Penta SECURITY
TRUST FOR AN OPEN SOCIETY

Web Application Threat Report

: Trends for the Second Half of 2015

Table of Contents

Web Application Threat Report 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 data analyzed from WAPPLES statistical information. It contains information on the following:

- What WAPPLES rules are most frequently detected?
- What kinds of attacks are detected most often based on the 2013 OWASP Top Ten?
- From which country did most of the threats originate?
- What were the purposes of the attacks?
- Distribution of attacks by risk level
- Distribution of primary attacks by month
  (See Appendix for descriptions of WAPPLES rules)

Report Summary

For the second half of 2015, hacking attempts aimed at website vulnerabilities were the most prevalent. Critical risk level attacks accounted for 35% of all risk levels, and Vulnerability Assessment accounted as the purpose for 34% of all web attacks. The first half of 2015 indicated that 400 million attacks were identified as Vulnerability Assessment based, continuing to make it the top purpose of web attacks for the second half of 2015. Critical Risk Level type attacks can cause data loss and destruction, compromised server security and stolen administrative credentials. It is necessary for server users and security officers to pay close attention to prevent secondary damage using vulnerability scanning and policy enforcement.

Based on the 2013 OWASP Top Ten, the WAPPLES rule with the highest number of detections was Include Injection making up 31% of the detections total. This corresponds with A1 – Injection. This is where the Include function is used in the server side script, which then causes Website Defacement and Denial-of-Services. The level of difficulty to execute this attack type is relatively simple. In contrast to its execution, the consequences are quite detrimental and demands more appropriate countermeasures be taken. Following behind Injection risks, the second highest number of detections corresponded to A5 – Security Misconfiguration comprising 26% of the detections total. Attacks of this type exploit errors within security configurations, taking advantage of administrative privileges to hack target systems. During the second half of 2015, attacks of like these utilized information related to vulnerabilities to attack websites, specifically targeting the acquisition of administrator credentials.

Some sensitive data exposure attacks targeted configuration files (such as dll, conf, ini, etc.), att empting to access and gain confidential data such attacks detected by Extension Filtering. Vuln erability Assessment, which is commonly launched by an automated tool, and Invalid HTTP, whi ch is 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 dama ge through downtime. Penta Security Systems Inc. highly recommends an appropriate configur ation (Extension Filtering – 'Only files with secure extensions are allowed access').

Rank	Web Attack Type	Percent
1	Vulnerability Assessment	34%
2	Website Defacement	26%
3	Denial-of-service	17%

Rank	Detection Rule	Percent
1	Include Injection	24%
2	Request Header Filtering	12%
3	Buffer Overflow	11%

Risk Level	Percent
Critical	35%
High	29%
Average	24%
Low	12%

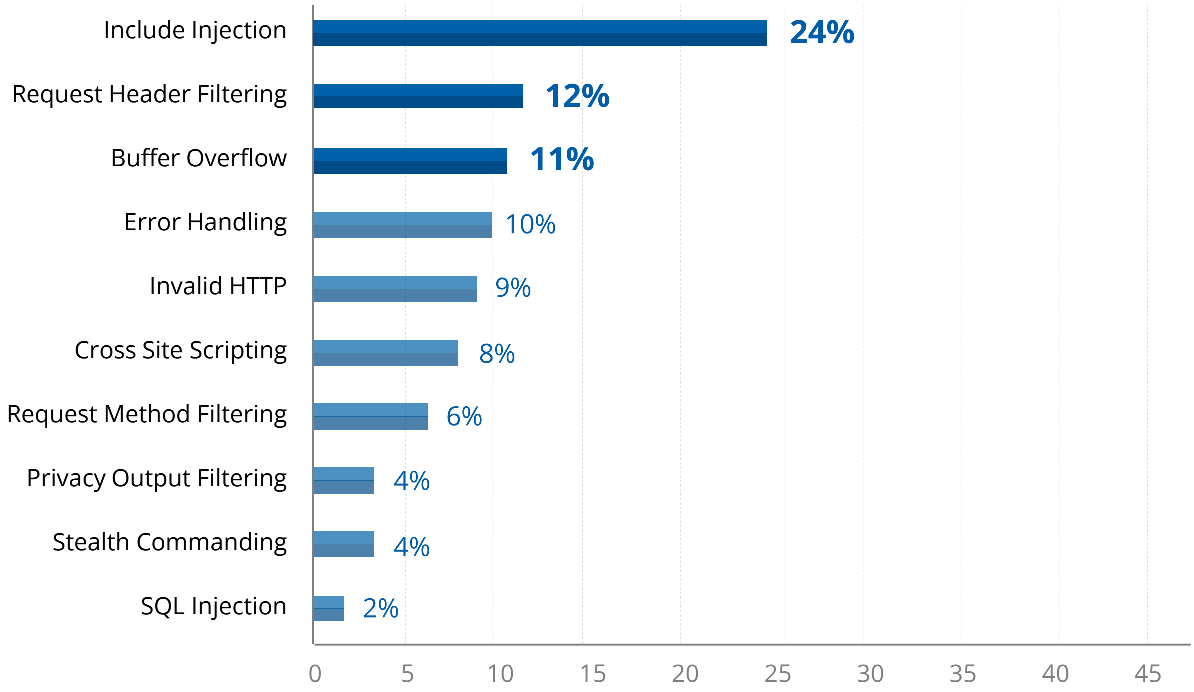
※ The data for this report was collected from 1,064 WAPPLES appliances with customers giving consent to use their statistical data. The data collection period was from July 1, 2015 to December 31, 2015.

※ The accumulated data does not contain any other customer information, and contains only statiscally analyzed data. For accurate analysis purposes, WAPPLES units that were undergoing evaluation were excluded.

※ The statistical information included in this report is provided by the WAPPLES Management System (WAPPLES MS), which can manage multiple WAPPLES at once.

데이터 분석

1. Top 10 Detected WAPPLES Rules



The above graph shows which rules are the rules with the most frequent detections during the period from July 1, 2015 to December 31, 2015. Include Injection showed the highest frequency followed Request Header Filtering and then Buffer Overflow. These fall into the Critical and High Risk Levels that when successfully executed can have severe consequences on the target systems.

▶ **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.

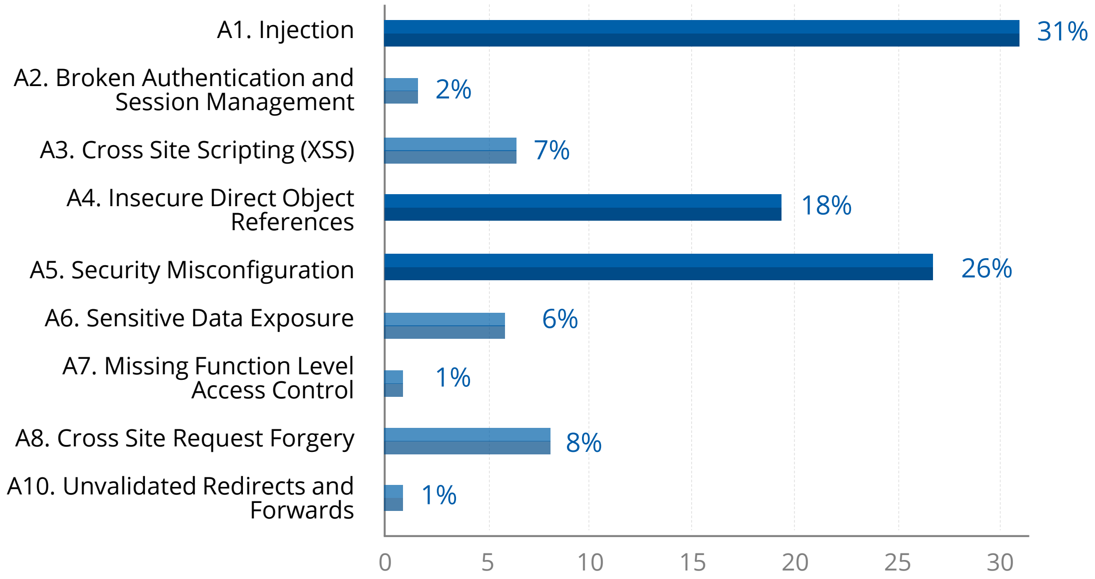
▶ **Request Header Filtering** is when an HTTP request has a header that is missing important information or has been modified abnormally, such as requests from automatic attack tools..

▶ **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	No. of Detections
Include Injection	Detailed information is available only to WAPPLES customers.
Request Header Filtering	
Buffer Overflow	
Error Handling	
Invalid HTTP	
Cross Site Scripting	
Request Method Filtering	
Privacy Output Filtering	
Stealth Commanding	
SQL Injection	

Table 1. Top 10 Detection Rules Based On WAPPLES Detections

2. Detection Figures Of 2013 OWASP Top Ten



The above graph shows the number of attacks detected for each of the 2013 OWASP Top Ten risks. During the period from July 1, 2015 to December 31, 2015, Injection showed the highest frequency. This was followed by Security Misconfiguration.

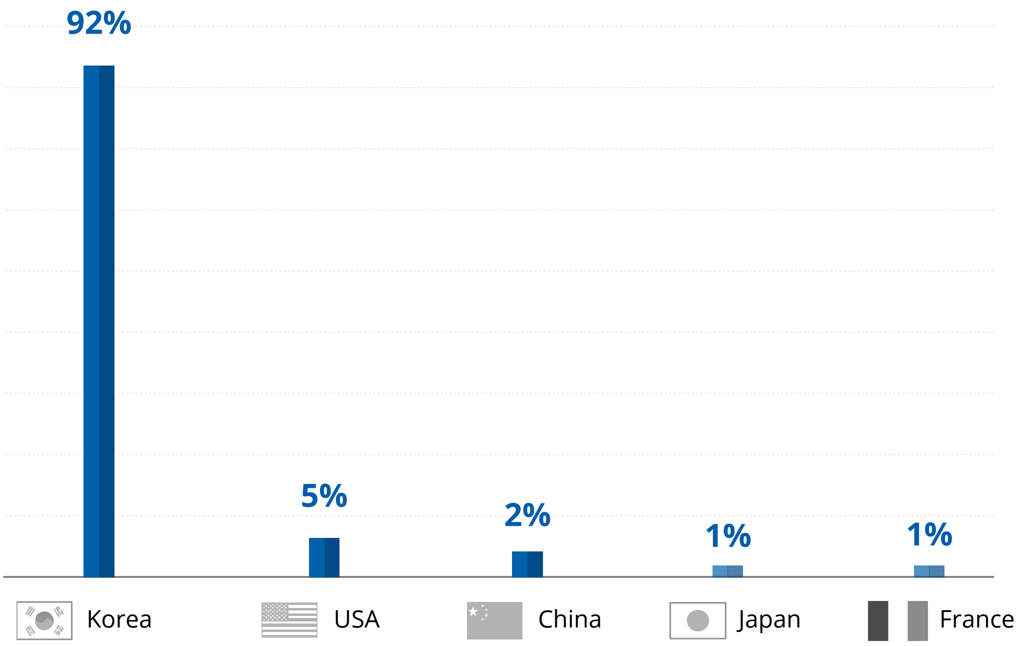
Injection is listed as A1 on the OWASP Top Ten. Using a little text, the extensive damage far outweighs the simplicity of the execution. Injection can cause the source of all data to be compromised. Extra measures must be taken to safeguard against injection vulnerabilities.

2013 OWASP Top Ten Type	No. Of Detections
A1. Injection	Detailed information is available only to WAPPLES customers.
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	

Table 2. Number of WAPPLES Detections For Each Of The 2013 OWASP Top Ten

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

3. Top 5 Geographic Origins Of Web Attacks



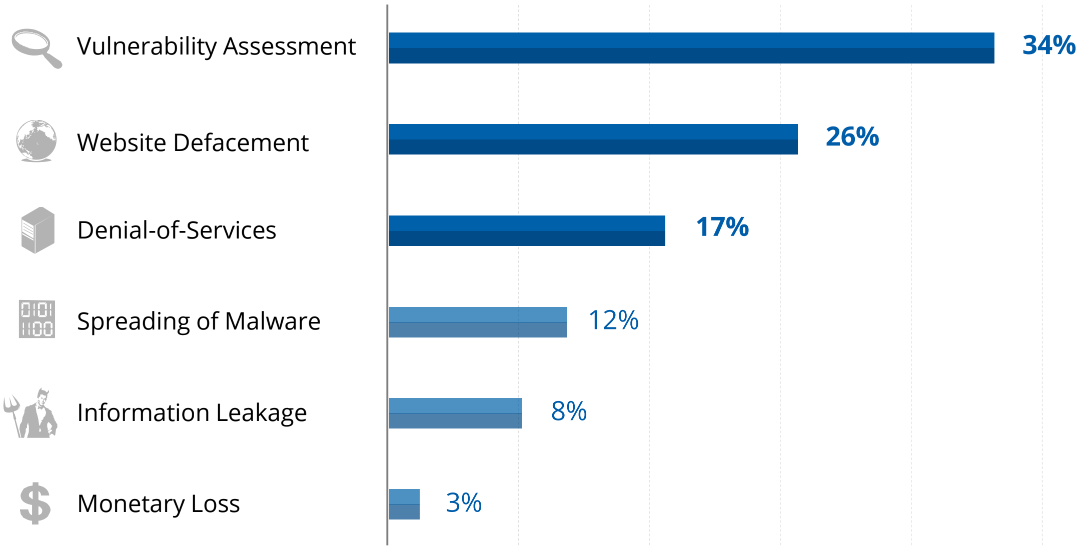
The above graph shows the countries where the highest frequency of attacks originate from. During the period from July 1, 2015 to December 31, 2015, the Republic of Korea encompassed the majority of the attacks followed by the United States and then China.

In should be known that the data for this report is mostly based on the WAPPLES located within Korea. This accounts for the overwhelming number of threats originating from Korea.

Source of Web Attacks	No. Of Detections
Korea	Detailed information is available only to WAPPLES customers.
USA	
China	
Japan	
France	

Table 3. Top 5 Geographic Origins Of Web Attacks Based On WAPPLES Detections

4. Purpose of Web Attacks



The above graph shows the purposes behind web attacks. During the period from July 1, 2015 to December 31, 2015, Vulnerability Assessment showed the highest frequency at 34% with 550 million detections. This was followed by Website Defacement and Denial-of-Service attacks. Vulnerability Assessment refers to attempts to determine the existence and position of vulnerabilities in a web server.

This has increased significantly since the last report. Attacks such as Invalid HTTP request, Directory Listing, Error Handling follow, and are preparatory actions prior to a serious attack taking place. Penta Security recommends protecting web servers and eliminating website vulnerabilities before being compromised by attacks that can cause severe damage.

- **Vulnerability Assessment** 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.

- **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 (File Upload), and the injection of risky scripts, files, and/or malicious code (Include Injection).

- **Denial-of-Service** 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.

- **Spreading of Malware** 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 (Stealth Commanding), and transmitting malicious code by suspicious access (Suspicious Access).

- **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)

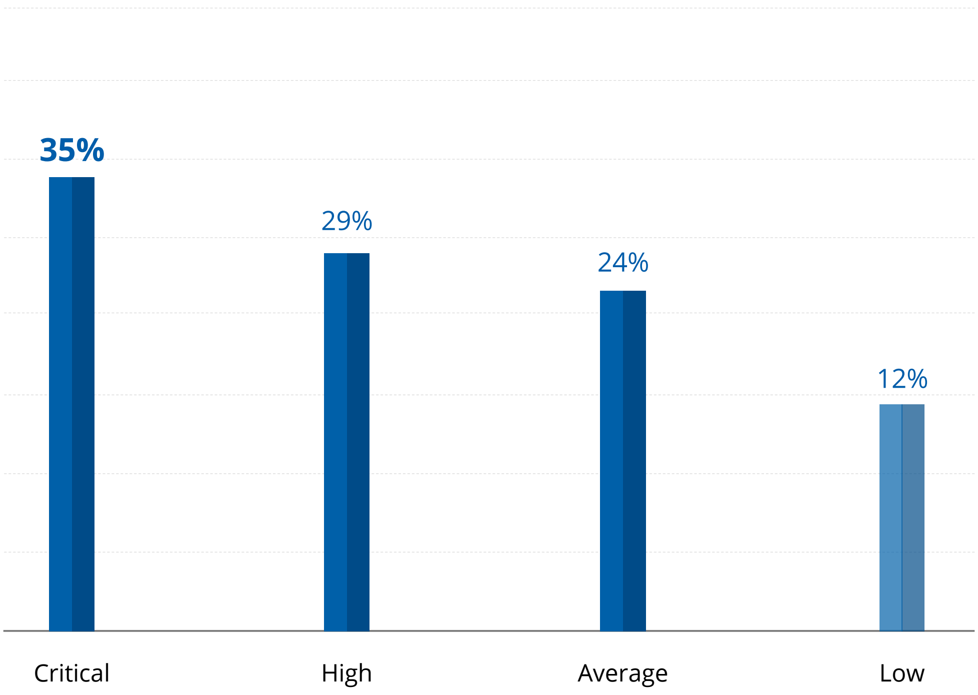
- **Monetary Loss** induces money fraud (transfer of user's money to unauthorized users) by acquiring personal user information. This can be done by modifying cookies to avoid the certification process (Cookie Poisoning), or by causing abnormal application actions by using unauthorized parameter values (Parameter Tampering).

Purpose of Web Attack	No. Of Detections
Vulnerability Assessment	Detailed information is available only to WAPPLES customers.
Website Defacement	
Denial-of-Service	
Spreading of Malware	
Information Leakage	
Monetary Loss	

Table 4. Purpose of Web Attacks Based On WAPPLES Detections

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

5. Risk Level of Detections



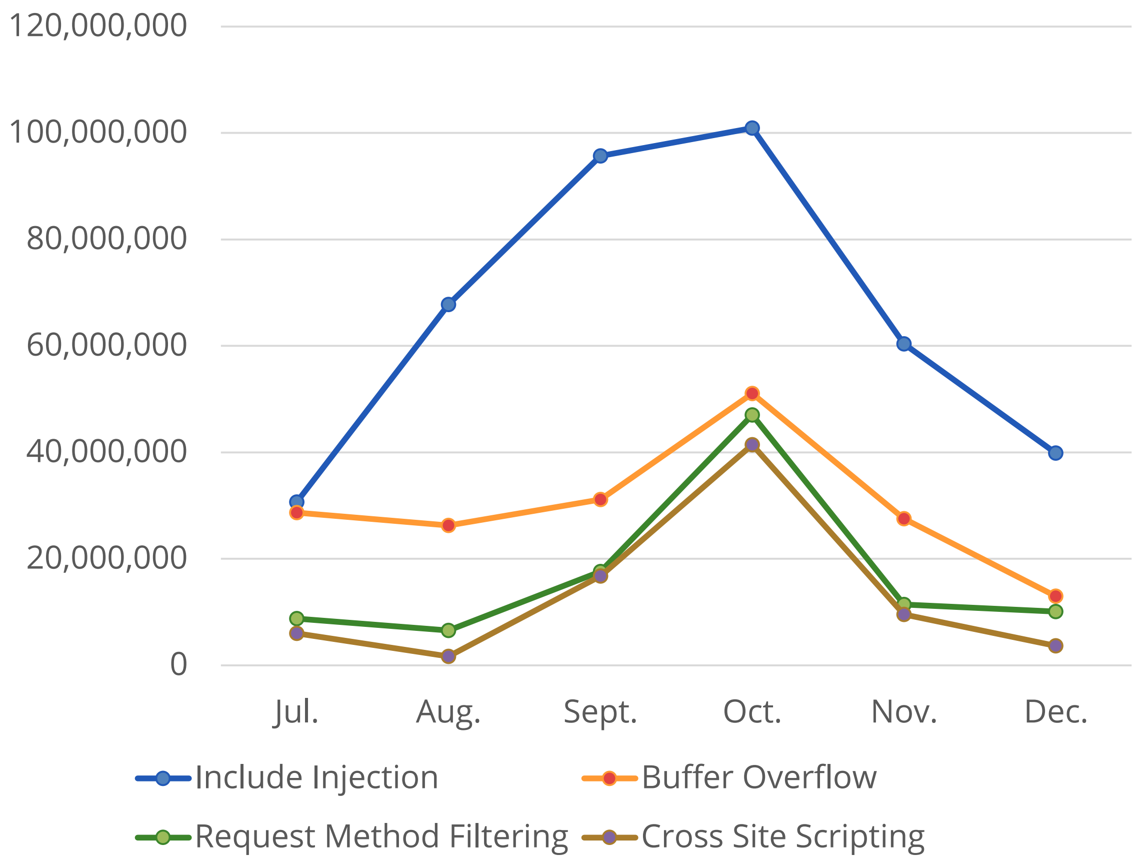
The above graph shows the distribution of attacks based on risk level. During the period from July 1, 2015 to December 31, 2015, the highest number of detections fell into the Critical risk level followed by High risk level types and then Average. The number of attacks were approximately 571 million, 462 million, and 388 million, respectively.

Risk Level	Detections
Critical	Detailed information is available only to WAPPLES customers.
High	
Average	
Low	

Table 5. Number of Detections By Risk Level

※ See the Appendix for details on the relationship between Risk Levels and the WAPPLES Rules.

6. Web Attack Trends



The above graph shows the monthly fluctuations for the four primary high risk attacks. Include Injection has been deemed the most prevalent attack during the second half of 2015. This was followed by Buffer Overflow, which can send excessive input streams or malicious codes causing denial-of-service.

Top 4 High Risk	Jul.	Aug.	Sept.	Oct.	Nov.	Dec.
Include Injection	Detailed information is available only to WAPPLES customers.					
Buffer Overflow						
Request Method Filtering						
Cross Site Scripting						

Table 6. Top 4 High Risk Level Web Attack Distributed By Month

Appendix

1. WAPPLES Rules Grouped by Category

1) Grouped According to OWASP Top 10

OWASP (Open Web Application Security Project) publishes 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) Grouped According to Risk Level

Risk Level	Description	WAPPLES Rules
Critical	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
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
Average	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
Low	The preparation stages of an attack, during which data vulnerabilities are gathered.	Directory Listing
		Input Content Filtering
		Error Handling
		Response Header Filtering

3) According to Web Attack Purpose

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. WAPPLES Rules Overview

WAPPLES Rule	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 that might possibility to be executed by the client
Directory Listing	Blocks the leakage of web sites' directory and files
Error Handling	Controls error messages so as to avoid exposure of information related to the web server, WAS, DBMS server, etc.
Extension Filtering	Blocks access of files which do not have permitted file extensions
File Upload	Blocks uploading of files that can be executed in 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 IP when more than the set value of access attempts from the same source 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

3. 2015 H2 WAPPLES Black List Top 30

Rank	Source IP	Country	Danger Level	Type
1	188.143.x.x	Russia	98.17	Spam
2	14.63.x.x	Korea	96.2	Hacking
3	117.21.x.x	China	95.3	Hacking
4	221.231.x.x	China	94	Hacking
5	37.187.x.x	TOR Network	93.9	Hacking
6	188.138.x.x	TOR Network	93.9	Hacking
7	185.65.x.x	TOR Network	93.7	Hacking
8	180.97.x.x	China	93.7	Hacking
9	91.121.x.x	France	93.4	Hacking
10	85.10.x.x	Germany	93.4	Hacking
11	77.247.x.x	Norway	92.2	Hacking
12	62.210.x.x	France	92.1	Hacking
13	85.25.x.x	TOR Network	91.75	Hacking
14	194.150.x.x	TOR Network	91.5	Hacking
15	64.79.x.x	US	91.3	Spam
16	176.10.x.x	ToR Network	91	Hacking
17	210.102.x.x	KR	90.8	Hacking
17	178.217.x.x	Poland	90.8	Hacking
19	5.79.x.x	US	90.2	Hacking
20	62.210.x.x	France	89.8	Hacking
21	46.4.x.x	Germany	89.8	Hacking
21	94.242.x.x	Greece	89.7	Hacking
23	192.42.x.x	ToR Network	89.6	Hacking
24	195.154.x.x	France	89.5	Hacking
25	176.126.x.x	US	88.9	Hacking
26	158.85.x.x	US	88.8	Spam
27	66.96.x.x	US	88.6	Hacking
28	98.19.x.x	US	88.5	Spam
29	66.76.x.x	US	88.1	Spam
30	64.251.x.x	US	88.1	Hacking

* This data was provided by the ICS Inspector and is available exclusively to WAPPLES customers.

Penta SECURITY
TRUST FOR AN OPEN SOCIETY

Penta Security Systems Inc. Corporate Headquarters
20F, 25, Gukjegeumyung-ro 2-gil, Yeongdeungpo-gu, Seoul, Korea 07327
Phone 02-780-7728 Fax 02-786-5281 | www.pentasecurity.com/en
Inquires 02-2125-6694 | global@pentasecurity.com

Penta Security Systems Co.
Houston, Texas | www.pentasecurity.com/en

Penta Security Systems K.K
Shinjuku-Ku, Tokyo | www.pentasecurity.co.jp