Web Application Firewalls (WAFs): o impacto do número de regras na latência das requisições Web

Felipe Homrich Melchior

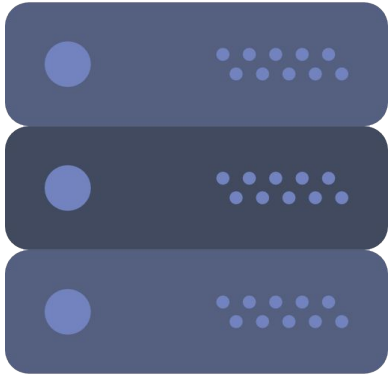
WRSeg - 2019

Requisição

Alice

Requisita Imagem

Retorna Imagem

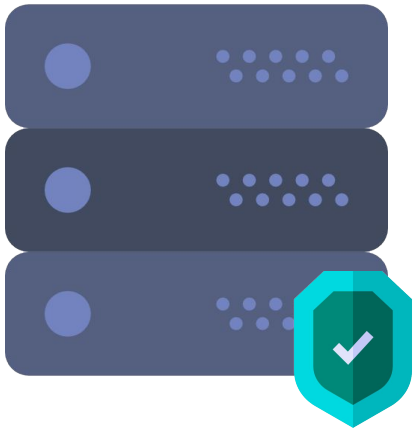


Requisição

Alice

Requisita Imagem

Retorna Imagem

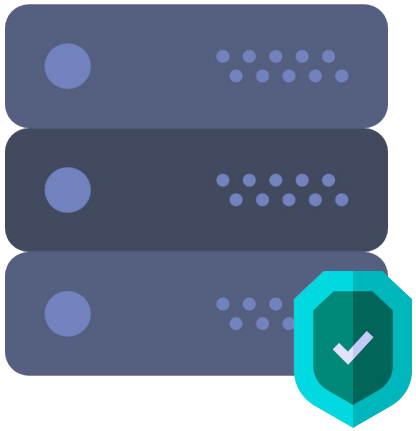


Requisição

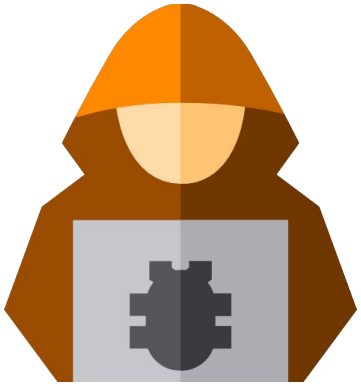
Alice

Requisita Imagem

Retorna Imagem



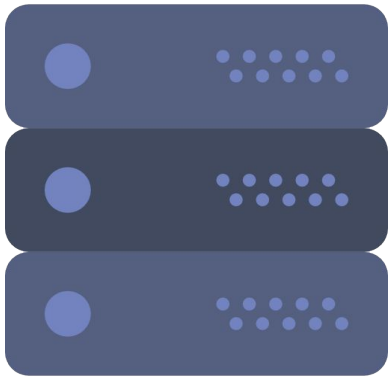
Problema?



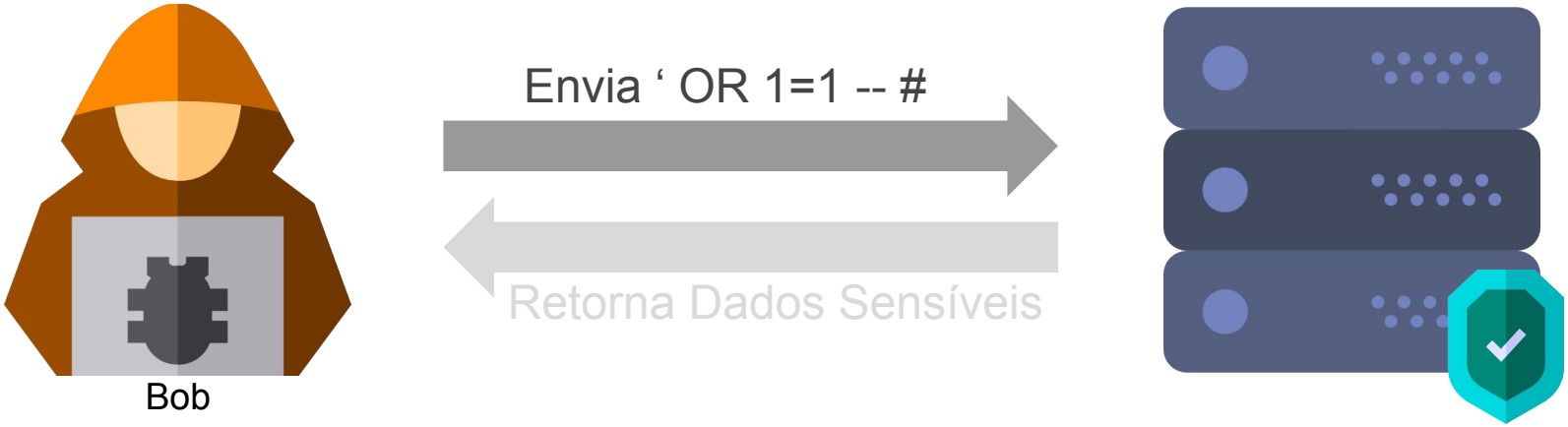
Bob

Envia ‘ OR 1=1 -- #

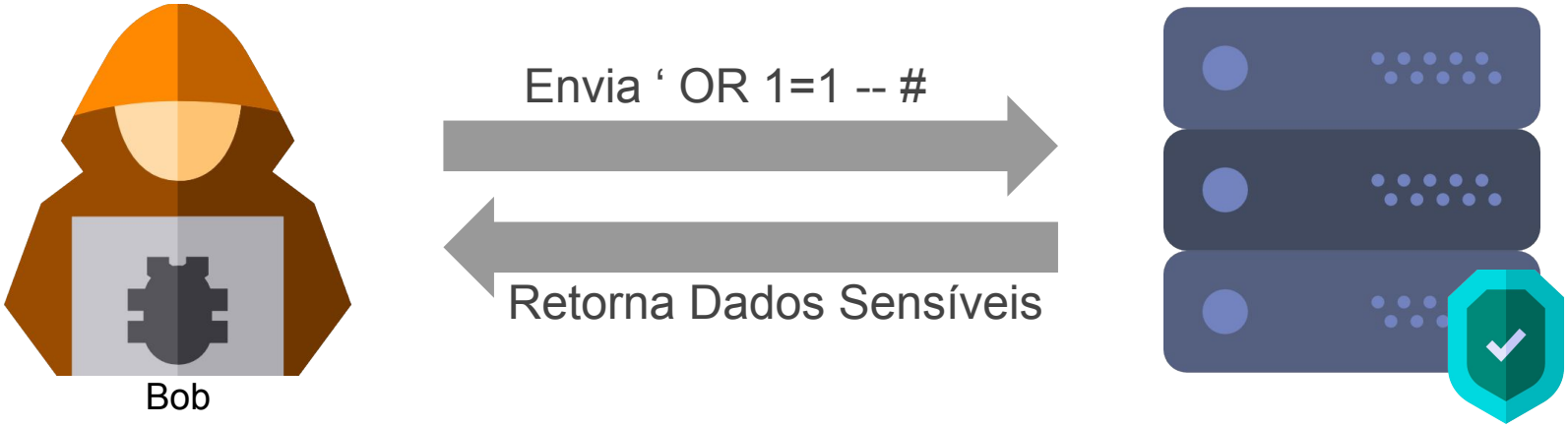
Retorna Dados Sensíveis



Problema?



Problema?



Vulnerabilidades na Web

Metade dos sistemas vulneráveis com falhas críticas

Pelo menos uma falha de nível médio em 90% das aplicações *web*

***Cross-site scripting* é a falha mais recorrente**

Vulnerabilidades na Web

Como melhorar este cenário?

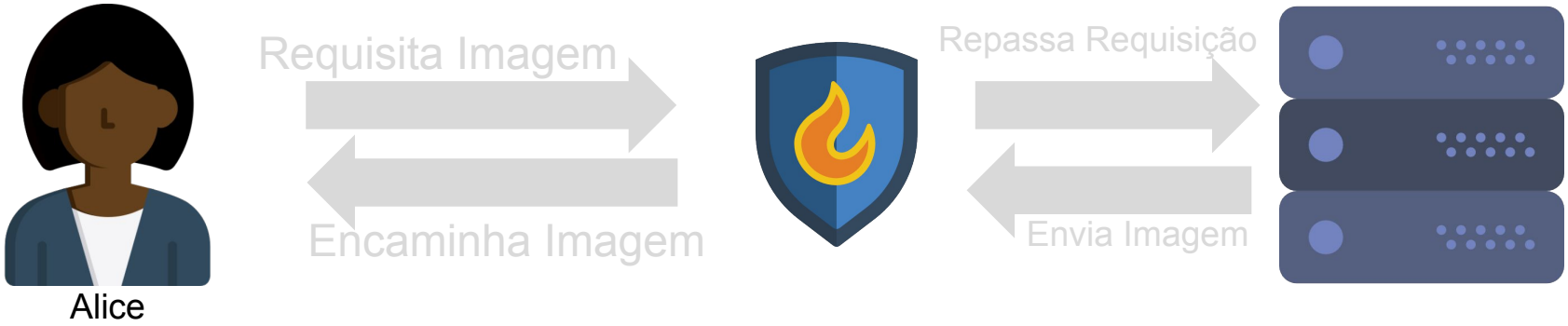
Web Application Firewall

Intermediador entre o Cliente e a Aplicação

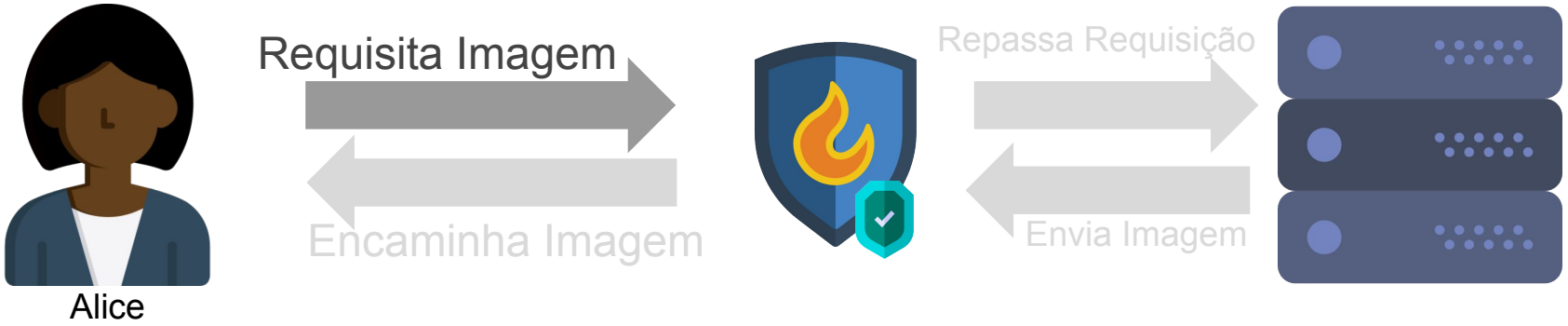
Processa e filtra requisições

Regras pré-definidas

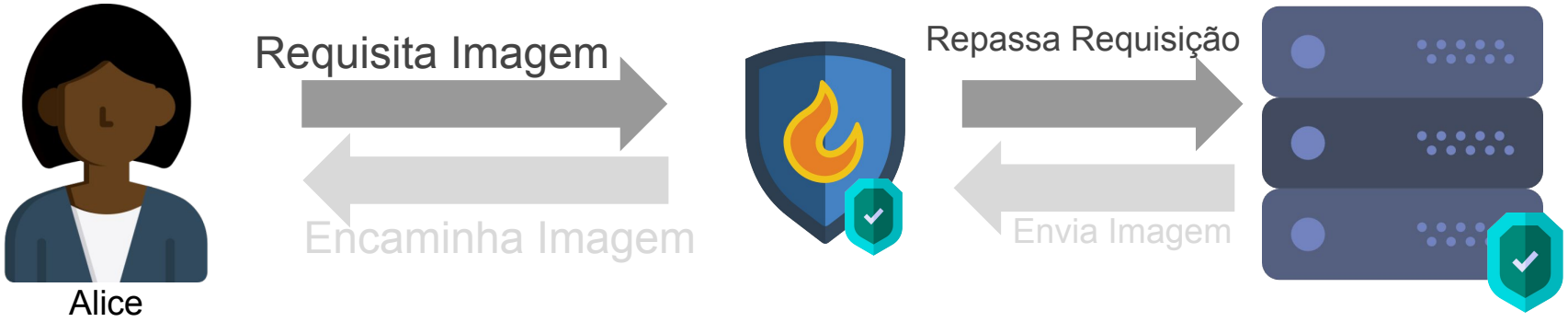
Requisição com WAF - Sem Bloqueio



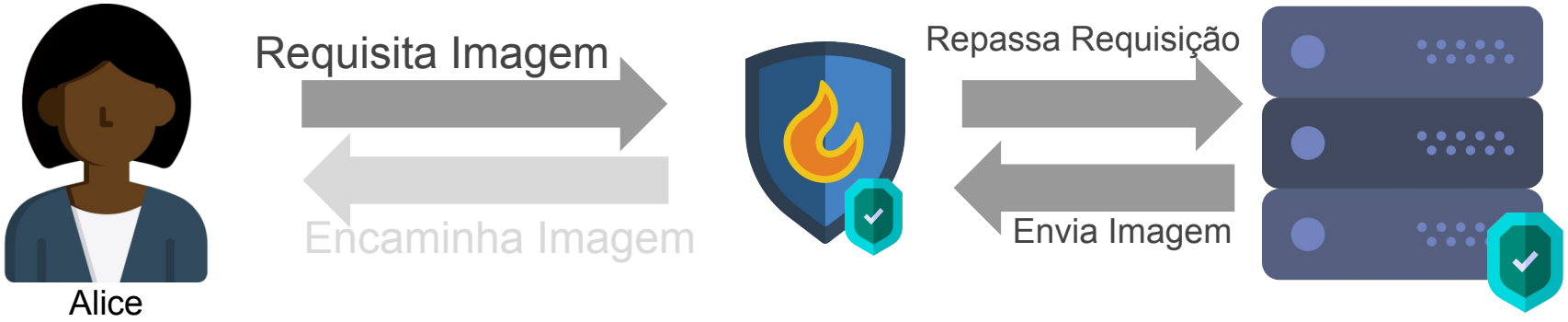
Requisição com WAF - Sem Bloqueio



Requisição com WAF - Sem Bloqueio



Requisição com WAF - Sem Bloqueio



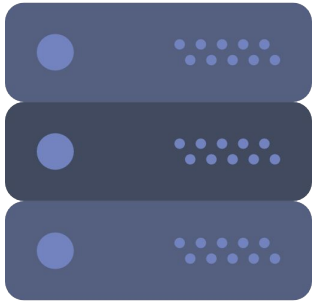
Requisição com WAF - Sem Bloqueio

Requisição com WAF - Com Bloqueio

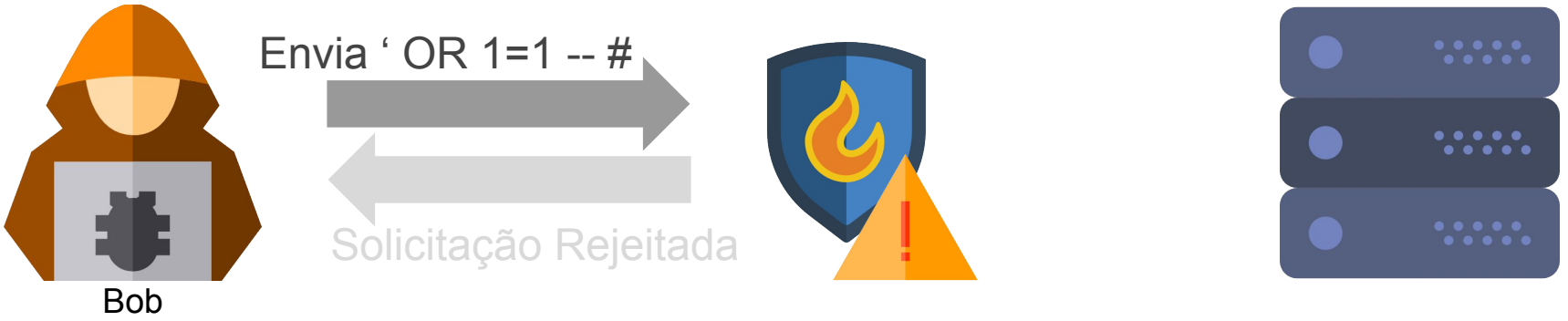
Bob

Envia ‘ OR 1=1 -- #

Solicitação Rejeitada



Requisição com WAF - Com Bloqueio



Requisição com WAF - Com Bloqueio

WAFs

Estudos sobre WAFs

Desenvolvimento

Resultados

Considerações Finais

WAFs

Standalone

Security as a Service

WAFs - Standalone

- Executados junto ao Servidor Web
- Gratuitos e Comerciais

WAFs - Standalone

WAFs - Standalone

WAFs - Standalone

WAFs - Standalone

Cliente

WAF

Aplicação Web

WAFs - Standalone

Cliente

WAF

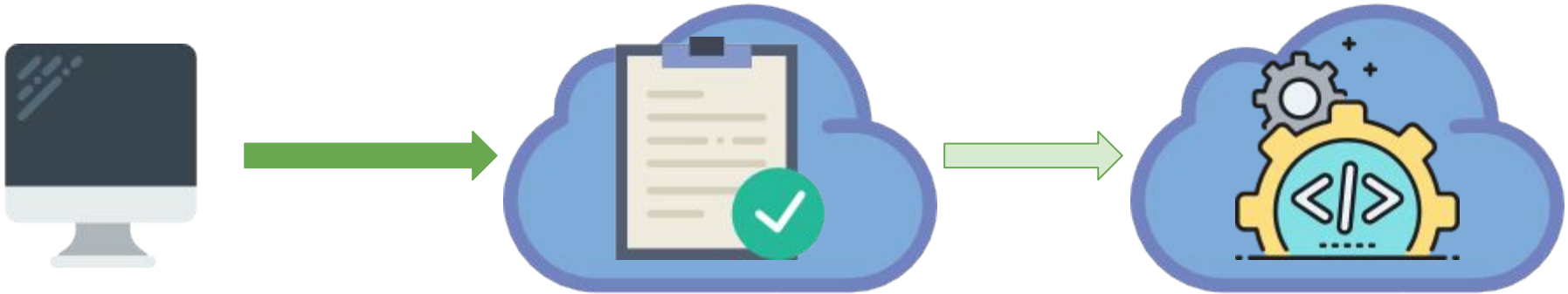
Aplicação Web

WAFs - SaaS

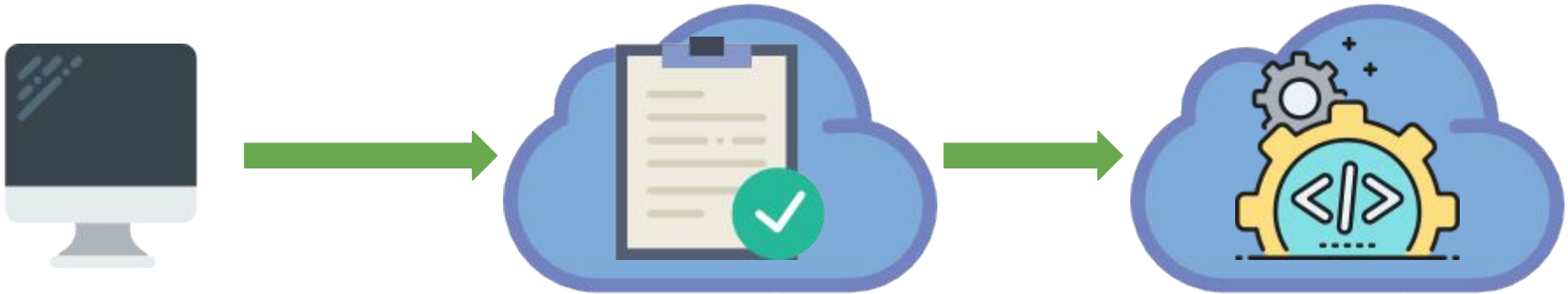
- Oferecidos sob demanda por terceiros
- Redirecionamento DNS
- *Proxy* de Redirecionamento

WAFs - SaaS

WAFs - SaaS



WAFs - SaaS



WAFs - SaaS

WAFs - SaaS

WAFs

Estudos sobre WAFs

Desenvolvimento

Resultados

Considerações Finais

Principais Desafios

Detecção de Ataques

Domínio da Ferramenta

Avaliação em Cenários Controlados

Principais Desafios

Detecção de Ataques

Domínio da Ferramenta

Avaliação em Cenários Controlados

Detecção de Ataques

- Algoritmos capazes de detectar CSRF e XSS
- Autenticação Adicional
- Histórico de Similaridade

Principais Desafios

Detecção de Ataques

Domínio da Ferramenta

Avaliação em Cenários Controlados

Domínio da Ferramenta

- Conhecer a solução pode otimizar resultados
- Níveis de Paranoia do ModSecurity
- Aumento das taxas de Detecção e de Falsos Positivos

Principais Desafios

Detecção de Ataques

Domínio da Ferramenta

Avaliação em Cenários Controlados

Avaliação em Cenários Controlados

- Avaliação da segurança em Cenários Controlados
- Frameworks de Desenvolvimento junto com WAFs
- Framework Laravel sozinho mitiga 60% das vulnerabilidades
- Com ModSecurity, sobe para 70%

Avaliação em Cenários Controlados

- Avaliação da segurança em Cenários Controlados
- Frameworks de Desenvolvimento junto com WAFs
- Framework Laravel sozinho mitiga 60% das vulnerabilidades
- Com ModSecurity, sobe para 70%
- **Nota:** Framework Symfony protege 60% e ao adicionar WAFs como Naxsi e ShadowDaemon, esta proteção cai para 50%

Problemas em aberto

- Impacto da quantidade de regras
- WAFs SaaS
- Caso específico

Problemas em aberto

- Impacto da quantidade de regras
- WAFs SaaS
- Caso específico

WAFs

Estudos sobre WAFs

Desenvolvimento

Resultados

Considerações Finais

Desenvolvimento

- ModSecurity
- Naxsi
- ShadowDaemon
- xWAF

Máquina Hospedeira

- Processador i5 7300-HQ quad-core 2.5Ghz
- 8GB de memória RAM
- Placa de Vídeo GTX 1050
- HD 1TB HM170/QM170 Chipset SATA de 6.0Ghz
- Distribuição Linux Manjaro 18.0.4
- VirtualBox 6.0.6

Máquinas Virtuais

- 1vCPU
- 2GB de memória RAM
- Distribuição Linux Ubuntu Server 16.0.4

Cenário Controlado

- Sistema Web que implementa as dez vulnerabilidades mais recorrentes (Top Ten OWASP)
- PHP 7.0.3
- MySQL 5.7.25
- Servidores Apache 2.4.18 e Nginx 1.13.1

Teste de Funcionamento

Algorithm 1 Bloqueia requisições do cURL

```
1: SecRuleEngine On
2: SecRule REQUEST_HEADERS:User-Agent "@pmFromFile curl.txt
   id:12345,deny,log,status:403,msg:'cURL tentando enviar requests'"
```

Teste de Funcionamento

Algorithm 1 Bloqueia requisiçõe do cURL

```
1: SecRuleEngine On
2: SecRule REQUEST_HEADERS:User-Agent "@pmFromFile curl.txt
   id:12345,deny,log,status:403,msg:'cURL tentando enviar requests'"
```

Teste de Funcionamento

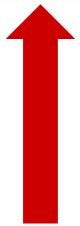
Algorithm 1 Bloqueia requisiçõe do cURL

```
1: SecRuleEngine On
2: SecRule REQUEST_HEADERS:User-Agent "@pmFromFile curl.txt
   id:12345,deny,log,status:403,msg:'cURL tentando enviar requests'"
```

Teste de Funcionamento

Algorithm 1 Bloqueia requisições do cURL

```
1: SecRuleEngine On
2: SecRule REQUEST_HEADERS:User-Agent "@pmFromFile curl.txt
   id:12345,deny,log,status:403,msg:'cURL tentando enviar requests'"
```



WAFs

Estudos sobre WAFs

Desenvolvimento

Resultados

Considerações Finais

Resultados

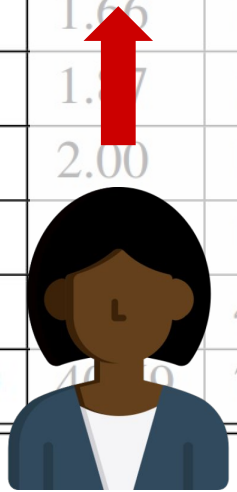
- Programa em Python que simula acessos ao sistema
- Considerando um ataque bloqueado por uma regra no início do conjunto
- Média de tempos de mil requisições
- Aumento gradativo da ativação das regras

Resultados

	ModSecurity		Naxsi		ShadowD.		xWAF	
	Pass	Match	Pass	Match	Pass	Match	Pass	Match
200	1.66	1.39	1.71	1.21	1.64	1.40	1.62	1.53
+ 500	1.87	1.40	1.61	1.25	1.98	1.74	1.75	1.68
+ 1000	2.00	1.42	1.72	1.31	3.17	1.99	1.79	1.64
+ 10000	5.62	1.91	3.59	2.89	7.34	4.12	2.52	1.75
+ 50000	20.68	4.35	14.56	12.72	12.27	9.44	5.52	2.57
+ 100000	40.69	7.77	26.96	23.75	24.13	16.38	9.69	3.71

Resultados

	ModSecurity		Naxsi		ShadowD.		xWAF	
	Pass	Match	Pass	Match	Pass	Match	Pass	Match
200	1.66	1.39	1.71	1.21	1.64	1.40	1.62	1.53
+ 500	1.[illegible]7	1.40	1.61	1.25	1.98	1.74	1.75	1.68
+ 1000	2.00	1.42	1.72	1.31	3.17	1.99	1.79	1.64
+ 10000	[illegible]	1.91	3.59	2.89	7.34	4.12	2.52	1.75
+ 50000	[illegible]	4.35	14.56	12.72	12.27	9.44	5.52	2.57
+ 100000	[illegible]	7.77	26.96	23.75	24.13	16.38	9.69	3.71



Resultados

	ModSecurity		Naxsi		ShadowD.		xWAF	
	Pass	Match	Pass	Match	Pass	Match	Pass	Match
200	1.66	1.39	1.71	1.21	1.64	1.40	1.62	1.53
+ 500	1.87	1.4	1.61	1.25	1.98	1.74	1.75	1.68
+ 1000	2.00	1.42	1.72	1.31	3.17	1.99	1.79	1.64
+ 10000	5.62		3.59	2.89	7.34	4.12	2.52	1.75
+ 50000	20.68		14.56	12.72	12.27	9.44	5.52	2.57
+ 100000	40.69		26.96	23.75	24.13	16.38	9.69	3.71

Resultados

	ModSecurity		Naxsi		ShadowD.		xWAF	
	Pass	Match	Pass	Match	Pass	Match	Pass	Match
200	1.66	1.39	1.71	1.21	1.64	1.40	1.62	1.53
+ 500	1.87	1.40	1.61	1.25	1.98	1.74	1.75	1.68
+ 1000	2.00	1.42	1.72	1.31	3.17	1.99	1.79	1.64
+ 10000	5.62	1.91	3.59	2.89	7.34	4.12	2.52	1.75
+ 50000	20.68	4.35	14.56	12.72	12.27	9.44	5.52	2.57
+ 100000	40.69	7.77	26.96	23.75	24.13	16.38	9.69	3.71

Resultados

	ModSecurity		Naxsi		ShadowD.		xWAF	
	Pass	Match	Pass	Match	Pass	Match	Pass	Match
200	1.66	1.39	1.71	1.21	1.64	1.40	1.62	1.53
+ 500	1.87	1.40	1.61	1.25	1.98	1.74	1.75	1.68
+ 1000	2.00	1.42	1.72	1.31	3.17	1.99	1.79	1.64
+ 10000	5.62	1.91	3.59	2.89	7.34	4.12	2.52	1.75
+ 50000	20.68	4.35	14.56	12.72	12.27	9.44	5.52	2.57
+ 100000	40.69	7.77	26.96	23.75	24.13	16.38	9.69	3.71

Resultados

	ModSecurity		Naxsi		ShadowD.		xWAF	
	Pass	Match	Pass	Match	Pass	Match	Pass	Match
200	1.66	1.39	1.71	1.21	1.64	1.40	1.62	1.53
+ 500	1.87	1.40	1.61	1.25	1.98	1.74	1.75	1.68
+ 1000	2.00	1.42	1.72	1.31	3.17	1.99	1.79	1.64
+ 10000	5.62	1.91	3.59	2.89	7.34	4.12	2.52	1.75
+ 50000	20.68	4.35	14.56	12.72	12.27	9.44	5.52	2.57
+ 100000	40.69	7.77	26.96	23.75	24.13	16.38	9.69	3.71

Resultados

	ModSecurity		Naxsi		ShadowD.		xWAF	
	Pass	Match	Pass	Match	Pass	Match	Pass	Match
200	1.66	1.39	1.71	1.21	1.64	1.40	1.62	1.53
+ 500	1.87	1.40	1.61	1.25	1.98	1.74	1.75	1.68
+ 1000	2.00	1.42	1.72	1.31	3.17	1.99	1.79	1.64
+ 10000	5.62	1.91	3.59	2.89	7.34	4.12	2.52	1.75
+ 50000	20.68	4.35	14.56	12.72	12.27	9.44	5.52	2.57
+ 100000	40.69	7.77	26.96	23.75	24.13	16.38	9.69	3.71

Resultados

	ModSecurity		Naxsi		ShadowD.		xWAF	
	Pass	Match	Pass	Match	Pass	Match	Pass	Match
200	1.66	1.39	1.71	1.21	1.64	1.40	1.62	1.53
+ 500	1.87	1.40	1.61	1.25	1.98	1.74	1.75	1.68
+ 1000	2.00	1.42	1.72	1.31	3.17	1.99	1.79	1.64
+ 10000	5.62	1.91	3.59	2.89	7.34	4.12	2.52	1.75
+ 50000	20.68	4.35	14.56	12.72	12.27	9.44	5.52	2.57
+ 100000	40.69	7.77	26.96	23.75	24.13	16.38	9.69	3.71

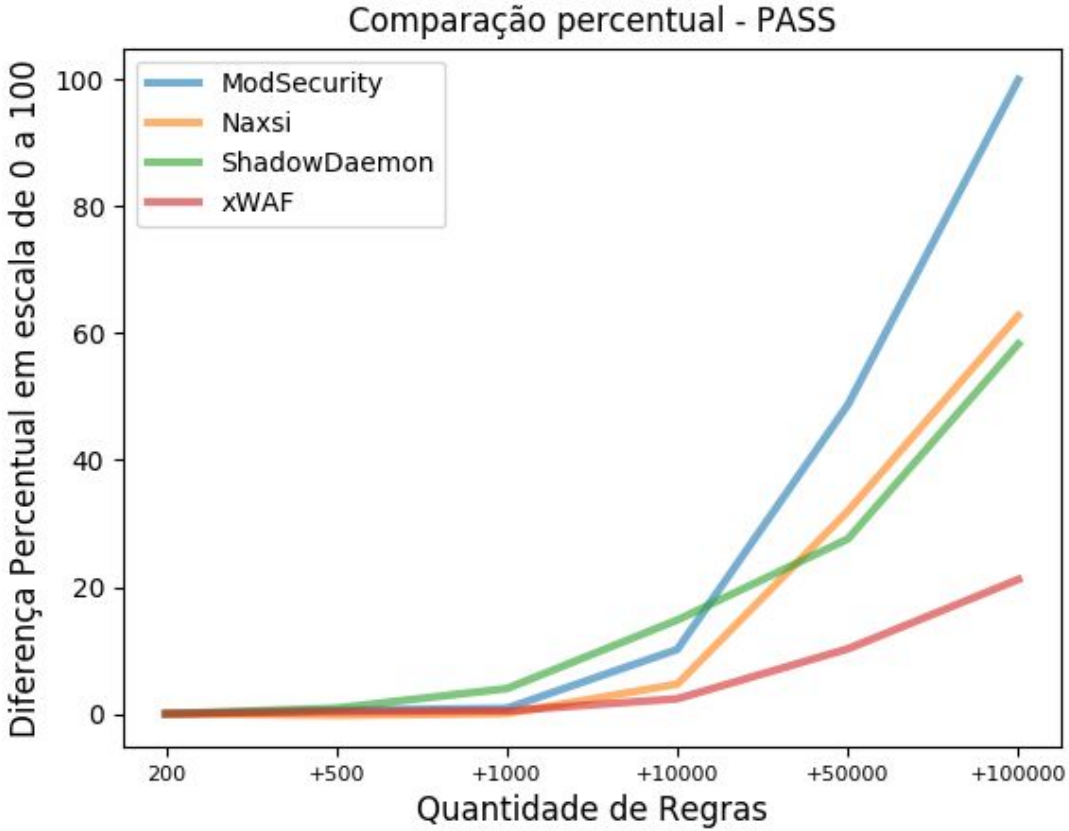
Nota: Ao aproximar-se deste ponto, o acesso ao servidor local leva quase o mesmo que acessar um serviço externo, como o DNS da Google

```
Traceroute ao DNS Google
.
8 google-public-dns-a.google.com (8.8.8.8)24.003 ms 24.904 ms 25.148 ms
```

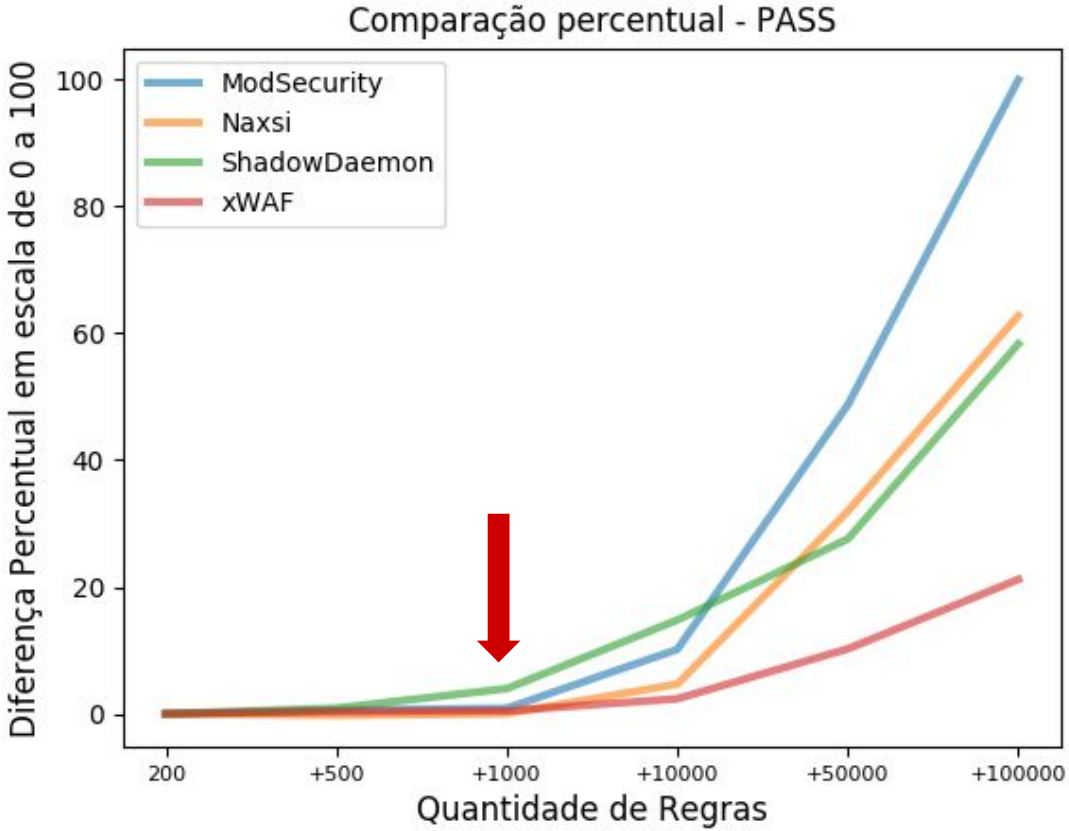
Resultados

	ModSecurity		Naxsi		ShadowD.		xWAF	
	Pass	Match	Pass	Match	Pass	Match	Pass	Match
200	1.66	1.39	1.71	1.21	1.64	1.40	1.62	1.53
+ 500	1.87	1.40	1.61	1.25	1.98	1.74	1.75	1.68
+ 1000	2.00	1.42	1.72	1.31	3.17	1.99	1.79	1.64
+ 10000	5.62	1.91	3.59	2.89	7.34	4.12	2.52	1.75
+ 50000	20.68	4.35	14.56	12.72	12.27	9.44	5.52	2.57
+ 100000	40.69	7.77	26.96	23.75	24.13	16.38	9.69	3.71

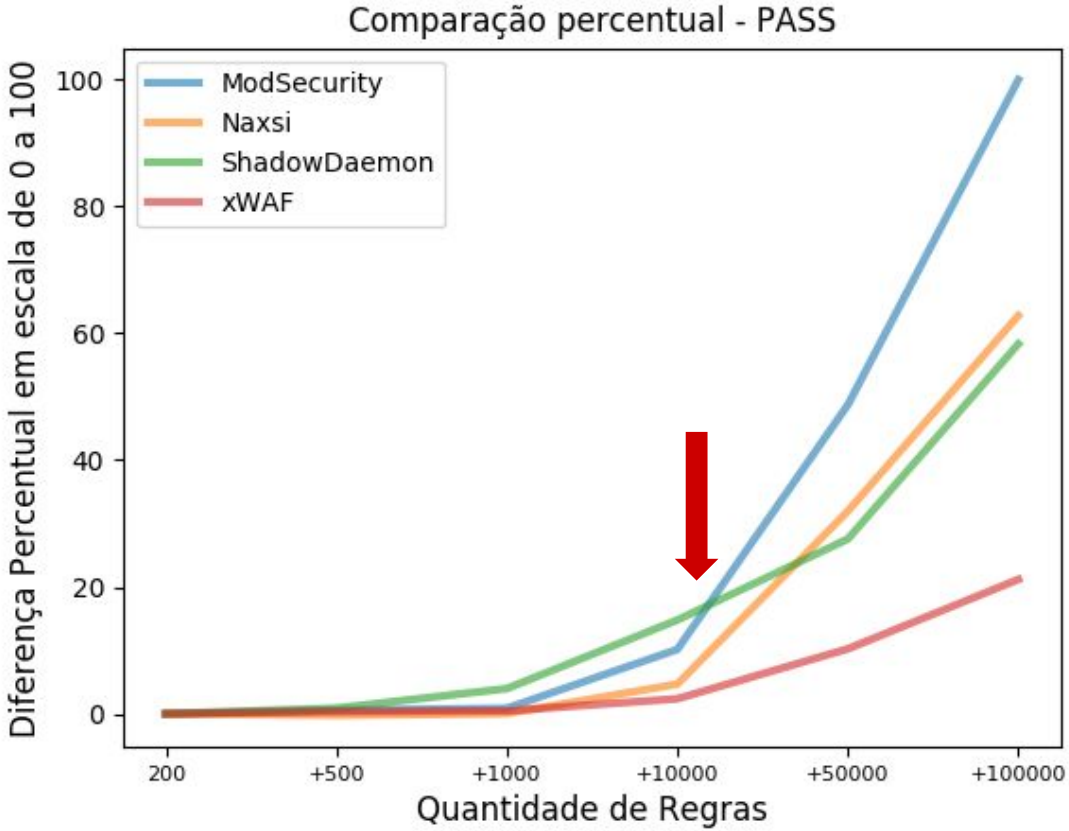
Resultados


Comparação percentual - PASS
ModSecurity
Naxsi
ShadowDaemon
xWAF
Diferença Percentual em escala de 0 a 100
100
80
60
40
20
0
200
+500
+1000
+10000
+50000
+100000
Quantidade de Regras

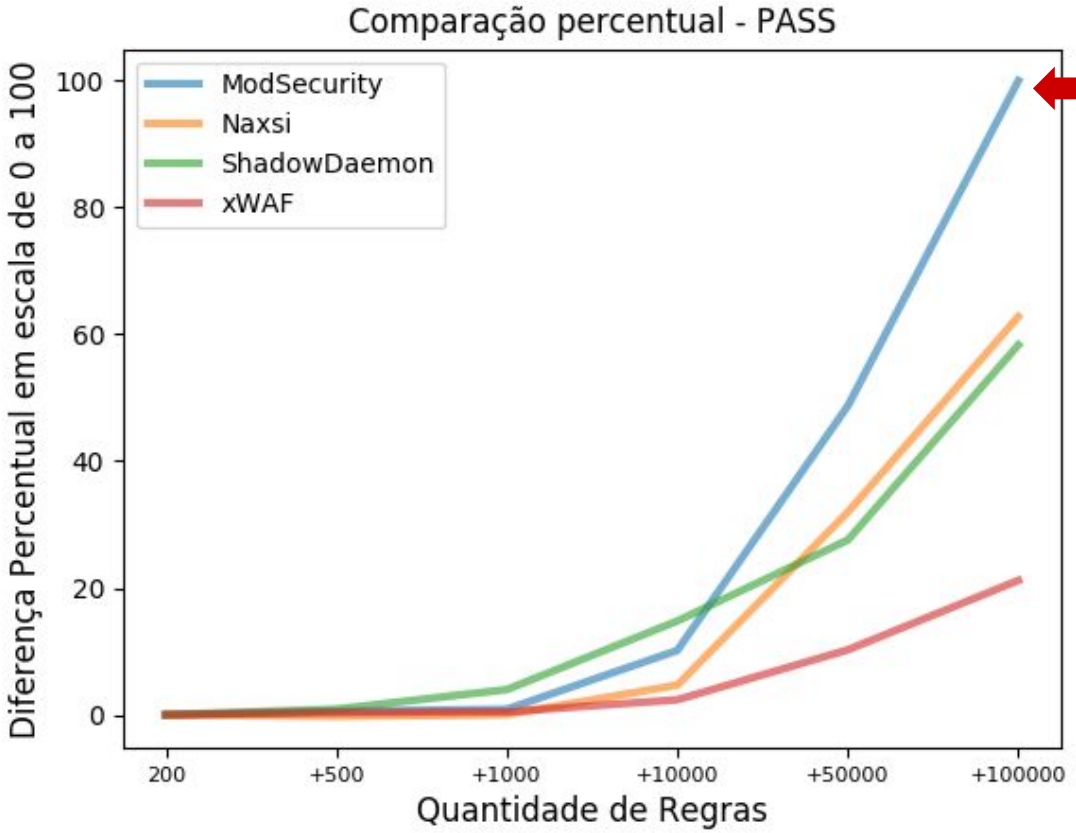
Resultados


Comparação percentual - PASS
ModSecurity
Naxsi
ShadowDaemon
xWAF
Diferença Percentual em escala de 0 a 100
0
20
40
60
80
100
200
+500
+1000
+10000
+50000
+100000
Quantidade de Regras

Resultados

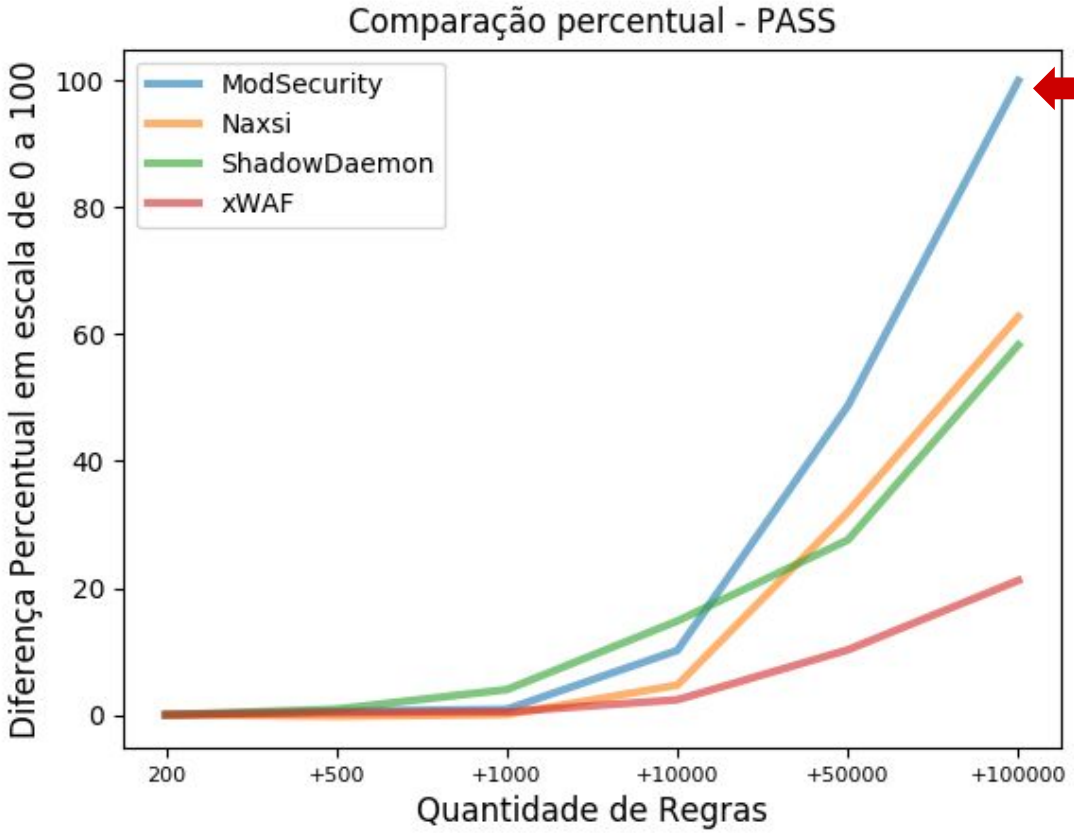

Comparação percentual - PASS
ModSecurity
Naxsi
ShadowDaemon
xWAF
Diferença Percentual em escala de 0 a 100
100
80
60
40
20
0
200
+500
+1000
+10000
+50000
+100000
Quantidade de Regras

Resultados



1.66 ms
40.69 ms

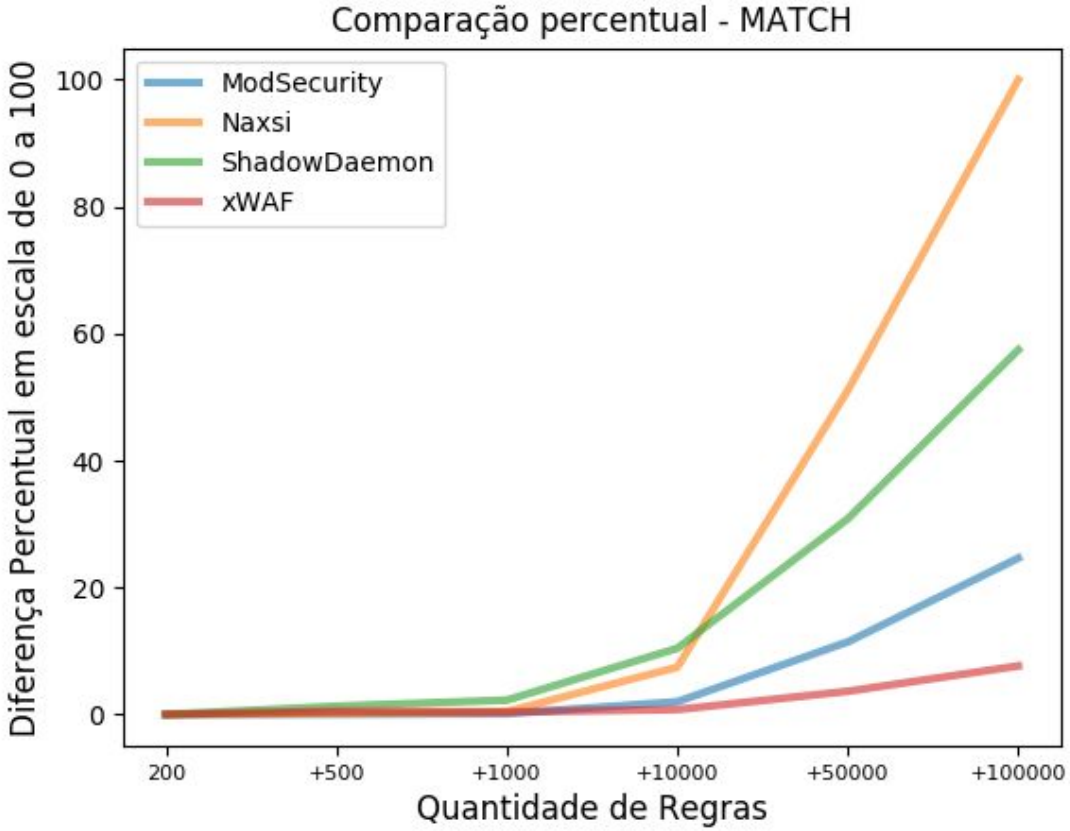
Resultados



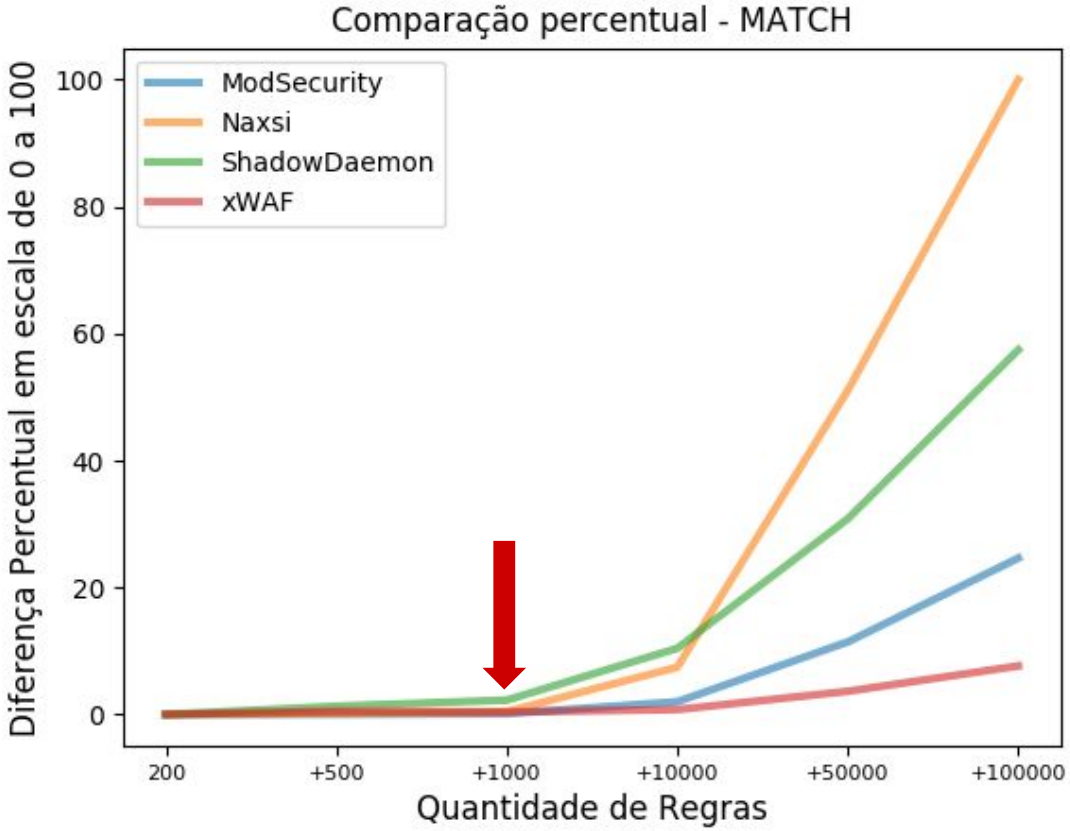
1.66 ms
40.69 ms

2367%

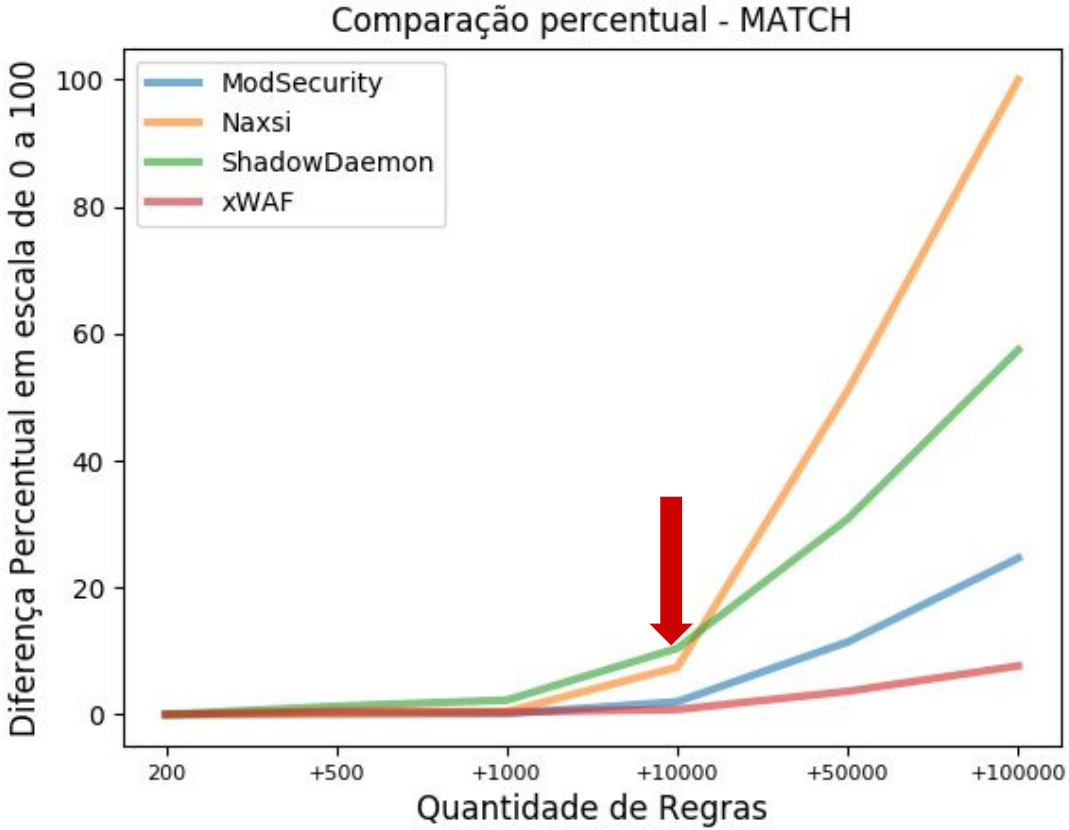
Resultados


Comparação percentual - MATCH
ModSecurity
Naxsi
ShadowDaemon
xWAF
Diferença Percentual em escala de 0 a 100
100
80
60
40
20
0
200
+500
+1000
+10000
+50000
+100000
Quantidade de Regras

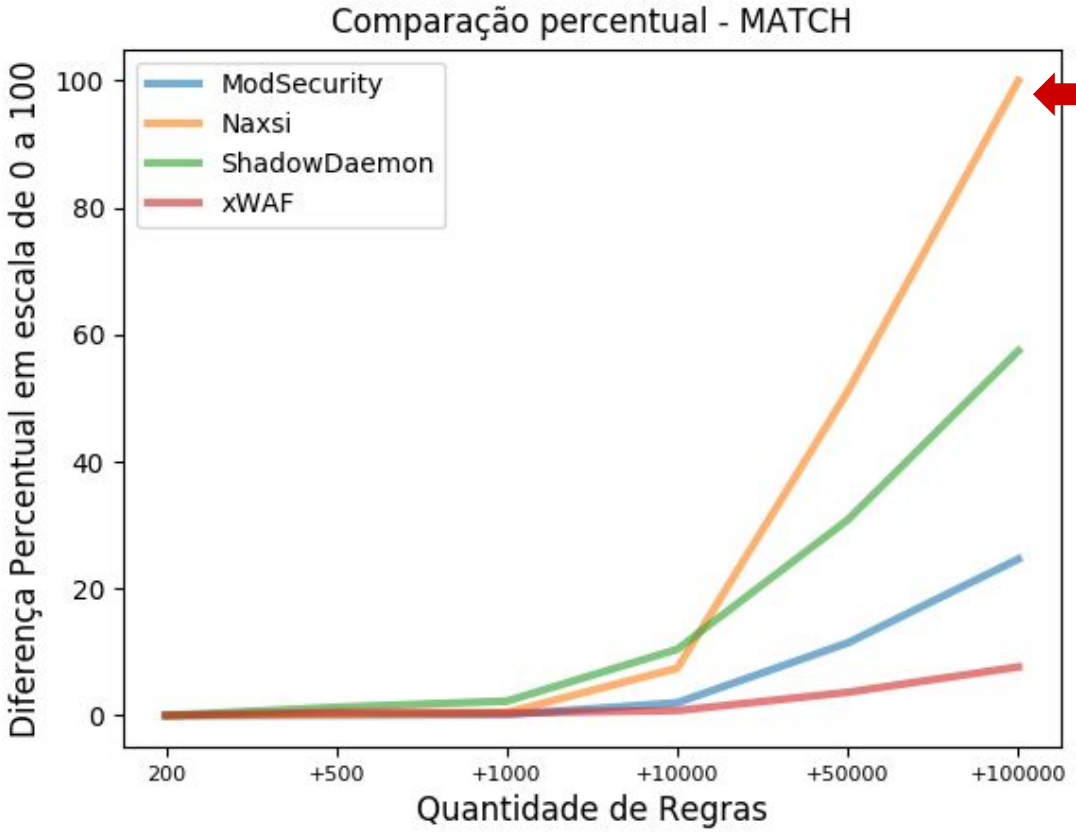
Resultados


Comparação percentual - MATCH
ModSecurity
Naxsi
ShadowDaemon
xWAF
Diferença Percentual em escala de 0 a 100
100
80
60
40
20
0
200
+500
+1000
+10000
+50000
+100000
Quantidade de Regras

Resultados

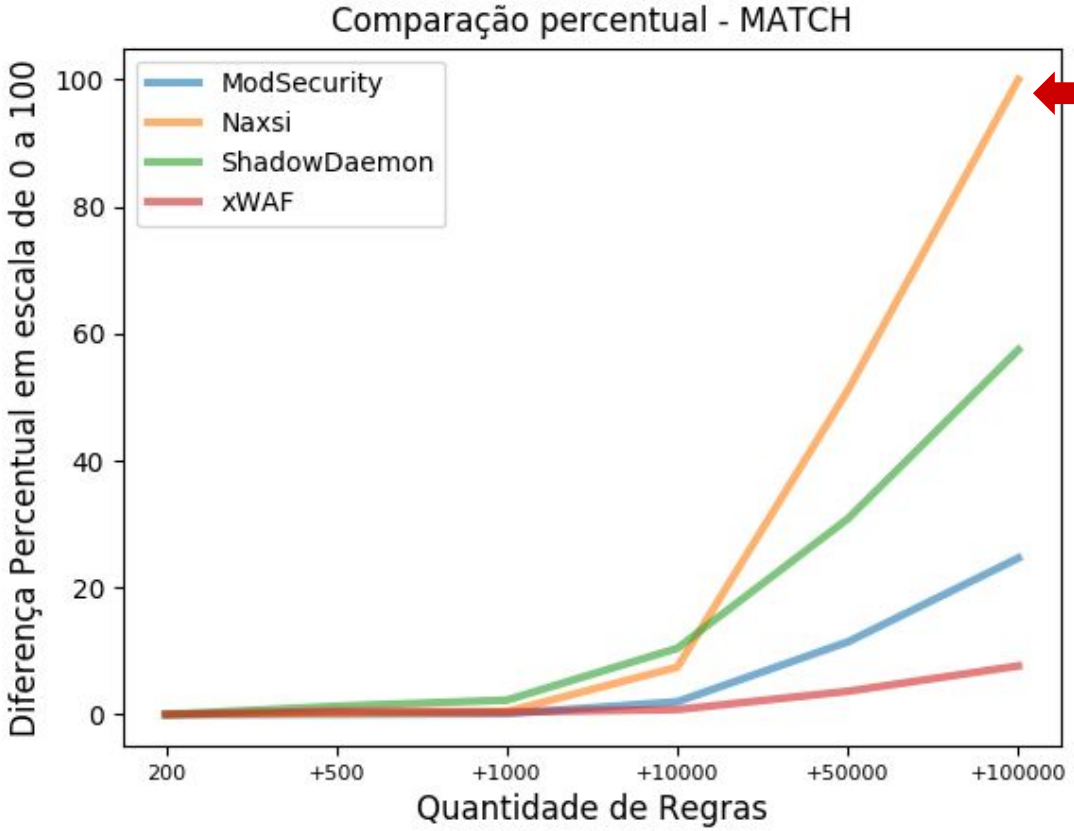

Comparação percentual - MATCH
ModSecurity
Naxsi
ShadowDaemon
xWAF
Diferença Percentual em escala de 0 a 100
100
80
60
40
20
0
200
+500
+1000
+10000
+50000
+100000
Quantidade de Regras

Resultados



1.21 ms
23.75 ms

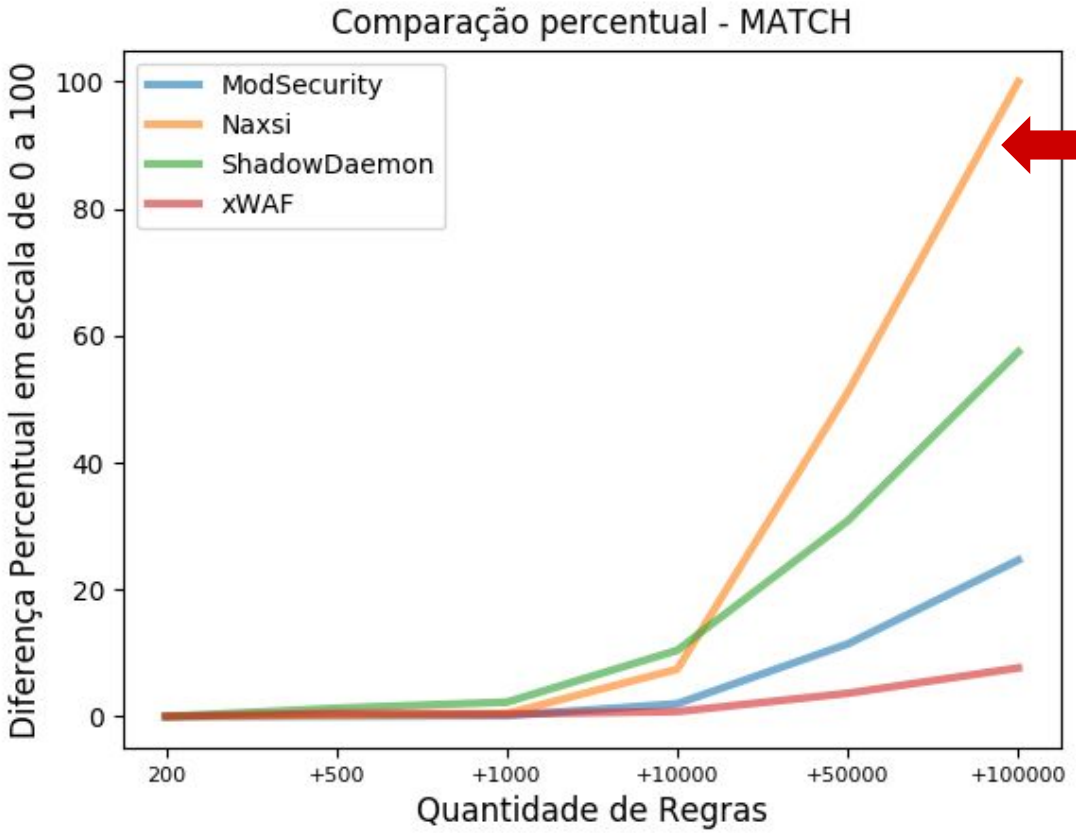
Resultados



1.21 ms
23.75 ms

1862%

Resultados



Problema na *engine*?

WAFs

Estudos sobre WAFs

Desenvolvimento

Resultados

Considerações Finais

Considerações Finais

Grande impacto da quantidade de regras na latência

Usuários comuns são mais prejudicados

Obrigado!

Contato:
fehmel@gmail.com

Figuras retiradas do site flaticon.com

Web Application Firewalls (WAFs): o impacto do número de regras na latência das requisições Web

Felipe Homrich Melchior

WRSeg - 2019