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

Felipe Melchior[1,3], **Diego Kreutz**[1,2,3], **Mauricio Fiorenza**[2,3]

[1]Laboratório de Estudos Avançados (LEA)
[2] Mestrado Profissional em Engenharia de Software (MPES)
[3] Universidade Federal do Pampa (UNIPAMPA)
fehmel@gmail.com,{Nome.Sobrenome}@unipampa.edu.br

Abstract. *Specialized reports indicate that nearly 90% of applications available on the Internet have some kind of vulnerability. Luckily, recent findings show that WAFs (Web Application Firewalls) and software development frameworks can be useful tools for detecting and preventing the exploitation of over 70% of the most common vulnerabilities found in Web applications. In this work, we provide an overview of existing research on WAFs and we also empirically evaluate the impact of the number of active rules on the latency of Web requests. Our findings show that the number of rules of a WAF has a significant impact on the latency of Web requests, increasing over 2000% for 100k rules.*

Resumo. *Relatórios especializados indicam que aproximadamente 90% das aplicações disponibilizadas na Internet apresenta algum tipo de vulnerabilidade. Felizmente, estudos recentes demonstram que frameworks de desenvolvimento de software e WAFs (Web Application Firewalls) podem ajudar a detectar e impedir a exploração de mais de 70% das vulnerabilidades mais recorrentes em aplicações Web. Este trabalho tem como objetivo realizar um levantamento do estado da arte de WAFs e uma avaliação empírica do impacto da quantidade de regras ativas na latência das requisições Web. Os resultados experimentais demonstram que o número de regras de um WAF tem um impacto significativo na latência das requisições Web, ultrapassando 2000% para 100 mil regras.*

1. Introdução

O número de ataques e incidentes de segurança não para de crescer. Grande parte dos ataques explora vulnerabilidades de sistemas utilizados por múltiplas instituições. Por exemplo, recentemente (em julho de 2019), mais de 60 universidades e colégios dos Estados Unidos foram comprometidos devido a um conjunto de vulnerabilidades existentes num único sistema [Machado et al. 2019]. Outro exemplo recente, em junho de 2019, foram descobertas, por técnicos de uma prefeitura do RS, diferentes vulnerabilidades críticas em um sistema Web utilizados por várias prefeituras municipais do estado.

Um dos principais problemas que tem levado a essa onda crescente de incidentes de segurança é a falta de formação e conhecimento na área. Por exemplo, estudos recentes apontam que ferramentas de segurança, como os *Web Application Firewalls* (WAFs), podem contribuir significativamente na proteção de sistemas contra a exploração das vulnerabilidades mais recorrentes em aplicações Web. Um WAF é um serviço de segurança implementado entre o cliente (e.g. navegador/browser) e a aplicação (e.g. sistema PHP rodando num servidor Web Apache). A função do WAF é interceptar e processar as

requisições entre o cliente e a aplicação. A partir de um conjunto de regras, o WAF classifica as requisições em maliciosas, que são geralmente bloqueadas, e não-maliciosas, isto é, que são encaminhadas até a aplicação. Um WAF como o ModSecurity, na configuração padrão, ou seja, sem nenhuma otimização, associado a um *framework Hypertext Preprocessor* (PHP) como o Laravel, é capaz de mitigar em 70% a exploração de vulnerabilidades recorrentes em sistemas Web [Ferrão 2018].

Há diferentes desafios e oportunidades de pesquisa no contexto de WAFs, como algoritmos para detectar ataques que objetivam explorar vulnerabilidades específicas (e.g. *cross-site request forgery* (CSRF) e *cross-site scripting* (XSS)) [Srokosz et al. 2018, Rao et al. 2016], mecanismos para aumentar o desempenho de processamento de requisições em cenários com grandes volumes de requisições (e.g. milhares de requisições por segundo) [Moosa and Alsaffar 2008] e análises empíricas de funcionalidades e WAFs disponíveis no mercado [Clincy and Shahriar 2018, Razzaq et al. 2013].

Os objetivos deste trabalho são revisar o estado da arte e avaliar empiricamente o impacto de WAFs na latência das requisições Web. Para atingir os objetivos, foram investigados trabalhos relacionados existentes na literatura e WAFs disponíveis gratuitamente no mercado. Resumidamente, as contribuições deste trabalho são: (a) uma síntese do estado da arte; e (b) uma avaliação do impacto da quantidade de regras dos WAFs ModSecurity[1], Naxsi[2], ShadowDaemon[3] e xWAF[4] na latência das requisições Web. Os resultados dos testes experimentais indicam que há um impacto significativo na latência das requisições Web, que aumenta de acordo com o número de regras do WAF, podendo ultrapassar 2000% para 100k regras.

O restante do trabalho está organizado como segue. A Seção 2 apresenta uma revisão do estado da arte. Nas Seções 3, 4 e 5 são apresentados o desenvolvimento do trabalho, os resultados e as considerações finais, respectivamente.

2. Trabalhos Relacionados

A Tabela 1 resume as principais contribuições, oportunidades de pesquisa e evidências empíricas de trabalhos relacionados a WAFs. Com relação à **Principal Contribuição**, há diferentes propostas de novos algoritmos para de detecção de ataques a vulnerabilidades específicas (e.g. CSRF e XSS). Por exemplo, ataques que visam explorar vulnerabilidades XSS podem ser bloqueados através da análise e identificação de padrões (e.g. caracteres "<" e ":") utilizados em requisições maliciosas aos sistemas Web [Rao et al. 2016].

Outro exemplo são as boas práticas na criação de novas regras para um WAF. O primeiro passo é entender o objetivo da regra que está sendo criada [Clincy and Shahriar 2018]. Isto é crucial para o correto funcionamento e bom desempenho de um WAF. Por exemplo, uma regra estática, que bloqueia ataques de *SQL Injection* que utilizam a expressão "' OR 1=1– #", não irá bloquear um ataque que utilize a expressão "' OR 2=2– #".

A maioria dos estudos indica de forma explícita ou implícita **Oportunidades de Pesquisa** como implementar novas heurísticas para melhorar a taxa de detecção de WAFs

[1] `https://modsecurity.org`
[2] `https://github.com/nbs-system/naxsi`
[3] `https://shadowd.zecure.org`
[4] `https://github.com/Alemalakra/xWAF`

Tabela 1. Trabalhos Relacionados

	Principal Contribuição	**Oportunidades de Pesquisa**	**Evidências Empíricas**
[Funk et al. 2018]	Aumento na taxa de detecção de ataques	Comparar com outros WAFs	Taxa de detecção 60% maior que o ModSecurity
[Srokosz et al. 2018]	Detecção de ataques *CSRF*	Implementar e avaliar os algoritmos	
[Rao et al. 2016]	Detecção de ataques *XSS*	Implementar e avaliar os algoritmos	
[Moosa and Alsaffar 2008]	WAF híbrido, usando heurísticas	Evoluir o WAF com novas heurísticas	WAF suporta um grande volume de requisições
[Razzaq et al. 2013]	Comparação analítica de quinze WAFs tradicionais	Comparar empiricamente os WAFs	
[Clincy and Shahriar 2018]	Boas práticas para criação de regras	Avaliar configurações padrão de WAFs	
[Rietz et al. 2016]	Visão de WAF no estado atual da Internet	Avaliar WAFs em cenários controlados	
[Singh et al. 2018]	Análise dos níveis de Paranoia do ModSecurity	Avaliar diferentes configurações	Maior taxa de detecção e de falsos positivos
[Ferrão 2018]	Avaliação de três WAFs em cenários controlados	Analisar outros WAFs	ModSecurity mitiga até 70% das vulnerabilidades

e avaliar a eficácia e o desempenho dos WAFs através de estudos empíricos. Um dos principais objetivos deste trabalho é justamente avaliar empiricamente diferentes WAFs com relação ao impacto do número de regras na latência das requisições Web.

As **Evidências Empíricas** são dados concretos que permitem melhor avaliar e validar uma pesquisa [Explorable 2009]. Por exemplo, o ModSecurity, em combinação com *frameworks* de desenvolvimento, é capaz de mitigar até 70% dos ataques que exploram as vulnerabilidades recorrentes em aplicações Web [Ferrão 2018]. Indo um pouco além, resultados recentes de pesquisa indicam que implementações específicas de WAFs podem atingir uma eficácia de detecção até 60% maior que a do ModSecurity [Funk et al. 2018]. Entretanto, como pode ser observado na tabela, a maioria dos trabalhos não apresenta evidências empíricas sobre os algoritmos ou mecanismos propostos.

3. Desenvolvimento

O desenvolvimento do trabalho pode ser dividido nas seguintes etapas:

Etapa 1: Seleção dos WAFs ModSecurity, Naxsi, ShadowDaemon e xWAF, utilizando os seguintes parâmetros: (a) WAFs *standalone*, (b) gratuitos e (c) de código aberto.

Etapa 2: Preparação e instalação de máquinas virtuais, uma para cada WAF, com 1 vCPU, 2GbB de RAM e a distribuição Linux Ubuntu Server 16.04. A máquina hospedeira possui processador i5 7300-HQ *quad-core* de 2.5GHz, 8GB de memória RAM, disco rígido *Western Digital*, modelo WD10SPZX, controladora HM170/QM170 Chipset SATA de 6.0GHz, com 5400 rotações por minuto e cache de 128MB, executando a distribuição Linux Manjaro versão 18.0.4 e o VirtualBox na versão 6.0.6.

Etapa 3: Instalação dos WAFs seguindo a documentação de cada ferramenta. O ModSecurity foi instalado através do gerenciador de pacotes do Ubuntu, enquanto que o Naxsi

e o ShadowDaemon foram instalados a partir do código fonte, disponível no site oficial dos respectivos WAFs. Já no caso do xWAF, que é implementado em PHP, foi necessário adicionar o arquivo da ferramenta ao parâmetro `auto_prepend_file` do arquivo de configuração do PHP (`php.ini`) do servidor Apache. Isto faz com que o código do xWAF seja automaticamente incluído no início de cada arquivo PHP da aplicação.

Etapa 4: Instalação da aplicação Web PHP que implementa as dez vulnerabilidades mais recorrentes em sistemas Web segundo a OWASP [Ferrao et al. 2018]. Para executar a aplicação, foi utilizado o PHP versão 7.0.3, o MySQL versão 5.7.25 e o servidor Web Apache (versão 2.4.18), exceto no caso do WAF Naxsi, que é compatível apenas com o servidor Web Nginx (foi utilizada a versão 1.13.1).

Etapa 5: Teste de funcionamento dos WAFs através da criação de uma regra que bloqueia requisições específicas provenientes do comando `curl` do Linux. Utilizando como exemplo o ModSecurity, a regra utiliza o arquivo `curl.txt`, que contém uma lista dos `User-Agents` (e.g. *curl/7.64.1*), um por linha, do comando `curl`. O WAF bloqueia (`deny` no algoritmo) e registra (`log`) todas as requisições cujo cabeçalho contém um `User-Agent` listado no arquivo `curl.txt`. Ao bloquear uma requisição, o WAF registra o motivo do bloqueio (`msg`) e os detalhes da solicitação, como URL da requisição e endereço IP do cliente, por fim, retorna como resposta ao cliente o código HTTP 403 (`status`), que significa que a solicitação foi entendida pelo servidor, porém não será atendida.

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

4. Resultados

Ao instalar um WAF, o administrador do sistema deve analisar as necessidades da aplicação e configurar o WAF de acordo, incluindo regras próprias para ataques específicos ou aumentando o número de regras ativas, por exemplo [Rao et al. 2016, Clincy and Shahriar 2018]. Enquanto que, por um lado, um número maior de regras ativas pode levar a uma maior capacidade de detecção, por outro lado, isto pode impactar a latência de processamento das requisições Web.

Com o objetivo de identificar o impacto do número de regras na latência das requisições, em diferentes WAFs, foi implementado um programa em Python utilizando a biblioteca `Requests` [5]. O programa simula dois tipos de usuários, um não malicioso e outro malicioso. Enquanto que as requisições do primeiro não são bloqueadas (**Pass**), as do segundo são bloqueadas (**Match**) pelo WAF.

Os WAFs e o sistema Web (cenário controlado) foram virtualizados, enquanto que o programa Python foi executado a partir da máquina hospedeira. Na Tabela 2, a latência de uma requisição (em milissegundos) representa a média aritmética de mil requisições. Vale ressaltar que, inicialmente, os WAFs foram configurados com 200 regras ativas e as regras que bloqueiam as requisições dos agentes maliciosos foram inseridas no início do

[5]Scripts utilizados nos testes: `https://bit.ly/2LcaF8m`

conjunto de regras de cada WAFs. Posteriormente, foram adicionadas novas regras ao conjunto.

Tabela 2. Tempo de acesso de acordo com a quantidade de regras

	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

Os resultados mostram que, por via de regra, o usuário não malicioso acaba sendo o mais prejudicado com o aumento do número de regras ativas. Isto ocorre devido ao fato de uma requisição normal (**Pass**) ser analisada e processada por todas as regras ativas. Por outro lado, uma solicitação maliciosa é bloqueada na primeira regra que identificar o ataque (i.e. primeiro **Match**).

Com o aumento progressivo no número de regras, o ModSecurity passou de 1.66ms (200 regras) para cerca de 40ms de latência (100k regras), o que representa um aumento percentual aproximado de 2.350%. Este aumento, somado ao tempo de latência da rede de um usuário, pode impactar o desempenho do sistema e a experiência do usuário. Como pode ser facilmente observado na tabela, o ModSecurity é o WAF que mais impactou na latência das requisições Web. Já o xWAF resultou no menor aumento de latência até 100k regras, atingindo apenas 10ms, o que representa um aumento de cerca de 500%. Entretanto, mesmo no caso do xWAF, o aumento na latência das requisições Web é significativo. Vale também ressaltar que o xWAF funciona apenas com sistemas PHP.

Nos experimentos com requisições bloqueadas pelos WAFs (**Match**), a ferramenta Naxsi chegou a uma latência aproximada de 24ms na detecção dos ataques. Adicionalmente, este WAF atingiu também o maior aumento percentual no caso do **Match**, chegando a 1.800%. Enquanto isso, o xWAF aumentou percentualmente a latência das requisições em apenas 150%.

Tanto no caso do usuário não malicioso, quanto no caso do agente malicioso, os menores tempos de latência (10ms e 4ms) e menores percentuais de aumento (500% para o **Pass** e 150% para o **Match**, respectivamente), de acordo com o número de regras, foram do xWAF. Esta latência significativamente menor do xWAF, para grandes números de regras, pode ser parcialmente explicada pelo fato de o código do xWAF ser incluído diretamente no código fonte das aplicações PHP. Este é um aspecto interessante para ser explorado em pesquisas futuras.

Como pode ser observado nos resultados da Tabela 2, ao se aproximar de 100k regras adicionais, a latência média das requisições fica próxima de 27ms utilizando o Naxsi. A título de comparação, considerando uma rede cabeada de fibra óptica e oito saltos, a latência de acesso ICMP ao servidor de resolução de nomes (DNS) do Google (endereço IP 8.8.8.8) é de cerca de 24ms. Neste exemplo, o WAF está simplesmente

dobrando o tempo de acesso a um serviço similar ao DNS da Google.

5. Conclusão

Neste trabalho foi realizado um levantamento do estado da arte e uma avaliação empírica dos WAFs ModSecurity, Naxsi, ShadowDaemon e xWAF. Os resultados mostram que há um impacto significativo na latência das requisições Web com o aumento do número de regras no WAF. Segundo os experimentos realizados, o melhor desempenho foi do xWAF, mantido e criado pela comunidade, com cerca de 10ms de latência para 100k regras. Entretanto, o xWAF é limitado a sistemas PHP e precisa ser adicionado ao código fonte. Já os WAFs ModSecurity, Naxsi e ShadowDaemon atingiram tempos de latência de aproximadamente 40ms, 27ms e 24ms, respectivamente.

Os resultados permitiram verificar, também, que os usuário não maliciosos são os mais prejudicados com o aumento no número de regras. Isto ocorre devido ao fato de as requisições do agente malicioso serem rejeitadas no primeiro **Match**, enquanto que as requisições dos demais usuários precisam ser processadas por todas as regras. Um dos objetivos futuros é aprofundar esta investigação através da análise de diferentes parâmetros de configuração ou implementação dos WAFs e analisar o consumo de recursos computacionais afim de identificar possíveis gargalos no uso de cada mecanismo. Por fim, avaliar e propor mecanismos que penalizem também as requisições dos usuários maliciosos.

Referências

Clincy, V. and Shahriar, H. (2018). Web application firewall: Network security models and configuration. In *IEEE 42nd Annual COMPSAC*, volume 01, pages 835–836.

Explorable (2009). Evidencia empirica. `https://bit.ly/2UaKa7j`.

Ferrao, I. G., de Macedo, D. D. J., and Kreutz, D. (2018). Investigação o do impacto de frameworks de desenvolvimentode software na segurança de sistemas web. In *16a Escola Regional de Redes de Computadores (ERRC)*. `https://bit.ly/2WQAfZd`.

Ferrão, I. G. (2018). Análise black-box de ferramentas de segurança na web. Trabalho de conlusão de curso, Universidade Federal Do Pampa. `https://bit.ly/2XjhblU`.

Funk, R., Epp, N., and A., C. C. (2018). Anomaly-based Web Application Firewall using HTTP-specific features and One-Class SVM. *ReABTIC*, 2(1).

Machado, R. B., Kreutz, D., Paz, G., and Rodrigues, G. (2019). Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados. In *4o WRSeg*. SBC. `http://tiny.cc/wrseg19-dl`.

Moosa, A. and Alsaffar, E. M. (2008). Proposing a Hybrid-intelligent Framework to Secure e-Government Web Applications. In *Proceedings of the 2nd ICEGOV*, pages 52–59. ACM.

Rao, G. R. K., Prasad, R. S., and Ramesh, M. (2016). Neutralizing cross-site scripting attacks using open source technologies. In *ICTCS*, pages 24:1–24:6. ACM.

Razzaq, A., Hur, A., Shahbaz, S., Masood, M., and Ahmad, H. F. (2013). Critical analysis on web application firewall solutions. In *IEEE 11th ISADS*, pages 1–6.

Rietz, R., König, H., Ullrich, S., and Stritter, B. (2016). Firewalls for the web 2.0. In *IEEE QRS*.

Singh, J. J., Samuel, H., and Zavarsky, P. (2018). Impact of Paranoia Levels on the Effectiveness of the ModSecurity Web Application Firewall. In *ICDIS*, pages 141–144.

Srokosz, M., Rusinek, D., and Ksiezopolski, B. (2018). A New WAF-Based Architecture for Protecting Web Applications Against CSRF Attacks in Malicious Environment. In *FedCSIS*.