Penta SECURITY
enterprise · iot · blockchain
cloudbric

Web Application Threat Trend Report

Trends for the Second Half of 2020

Penta Security Systems Inc.
Cloudbric Pte. Ltd.

Penta SECURITY
cloudbric

Contents

I. Overview

1. Objective of Report

This Web Application Threat Trend Report (WATT Report) is complied with the detection log data from Penta Security's WAPPLES, the web application firewall with No. 1 market share in the Asia Pacific[1)], along with the detection log data from Cloudbric's WAF, an edge-computing security services company. This report only contains data that customers have agreed to share, all of which are collected by Penta Security's Intelligent Customer Support (ICS) system and Cloudbric.

This WATT Report was analyzed and written based on the worldwide distribution of Cloudbric WAF's web attack data and machine learning technology, developed by Penta Security. The main purpose of this report is to identify web attack patterns through the latest attack trend analysis and reflect the predicted results to WAPPLES/Cloudbric operations.

This report is written and distributed for the purpose of providing information on web attack trends to all readers interested in web security trends, including WAPPLES/Cloudbric customers, partners, security managers of companies and institutions, and researchers at academic institutions.

Through this report, readers are provided with various statistical information on major web attacks based on the detection rules of WAPPLES/Cloudbric, trend information on attack types and malicious IPs of major attackers, statistical information on regions where major web attacks originate, and web attack trends by industry and timeframe.

1) Industry Quotient, Frost & Sullivan, 2015.

II. Executive Summary

This report analyzes attack data based on the top 5 rules that are deemed most important amongst all detection rules of WAPPLES and Cloudbric. The analysis is conducted with regards to attack types by malicious IP trend, industry, and country of origin.

In the second half of 2020, more than 50% of all attacks were targeted for information leakage. Exploitations have been carried out through File Upload, and SQL Injection, which uploads files such as exe, .jsp, .php to the web server by unauthorized users that add malicious codes to codes running on the server, in addition to acquiring or manipulating dangerous script information.

We compared the rules of WAPPLES/Cloudbric and the top 10 web attack types selected by OWASP. The most detected attacks were Injection type that use the Include function in server-side scripts to interfere with website modulation and server operation, followed by Broken Authentication attack type which is caused by mis-implementation of services associated with authentication and session management that can cause exploitation of privileges via passwords, keys, and session tokens. To prevent these attacks, we recommend that your organization creates an account password to prevent attackers from exploiting it. Additionally, companies must take security measures sequentially by checking authorization and admin privileges.

The highest number of attacks detected by WAPPLES and Cloudbric was from Extension Filtering. In terms of Request Header Filtering, unlike HTTP Requests that are normally sent by a web browser, the header detects the request as an abnormal request if the prerequisite is missing or invalid.

Below is the summary table of web attacks analyzed by WAPPLES/Cloudbric from July 1st to December 31st.

Ranking	Type of Attack	Percentage
No. 1	Extension Filtering	23.72%
No. 2	Request Header Filtering	16.73%
No. 3	SQL Injection	15.21%

<Top 3 Detected Attacks>

Ranking	Objective	Percentage
No. 1	Information Leakage	51.91%
No. 2	Scan Vulnerabilities	28.58%
No. 3	Malicious Code Distribution	9.28%

<Top 3 Purposes of Attack>

Ranking	OWASP TOP3	No. of Detects
No. 1	injection	17022983
No. 2	Broken Authentication	13204227
No. 3	Sensitive Data Exposure	7632723

<Types and No. of Attacks in OWASP TOP 10>

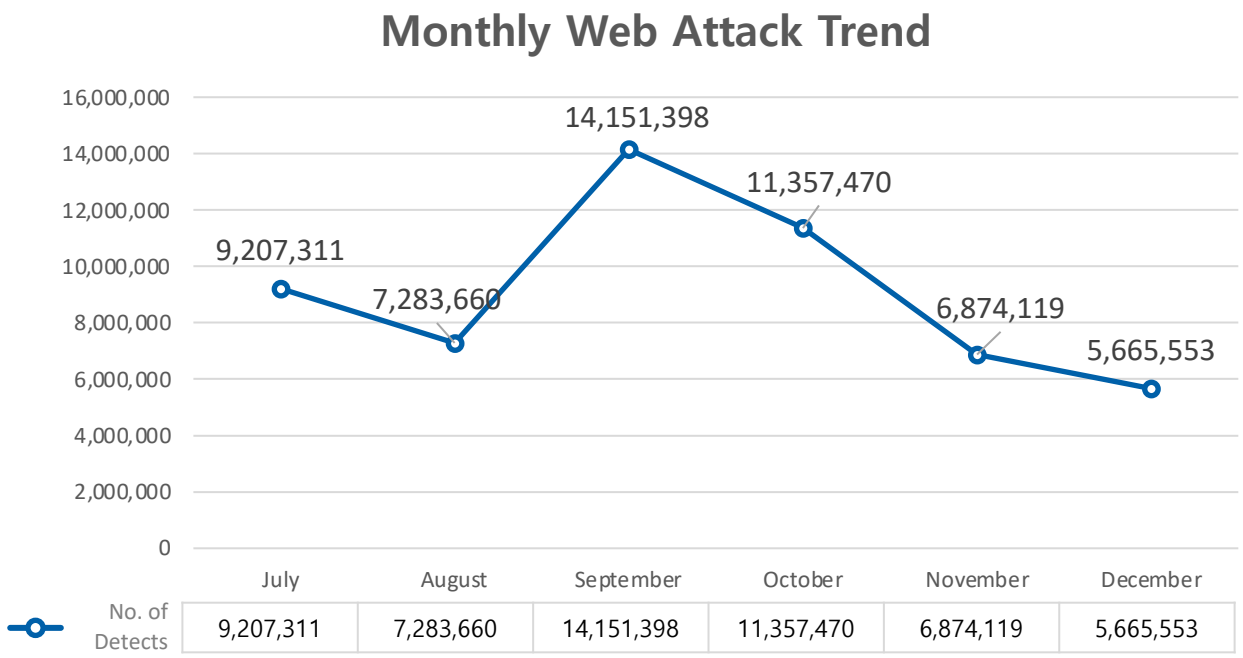
Ranking	Type of Attack	Percentage
No. 1	Cross Site Scripting	30.25%
No. 2	SQL Injection	19.73%
No. 3	Stealth Commanding	15.37%

<Top 3 Types of Attack>

III. Trends in Web Attacks for the Second Half of 2020

1. Monthly Web Attack Trend

This monthly trend in web attacks shows the details of monthly attacks. This helps prevent web attacks and prepare countermeasures in advance. The graph below shows an analysis of web attacks detected through WAPPLES and Cloudbric WAF in the second half of 2020.



This shows the trend of detected attacks from July to December 2020. The average number of attacks increased to about 9 million between August and September, and more than 14 million attacks occurred in September. Then the number of attacks gradually decreased since September.

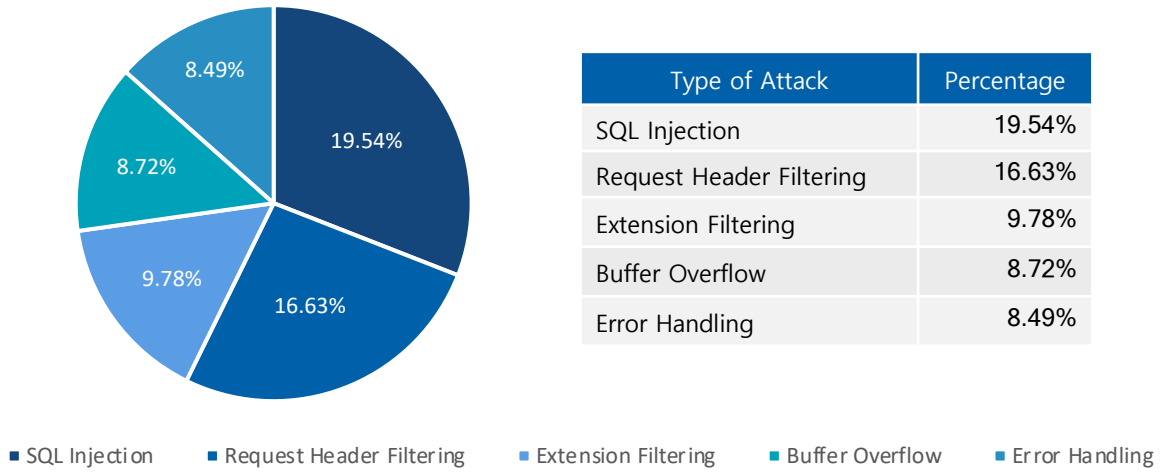
It is estimated that a large number of attacks were aimed during the holidays in Asia, in September. In connection with this trend, the hacking incidents that occurred in September were mainly targeted at 1) Financial Institutions and 2) Financial Certifications Institution.

Especially in 2020, there were many online classes and activities due to COVID-19, so there were many attacks that targeted these web activities. Recently, many new websites and services that were created due to COVID-19 were found to have more security vulnerabilities than other websites.

III. Trends in Web Attacks for the Second Half of 2020

The web attack trend by rule analysis shows which attacks occurred frequently throughout the second half of 2020. Based on this, basic web attack response guidelines can be established for security countermeasures against web attacks. The graph below is an analysis of web attacks through WAPPLES and Cloudbric detection rules.

Web Attack Trends by Rule



Type of Attack	Percentage
SQL Injection	19.54%
Request Header Filtering	16.63%
Extension Filtering	9.78%
Buffer Overflow	8.72%
Error Handling	8.49%

SQL Injection(19.54%) accounted for the highest number of attack detentions, with Request Header Filtering(16.63%), Extension Filtering(9.78%), Buffer Overflow(8.72%), Error Handling(8.49%) following behind.

SQL Injection attack is an injection attack technique, which attacks the database by executing SQL statements that are not allowed or unrelated that occurs very frequently every year. Although it is one of the most common attacks, it requires a lot of attention because it can end up causing a severe information leakage. As various SQL injection attack methods are already discovered and well-known, it is critical to be prepared for SQL injection attacks.

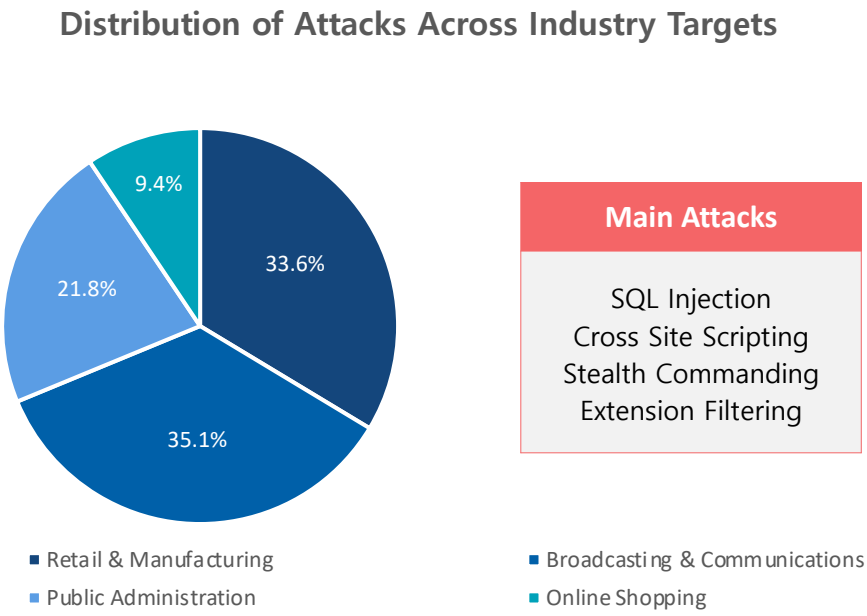
Request Header Filtering attack is an attack using HTTP Request request sent from a web browser. Unlike normal HTTP Request requests, hackers remove essential elements from the header of the request or writes other elements to make abnormal requests. Such attack can cause secondary damages as the information of the web server could be altered or the web server could be damaged.

Extension Filtering refers to access attempts to configuration files (dll, conf, ini, etc.) rather than the ones in extension formats commonly used by websites. This is a very dangerous attack as it can directly have impact on web server behaviors and web services once exposed to other users.

Attacks such as Buffer Overflow and Error Handling are also well known which can cause severe damages, so it is critical to establish security measures in advance.

III. Trends in Web Attacks for the Second Half of 2020

3. Trend by Industry



The graph above shows the percentage of web attacks by industry as detected by WAPPLES and Cloudbric. In addition to the "Web Attack Trends by Rule", this analysis provides further insights for each specific industry on how to stay prepared.

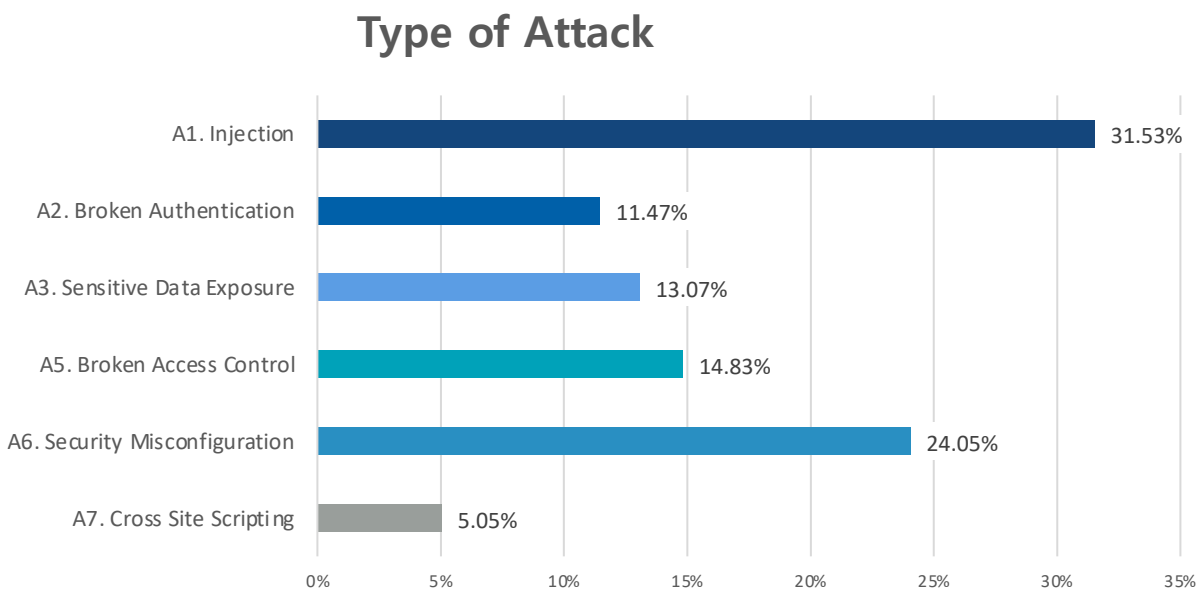
Attacks were distributed across the following industry targets: retail and manufacturing, broadcasting and communications, public administration, and online shopping. For the retail and manufacturing industry, the tremendous customer databases are highly tempting targets for hackers. This makes it crucial for retail and manufacturing firms to protect the personal data of their customers.

The broadcasting and communications industry industry are also facing frequent web attacks. Due to the COVID-19 pandemic, consumption of online media and usage of online lectures have grown significantly. Security personnel must pay close attention and establish multiple security measures to protect sensitive personal information from the hands of hackers.

The danger is not only limited to personal information. Each industry contains sensitive and valuable data from financial statements and contracts to intellectual property and trade secrets, all of which must be protected with adequate security measures.

III. Trends in Web Attacks for the Second Half of 2020

4. OWASP Top 10 Attack Trend by Attack Type



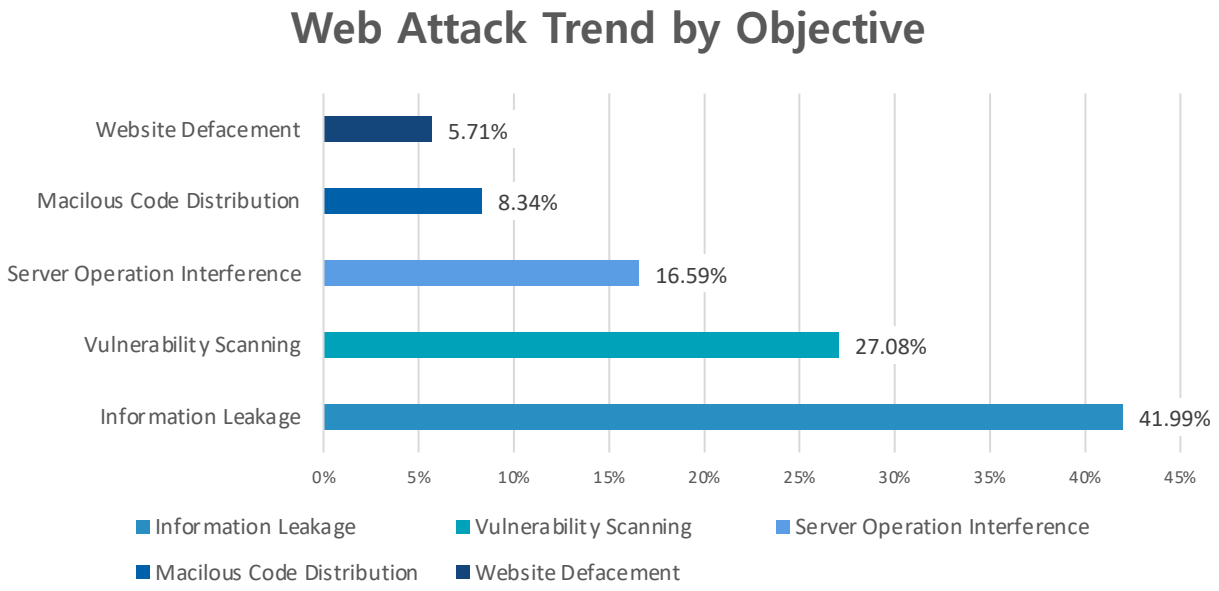
The graph above shows the frequency of attack types that matched the WAPPLES rule detection information with the 10 OWASP vulnerabilities. Injection attacks occurred the most followed by broken authentication.

In particular, Security Misconfiguration was ranked 5th in the OWASP Top 10 Attacks in the second half of 2020, however, it had ranked 2nd place in the second half with much higher risks. This usually is caused by being exposed to attacks by missing or vulnerable versions of the application server and the framework or cloud server's security settings, which shows how corporates must take quick and up-to-date security measure for protection.

OWASP TOP 10 Attack Types	No. of Detects
A1. injection	13505620
A2. Broken Authentication	4914103
A3. Sensitive Data Exposure	5596531
A5. Broken Access Control	6350053
A6. Security Misconfiguration	10301391
A7. Cross Site Scripting	2162824

III. Trends in Web Attacks for the Second Half of 2020

5. Web Attack Trend by Objective



The graph above is an analysis of web attack detection data for the second half of 2020, classified by objectives. The percentage of attacks originating from South Korea was in the order of information leakage (41.99%), vulnerability scanning (27.08%), malicious code distribution (8.34%), server operation interference (5,79%), and website defacement (4.30%).

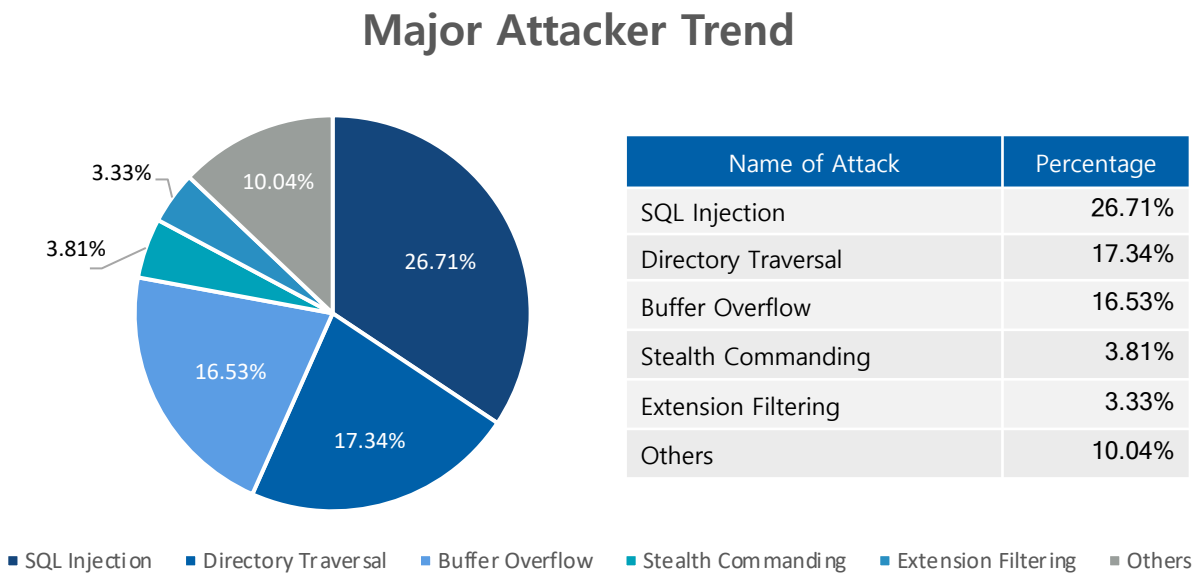
More than about 40% of the attacks were aimed at information leakage, unauthorized modification and manipulation of the website by unauthorized users such as website defacement that causes unauthorized alteration of a designated web page. Also, the attacks occurred through SQL Injection that steals or manipulates user information by adding malicious code to the SQL server and File Upload which uploads .exe, .jsp, .php, etc. that can be executed on the web server and Include Injection technique that injects dangerous scripts, files, and malicious codes.

The second most common objective is vulnerability scanning (27.08%). It uses an automated tool to make a request or response out of the standard of HTTP (Invalid HTTP), request a URI outside the format defined in RFC (Invalid URL), or expose directory contents of a website), error handling, etc. to determine which vulnerabilities exist on the website. Attacks are also attempted based on prior information obtained from these actions.

In addition, attacks aimed at server operation interference and website defacement have also occurred. Most common attacks were related to information leakage, which explains why users and corporates need precise attention and strengthened security measures.

III. Trends in Web Attacks for the Second Half of 2020

6. Major Attacker Trend



Name of Attack	Percentage
SQL Injection	26.71%
Directory Traversal	17.34%
Buffer Overflow	16.53%
Stealth Commanding	3.81%
Extension Filtering	3.33%
Others	10.04%

The table above is the result of selecting the top 10 web attackers July to December 2020 and analyzing their web attack trend. It is important to keep an eye on their web attack trend as their attack patterns are likely to cause real damage in the future.

Web attacks used by major attackers based on the second half of 2020 web attack trend analysis were SQL Injection(26.71%), Directory Traversal(17.34%), Buffer Overflow(16.53%), Stealth Commanding(3.81%), Extension Filtering(3.33%).

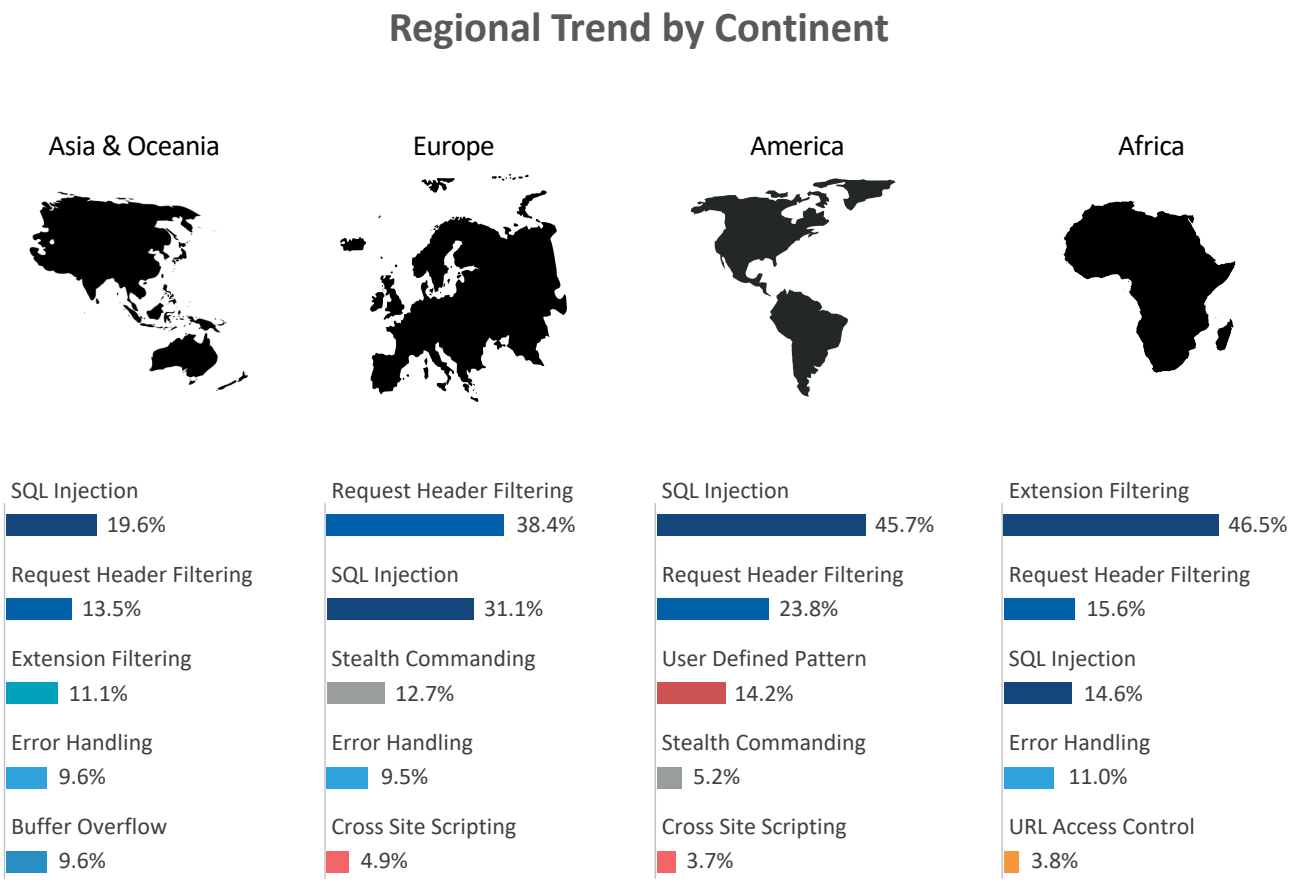
SQL Injection attack is a well-known attack technique that is considered very risky. It can attack a server's database by manipulating the client's input values and it usually occurs when user-entered data is not filtered properly. This attack is dangerous enough to manipulate the server database which requires special security attention.

The second highest attack Directory Traversal, allows non-accessible directories to end users to be accessed through websites. It can steal important data from the web server, such as passwd files with account information or log files that shows the server's status.

The main objective for these attacks is that it takes advantages of the vulnerabilities to steal information or to attack the web for the purpose of taking over the server. It is strongly recommended to prepare a guideline in advance to prevent these attacks.

III. Trends in Web Attacks for the Second Half of 2020

7. Regional Trend by Continent



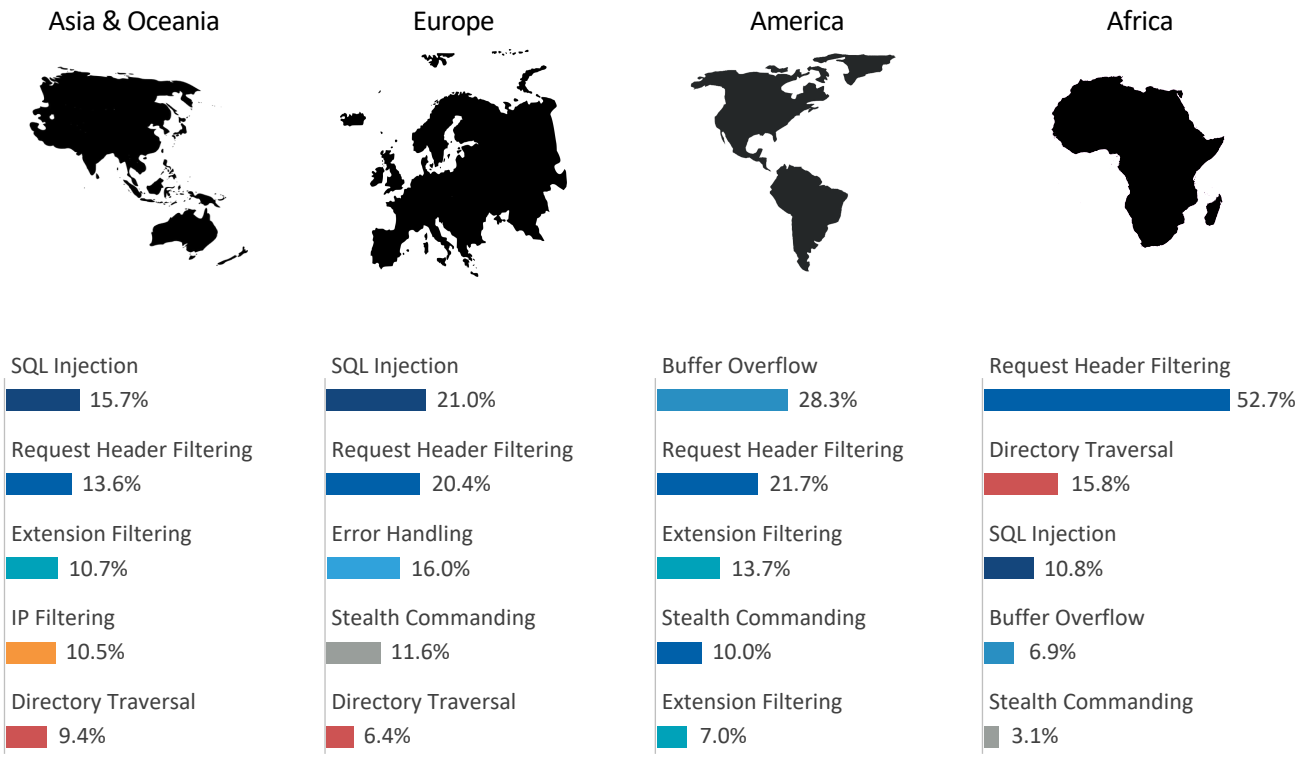
The graph above exhibits the breakdown of the web attack rules by their continent of origin. Similar to the breakdown last year, SQL Injection occurred the most in Asia & Oceania and in the Americas, Request Header Filtering in Europe, and Extension Filtering in Africa.

In addition, when looking at the count of all web attacks by continent, Request Header Filtering accounted for the largest percentage, while SQL Injection attacks are commonly occurred across all three continents. SQL Injection attacks were the highest in the Americas, Asia & Oceania. In particular, more than 40% of attempts of the attacks occurred in the Americas meaning cybersecurity professionals across the continent should prepare for web attacks based on such trend.

III. Trends in Web Attacks for the Second Half of 2020

7. Web Attack Trend by Continent

Breakdown of Attacks by Continent



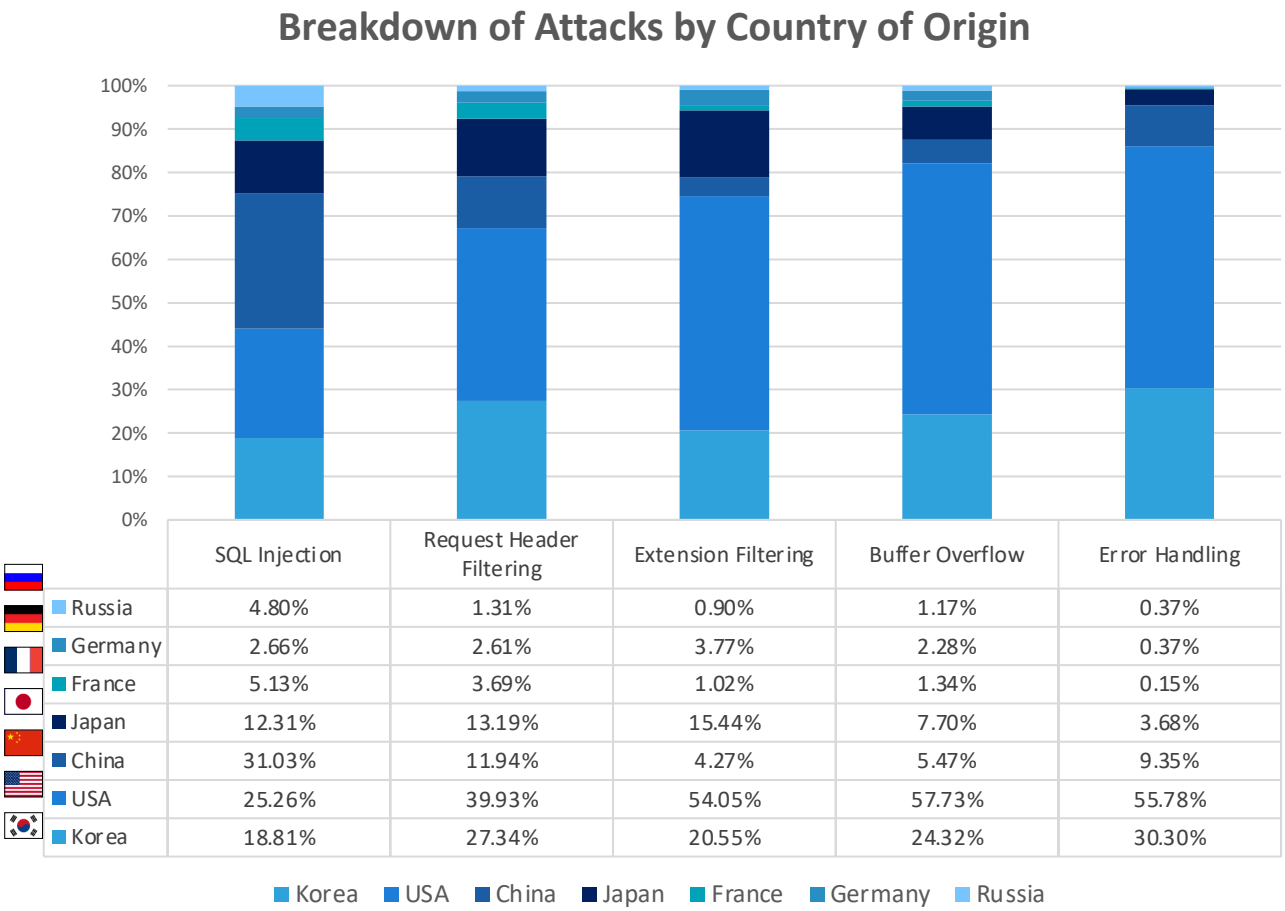
The graph above illustrates where the highest proportions of of web attacks originated from. SQL Injection originated the most from Asia & Oceania, Buffer Overflow from the Americas, and Request Header Filtering from Africa.

As seen in the graph, Request Header is one of the top 2 most common web attacks overall regardless of their country of origin. Also, as SQL Injection attack occurred the most in Asia & Oceania and Europe, these continents must enhance their web security measures to prevent these attacks.

Especially attackers in the Americas attempted a lot of Buffer Overflow attacks. Buffer Overflow attack can run arbitrary code on the server or disrupt program operations and can lead to information hijacking. In addition to these attacks, it is strongly suggested to establish security measures against various attacks such as Directory Traversal and Extension Filtering in advance.

III. Trends in Web Attacks for the Second Half of 2020

8. Web Attack Trend by Country of Origin



	SQL Injection	Request Header Filtering	Extension Filtering	Buffer Overflow	Error Handling
Russia	4.80%	1.31%	0.90%	1.17%	0.37%
Germany	2.66%	2.61%	3.77%	2.28%	0.37%
France	5.13%	3.69%	1.02%	1.34%	0.15%
Japan	12.31%	13.19%	15.44%	7.70%	3.68%
China	31.03%	11.94%	4.27%	5.47%	9.35%
USA	25.26%	39.93%	54.05%	57.73%	55.78%
Korea	18.81%	27.34%	20.55%	24.32%	30.30%

The graph above illustrates the top seven countries where the highest proportions of of web attacks originated from. Compared to the previous report, Russia is new to the list. As always, South Korea, China, USA, and Japan maintained their top spots on the list. There are slight changes, however, it is seen that countries that are at the top of the list are the main country of origin.

As shown on the above graph, SQL Injection, Request Header Filtering attacks have occurred across all countries. Also, most web attacks come from countries such as the U.S. and China, with high economic outputs. In particular, SQL Injection attack was the most occurred attack in the second half of 2020.

III. Trends in Web Attacks for the Second Half of 2020

9. Current Status of Major Web Vulnerabilities

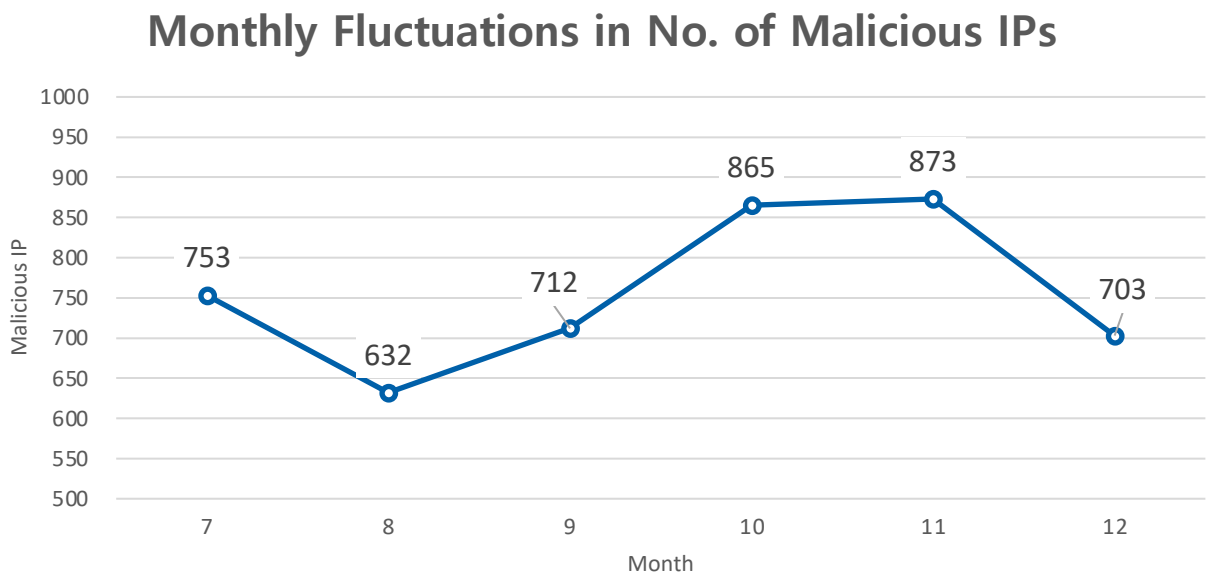
The main web vulnerability issue in the second half of 2020 was caused by CVE-2020-15999, which occurred from the browser Chrome. The vulnerability was able to attempt a heap buffer overflow attack, which is a buffer overflow attack in the heap data area and is one of the most dangerous attacks that can access or execute arbitrary code on the server. As a result, Google has patched a Chrome Zero Day vulnerability accordingly.

The vulnerability occurred on versions below 86.0.4240.111. Google Chrome uses an open-source development library called Freetype for font rendering, and the open-source version had a memory corruption defect problem that led to the attack.

To address the CVE-2020-15999 vulnerability properly, users must update to Google Chrome version 86.0.4240.111 or higher and Freotype 2.10.4 or higher. Updating each program to the latest version helps improve security tremendously. We recommend that you always look at security updates for not only the browsers, but also other programs to maintain your applications up-to-date for safety reasons.

III. Trends in Web Attacks for the Second Half of 2020

10. Variation Trend in No. of Malicious IPs



The graph above shows the fluctuations in the number of detected malicious IPs, the ultimate weapon used for web attacks. The reason we look at the number of malicious IPs is because they are a fair indicator of the frequency and severity of web attacks. Nevertheless, it is not meant to be a reliable indicator because there are times when a single attacker uses multiple malicious IPs, and other times when a single malicious IP causes significant damage.

In this report, any attacker that was detected more than 6 times a month was defined as Malicious IP. By analyzing the fluctuations with specific events that occurred in the second half of 2020, it has helped us to identify attacker patterns and further enhance security against web attacks in the future when similar patterns and attacks are expected occur.

In 2020, Malicious IP fluctuation range reached from 632 to873, with and an average number of 756 each month. Especially in the second half of 2020, there were various hacking incidents related to COVID-19 and the U.S. presidential election. In October and November, when the number of Malicious IP cases was high, there were incidents like MS hacking incident related to the presidential election, and COVID-19 vaccine related hacking incidents.

Of course, there is a limit to the connection between various events and defining Malicious IPs. However, it is important to be prepared and checked for the risk of various web attacks, and to be prepared to respond quickly and accurately in accordance with the manual when an attack occurs.

IV. APPENDIX

1. Method of Analysis

The data reported in this WATT Report is collected from the logs of WAPPLES, a web application firewall widely distributed in the Asia Pacific region, and Cloudbric, a cloud and edge computing-based web application firewall (WAFaaS) distributed worldwide. The data collection duration is between July 1st to December 31st.

2. Key Differences from Previous Reports

Different from the previous WATT Reports, the 2020 H1 WATT Report included data from Cloudbric, a cloud-based web application firewall distributed around the world. Additionally, Penta Security's newly developed machine learning technology allowed for more accurate prediction of future attacks. In addition, by analyzing web attacks based on their objectives and based on OWASP Top 10, a more advanced report was created.

The WATT Report, which is published semi-annually, is prepared with both industry professionals and casual readers in mind. On the professional end, it provides insights for security managers, many of them being users of WAPPLES and Cloudbric. On the casual end, it is an easy read for general readers like those involved in research institutions who are interested in web security trends. In the future, we plan to update information through continuous research and analysis and publish a report semi-annually to identify and compare the latest trends.

3. Glossary

▪ Buffer OverFlow

A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations. Attackers can exploit this vulnerability to cause massive damage, inclu ding server data corruption, malfunction, and information leakage.

Potential Consequences: Server Errors and Information Leakage

▪ Website Defacement

An attack on a website that changes the visual appearance of a website or a web page. These are typically the work of d efacers, who break into a web server and replace the hosted website with one of their own.

Potential Consequences: Malicious codes that cause server terrorism, deletion of important files or information leakage

▪ Include Injection

In server-side scripts, an input function exists that allows you to read and execute the contents of a particular file. This is an attack that uploads malicious code that can cause the include function to run on an executable site.

Potential Consequences: Malicious codes that cause server terrorism, deletion of important files or information leakage

IV. APPENDIX

4. OWASP and WAPPLES/Cloudbric Rules

OWASP(Open Web Application Security Project) creates a list every three years of the most exploited and dangerous web application vulnerabilities, commonly referred to as the OWASP Top 10. Below is a list of the latest OWASP Top 10 and the respective WAPPLES/Cloudbric Rules used to protect them.

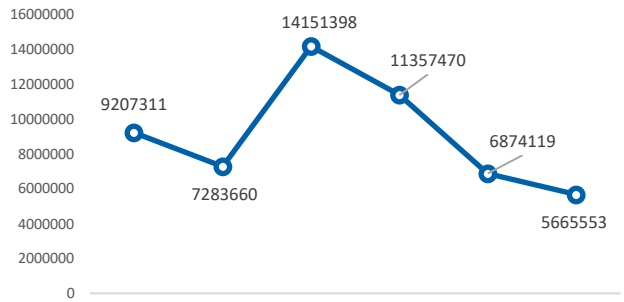
TOP	OWASP TOP 10	WAPPLES/Cloudbric Rules
1	injection	SQL Injection
		Stealth Commanding
		Cross Site Scripting
2	Broken Authentication	Cookie Poisoning
		Directory Traversal
		Cross Site Request Forgery
		SQL Injection
3	Sensitive Data Exposure	Privacy File Filtering
		Privacy Input Filtering
		Privacy Output Filtering
		Input Content Filtering
		Response Header Filtering
		Error Handling
4	XML External Entities	User Defined Pattern
5	Broken Access Control	Parameter Tampering
		Invalid URL
		Directory Traversal
		URL Access Control
6	Security Misconfiguration	Directory Listing
		Error Handling
		Response Header Filtering
7	Cross Site Scripting	Cross Site Scripting
8	Insecure Deserialization	Insecure Deserialization
9	Insecure Deserialization	User Defined Pattern
		Custom Rule
10	Using Components with Known Vulnerabilities	탐지로그 모니터링 및 연동

▪ WAPPLES/Cloudbric Rules may overlap throughout the list.

IV. APPENDIX

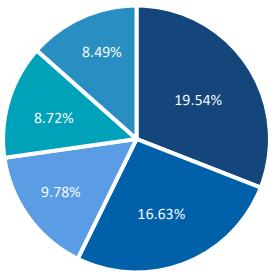
5. Table Summary

Monthly Web Attack Trend



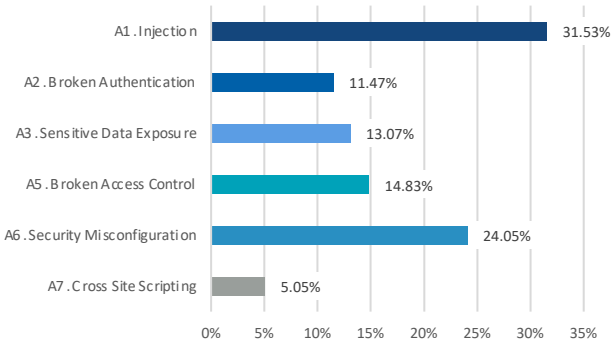
	July	August	September	October	November	December
No. of Detects	9207311	7283660	14151398	11357470	6874119	5665553

Web Attack Trends by Rule

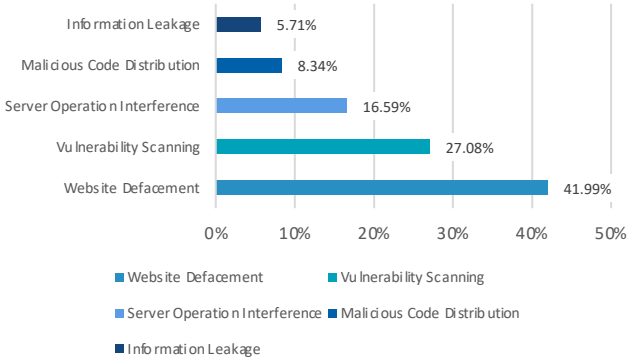


Type of Attack	Percentage
SQL Injection	19.54%
Request Header Filtering	16.63%
Extension Filtering	9.78%
Buffer Overflow	8.72%
Error Handling	8.49%

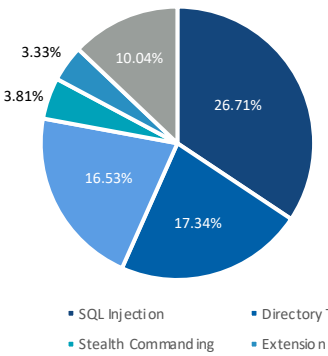
OWASP TOP 10 Attack Types



Web Attack Trend by Objective

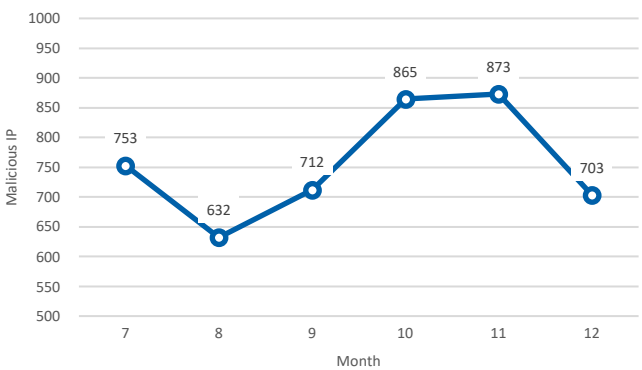


Major Attacker Trend



Name of Attack	Percentage
SQL Injection	26.71%
Directory Traversal	17.34%
Buffer Overflow	16.53%
Stealth Commanding	3.81%
Extension Filtering	3.33%
Others	10.04%

Variation Trend in No. of Malicious IPs



IV. APPENDIX

6. List of Top 40 Attackers

Ranking	IP Address	Country
1	175.21.X.X	China
2	221.158.X.X	Korea
3	175.21.X.X	China
4	115.171.X.X	China
5	1.235.X.X	Korea
6	121.78.X.X	Korea
7	66.249.X.X	United States
8	66.249.X.X	United States
9	110.53.X.X	China
10	153.127.X.X	Japan
11	129.21.X.X	United States
12	210.189.X.X	Japan
13	221.143.X.X	Korea
14	180.231.X.X	Korea
15	118.99.X.X	Indonesia
16	175.21.X.X	China
17	121.135.X.X	Korea
18	66.249.X.X	United States
19	66.249.X.X	United States
20	175.21.X.X	China
21	175.21.X.X	China
22	110.45.X.X	Korea
23	192.236.X.X	United States
24	110.45.X.X	Korea
25	110.45.X.X	Korea
26	172.104.X.X	United States
27	13.231.X.X	United States
28	148.72.X.X	Colombia
29	190.28.X.X	Colombia
30	35.200.X.X	United States
31	175.21.X.X	China
32	20.194.X.X	United States
33	211.253.X.X	Korea
34	41.193.X.X	South Africa
35	45.135.X.X	Unknown
36	54.180.X.X	United States
37	27.42.X.X	China
38	13.209.X.X	United States
39	89.187.X.X	Czech Republic
40	193.27.X.X	Unknown

Penta SECURITY
enterprise · iot · blockchain

KOREA www.pentasecurity.co.kr
GLOBAL www.pentasecurity.com
JAPAN www.pentasecurity.co.jp

cloudbric

GROBAL www.cloudbric.com
JAPAN www.cloudbric.jp

TU-Automotive AWARDS
TU-Automotive Awards
Best Auto Cybersecurity
Product/Service 2020

CYBER SECURITY EXCELLENCE AWARDS WINNER 2018
Cybersecurity
Excellence Awards
Winner 2018

CDM
Hot Company in
Web Application
Security for 2016

SC MAGAZINE
SC Magazine Europe
Best SME Solution

FROST & SULLIVAN
Asian Cyber
Security Vendor
of the Year

Gartner
Recognized on the
Gartner WAF
Magic Quadrant

1
No.1 WAF
Vendor in the
APAC Region

ICSA labs CERTIFIED
ICSA Labs
Certified WAF

The First and Only
CCEAL4 Certified
WAF

PCI DSS COMPLIANT
PCI-DSS
Compliance