



# Best Practices Guide: Web Application Firewalls

Alexander Meisel  
art of defence

## OWASP German Chapter

Copyright © The OWASP Foundation  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the OWASP License.

**The OWASP Foundation**  
<http://www.owasp.org>

# Big “Thank you!!!” to the Authors

- **Maximilian Dermann**
  - ▶ Lufthansa Technik AG
- **Mirko Dziadzka**
  - ▶ art of defence GmbH
- **Boris Hemkemeier**
  - ▶ OWASP German Chapter
- **Achim Hoffmann**
  - ▶ SecureNet GmbH
- **Alexander Meisel**
  - ▶ art of defence GmbH
- **Matthias Rohr**
  - ▶ SecureNet GmbH
- **Thomas Schreiber**
  - ▶ SecureNet GmbH

# Contents

- Introduction and aim
- Characteristics of web apps with regards to security
- Overview of what WAFs can do
- Benefits and risks of WAFs
- Protection against the OWASP TOP 10 (App vs. WAF vs. Policy)
- Criteria for deciding whether or not to use WAFs
- Best practices for introduction and operation of WAFs

# Introduction and aim

## ■ Introduction

- ▶ Online Businesses
- ▶ Weak spot HTTP
- ▶ Reference to PCI DSS

## ■ Definition of the term “Web Application Firewall”

- ▶ NOT a Network Firewall
- ▶ Not only Hardware

## ■ Targeted audience

- ▶ Technical decision-makers
- ▶ People responsible for operations and security
- ▶ Application Owners

# Characteristics of web applications with regards to security

## ■ Higher level aspects in the company

- ▶ Prioritizing Web Apps in regard to their importance
  - Access to personal customer data
  - Access to (confidential) company information
    - Image loss
  - Certifications

## ■ Technical Aspects

- ▶ Test and quality assurance
- ▶ Documentation
- ▶ Vendor-Contracts

# Overview of what WAFs can do

- Where do WAFs fit into the Web App Sec field
  - ▶ WAFs are part of a solution
  - ▶ Main benefits of a WAF
  - ▶ Additional functionality
- What can be archived with WAFs
  - ▶ Table with (wanted) functionality
    - examples: CSRF, Session fixation, \*-Injection
  - ▶ Rating / Evaluation:
    - + can be very well implemented using a WAF
    - - can not be implemented
    - ! depends on the WAF/application/requirements
    - = can partly be implemented with a WAF

# Benefits and risks of WAFs (I)

## ■ Main benefits of WAFs

- ▶ Base line security
- ▶ Compliance
- ▶ Just-in-time patching of problems

## ■ Additional benefits of (depending on functionality)

- ▶ Central reporting and error logging
- ▶ SSL termination
- ▶ URL-Encryption
- ▶ ....

# Benefits and risks of WAFs (II)

## ■ Risks involved using WAFs

- ▶ False positives
- ▶ Increased complexity
- ▶ Yet another proxy
- ▶ Potential side effects if the WAF terminates the application

# Protection against the OWASP TOP 10

## App vs. WAF vs. Policy

- Three types of applications:
  - ▶ T1: Web application in design phase
  - ▶ T2: Already productive app which can easily be changed (e.g. with MVC architecture)
  - ▶ T3: Productive app which cannot be modified or only with difficulty
- Table of OWASP TOP 10 in regards to work required with the 3 types of application to fix the problem
  - ▶ in the application itself
  - ▶ using a WAF
  - ▶ using a policy

# Criteria for deciding whether or not to use Web Application Firewalls (I)

## ■ Company wide criteria:

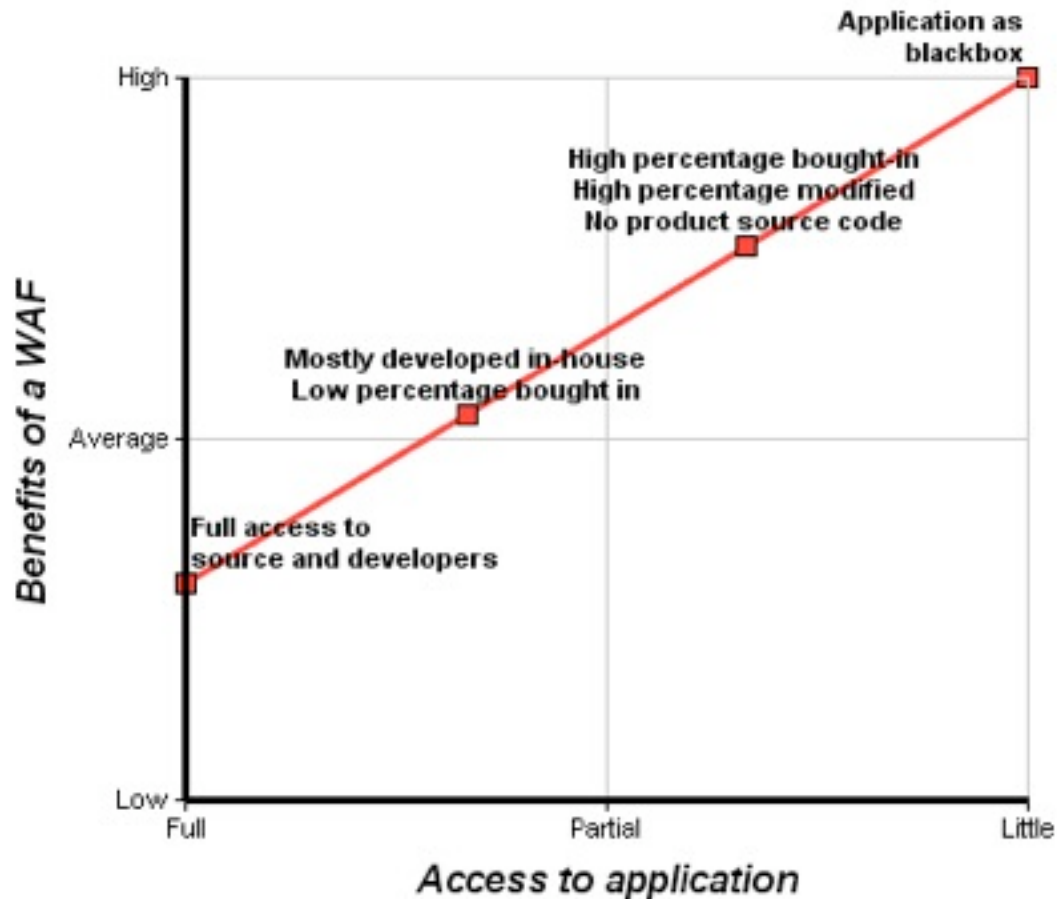
- ▶ Importance of the app for the success of the company
- ▶ Number of web applications
- ▶ Complexity
- ▶ Operational costs
- ▶ Performance and scalability

# Criteria for deciding whether or not to use Web Application Firewalls (II)

- Criteria with regard to the web application
  - ▶ Changeability of the application
  - ▶ Documentation
  - ▶ Maintenance contracts
  - ▶ Time required fixing bugs in third-party products
- Consideration of financial aspects
  - ▶ Avoidance of financial damage via successful attacks
  - ▶ Costs of using a WAF
    - License costs
    - Update costs
    - Project costs for evaluation and introducing a WAF
    - Volume of work required / Personnel costs

# Criteria for deciding whether or not to use Web Application Firewalls (II)

## ■ Evaluation and Summary



# Best practices for introduction and operation of Web Application Firewalls (I)

## ■ Infrastructure

### ▶ Central or decentralized infrastructure

- central proxy application
- host based - plug-in approach
- virtualization !!???!!!

### ▶ Performance

- GBits/Second throughput on hardware does NOT matter
- HTTP requests processed per second is important
- Simultaneous web application users
- Think of peak load times (pre Christmas rush)

# Best practices for introduction and operation of Web Application Firewalls (II)

## ■ Organizational aspects

### ▶ Security Policies

- Try not to change security policies already in place

### ▶ Suggestion of new job position

- WAF application manager
  - One-off task of commissioning a WAF
  - In-depth knowledge of WAF capabilities
  - Alarm and Error management
  - Changes to the rule-set
  - Talking to the development department(s)

# Best practices for introduction and operation of Web Application Firewalls (III)

## ■ Iterative procedure

### ▶ Step 1

- Definition of the people responsible for security
  - ideally the “WAF application manager”

### ▶ Step 2

- Baseline security for all web applications
  - mostly blacklisting using vendor signatures
  - monitor for false positives/negatives and get rid of them

### ▶ Step 3

- Prioritized list of all web applications which need to be secured
  - Use the checklist (attached to the paper)

### ▶ Further Steps:

- Work through the list and systematically secure the app



# Appendices

- Checklist to define the 'accessibility' of the web application
  - ▶ The more points you score the, the better is the access to web application
- Job descriptions for the 'new guys'
  - ▶ WAF platform manager
    - needed in really complex/big environments
  - ▶ WAF application manager (per application)
  - ▶ Application manager

# Where to find on the net?

- OWASP Wiki of course

- ▶ [https://www.owasp.org/index.php/Best\\_Practices:\\_Web\\_Application\\_Firewalls](https://www.owasp.org/index.php/Best_Practices:_Web_Application_Firewalls)

# Questions

**Thank you!**

Alexander Meisel

[alexander.meisel@artofdefence.com](mailto:alexander.meisel@artofdefence.com)

