

# Web Application Firewalls

Jerônimo Zucco  
[jeronimo.zucco@owasp.org](mailto:jeronimo.zucco@owasp.org)



# Jerônimo Zucco

- CISSP - Certified Information Systems Security Professional
- Blog: <http://jczucco.blogspot.com>
- Twitter: @jczucco
- <http://www.linkedin.com/in/jeronimozucco>
- [http://www.owasp.org/index.php/User:Jeronimo\\_Zucco](http://www.owasp.org/index.php/User:Jeronimo_Zucco)



Onde os dados estão ?



Quem acessa os dados ?



Onde estão as  
aplicações ?





# O NOVO PERÍMETRO



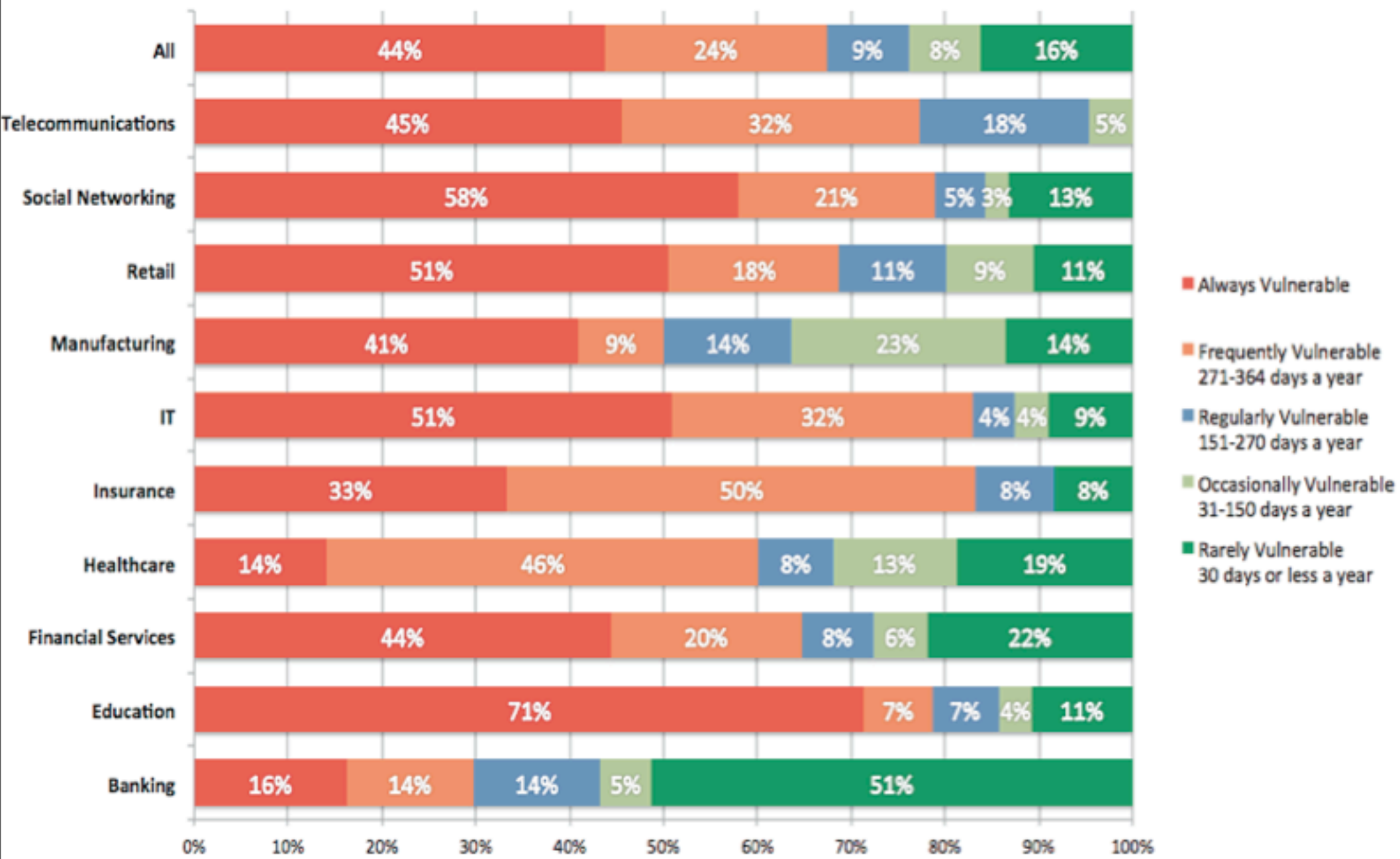
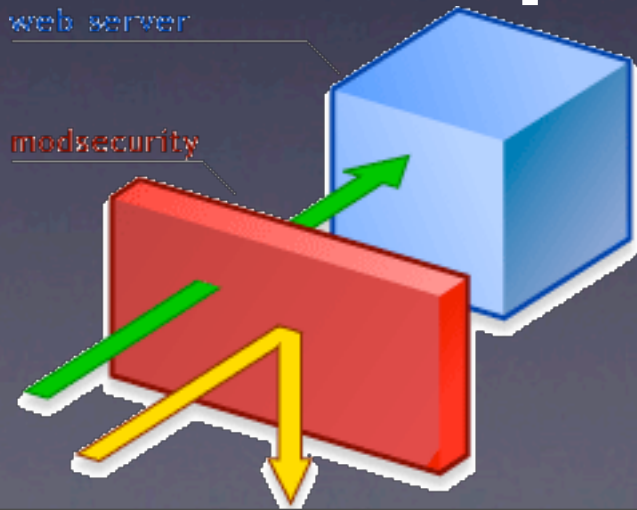


Figure 2. Window of Exposure by Industry (2010)

Fonte: WhiteHat Website Security Statistics Report

# WAF ?

Dispositivo (Camada 7)  
especializado em  
aplicações Web





# Capacidade de detectar e bloquear ataques

- Ataques Diretos
- Ataques Indiretos
- Modelo Positivo
- Modelo Negativo
- Modo de Aprendizagem



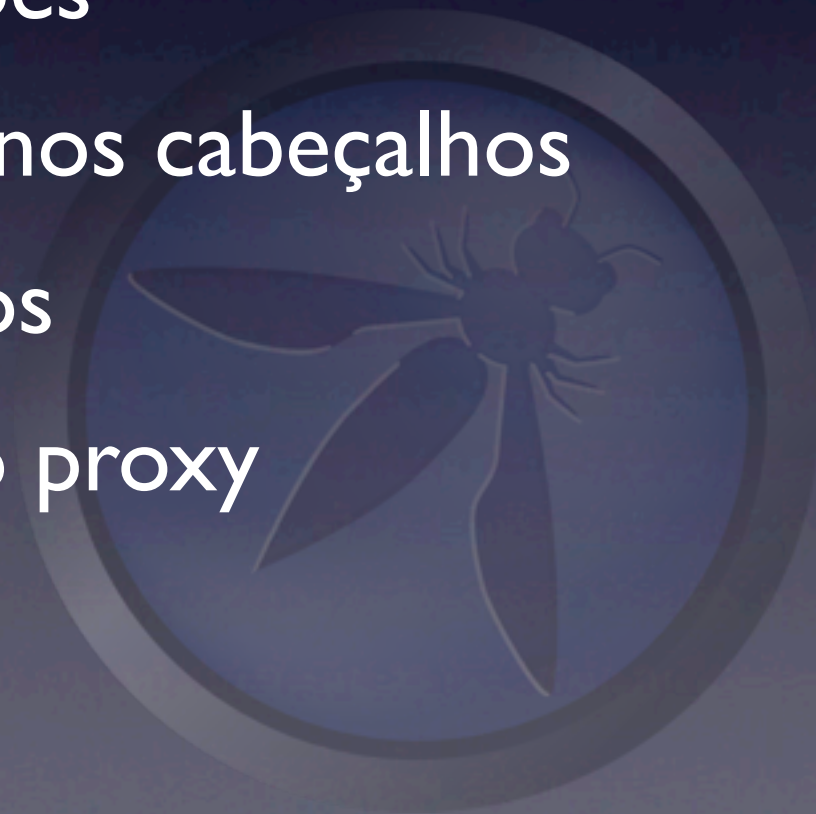
# Detecção

- Inspecciona cabeçalho e o corpo da requisição
- Inspecciona cabeçalho e corpo da resposta
- Inspeção de arquivos upload



# Violação de protocolo

- Vulnerabilidades do protocolo
- Tamanho das requisições
- Caracteres não ASCII nos cabeçalhos
- Validação de cabeçalhos
- Tentativa de uso como proxy



# Políticas

- Whitelists
- Tamanho do request/upload
- Restrição de métodos (WebDAV, CONNECT, TRACE, DEBUG)
- Extensão de arquivos



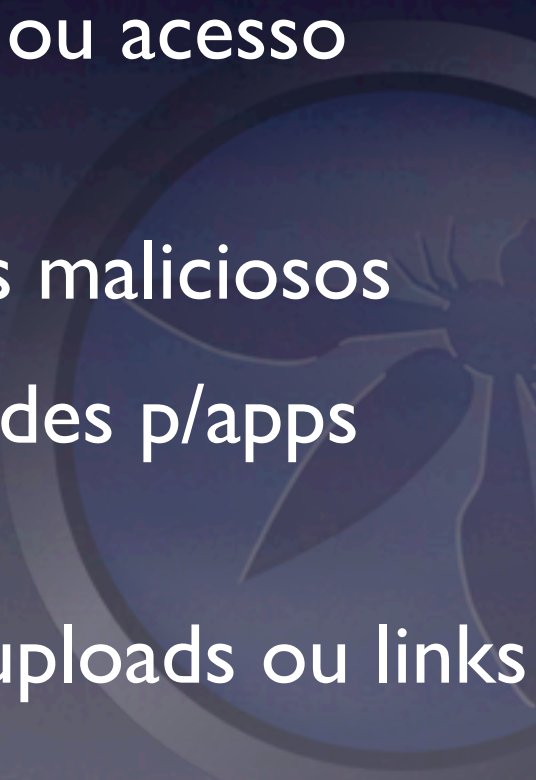
# Cientes Maliciosos

- Comentários SPAM
- Blacklists
- Scanners





# Ataques na Aplicação

- SQL injection e blind SQL injection
  - Cross site scripting (XSS)
  - Injeção de comando no SO ou acesso remoto
  - Inclusão remota de arquivos maliciosos
  - Assinaturas de vulnerabilidades p/apps conhecidas
  - Detecção de malware em uploads ou links maliciosos
- 

# Virtual Patching

- Correção de um erro da aplicação através de criação de regra no WAF
- Correções rápidas
- Zero Days
- Aplicações fechadas
- Custo para correção



# Vazamento de Informação

- Última linha de defesa
- Vazamento de informações (Nro. Cartão de crédito, CPF, etc)
- Erros HTTP
- Informações do Banco de Dados
- Stack Dumps



# Debug

- Detecção de erros na aplicação
- Reprodução de eventos
- Registro de eventos
- Auxílio no debug de aplicação



# WAFs Comerciais

- WebDefend - Trustwave
  - SecureSphere - Imperva
  - Hyperguard - Art of Defence
  - Barracuda Web Application Firewall
  - Cisco ACE Web Application Firewall
- 



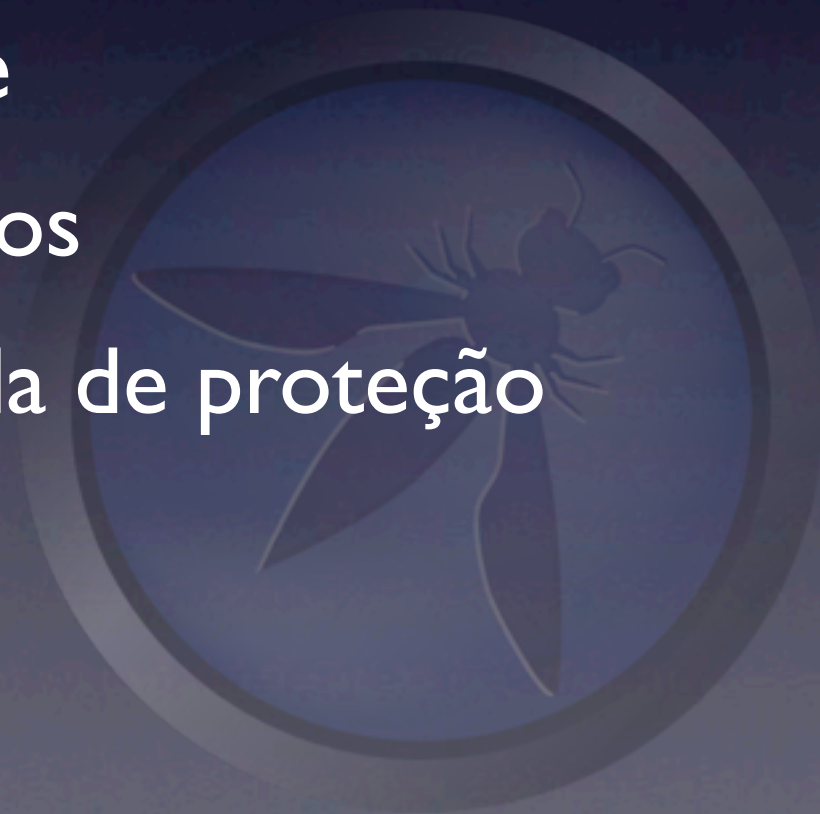
# WAFs Código Aberto

- ModSecurity - Trustwave
- WebKnight - Aqtronix (dll IIS)
- IronBee - Qualys



# Conclusões

- Porque não corrigir a aplicação ?
- Impacto na performance
- Falso positivos e negativos
- WAF = Mais uma camada de proteção



# Referências

- Web Application Firewall Evaluation Criteria (WAFEC) - <http://is.gd/kYpTjO>
  - Web Application Security Consortium - <http://www.webappsec.org>
  - OWASP Best Practices: Web Application Firewalls - <http://is.gd/Uat2Lw>
  - OWASP Securing WebGoat using ModSecurity - <http://is.gd/imfq0z>
- 

Perguntas ?







# AppSec Brasil '11

1st Global Appsec Latin  
America Conference

Porto Alegre - Rio Grande do Sul

<http://www.appseclatam.org>



Obrigado !

[jeronimo.zucco@owasp.org](mailto:jeronimo.zucco@owasp.org)

