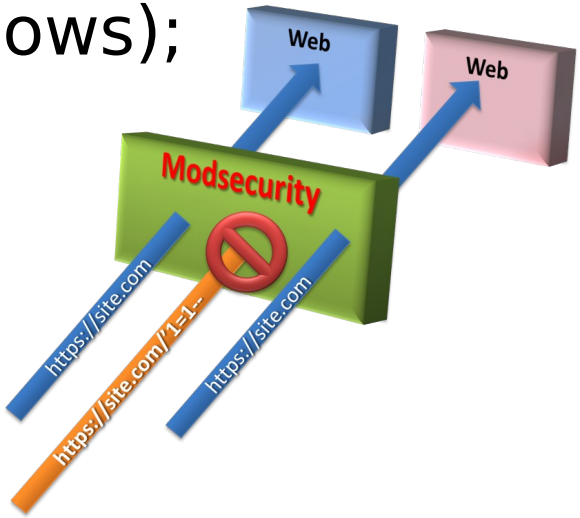
WAF-FLE: o Modsecurity como você nunca viu

Klaubert Herr Silveira
Waf-fle Project
klaubert {at}gmail.com

OWASP
07/10/2011

ModSecurity

- Firewall Open Source para Aplicações Web
- Módulo do Apache (*nix ou Windows);
- Muito flexível;
  - Virtual patching;
  - Funções anti-dos;
- Crescentes recursos;
- Conjunto de regras (Core Rules: um projeto OWASP desde de Agosto/09);



Muito Log...

- Muitas aplicações
- Múltiplos servidores (2, 4 ... 10.000 ...)
- DoS
- Robôs
- Falsos positivos

OWASP

Imagem: http://www.freefoto.com/preview/07-15-16/Round-Hay-Bales

Uma console deve...

- Ser rápida
- Ser escalável
- Oferecer informação agregada (dashboard)
- Destacar o que é mais importante
- Chegar aos detalhes
- Agregar várias fontes de informação
- Agregar inteligência

Imagem: http://www.flickr.com/photos/mr_t_in_dc/2415124094/sizes/m/in/photostream/

Consoles para ModSecurity

	Open Source	Gratuito	Especializado	Ativamente mantido
Modsecurity Console	Não	Até 3 sensores	Sim	Descontinuado ~ 2009
WeBecki	Sim	Sim	Sim	Descontinuado (2007)
Modsec2sguil	Sim	Sim	Não (Log feed para Sguil)	Sim
AuditConsole	Não	Sim (confuso)	Sim	Sim

O que você ainda não viu...

	Open Source	Gratuito	Especializado	Ativamente mantido
Modsecurity Console	Não	Até 3 sensores	Sim	Descontinuado ~ 2009
WeBecki	Sim	Sim	Sim	Descontinuado (2007)
Modsec2sguil	Sim	Sim	Não (Log feed para Sguil)	Sim
AuditConsole	Não	Sim (confuso)	Sim	Sim
WAF-FLE	**Sim**	**Sim**	**Sim**	**Sim**

Web Application Firewall – Fast log and Event Console

http://waf-fle.org

Versão 0.5

Primeira versão pública

WAF-FLE

- Console centralizadora de logs para modsecurity
- Suporta “Traditional” e “Anomaly Scoring”
- Recebe eventos em tempo real ou em batch, com mlogc
- Sem limite de sensores
- Download dos eventos
- PHP e Mysql DB
- Open Source: GPL v2

Performance

- Testado com milhões de eventos
- Servidor de banco de dados pode ser separado
- Já observado:
  - Base com 30GB
  - ~170 eventos/seg
  - +10Milhões eventos

Imagem: http://www.fotopedia.com/items/flickr-1505886543

Dashboard

- Eventos por dia
- Top Sources
- Top Sensors
- Top Rules
- Top Targets
- Status http

OWASP

Imagem: http://www.seriouswheels.com/2009/a/2009-Audi-R8-5-2-FSI-quattro-Dashboard-2-1920x1440.htm

Filtros

- Drill-down
- Cada campo deve ser uma pesquisa
- Invertidos (not)
- A partir do dashboard
- Por faixa de rede
- Por score

OWASP

Imagem: http://www.flickr.com/photos/hourann/531780382/

Participação da comunidade

- Patches
- Bugtracking
- Feature request
- Colaboradores, precisamos de vocês!

Imagem: http://www.flickr.com/photos/lumaxart/2137737248/

Roadmap

0.6	. Dashboard, novas informações agregadas; . Filtro com múltiplos objetos do mesmo tipo; . Agregar outras fontes de informações aos eventos (GeoIP e Whois); . Melhor manutenção de eventos antigos;
0.7	. Agregação periódica dos dados; . Coleta de métricas do servidor http
0.8	. Estender os filtros para: - “Filter on receive”: execução de ações na recepção do evento; - exclusão de eventos; . Otimização dos filtros . Autenticação em bases externas
0.9	. Melhorar escalabilidade e performance . Suporte a outros Bancos de Dados . Internacionalização
1.0	. Gerenciamento das regras

OWASP

Demonstração

Imagem: http://www.flickr.com/photos/oberazzi/318947873/

Obrigado e
Bom almoço

WAF-FLE.org