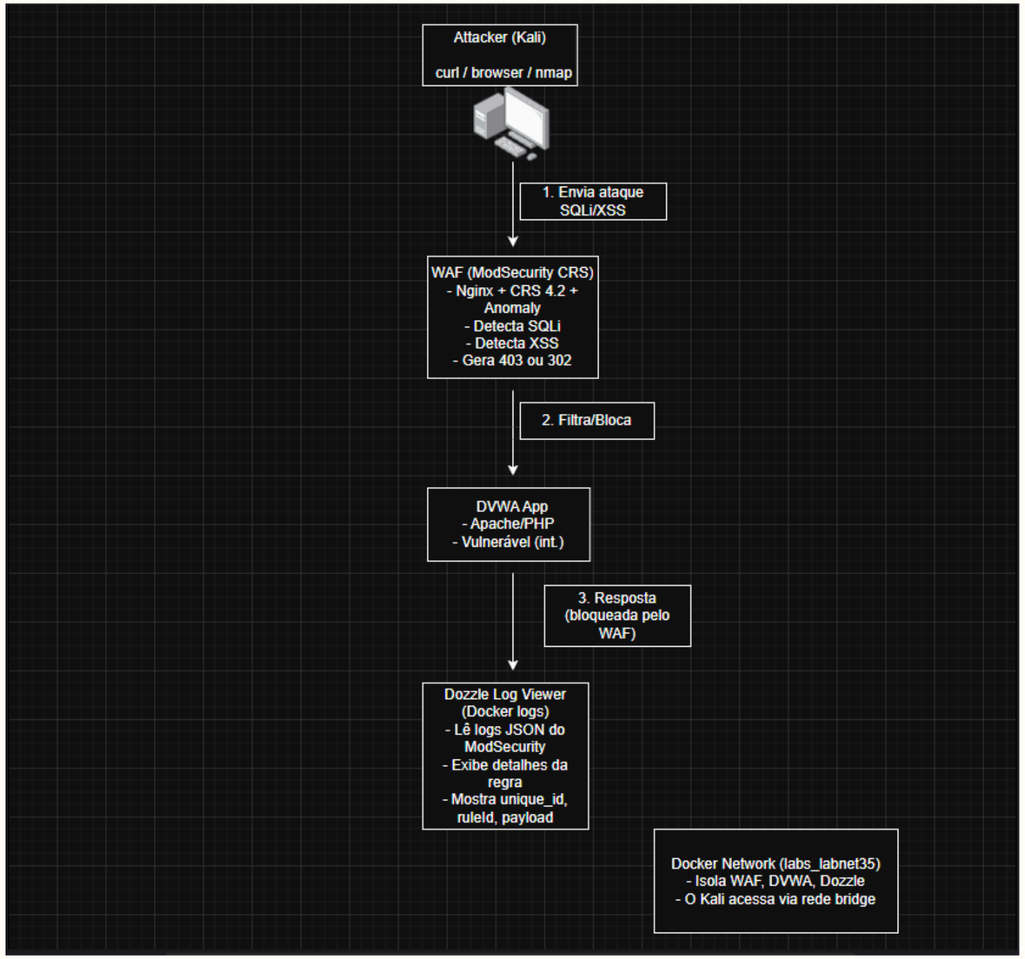
Este é o log duzzle com a mensagem 403, que informa o bloqueio do ataque - XSS

resultado 2

A mesma informação porém - SQLI

Arquitetura (Diagrama)

diagrama ASCII claro e completo mostrando o fluxo Attacker → WAF → DVWA → Logs, exatamente como ocorre no seu ambiente.



Recomendações 80/20

1. Reduzir o Paranoia Level do OWASP CRS para PL1
Diminui falsos positivos e mantém proteção essencial. É só alterar uma linha no arquivo de configuração.
2. Ajustar o Anomaly Score Threshold (ex.: de 5 para 10)
Evita bloqueios desnecessários e mantém detecção eficaz. Impacto alto com mudança mínima.
3. Centralizar os logs do WAF (ex.: enviar para Dozzle/ELK)
Facilita análise, auditoria e monitoramento. Aproveita infraestrutura já existente.
4. Isolar containers em redes Docker dedicadas
Reduz superfícies internas e limita movimentos laterais. Simples de aplicar com docker network.
5. Criar regras de exceção básicas (whitelists por rota)
Permite que rotas conhecidas passem sem acionar o CRS. Evita ruído e melhora a precisão do WAF.

Resposta a Incidente (NIST IR)

Detecção
O WAF identificou e alertou tentativas de SQLi e XSS, registrando tudo nos logs.
Contenção
As requisições maliciosas foram imediatamente bloqueadas com código 403.
Erradicação
Não houve comprometimento; apenas revisão das regras do WAF para evitar falsos positivos.
Recuperação
Serviços continuaram íntegros; apenas confirmação do funcionamento normal do ambiente.
Lições Aprendidas
Reforçar uso do WAF, centralizar logs e ajustar configurações para melhorar precisão e proteção.

Conclusão

Foi feito um reconhecimento do Nmap executado em scan, foi verificado que após configurar um WAF em modo de detecção, foi constatado que estava acontecendo um ataque. Logo em seguida foi feito uma configuração na WAF, para bloquear o ataque.