Penta SECURITY
TRUST FOR AN OPEN SOCIETY

Web Application Threat Report

: Trends for the First Half of 2015

Table of Contents

Web Application Threat Report: An Introduction

This report is based on statistical data detected by WAPPLES, the Web Application Firewall (WAF) developed by Penta Security Systems Inc., with analysis conducted by Penta Security's Intelligent Customer Support (ICS) system.
This report was written for the purpose of providing enhanced security services to the customers using WAPPLES by sharing our statistical data collected from several of our products and analyzed by Penta to highlight trends regarding web application threats.

This report is based on the rules of the WAPPLES statistical information for OWASP Top Ten Risks and WAPPLES rules that respond to:

- What WAPPLES rules are the most frequently detected?
- What kinds of attacks are detected most often based on the 2013 OWASP Top 10?
- From which country 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 2015, hacking attempts aimed at website vulnerabilities were the most prevalent ('Normal' risk level attacks accounted for about 68% of all risk levels, and Vulnerability Scanning accounted for about 48% of all web attack types). 260 million Vulnerability Scanning attacks were detected, making it most common among attack types defined by WAPPLES. The number increased by 150 million compared to the second half of 2014. Attacks detected from the rules such as Invalid HTTP, Directory Listing, and Error handling, were revealed to be the primary attacks. Security Inc. recommends an appropriate configuration for WAPPLES (Invalid HTTP-'Block dangerous HTTP', Directory Listing –'Detect pages that are suspected as directory listing', Error Handling –'Block at the 1nd level').

According to OWASP's Top Ten Risks (2013), the most detected rule with a detection rate of 29.9% was Sensitive Data Exposure, which attempts to expose sensitive data. The second most highly detected rule with a 29% detection rate was Missing Function Level Access Control, which has an ability to bypass access control by an unauthorized attacker. Likewise, during the first half of 2015, second and third follow up attacks were launched following a successful initial attack. This included gathering vulnerabilities, personal and confidential information, or obtaining admin privilege from bypassing access control.

Some sensitive data exposure attacks targeted configuration files (such as dll, conf, ini, etc.), attempting to access and gain confidential data such attacks detected by Extension Filtering. Vulnerability Scanning, which commonly be launched by an automated tool, and Invalid HTTP, which was a request-based, are detected the most frequently. If these attacks are successful, the target website's vulnerabilities and confidential information can be exposed, causing secondary damage through downtime. Penta Security Inc. highly recommends an appropriate configuration (Extension Filtering – 'Only files with secure extensions are allowed access').

The results of the summarized data analysis in the first half of 2015 is shown on the table below

NO.	Web Attack Type	%
1	Vulnerability Scanning	48.3%
2	Server Disruption	13.8%
3	Monetary Loss	12.7%

NO.	Detection Rules	%
1	Extension Filtering	42.5%
2	Invalid HTTP	11.4%
3	Request Header Filtering	8.5%

NO.	Risk Levels	%
1	Urgent	10.7%
2	High	12.3%
3	Normal	68.8%
4	Low	8.1%

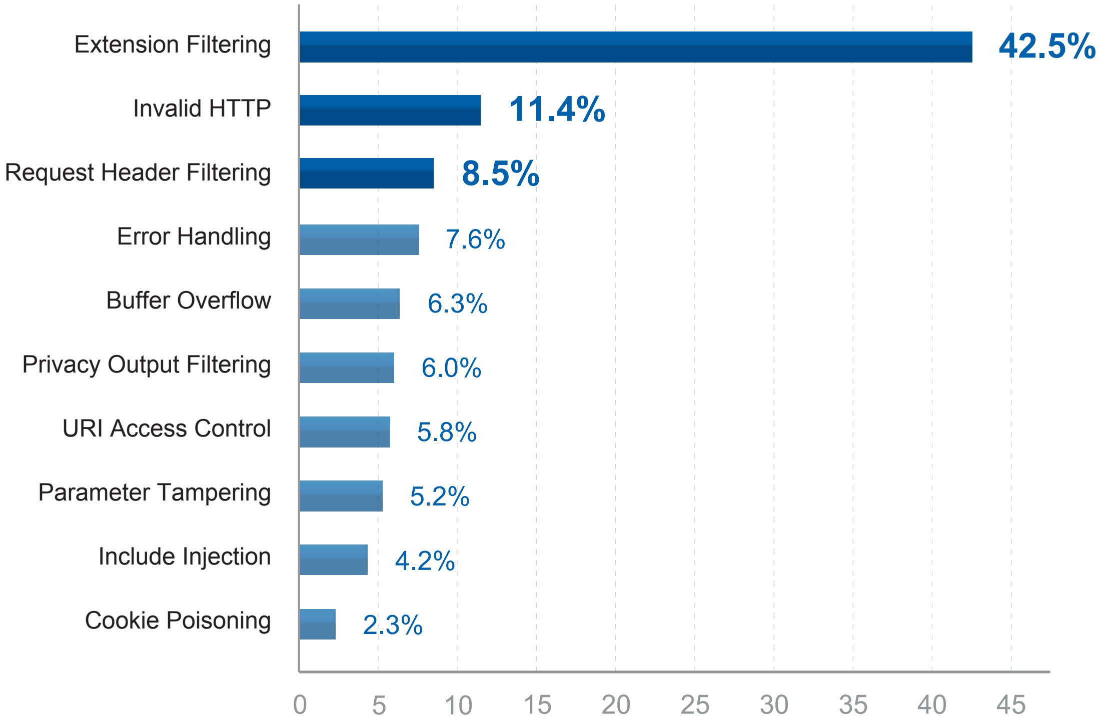
The data of this report was collected from 1,143 WAPPLES hardware with customers consenting to usage of their statistical data during the period between 2015-01-01 ~ 2015-06-30.

This accumulated data does not contain any other customer information, and contains only statistically analyzed data. In consideration to accurate analysis, 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



Graph 1 above shows which WAPPLES rules are the most frequently detected, during the collection period between 2015-01-01~2015-06-30. Extension Filtering showed the highest frequency followed by Invalid HTTP and Request Header Filtering.

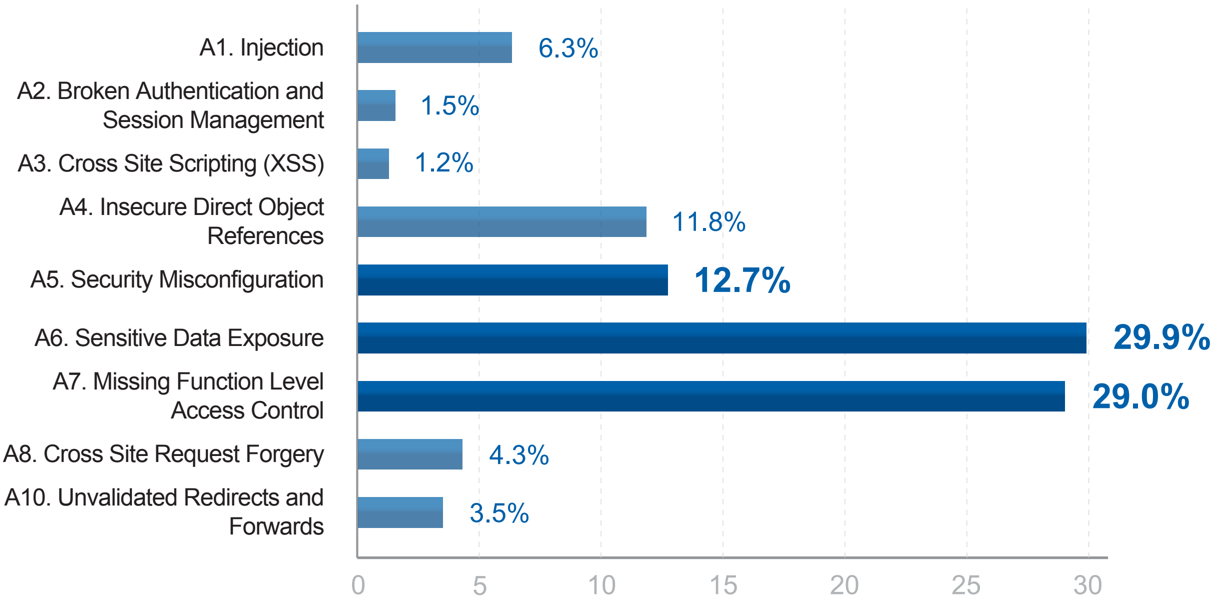
- **Extension Filtering** detects the attempts to access file extensions with vulnerabilities (.dll, conf, ini, etc) that could cause the malfunctioning of a web server or leakage of confidential information.

- **Invalid HTTP and Request Header Filtering** detects scanning vulnerability attempts of web servers, which can be performed by an automated tool such as ‘The Slapper worm’.

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

< Table 1. Top 10 Detections by WAPPLES Rules >

2. Top 10 Web Attack Based on OWASP 2013



The graph above shows which kinds of attacks were the most frequently detected, as defined by the 2013 OWASP Top 10. During the period between 2015-01-01 ~ 2015-06-30, Sensitive Data Exposure showed the highest frequency. Missing Function Level Access Control showed a high detection rate as well.

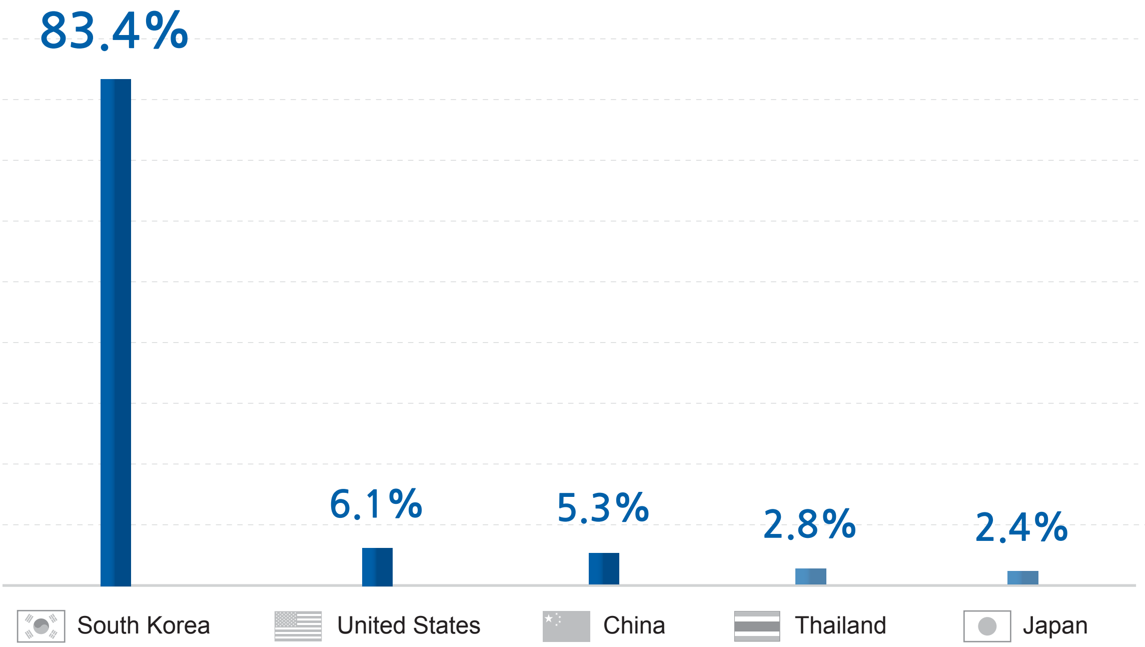
Sensitive Data Exposure is listed as A6 on OWASP top 10. This means that there have been many attempts to expose sensitive data such as bank card information, passwords, and transcription records, which must be well protected and managed. When successful, these attacks expose information transmitted as a plaintext and have huge impacts on businesses, unless a secure encryption system or a strong access control system is deployed.

Web Attack corresponding to OWASP 2013	Detected
A1. Injection	※ Only WAPPLES report for customers provides detailed numerical information
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	

< 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



Graph 3 above shows the countries detected as the most frequent origins of attacks.
During the period between 2015-01-01 ~ 2015-06-30, the Republic of Korea (South Korea) encompassed the greatest number of attacks, followed by the United States of America and China.

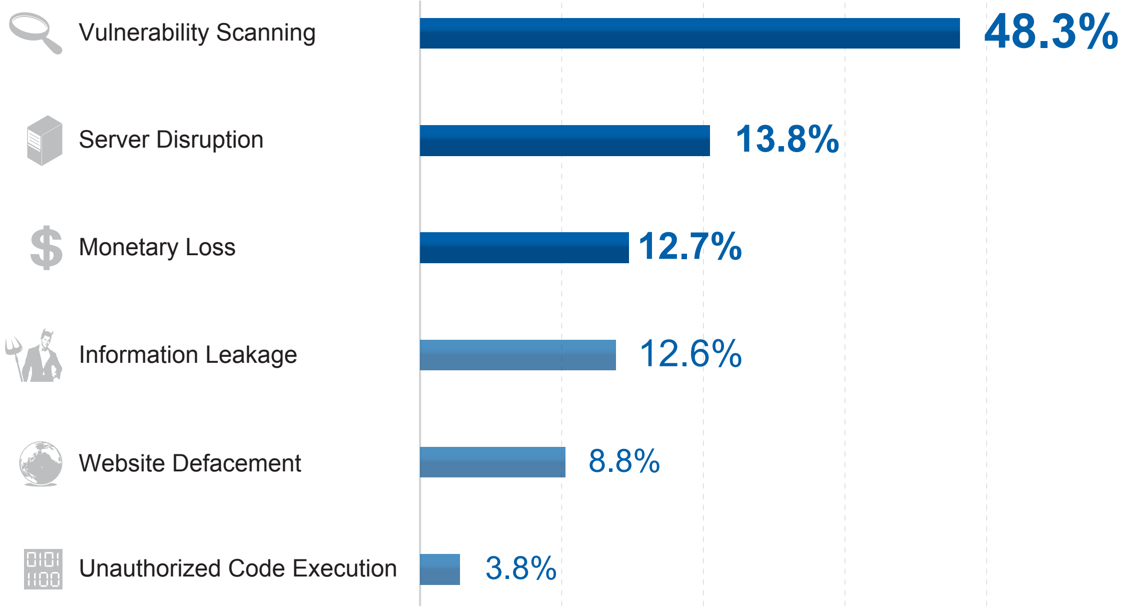
Since the data dealt with in this report is mostly based on the WAPPLES located within Korea, this accounts for the overwhelming number of threats originating from Korea.

Country Attack Origination Top 5	Detected
South Korea	※ Only WAPPLES report for customers provides detailed numerical information
United States	
China	
Thailand	
Japan	

< 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



Graph 4 above shows the top purposes behind web attacks. During the period between 2015-01-01~2015-06-30, Vulnerability Scanning showed the highest frequency (48.3%), followed by Server Disruption and Monetary Loss. Vulnerability Scanning refers to attempts to determine the existence and position of vulnerabilities in a web server.

This has increased significantly since the last report (2014). Invalid HTTP request, Directory Listing, Error Handling follow, and these attacks are preparatory actions prior to a serious attack taking place. Penta Security Inc. recommends protecting web servers and eliminating website vulnerabilities before being compromised by attacks that can cause material and immaterial damages.

- **Vulnerability Scanning** refers to attempts to determine the existence and position of vulnerabilities of a web server. This is most frequently conducted by using automatic attack tools which send invalid HTTP requests or URIs which do not comply with RFC standards, or by exposing the directory and error messages.

- **Server Disruption** includes disrupting the normal operation of the server through any means, such as flooding the server buffer (Buffer Overflow) or use of a sending method and header which have one or more vulnerabilities.

- **Monetary Loss** induces money fraud (transfer of user's 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 causing abnormal application actions by using unauthorized parameter values (Parameter Tampering).

- **Information Leakage** is defined as exposing important private information to or from websites (Privacy Input/Output Filtering), uploading files containing private information (Privacy File Filtering), or exposing a website's directory (Directory Listing)

- **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).

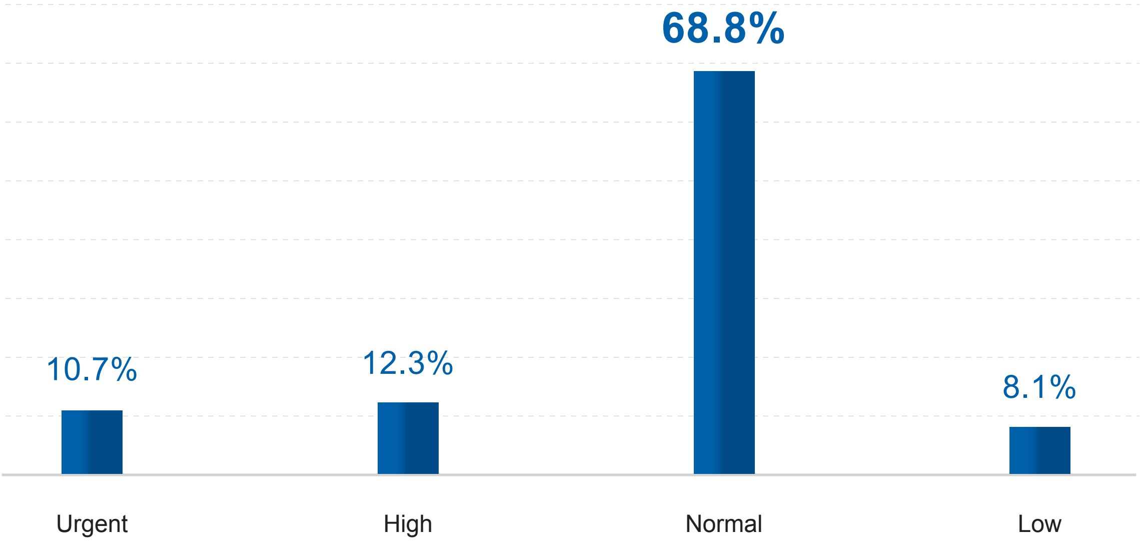
- **Unauthorized Code Execution** means the dissemination of Trojan or other viruses via server vulnerabilities. Hackers try to extract user information by adding malicious script codes (XSS), executing commands and acquiring information by adding server-side script to input (StealthCommanding), and transmitting malicious code by suspicious access (Suspicious Access).

Purpose of Web Attack	Detected
Vulnerability Scanning	※ Only WAPPLES report for customers provides detailed numerical information
Server Disruption	
Monetary Loss	
Information Leakage	
Website Defacement	
Unauthorized Code Execution	

< 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



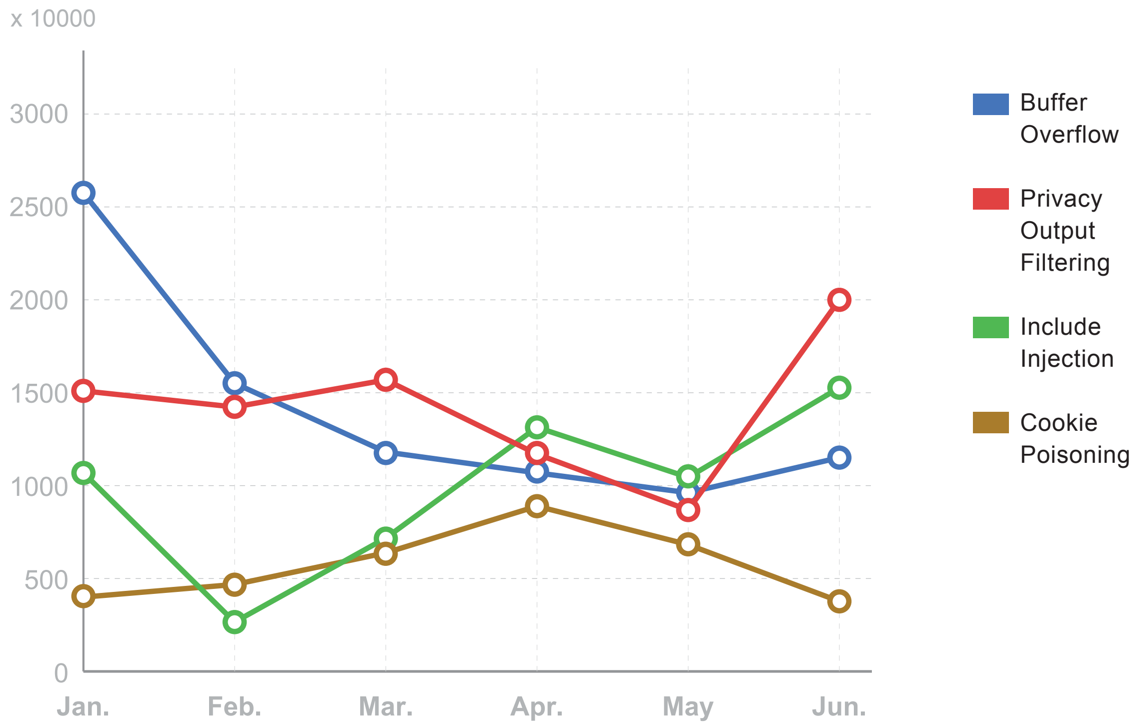
Graph 5 above shows the distribution of attacks based on risk level. During the period from 2015-01-01 ~ 2015-06-30, the ‘High’ level showed the highest frequency, followed by ‘Very High’ and ‘Urgent’ respectively (The number of High level attacks exceeded one billion, marking a 600 million increase from the 2nd half of 2014. See the Appendix for details on the relationship between Risk Levels and WAPPLES Rules).

Level of Risk	Detected
Urgent	※ Only WAPPLES report for customers provides detailed numerical information
High	
Normal	
Low	

< Table5. Risk Levels of WAPPLES Rules >

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

6. Web Attack Trends



Graph 6 above shows the monthly fluctuations for the 4 primary high-risk attacks. Buffer Overflow has been deemed the most prevalent attack during the first half of 2015. It can send excessive input streams or malicious codes which can cause denial of service, memory access error, or server side code execution in order to interrupt server operations or execute commands. Privacy Output Filtering was the second most prevalent attack during the period. These attacks are not difficult to execute, but the result can be just as fatal as server malfunction, denial of service, or confidential exposure. Penta Security Inc. highly recommends an appropriate WAPPLES configuration (Privacy Output Filtering –'Detect all kinds of private information').

High Risk top 4	Jan.	Feb.	Mar.	Apr.	May	Jun.
Buffer Overflow						
Privacy Output Filtering						
Include Injection						
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

The purposes of web attacks include:

1. Hurting a user's finances or to attain financial benefits.
2. Cause excessive damage to a server or interrupt server operations.
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 simple for vandalism purposes.
6. Leak individual, server, or database information

Type	WAPPLES Rules
Monetary 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
Unauthorized Code Execution	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
TRUST FOR AN OPEN SOCIETY

Penta Security Systems Inc. (Headquarter)
20F, 25, Gukjegeumyung-ro 2-gil, Yeongdeungpo-gu, Seoul, Korea 07327
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. (U.S.A)
Houston, Texas   www.pentasecurity.com/en

Penta Security Systems K.K (JAPAN)
Shinjuku-Ku, Tokyo   www.pentasecurity.co.jp