

Web Application Threat Report

: Trends for the First 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 first half of 2014, the most frequently detected attack was aimed at website vulnerabilities in the access control system vulnerabilities, classified by OWASP 2013 as the “Missing Function Level Access Control risk.” Penta Security classifies this vulnerability as the Error Handling risk. This is a continuation of the same trend since the second half of 2013. The purpose of these attacks is to expose confidential information. This implies that the current hacking attempts have bigger goals than just damaging web services or causing short-term downtime. These hacking attempts are aimed to set the groundwork for a second attack, which can lead to serious results, such as the leakage of personal information or turning computers into zombies.

More importantly, the number of very high risk level attacks has increased compared with the previous year. The risk of very high or urgent level attacks can expose full administrator privileges or result in the leakage of large amounts of information. To prevent these threats, developers should take security seriously from the development stage. The access level control should be configured appropriately, and an authentication process should be implemented. After the development stage, installing security systems, such as a WAF or database encryption, can minimize the security threats resulting from web attacks. WAFs can block a diverse number of web threats, and data encryption can avoid the possibility of a second attack, even when a large amount of data is exposed.

The statistic tables below show the web application attacks that were detected by WAPPLES during the first half of 2014 (January 1, 2014-June 30, 2014).

NO.	Purposes of Web Attacks	Percentage (%)
1	Vulnerability Scanning	38.1%
2	Information Leakage	20.4%
3	Server Disruption	14.8%

NO.	Risk Levels	Percentage (%)
1	Urgent	26.5%
2	Very High	19.9%
3	High	34.1%
4	Normal	19.5%

NO.	Detection Rules	Percentage (%)
1	Error Handling	18.5%
2	Extension Filtering	16.9%
3	Privacy Output Filtering	15.6%

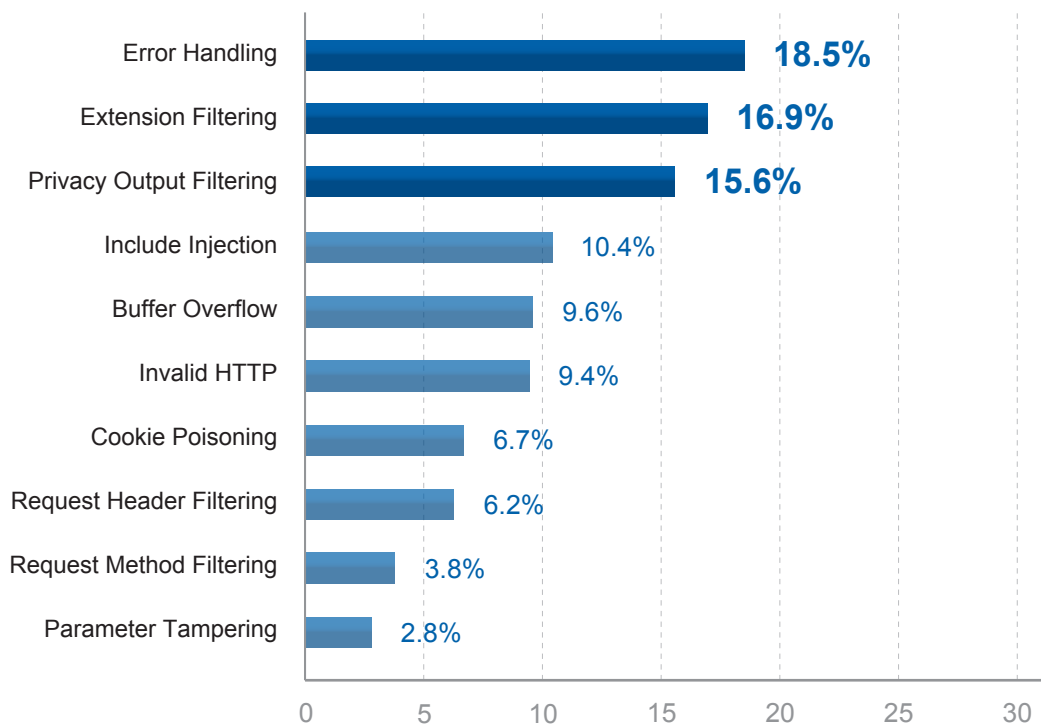
The data of this report was collected from 1,023 WAPPLES customers who have agreed to our usage of their statistical data, during the period between January 1, 2014 and June 30, 2014

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 (January 2014-June 2014), Error Handling showed the highest frequency, followed by Extension Filtering and Privacy Output Filtering.

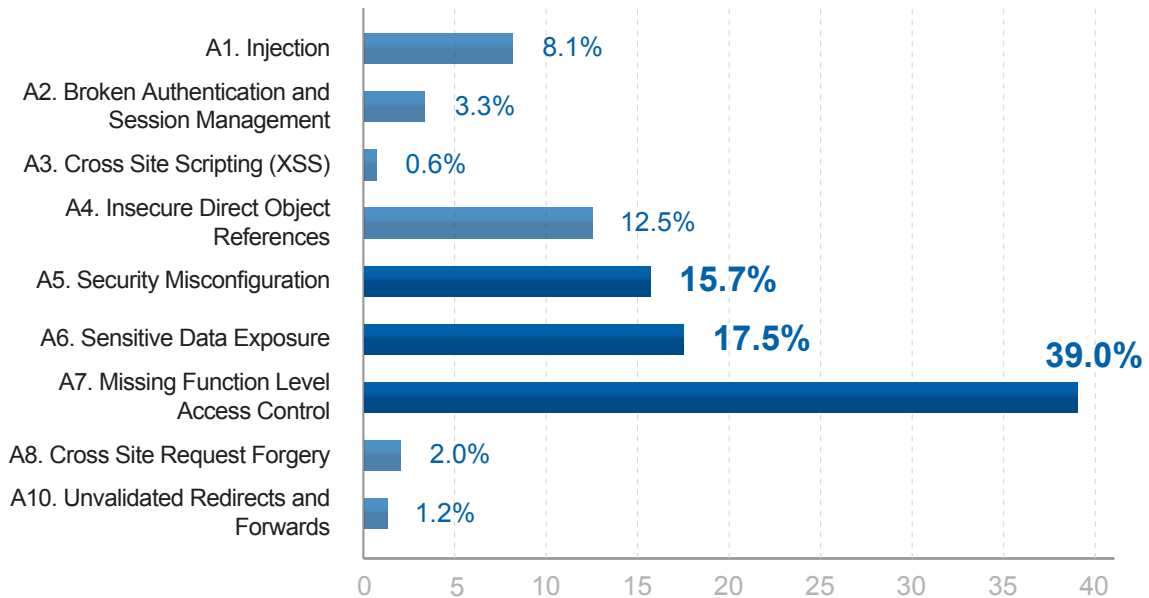
- ▶ **The Error Handling** rule detects attacks that produce errors by sending bad requests intentionally to acquire information about the web server, the web application database, the linked web server and application version. These attempts might enable attackers to find a point of vulnerability in the target site. Based on the information gathered from these attacks, a second attack is very likely.
- ▶ **The Extension Filtering** rule detects attempts to access files with extension vulnerabilities (.dll, .conf, .ini, etc.) that could cause the web server to malfunction, or to expose confidential information.

- ▶ **The Privacy Output Filtering** rule detects attack attempts that aim to expose sensitive data from the web server. Sensitive data includes social security numbers, credit card numbers, email addresses, and phone numbers. When successful, these attacks result in the target organization's decrease in value, the loss of brand perception and legal responsibility for the leakage.

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

< Table 1. Top 10 Detections by WAPPLES Rules >

2. Top 10 OWASP 2013 Web Attacks



The graph above shows what kinds of attacks were the most frequently detected, as defined by the 2013 OWASP Top 10. During the first half of 2014, Missing Function Level Access Control showed the highest frequency.

The Missing Function Level Access Control was clarified as the Failure to Restrict URL Access by OWASP in 2007 and 2010. The rule now includes not only URL level attacks, but also all attacks pertaining to the access control function level. This vulnerability can be the target of a Brute Force Attack, which can cause fatal damage, such as the exposure of trade secrets. The attacks can result in the target organization’s decrease in value, the loss of brand perception and legal responsibility for the leakage. The impact of these attacks can be severe, meaning that proper response measures should be implemented.

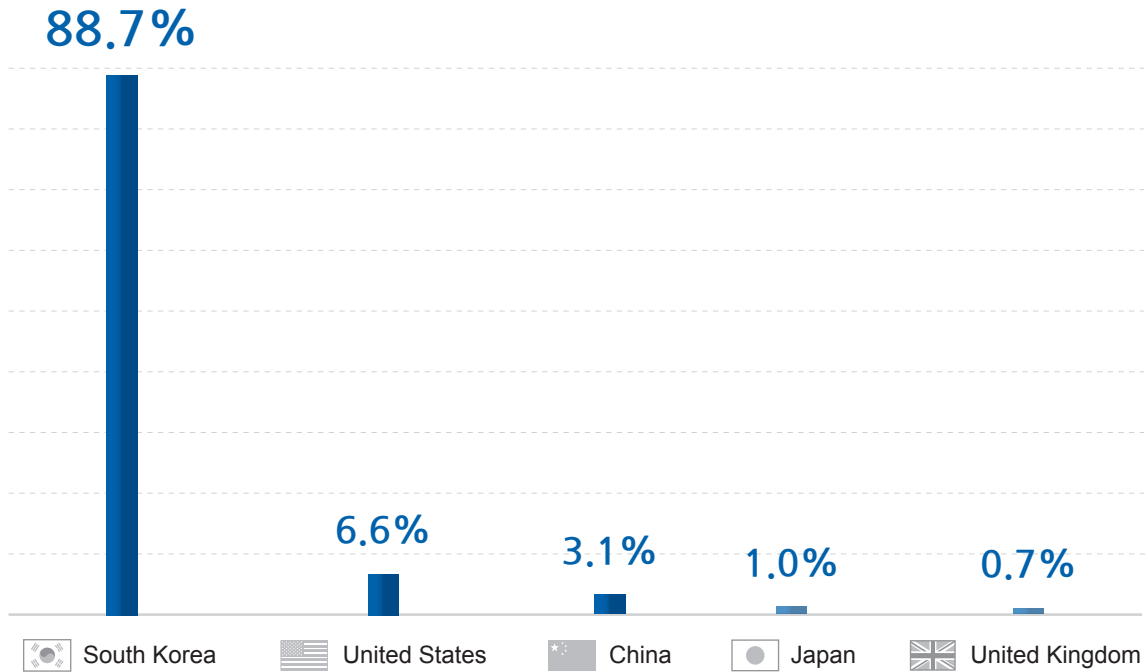
OWASP Top 10 Web Application Security Risks 2010	The number of detection
A1. Injection	
A2. Broken Authentication and Session Management	
A3. Cross Site Scripting (XSS)	
A4. Insecure Direct Object References	
A5. Security Misconfiguration	
A6. Sensitive Data Exposure	
A7. Missing Function Level Access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

※ Only WAPPLES report for customers provides detailed numerical information

< Table2. OWASP Top 10 Web Application Security Risks 2013 >

※ 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



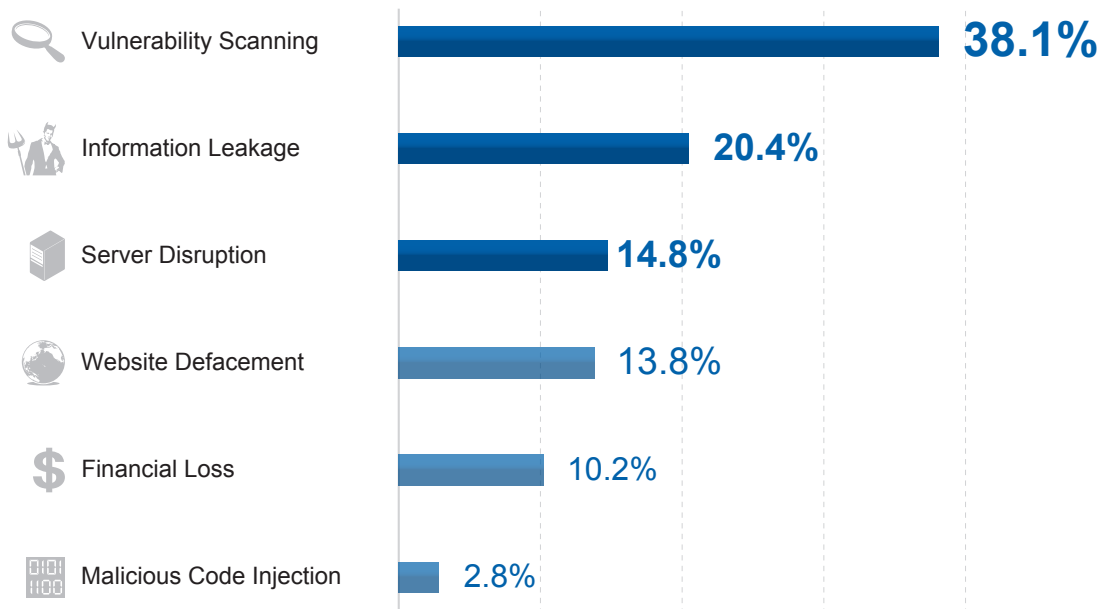
The graph above shows the countries from which most threats originated. During the period between January 1, 2014 and June 30, 2014, the Republic of Korea (South Korea) was the origin point for the greatest number of attacks, followed by the United States and China. This trend was the continuation of the same trends from 2013.

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	
United Kingdom	

< Table3. Top 5 Origins (Countries) of Web Attacks >

※ 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 January and June 2014, Vulnerability Scanning showed the highest frequency, followed by Information Leakage 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.
- ▶ **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).
- ▶ **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.

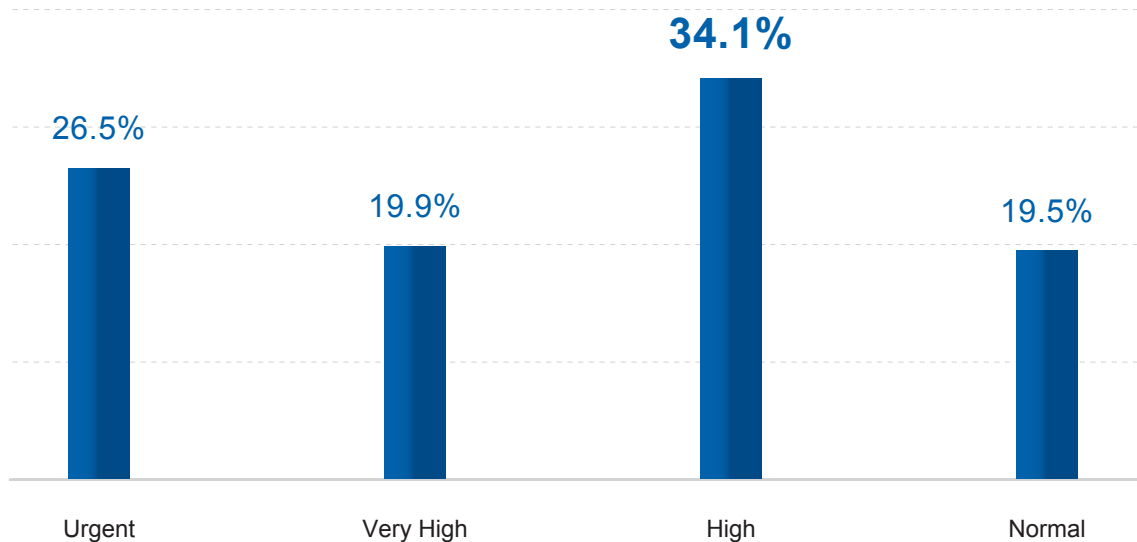
- ▶ **Website Defacement** refers to the manipulation of websites by unauthorized individuals, and includes the falsification of website contents, the acquisition of information by unauthorized individuals via the addition of malicious codes to a SQL server (SQL injection), uploading unauthorized files 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).
- ▶ **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).
- ▶ **A 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		
 Information Leakage		
 Server Disruption		※ Only WAPPLES report for customers provides detailed numerical information
 Website Defacement		
 Financial Loss		
 Malicious Code Injection		

< Table4. 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



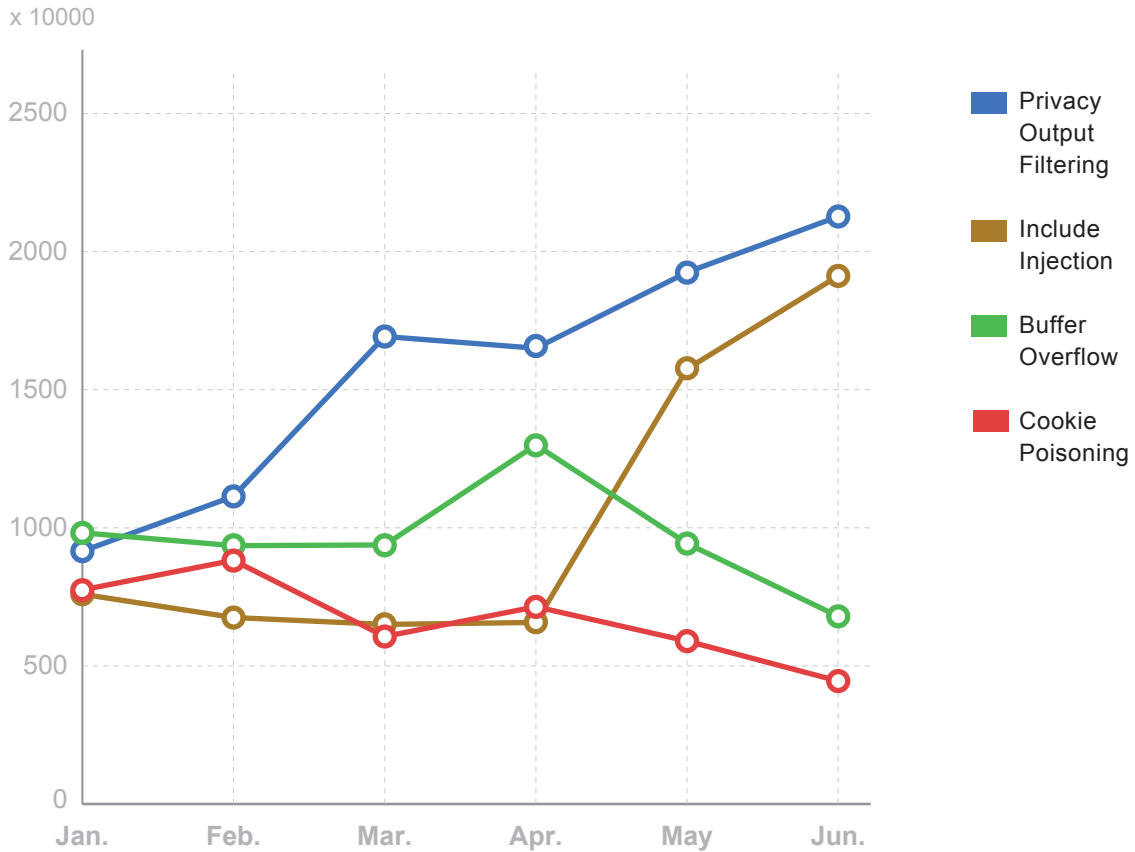
The graph above shows the distribution of attacks by risk level. During the period between January 2014 and June 2014, a High risk level showed the highest frequency, followed by Urgent and Very High. Please refer to the Appendix for a description of the relationship between the different Risk Levels 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	

< Table5. 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. During the first half of 2014, Privacy Output Filtering attacks, which attempt to expose private data, show the highest frequency, followed by Injection attacks. Include Injection are attempts to include malicious files by various methods, such as using a filename as a variable when requesting a specific URI to a web server.

Highly Risky Attack	Jan.	Feb.	Mar.	Apr.	May	Jun.
Privacy Output Filtering	—	—	—	—	—	—
Include Injection	—	—	—	—	—	—
Buffer Overflow	—	—	—	—	—	—
Cookie Poisoning	—	—	—	—	—	—

※ Only WAPPLES report for customers provides detailed numerical information

< Table6. 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. (Headquarter)

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 K.K. (Branch)

Akasaka Ascend Bldg 3F, 3-2-8 Akasaka, Minato-ku, Tokyo 107-0052, Japan
TEL. +81-3-5573-8191 FAX. +81-3-5573-8193 / www.pentasecurity.co.jp
INQUIRIES. +81-3-5573-8191 / japan@pentasecurity.com