A Call for Drastic Action

A Survey of Web Application Firewalls

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- Jaeson Yoo, Head of Global Business
- Responsible for Penta's international business interests, for all regions/countries outside of Korea and Japan
- Management Consulting and Investment Banking background, with experience in IT security industry

Trust for an Open Society

Penta SECURITY

OWASP
The Open Web Application Security Project

AGENDA

- Penta Security Systems Inc.
- Web Application Firewalls: An Overview
- Why Aren’t WAFs More Prevalent?
- The Traditional Signature-Based Approach is Failing
- What WAF Solution is Needed?

OWASP
The Open Web Application Security Project

Penta Security Systems Inc.

Penta Security Systems Inc.

OWASP
The Open Web Application Security Project

Trust for an Open Society
Penta SECURITY

Founded	• July 1997
CEO/Founder	• Seokwoo Gregory Lee
Headquarters	• Seoul, Korea
Revenues	• US$ 18.4M (2012)
Employees	• 120+
Overseas	• Penta Security Systems, K.K.,Tokyo, Japan (subsidiary) • Thailand, Singapore, Australia, Malaysia, Indonesia (distributors)
Products	• WAPPLES (Web Application Firewall) • D'Amo (DB Encryption Solution) • ISSAC (PKI Solution) • ISign Plus (SSO Solution)

- Leading technology provider of Web Application Firewalls, DBMS Encryption Systems, and PKI Solutions.
- Our appliance based WAF holds 70%+ market share in the growing Korean WAF market, and we hold 60% of the Korean market share in the DBMS encryption market.
- Over 2,000 clients including: government, small and medium businesses, enterprise, academic organizations, and financial organizations (including banks, securities, insurance, and credit card companies).

Company History

OWASP
The Open Web Application Security Project

2008 ~ Present

2012
01. WAPPLES granted Japanese patent for its algorithm- based, application-layer attack detection engine.

2011
12. Joined the VMware TAP program and became a VMware Solution Provider
12. Launched KT WAF service with WAPPLES V-Series
12. D'Amo granted US patent for its query processing system and method for DB query encryption transformation
08. D'Amo received v2.3 SAP Certification SAP in Germany
06 Became an OWASP sponsor
02. Received the Competitive Power Software Company award from KISA
03. Green-Biz Authorized

2010
07. Received the International Security Leadership Achievements (ISLA) Leadership Award
02. Received the Competitive Power Software Company award from KISA

2009
12. Acquired certification of PCI-DSS conformance for WAPPLES
11. Received the 2009 award for Deployment of Innovative Technology
04. Received the New Software Grand Award for WAPPLES
01. Penta Security Systems K.K.(Japan) was established

2008
11. WAPPLES received the Intelligence Award
10. GS Caltex, SSO and DB security system built
07. CIS-CC received Validation Certification from NIS
07. D'Amo for DB2 was introduced
06. WAPPLES received Security Compatibility Certification
05. D'Amo SG was introduced
04. QUEST in Japan, became a contract agent of WAPPLES
01. WAPPLES became CC (Common Criteria) Certified


2010 ISLA Award


2009 New Software Grand Award


2009 Intelligence Award


2007 GS Certification

1997 ~ 2007

2007
04. WAPPLES received GS (Good Software) certification
03. DB Encryption Established in the Ministry of Foreign Affairs and Trade

2006
10. D'Amo for SQL Server was introduced
07. Local office in Japan was established
06. Selected as an Innovative Business (INNO-BIZ)
03. SCP, PKI-based Security Library, was introduced
01. D'Amo received GS (Good Software) Certification

2005
05. WAPPLES, Web Application Firewall, was introduced

2004
12 . Initiated sales of D'Amo in Japan
03 . D'Amo, DB Database Security Solution, was introduced

2003
08 . CIS received encryption certification from NIST
01. Received an award from the Korean government for realizing the e-Government project

2002
09. Established GPKI system with the Korean government

2001
09 . ISign EAM Solution was introduced

2000
06. Received the Grand Award in the Information field of Venture business

1999
07. Established the first DB security business in Korea

1998
09. Penta Security Lab was founded
08. Siren, Intrusion Detection System, was introduced
01. ISSAC, PKI Solution, was introduced

1997
08. Information Security Technical cooperation with POSTECH
07. Penta Security Systems was founded

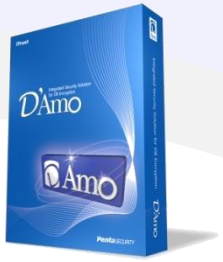
Penta Security Products

OWASP
The Open Web Application Security Project

Intelligent Web Application Firewall, WAPPLES

Leading WAF product in Korea with 70%+ market share

- Unique Logic Based Detection Engine
- Near-zero false positive detection rate, and immunity to unknown attacks
- Security Compatibility Certification from the Korean National Intelligence Service
- PCI-DSS Certificate of Conformity



WAPPLES

Amo

PKI Security Solution, ISSAC

The first PKI product in Korean meeting international technology standards

- User authentication is provided through the NPKI and GPKI systems
- Supports web session encryption and user authentication

ISSAC

PKI Development Toolkit, SCP

Cryptographic Module, CIS

Cryptographic function and security service development tool

- Supports embedded environment
- Able to support from PC to Mainframe

SCP

Integrated DB Security, D'Amo

No.1 Database Encryption Software in Korea since 2004 with 500+ customers of all sectors

- Runs on Oracle (Enterprise/Standard), MS SQL Server, DB2, and MySQL
- Supports various security configurationsthrough D'Amo SG and D'Amo SCP
- Enables realization of strong, compre-hensive DB security

SSO & EAM Solution, Isign Plus

The first SSO solution in Korea

- Single Sign On (SSO) solution for enterprise security since 2001
- Extranet Access Management based on RBAC (Role Based Access Control)

ISign

MySQL Encryption, MyDiamo

The world's first advanced encryption & access control solution for MySQL

- Open-source Software
- Offered as freeware to individuals with non-commercial interests, educational institutions
- One column of free encryption for all other users

MyDiamo

Select List of Clients

OWASP
The Open Web Application Security Project

International

Industrya	Customer
Online Shopping	AEON Mall
Data Center	DSR
Department Store	Shibuya109 Net Shop
Finance	Nissay Asset Management
Finance	Visa Credit Card Japan
Service Provider	Sanwa Comtech
Service Provider	ST-NET
Outsourcing	TECSEED Compass Inc
Education	Tokyo University of Agriculture
Government	Malaysia Ministry of Finance

Korea

Industry	Customer
Manufacturing	BMW Korea
Banking	HSBC Korea
Insurance	ING Life
Service	JW Marriott Seoul
Manufacturing	Honda Korea
Electronics	LG Electronics Inc.
IT	Samsung SDS
Insurance	MetLife Korea
Manufacturing	NIKE Sportswear Korea
Distribution	LG International Corp.

OWASP
The Open Web Application Security Project

Web Application Firewalls: An Overview

OWASP
The Open Web Application Security Project

A web application firewall (WAF) secures web applications!

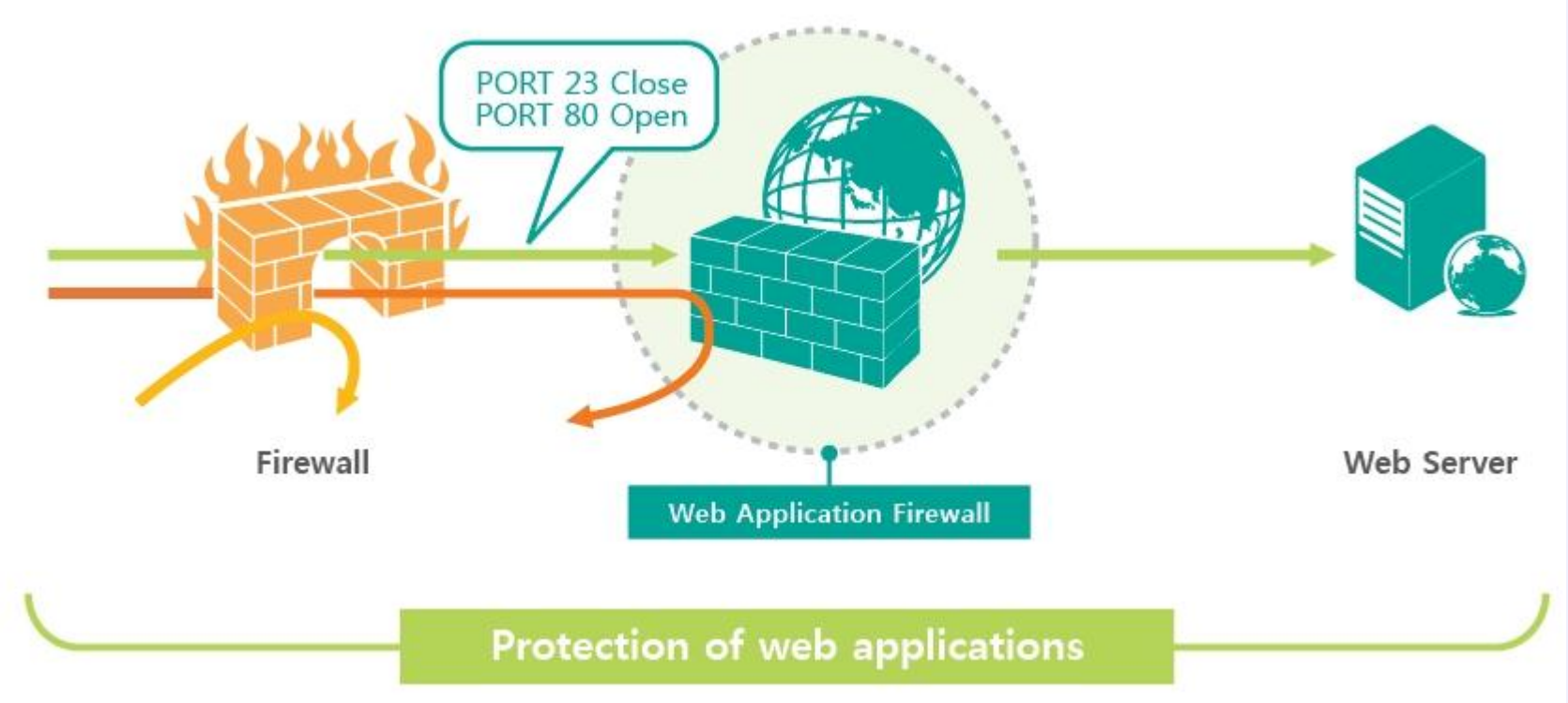
What is a WAF?

- **Web Application Firewall**
  - ✓ It executes a security **analysis of the OSI 7** layer between all messages of the web server and the web client.
  - ✓ It protects against attacks aimed at **web applications**.

- **Roles**
  - ✓ It protects web servers from **external attacks** (service in)
  - ✓ It **protects against leakage** of important information from the web server (service out)

Web Application Firewalls

OWASP
The Open Web Application Security Project



- **Protects against web attacks**
- **Prevents leakage of personal, confidential, and/or proprietary information**
- **Enables regulatory compliance**

Regulatory Compliance

OWASP
The Open Web Application Security Project

Web application firewalls enable regulatory compliance.

Payment Card Industry Data Security Standard (PCI DSS, 2004) is an international information security standard for companies dealing with electronic payment transactions (credit cards, debit cards, etc.).

- Requires secure management of cardholder data.
- Fines for violations can range from $5000-$100,000 USD per month.

Other well-known regulations which can be followed with accurate web application security include the **Health Insurance Portability and Accountability Act** (HIPAA, USA, 1996), and the **Federal Information Security Management Act** (FISMA, USA, 2002).

Network Firewalls, IDS/IPS, or Web Application Firewalls?

OWASP
The Open Web Application Security Project

Network Firewalls and IDS/IPS cannot protect web applications against the OWASP Top 10 Threats, but a Web Application Firewall (WAF) can!

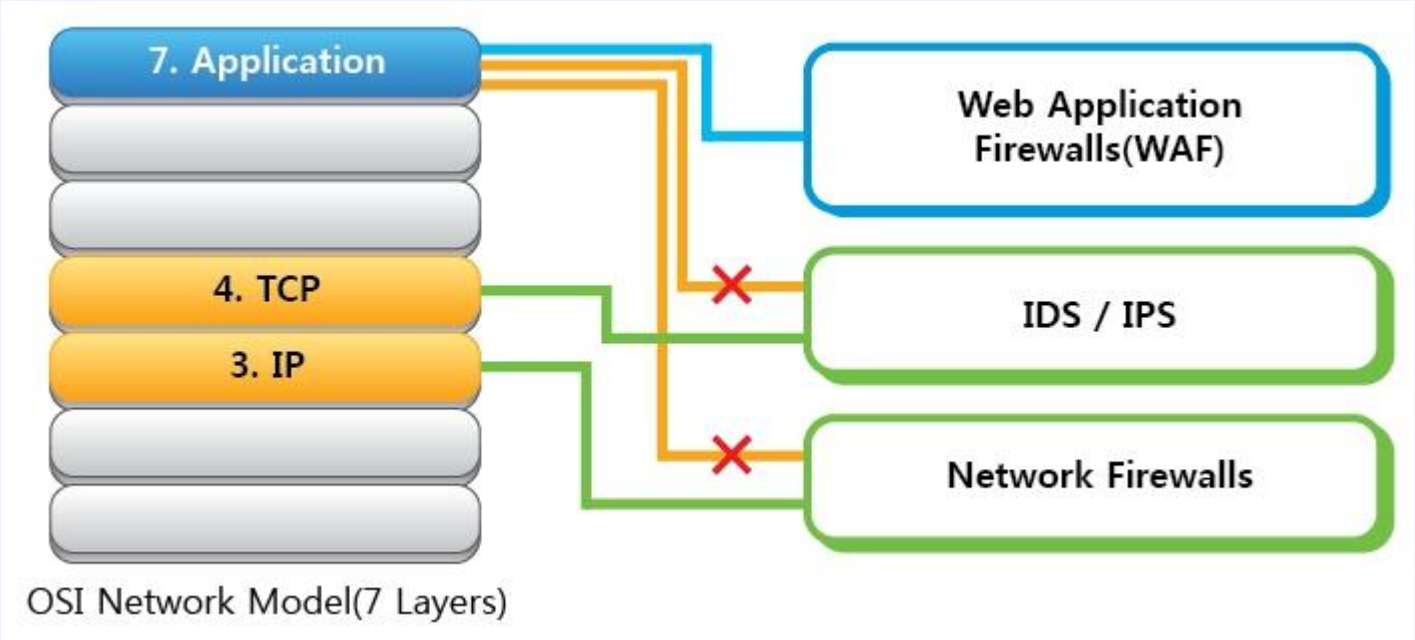
OWASP Top 10 (2010)	Network Firewall	IDS / IPS	WAF
A1: SQL Injection	X	△	√
A2: Cross Site Scripting (XSS)	X	△	√
A3: Broken Authentication and Session Management	X	△	√
A4: Insecure Direct Object References	X	X	√
A5: Cross Site Request Forgery (CSRF)	X	X	√
A6: Security Misconfiguration	X	X	√
A7: Failure to Restrict URL Access	X	X	√
A8: Insecure Cryptographic Storage	X	X	√
A9: Insufficient Transport Layer Protection	X	√	√
A10: Unvalidated Redirects and Forwards	X	X	√

Network Firewalls, IDS/IPS, or Web Application Firewalls?

OWASP
The Open Web Application Security Project

Comparing Network Firewalls, IDS/IPS, and WAFs:

Network Firewalls	IDS/IPS	Web Application Firewall
• Network Firewalls cannot detect or analyze attacks targeting web applications. • Network Firewalls generally cannot protect Port 80.	• Cannot typically analyze application layer attacks. • Easy for attackers to bypass	• Can inspect all traffic between the Web client and Web server • Can inspect protocol • Can inspect encrypted traffic



OWASP
The Open Web Application Security Project

Why Aren't WAFs More Prevalent?
A Survey of Web Application Firewalls

First-Generation WAFs

OWASP
The Open Web Application Security Project

The threats to web applications are clear. So why have so many large businesses been reluctant to Install web application firewalls?

The first generation web application firewalls was based on a pattern-matching detection mechanism.

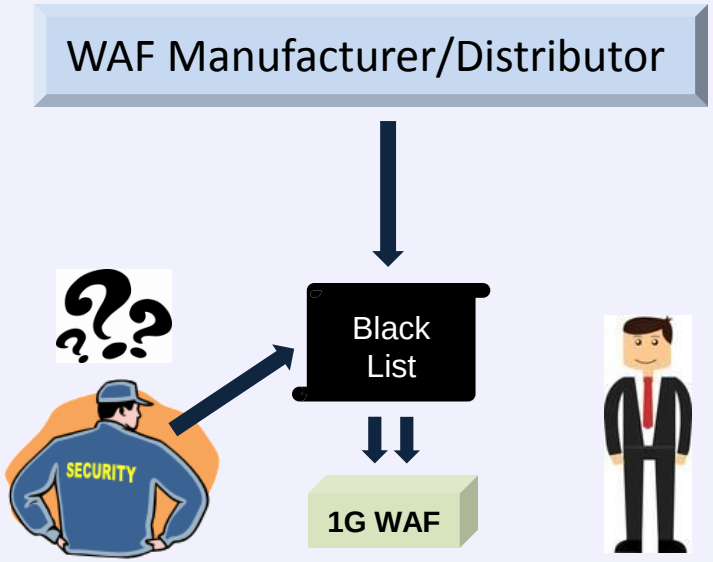
- **First Generation WAFs: Adoption of the Black List**
  - ✓ The administrator added a known attack pattern (black list) to block malicious traffic.
  - ✓ First generation WAFs compared web traffic to the updated pattern by analyzing them at the application level.
  - ✓ No detection system for new or modified attacks against the web application layer.

First-Generation WAFs

OWASP
The Open Web Application Security Project

The First Generation WAF was not particularly successful in the IT security market. Not only did it place a significant burden on system administrators, they were not seen as particularly effective.

- **Heavy Workload & HR Requirements**
  - ✓ Administrators needed to update known attack patterns on the black list
  - ✓ Attempts to add new conceivable patterns meant a heavy workload for the WAF administrative team
  - ✓ The high costs of manpower were significant, especially for smaller companies or IT security providers with limited budgets

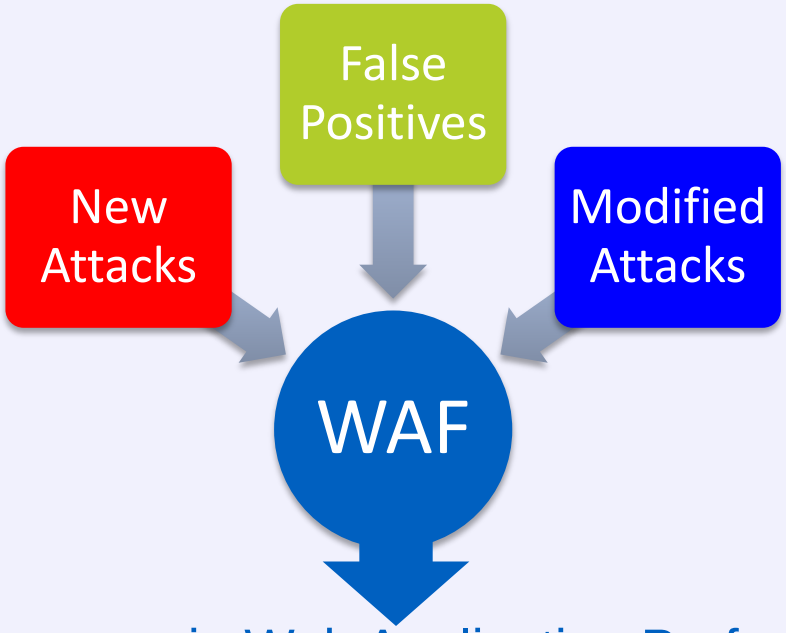


First-Generation WAFs

OWASP
The Open Web Application Security Project

❑ Vulnerabilities with Poor System Performance

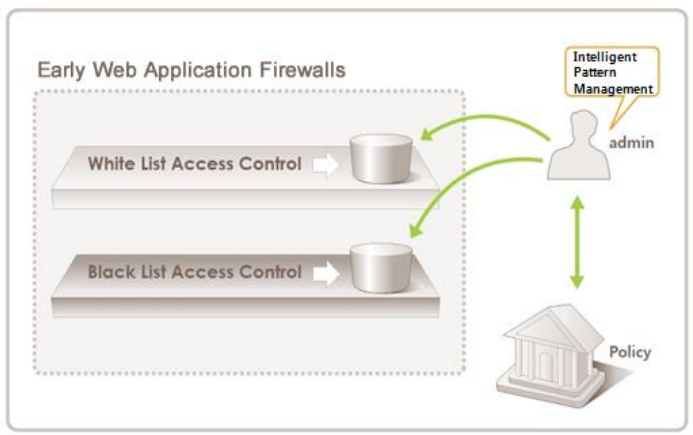
- ✓ No protection against new or modified attacks
- ✓ Significant increase in false positives
- ✓ Attempts to add patterns for all conceivable attacks led to a deterioration in web application performance



Second-Generation WAFs

OWASP
The Open Web Application Security Project

The second generation WAF attempted to remedy the flaws and limitations of its predecessor.



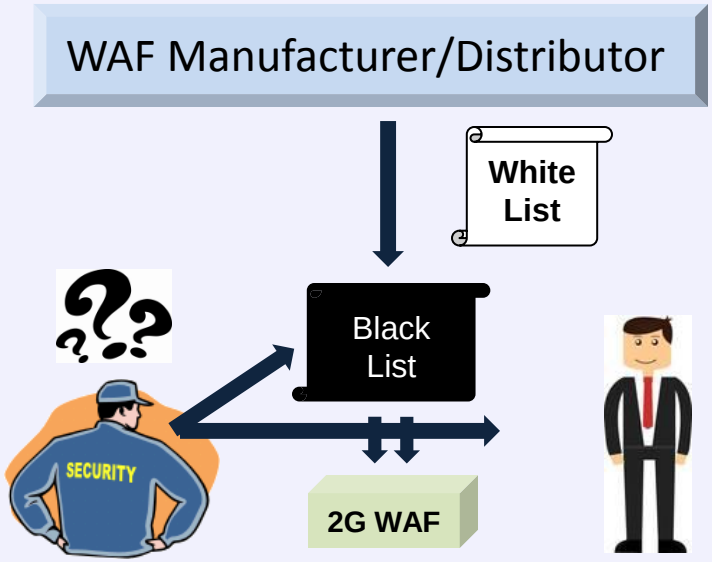
- **Second-Generation WAFs: The Advent of the automated policy**
  - ✓ By analyzing the web application(s) protected by the WAF, the second-generation WAF was able to automate the establishment of “white lists” for security policies.
  - ✓ Combined with a black list containing known and conceivable attacks against the application layer, the second generation WAF could figure out what was permissible traffic, and what was not permissible.

Second-Generation WAFs

OWASP
The Open Web Application Security Project

Unfortunately, the second generation WAF did little to increase application layer security, or alleviate manpower requirements.

- **Heavier Workload!**
  - ✓ The automatically established policies, or the white lists, could take up to two weeks to identify and implement.
  - ✓ Additionally, while the policies were established automatically, they still required manual configuration by an administrator, thereby increasing (not reducing) the administrative burden
  - ✓ The security administrator still has to maintain the black list of known web attacks

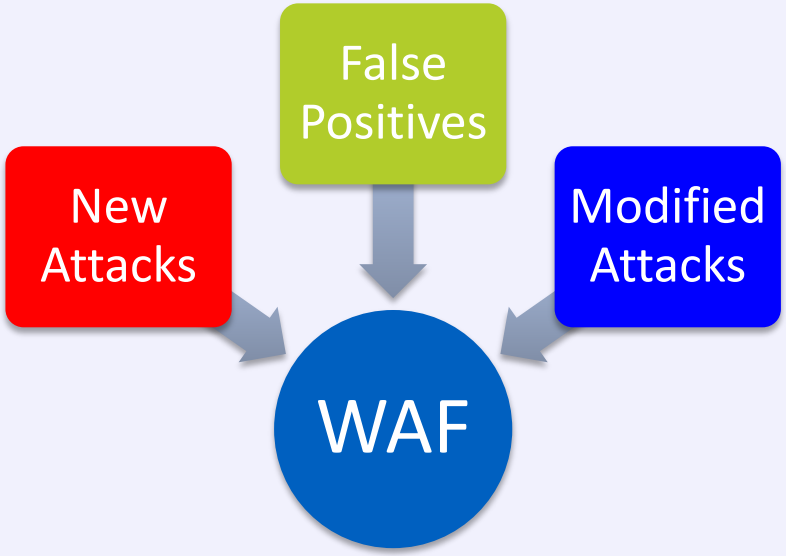


Second-Generation WAFs

OWASP
The Open Web Application Security Project

Unfortunately, the second generation WAF did little to increase application layer security, or alleviate manpower requirements.

- **Still Vulnerable with Poor System Performance**
  - ✓ Still a pattern-matching solution
  - ✓ Still an inability to protect against unknown attacks
  - ✓ Still a tendency to produce false positives
  - ✓ Still promoted slow system performance



Decrease in Web Application Performance

OWASP
The Open Web Application Security Project

The Traditional Signature-Based Approach is Failing

Signature-Based Solutions

OWASP
The Open Web Application Security Project

"There is widespread agreement that advanced attacks are **bypassing our traditional signature-based security controls** and persisting undetected on our systems for extended periods of time.

The threat is real. You are compromised; you just don't know it."

Source: Gartner, 2012

Gartner

The Exploit Database

The Exploit Database (EDB) - an ultimate archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database.

WordPress TimThumb Exploitation
vbSEO - From XSS to Reverse PHP Shell
Owned and Exposed

Remote Exploits

Date	D	A	V	Description		Plat.	Author
2012-08-21	⬇	-	✔	Sysax Multi Server 5.64 Create Folder Buffer Overflow	381	windows	metasploit
2012-08-20	⬇	-	✔	Adobe Flash Player 11.3 Font Parsing Code Execution	2356	windows	metasploit
2012-08-20	⬇	-	◷	Sysax Multi-Server 5.64 Create Folder Buffer Overflow	395	windows	Matt Andreko
2012-08-18	⬇	-	✔	Apple Quicktime plugin - Windows 4.1.2 (Japanese) Remote Overflow Vulnerability	937	windows	UNYUN
2012-08-16	⬇	-	✔	IE Time Element Memory Corruption Exploit (MS11-050)	2671	windows	Ciph3r
2012-08-16	⬇	-	✔	E-Mail Security Virtual Appliance (ESVA) Remote Execution	971	linux	iJoo
2012-08-15	⬇	-	✔	TestLink v1.9.3 Arbitrary File Upload Vulnerability	1051	php	metasploit

Local Exploits

Date	D	A	V	Description		Plat.	Author
2012-08-15	⬇	-	✔	globalSCAPE CuteZIP Stack Buffer Overflow	558	windows	metasploit
2012-08-15	⬇	-	✔	Windows Service Trusted Path Privilege Escalation	1622	windows	metasploit
2012-08-13	⬇	⚠	◷	OS X Local Root Exploit for Viscosity OpenVPN Client	1565	osX	zx2c4
2012-08-11	⬇	⚠	✔	Tunnelblick Local Root Exploit	1752	osX	zx2c4

OWASP
The Open Web Application Security Project

Example of misdetection with a Signature-Based Engine

– In the case that a WAF has the below signatures:

Example of SQL Injection Signature
- Below 'part' means substring-searching target. 'rgxp' means a regular expression.
- After finding a string of 'part', 'rgxp' is applied.

Signature	Signature Name
part="or 'a' = 'a"	SQL Injection WHERE Statement Manipulation
part="or 'a'= 'a"	SQL Injection WHERE Statement Manipulation 1
part="or 'a'= 'a"	SQL Injection WHERE Statement Manipulation 2
part="or 'a'='a"	SQL Injection WHERE Statement Manipulation 3
part="or 'a' ='a"	SQL Injection WHERE Statement Manipulation 4
part="or 'a'='a"	SQL Injection WHERE Statement Manipulation 5
part="or 'a' ='a"	SQL Injection WHERE Statement Manipulation 6
part="or a=a"	SQL Injection WHERE Statement Override
part="or 1=1"	SQL Injection WHERE Statement Override 1

If a SQL Injection source is modified from 'a'='a' to 'b'='b', the regular expression cannot detect the modified SQL Injection attack.

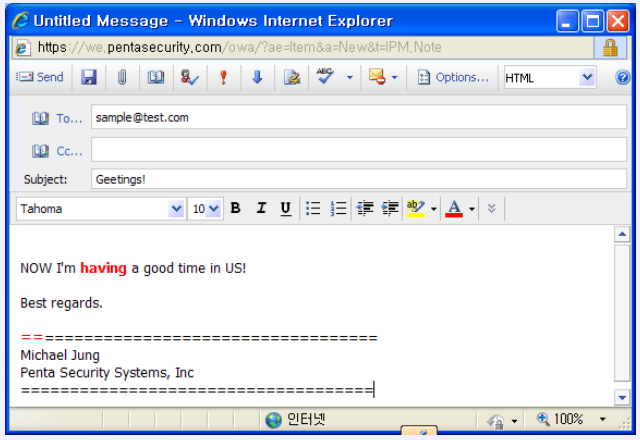
SQL Injection Signatures

OWASP
The Open Web Application Security Project

- **Example of a false-positive with a Signature Based Engine**
  - In the case that a WAF has the below signatures:

Signature	Signature Name
part="waitfor", rgxp="[^a-zA-Z]waitfor\s*delay"	SQL Injection - Waitfor
part="having", rgxp="[^A-Za-z]having[^\&]{0,20}=[^\&]{0,20}"	SQL Injection - "having" statement injection attempt
part="opendatasource", rgxp="select.*from.*opendatasource"	SQL Injection – opendatasource

If HTTP message includes string **"… having a good time… ==…"** such as shown below, a signature based WAF would generate a false-positive.



OWASP
The Open Web Application Security Project

WebShell Hacking…What is It?

- A broad term for a type of file that operates similarly to an Injection
- Once successfully uploaded, the WebShell file is capable of exploiting server vulnerabilities and eventually providing the attacker with access to the web server structure
- These files are often masked as harmless, and can be quite difficult to detect until damage has already been done

Implications?

- WebShell attacks pose a very threat because they can potentially lead to complete server access and privileges for the hacker
- As with most APTs, the conventional security systems in place are ill-equipped to handle the threats of WebShell attacks, and cannot keep up with how quickly their methods are modified.

OWASP
The Open Web Application Security Project

What Solution is Needed?

What WAF Solution is Needed?

OWASP
The Open Web Application Security Project

The threats against web applications continue to evolve. The web application remained vulnerable and a frequent target of hackers. So what solution is needed?

- **A Whole New Breed of WAF**
  - ✓ An “intelligent” WAF, based on an entirely new concept
  - ✓ Capable of analyzing web traffic
  - ✓ Detect attacks, analyzing and classifying them
  - ✓ Apply appropriate countermeasures to block detected attacks
  - ✓ Be able to perform all of these functions without the continual involvement of administrative staff

A new solution would be able to execute all of the functions above, in order to protect web applications in a stable manner, while easing the administrative workload and management costs.

OWASP
The Open Web Application Security Project

Thank You.

Trust for an Open Society

Penta SECURITY