

Web Application Threat Report

: Trends for the Second Half of 2014

Table of Contents

Web Application Threat Report: An Introduction

Report Summary

Data Analysis

1. Top 10 Detections by WAPPLES Rules
2. Top 10 OWASP 2013 Web Attacks
3. Top 5 Origins of Web Attacks by Country
4. Purposes of Web Attacks
5. The Risk Levels of WAPPLES Rules
6. Web Attack Trends

Appendix

1. Description Table of WAPPLES Rule
 - 1) WAPPLES Rules Corresponding to OWASP Top 10 (2013)
 - 2) WAPPLES Rules Corresponding to Risk Levels
 - 3) WAPPLES Rules Corresponding to Purposes of Web Attacks
2. About WAPPLES Rules

Web Application Threat Report: An Introduction

This report is based on statistical data detected by WAPPLES, a web application firewall (WAF) by Penta Security Systems Inc. The ensuing data has been analyzed by the Intelligent Customer Support (ICS) system of Penta Security.

This report was written to provide optimum security services to WAPPLES customers by sharing web application threat trends that have been analyzed by Penta Security. Statistical data has been gathered from actual WAPPLES customers who have shared their web security data with Penta Security.

The report cover the following:

- What WAPPLES rules are the most frequently utilized to detect web attacks
- What kinds of attacks are detected most frequently, based on the 2013 OWASP Top 10
- In what countries did most of the threats originate
- What were the purposes of the attacks
- The distribution of attacks by risk level
- Monthly detections according to WAPPLES rules

(See 'Appendix - 2. About WAPPLES Rules' for description of WAPPLES rules)



Report Summary

In the second half of 2014, the most frequently detected attack was the Injection attack (classified by 2013 as 'Injection' and by Penta Security Systems, Inc. as 'Include Injection').

One of the most prominent attacks within the OWASP TOP 10 attacks, Include Injection involves the use of the Include function in the server-side script to enable Website Defacement and Server Disruption. The attack warrants much caution, because it may lead to loss of data and/or server disruption/sabotage.

Furthermore, it is important to note that the percentage of detected web attacks with threat level 'Urgent' has risen to 31% (26.5% in the first half). Attacks at this level can lead to complete sabotage of the server or significant leak/loss of data. Hence, the server/security administrator must emplace multiple layers of security measures by performing regular vulnerability checks, using web security solutions and encrypting data.

The statistic tables below show the web application attacks that were detected by WAPPLES during the second half of 2014 (July 1, 2014-December 31, 2014).

NO.	Purposes of Web Attacks	Percentage (%)
1	Vulnerability Scanning	27.7
2	Website Defacement	26.1
3	Server Disruption	17.5

NO.	Risk Levels	Percentage (%)
1	Urgent	31.0
2	Very High	21.1
3	High	38.2
4	Normal	9.8

NO.	Detection Rules	Percentage (%)
1	Include Injection	22.5
2	Extension Filtering	15.4
3	Buffer Overflow	14.1

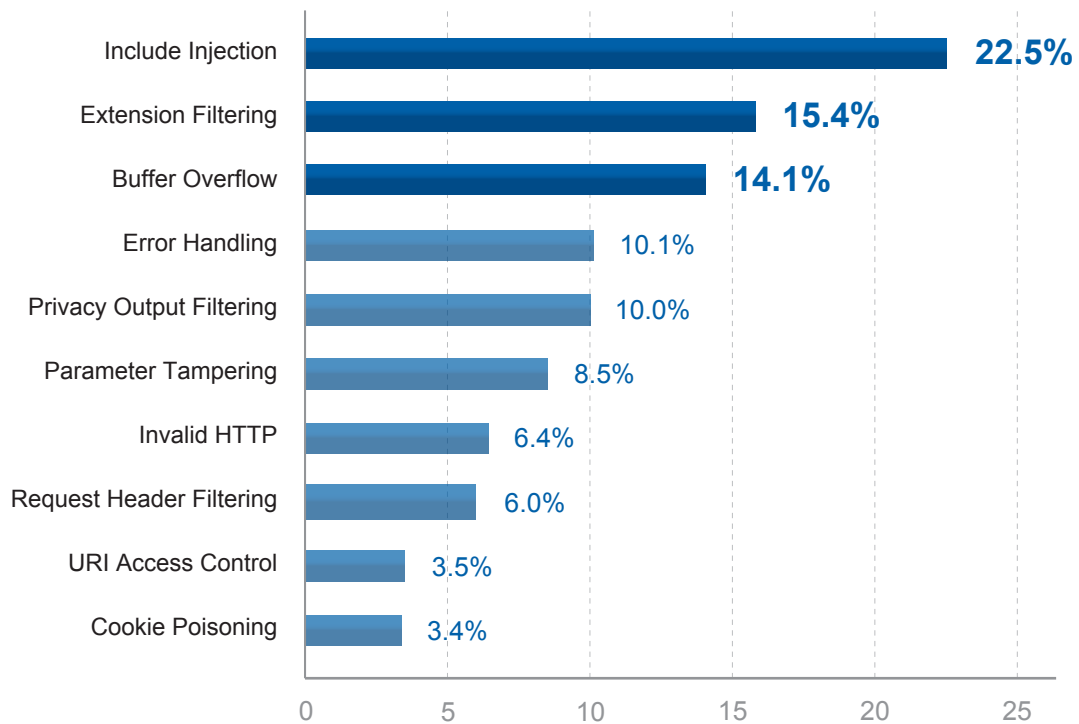
The data of this report was collected from 1,186 WAPPLES customers who have agreed to our usage of their statistical data, during the period between January 1 and July 2014 to December 2014.

The collected data do not contain any other private or customer information, and contains only statically analyzed data. Additionally, for accuracy, WAPPLES units that were only in the process of evaluation were excluded.

※ The statistical information included in this report is identical to that provided by WAPPLES Management Systems (WAPPLES MS), which manages multiple numbers of WAPPLES.

Data Analysis

1. Top 10 Detections by WAPPLES Rules



The graph above shows the WAPPLES rules that are the most frequently detected. During the collection period (July 2014-December 2014), Include Injection showed the highest frequency, followed by Extension Filtering and Privacy Buffer Overflow.

- ▶ **Include Injection** refers to attacks that utilize the Include function to upload and execute malicious code. Even able to upload webshells disguised as text files, Include Injection poses a major threat.
- ▶ **Extension Filtering** refers to attempting to access vulnerable files with extensions that are not normally used in websites (e.g. dll, conf, ini), which, if successful, can result in Server Disruption or exposure of confidential information.

- ▶ **Buffer Overflow** is an attack that involves the entry of excessively long request inputs, which can trigger problems such as remote code execution, denial of service and memory access errors. With the potential to disrupt program execution and/or force the program to execute foreign commands, Buffer Overflow must be prevented.

WAPPLES Rules	The number of detection
Include Injection	—
Extension Filtering	—
Buffer Overflow	—
Error Handling	—
Privacy Output Filtering	—
Parameter Tampering	※ Only WAPPLES report for customers provides detailed numerical information
Invalid HTTP	—
Request Header Filtering	—
URI Access Control	—
Cookie Poisoning	—

< Table 1. Top 10 Detections by WAPPLES Rules >

2. Top 10 OWASP 2013 Web Attacks

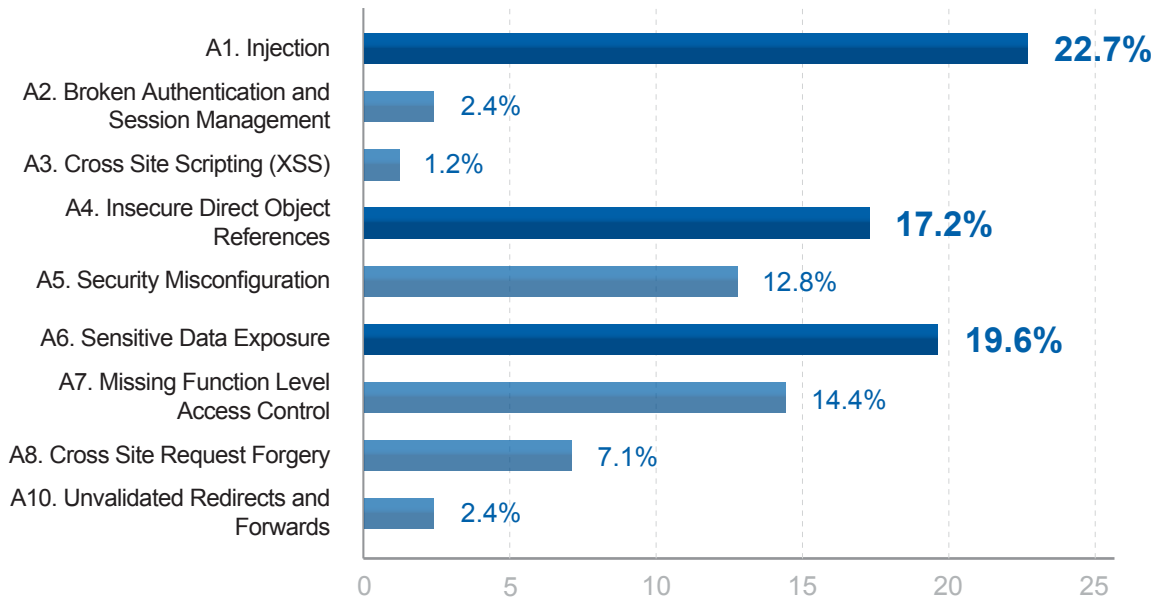


Figure 2 shows the distribution of detected attacks, categorized by OWASP Top 10. As can be seen Injection attacks were the most frequent during the period between July and December 2014.

Injection is a threat that is ranked A1 within the 2013 OWASP Top 10. It is a relatively easy method, as it can simply be text-based and all data sources can be used as injection paths. Despite being simple, it can cause severe damage; injections can have various effects including loss/destruction of data and denial of service, and is difficult to track back to its source. Hence, injection attacks warrant appropriate preventive measures.

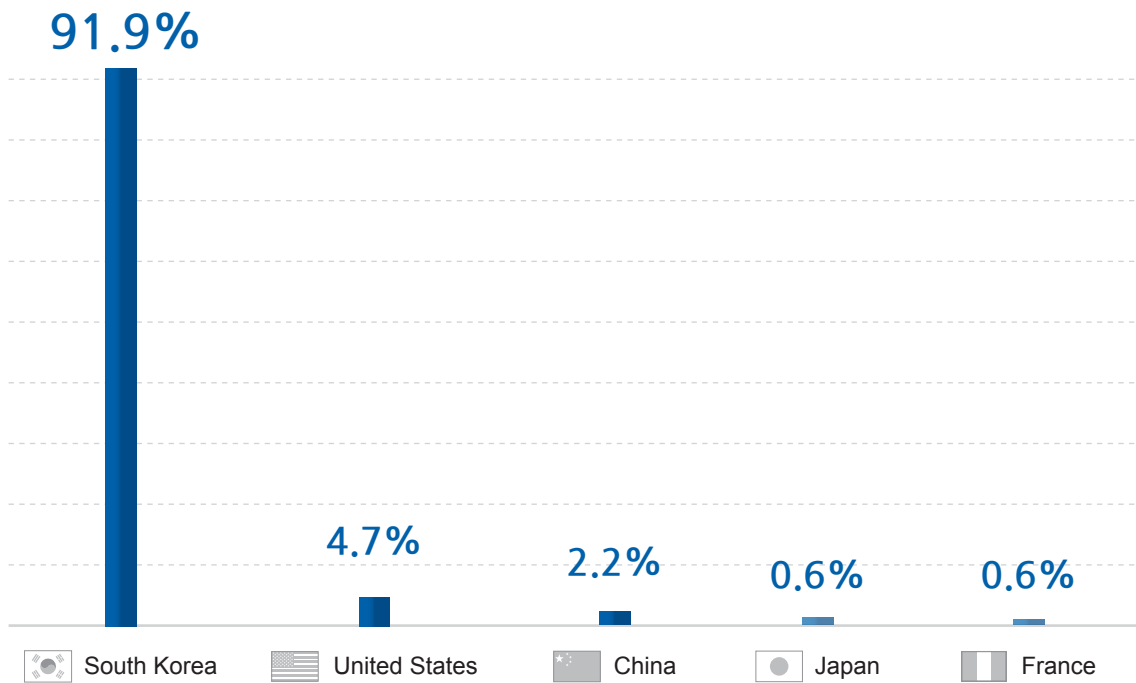
OWASP Top 10 Web Application Security Risks 2010	The number of detection
A1. Injection	—
A2. Broken Authentication and Session Management	—
A3. Cross Site Scripting (XSS)	—
A4. Insecure Direct Object References	—
A5. Security Misconfiguration	—
A6. Sensitive Data Exposure	—
A7. Missing Function Level Access Control	—
A8. Cross Site Request Forgery	—
A10. Unvalidated Redirects and Forwards	—

※ Only WAPPLES report for customers provides detailed numerical information

< Table 2. Top 10 OWASP 2013 Web Attacks >

※ See Appendix for a description for the relationship between OWASP Top 10 and the WAPPLES Rules.

3. Top 5 Origins of Web Attacks by Country



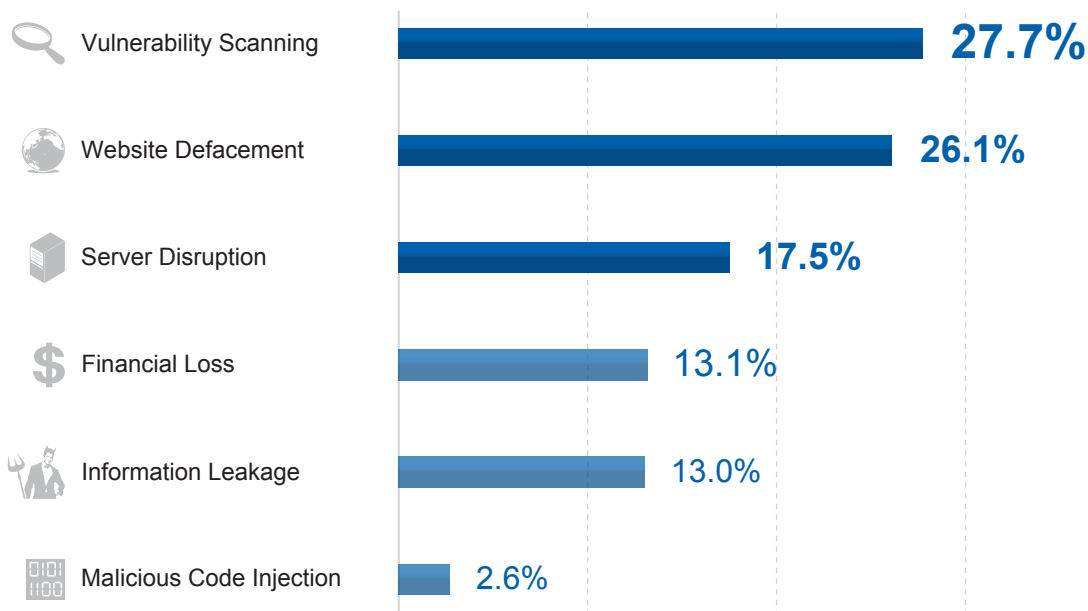
The graph above shows the countries from which most threats originated. During the period between July and December 2014, Korea most of the attacks were from Korea, followed by the United States and China, similarly to the first half of the year. However, while attacks from within Korea has risen by three hundred million cases, attacks from the United States, China and Japan have not changed significantly in frequency.

Top 5 Origins (Countries) of Web Attacks	The number of Detection
South Korea	※ Only WAPPLES report for customers provides detailed numerical information
United States	
China	
Japan	
France	

< Table 3. Top 5 Origins of Web Attacks by Country >

※ The data in this report are mostly based on WAPPLES customers located within Korea.







4. Purposes of Web Attacks



The graph above shows the top purposes behind web attacks. During the period between July and December 2014, the most common purpose was Vulnerability Scanning, followed by Website Defacement and Server Disruption.

- ▶ **Vulnerability Scanning** refers to attempts to determine the existence and position of a web server's vulnerabilities. These attempts most use automatic attack tools that send invalid HTTP requests or URIs that do not comply with RFC standards, or via the exposure of directory and error messages.
- ▶ **Website Defacement** refers to the manipulation of websites by unauthorized individuals, and includes the falsification of website contents, the acquisition of information by unauthorized individuals via the addition of malicious codes to a SQL server (SQL injection), uploading unauthorized files with extensions such as .exe, .jps, and .php to a web site (FileUpload), and the injection of risky scripts, files, and/or malicious code (Include Injection).
- ▶ **Server Disruption** includes the disruption of a server's normal operations by flooding the server buffer (Buffer Overflow), the use of a sending method and header that have one or more vulnerabilities.

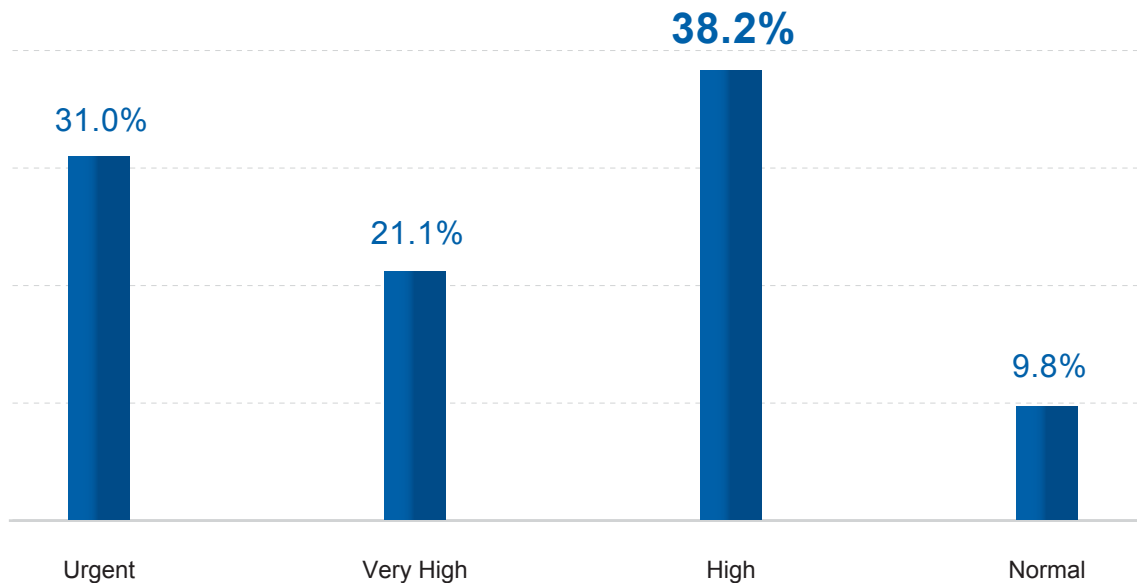
- ▶ **Financial Loss** intends to cause the transference of money to unauthorized users by acquiring personal user information. This can be done by modifying cookies to avoid the certification process (Cookie Poisoning), or by making applications work abnormally by using values of an unauthorized parameter (Parameter Tampering).
- ▶ **Information Leakage** pertains to the exposure of important private information to or from websites (Privacy Input/Output Filtering), the uploading of files containing private information (Privacy File Filtering), or the exposure of a web site's directory (Directory Listing).
- ▶ **Malicious Code Injection** means the dissemination of Trojan or other viruses via server vulnerabilities. Hackers try to extract user information by adding malicious script codes (XSS), executing commands and acquiring information by adding server-side script to input (StealthCommanding), and transmitting malicious code by suspicious access (Suspicious Access).

Purposes of Web Attacks		The number of detection
 Vulnerability Scanning		
 Website Defacement		
 Server Disruption		※ Only WAPPLES report for customers provides detailed numerical information
 Financial Loss		
 Information Leakage		
 Malicious Code Injection		

< Table 4. Purposes of Web Attacks >

※ See Appendix for a description for the relationship between Purposes of Web Attacks and the WAPPLES Rules.

5. The Risk Levels of WAPPLES Rules



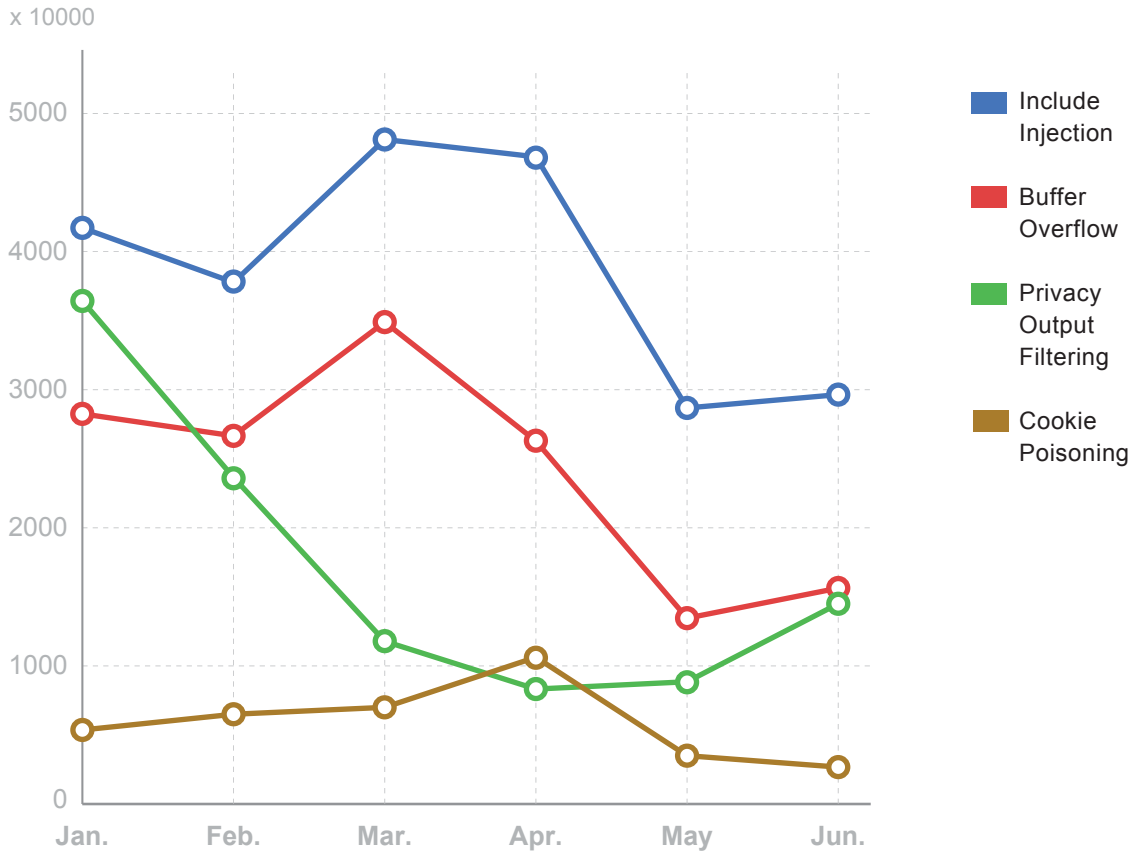
The graph above shows the distribution of attacks by risk level. In the period between July and December 2014, a High risk level showed the highest frequency, followed by Urgent and Very High. Please refer to the Appendix for a description of the relationship between the different Risk Levels and WAPPLES Rules, referred by OWASP classifications.

Risk Levels of WAPPLES Rules	The number of detection
Urgent	
Very High	※ Only WAPPLES report for customers provides detailed numerical information
High	
Normal	

< Table 5. The Risk Levels of WAPPLES Rules >

※ See Appendix for a description of the relationship between Risk Levels and WAPPLES Rules.

6. Web Attack Trends



The graph above shows the monthly changes for the four most high-risk attacks. From the first half of 2014, Include Injection (an attack that involves using rose to being the most frequent, while it was second place in the first half. It was followed by Buffer Overflow and then Privacy Output Filtering. Among the most frequently attempted attacks, these attacks warrants particularly serious caution and strong preventive measures.

Highly Risky Attack	Jul	Aug	Sep.	Oct	Nov	Dec.
Include Injection	—	—	—	—	—	—
Buffer Overflow	—	—	—	—	—	—
Privacy Output Filtering	—	—	—	—	—	—
Cookie Poisoning	—	—	—	—	—	—

※ Only WAPPLES report for customers provides detailed numerical information

< Table 6. Monthly Process of Highly Risky Attacks >

Appendix

1. Description Table of WAPPLES Rule

1) WAPPLES Rules Corresponding to OWASP Top 10 (2013)

OWASP (Open Web Application Security Project) makes reports about frequent and influential vulnerabilities related to web application security. The following table shows the 2013 OWASP Top 10 Web Application Risks and their corresponding WAPPLES rules.

NO.	OWASP 2013	WAPPLES Rules
1	Injection	Parameter Tampering
		SQL Injection
		Stealth Commanding
		Include Injection
2	Broken Authentication and Session Management	Cookie Poisoning
		Suspicious Access
3	Cross Site Scripting (XSS)	Cross Site Scripting
4	Insecure Direct Object References	URI Access Control
		Invalid URI
		Unicode Directory Traversal
		Error Handling
		Parameter Tempering
		Stealth Commanding
5	Security Misconfiguration	Directory Listing
		Error Handling
		Request Method Filtering
		Invalid HTTP
		File Upload
6	Sensitive Data Exposure	Privacy File Filtering
		Privacy Input Filtering
		Privacy Output Filtering
		Input Contents Filtering
		Extension Filtering
		Supported by transaction encryption function (e.g., TLS)
7	Missing Function Level Access Control	URI Access Control
		Unicode Directory Traversal
		Extension Filtering
8	Cross Site Request Forgery	Cross Site Scripting
		Parameter Tampering
9	Using Components with Known Vulnerabilities	ALL
10	Unvalidated Redirects and Forwards	URI Access Control

2) WAPPLES Rules Corresponding to Risk Levels

Type	Description	WAPPLES Rules
Urgent	When web server has been completely turned over to hackers, or when large amounts of information have been leaked.	Include Injection
		Privacy Output Filtering
		Stealth Commanding
		SQL Injection
Very High	When it is possible to transmit hack attempts through the web server, or when dangerous attacks are imminent.	Privacy File Filtering
		Request Method Filtering
		File Upload
		Invalid URI
		Buffer Overflow
		Cookie Poisoning
		Cross Site Scripting
High	When information pertaining to the web server has been falsified, or the web server has sustained limited damage.	Request Header Filtering
		URI Access Control
		Extension Filtering
		Web Site Defacement
		Invalid HTTP
		Suspicious Access
		Unicode Directory Traversal
		Parameter Tampering
Normal	The preparation stages of an attack, during which time data vulnerabilities are collected.	Directory Listing
		Input Content Filtering
		Error Handling
		Response Header Filtering

3) WAPPLES Rules Corresponding to Purposes of Web Attacks

Purposes of web attacks are to:

1. Damage other users' finance, or attain monetary benefit.
2. Cause excessive damage to a server, or to interrupt server operation.
3. Scan for vulnerabilities before an actual web attack.
4. Spread malicious code through a website.
5. Falsify a website, either in order to manipulate the website, or simply for vandalism purposes.
6. Leak individual, server, or database information.

Type	WAPPLES Rules
Financial Loss	Parameter Tampering
	Cookie Poisoning
Server Disruption	Suspicious Access
	Request Method Filtering
	Buffer Overflow
Vulnerability Scanning	Invalid URI
	Invalid HTTP
	Request Header Filtering
	Error Handling
	Directory Listing
	Response Header Filtering
Malicious Code Injection	Stealth Commanding
	Cross Site Scripting
Website Defacement	Include Injection
	File Upload
	SQL Injection
	Web Site Defacement
Information Leakage	SQL Injection
	Unicode Directory Traversal
	Privacy Output Filtering
	Privacy File Filtering
	Privacy Input Filtering

2. About WAPPLES Rules

WAPPLES Rules	Description
Buffer Overflow	Blocks invalid requests causing buffer overflow attacks
Cookie Poisoning	Blocks the falsification of cookies containing authentication information
Cross Site Scripting	Blocks malicious script code having the possibility to be executed by the client
Directory Listing	Block the leakage of web sites' directory and files
Error Handling	Controls error messages so as to avoid exposure of information about web server, WAS, DBMS server, etc.
Extension Filtering	Blocks access of files which do not have permitted file extensions
File Upload	Blocks the upload of files which can be executed on the web server
Include Injection	Blocks the injection of untrustworthy files and external URIs
Input Content Filtering	Blocks or substitutes words that are not permitted on a website
Invalid HTTP	Blocks access not in compliance with HTTP standards
Invalid URI	Blocks access not in compliance with standard URI syntax
IP Black List	Blocks when more than the set value of access attempts from the same source IP are detected during a specific time (value set by user)
IP Filtering	Blocks access to a specific IP range or countries (set by user)
Parameter Tampering	Blocks attacks which send maliciously manipulated parameters to websites
Privacy File Filtering	Blocks leakage of private information from files transmitted from the web server
Privacy Input Filtering	Blocks leakage of private information via HTTP request
Privacy Output Filtering	Blocks leakage of private information via HTTP response
Request Header Filtering	Blocks HTTP requests having headers that are missing important information or that have been abnormally modified, such as requests from automatic attack tools and abnormal HTTP requests
Request Method Filtering	Blocks risky HTTP request methods
Response Header Filtering	Blocks leakage of web server information via HTTP response
SQL Injection	Blocks requests to inject SQL Query statements
Stealth Commanding	Blocks requests to execute specific commands in the web server through HTTP Request
Suspicious Access	Blocks access which does not fit the standard web browser request
Unicode Directory Traversal	Blocks request of access to directory and files using vulnerabilities related to Unicode manipulation of the web server
URI Access Control	Controls requests of access to specific URIs and files
Website Defacement	Detects defacement of websites and recovers the web page.

Penta Security Systems Inc. (HQ)

20F, 25, Gukjegeumyung-ro 2-gil, Yeongdeungpo-gu, Seoul, Korea 150-949
TEL. +82-2-780-7728 FAX. +82-2-786-5281 / www.pentasecurity.com
INQUIRIES. +82-2-2125-6745 / wps@pentasecurity.com

Penta Security Systems Co.

Houston, Texas www.pentasecurity.com/en

Penta Security Systems K.K.

Shinjuku-Ku, Tokyo www.pentasecurity.co.jp