cloudbric

Penta SECURITY

cloud · iot · blockchain

Web Application Threat Trend Report

Trends for the Second Half of 2021

Cloudbric Corp.

Penta Security Systems Inc.

cloudbric
Penta SECURITY

Contents

I. Overview

1. Objective of report

The 2021 H2 Web Application Threat Trend Report (WATT Report) is compiled based on detection log data from both Penta Security's WAPPLES, the web application firewall with leading market share in the Asia Pacific[1]; and Cloudbric, an edge-computing security solutions provider. The reported attacks are detected and logged by Penta Security's proprietary machine learning technology, then collected from Penta Security's Intelligence Customer Support (ICS) system and Cloudbric, providing an accurate representation of web attacks worldwide during the second half of 2021.

Penta Security and Cloudbric conduct periodic data analyses to identify the latest web attack trends and patterns, which are then reflected in the future operations of WAPPLES and Cloudbric. This report contains the results of these analyses, compiled and distributed for the purpose of providing information to all readers interested in web security trends, including customers and partners of WAPPLES and Cloudbric; CISOs, CSOs, and security administrators at enterprises and government agencies; and researchers at academic institutions. All data are handled and disclosed in accordance with terms agreed upon by the customers.

1) *Industry Quotient*, Frost & Sullivan, 2015.

II. Executive Summary

The data presented in this report are selected based on the top five most important detection rules of WAPPLES and Cloudbric. Throughout the report, readers will be presented with analyses on trending attack types, most exploited OWASP Top 10 vulnerabilities, targeted industries, IP addresses of major threat actors, and regional trends on where attacks occur and originate.

During the second half of 2021, over 40% of attacks were aimed at stealing or leaking sensitive information, where attackers attempt to gain access to sensitive data by exploiting website vulnerabilities. One commonly used attack technique is **File Upload**, where attackers upload corrupted EXE, JSP, and PHP files containing malware to the server, enabling them to retrieve sensitive data from the database.

Putting all attacks into OWASP Top 10 categories, the most exploited vulnerability is **Cryptographic Failures**. Coming second is **Injection**, where attackers inject malicious scripts into the SQL and NoSQL queries and OS commands, allowing them to access the server.

Based on the top five detection rules of WAPPLES and Cloudbric, the most observed attack type is **Extension Filtering**, In these attacks, attackers normally gain access through modifying configuration files (e.g. DLL, CONF, INI, etc.) containing vulnerabilities. When unauthorized individuals access these files, they could gain control of the web server to directly affect the web service.

Below is a summary of the top 3 web attacks detected by WAPPLES and Cloudbric from July 1 to December 31, 2021.

Rank	Attack Type	Percentage
1	Extension Filtering	23.66%
2	Error Handling	15.61%
3	SQL Injection	13.23%

<Top 3 Detected Attacks>

Rank	Attack Objective	Percentage
1	Information Leakage	46.31%
2	Vulnerability Scanning	35.46%
3	Server Interference	7.52%

<Top 3 Attack Objectives>

Rank	OWASP TOP 3	Cases
1	Cryptographic Failures	19,948,457
2	Injection	17,130,978
3	Insecure Design	15,879,767

<Top 3 Attacks from OWASP Top 10>

Rank	Attack Type	Percentage
1	Cross Site Scripting	43.35%
2	Buffer Overflow	16.56%
3	SQL Injection	13.85%

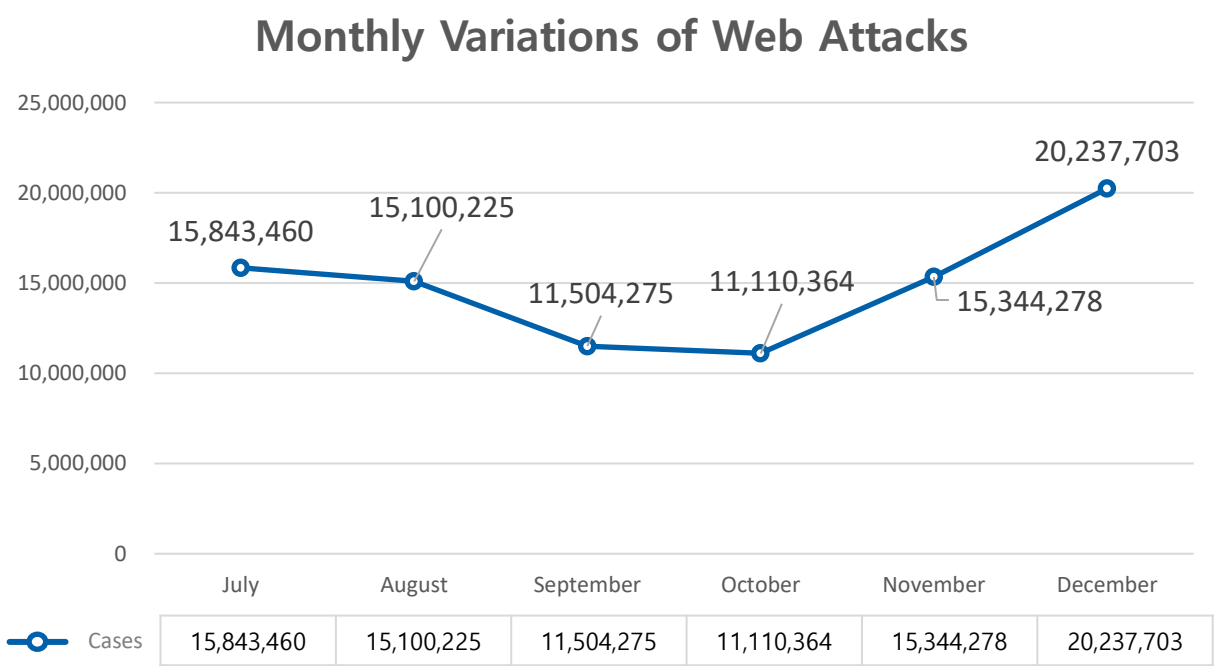
<Top 3 Picks by Major Attackers>

III. Web Attack Trends During H2 2021

1. Monthly variations

The monthly variation analysis depicts a clear view of when web attacks occur the most throughout the year, helping organizations to combat future attacks and prepare for countermeasures in advance.

The graph below illustrates the monthly breakdown of web attack cases detected by WAPPLES and Cloudbric during the second half of 2021.



According to the analysis, the number of web attack cases averaged at 14.8 million per month. There was a surge of web attacks in December with more than 20 million cases recorded, mainly because several highly critical vulnerabilities came to light during the month. The Apache Log4j vulnerability (Log4Shell, CVE-2021-44228)[1], often characterized as the "worst vulnerability of the decade", attracted some of the most sophisticated threat actors and ransomware groups across the globe, with victims ranging from all types of enterprises and organizations.

Besides the impact of Log4Shell, the COVID-19 pandemic has continued to make an impact on organizations as more and more employees adopt remote work and online conferencing applications. Given the large amount of personal information these applications process, more exploitation attempts are expected in the coming future. Security administrators should take precautionary measures in mitigating these risks.

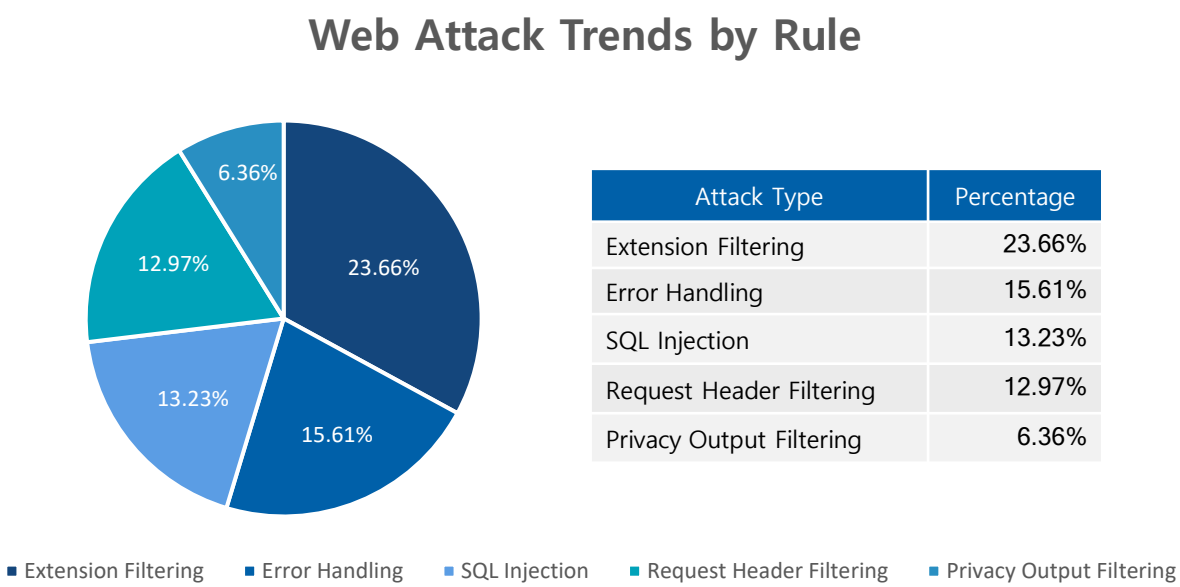
1) *"How WAPPLES Protects Against Log4j Vulnerability"*, Penta Security, 2021, https://www.pentasecurity.com/blog/how-wapples-protects-against-log4j-vulnerability/

III. Web Attack Trends During H2 2021

2. Web attack trends by rule

By categorizing web attacks according to the detection rules of WAPPLES and Cloudbric, this rule-based analysis illustrates which attack types occurred the most during the second half of 2021. Based on this information, security measures and response guidelines can be established.

The graph below demonstrates the top five attack types based on their respective detection rules.



Attack Type	Percentage
Extension Filtering	23.66%
Error Handling	15.61%
SQL Injection	13.23%
Request Header Filtering	12.97%
Privacy Output Filtering	6.36%

Between July 1 and December 31, 2021, the top five observed web attack types are **Extension Filtering** (23.66%), **Error Handling** (15.61%), **SQL Injection** (13.23%), **Request Header Filtering** (12.97%), and **Privacy Output Filtering** (6.36%).

As the most observed attack type year after year, **Extension Filtering** continues to top the list. It happens when attackers attempt to access configuration files (e.g. DLL, CONF, INI, etc.) that are prone to vulnerabilities. These attacks can be highly critical because when unauthorized individuals access these configuration files, they could tamper with the web server and directly control the web service.

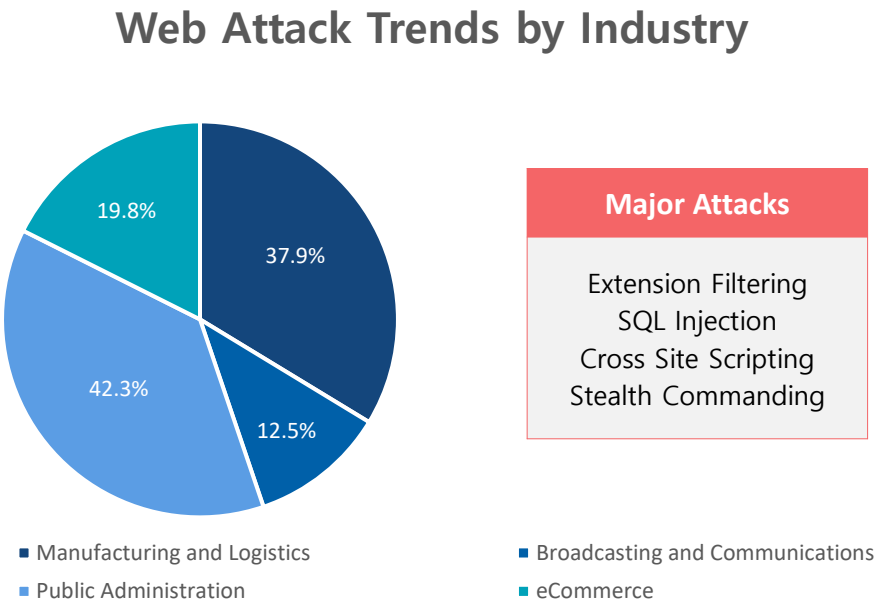
Error Handling is an attack method in which the attacker intentionally sends an invalid request to the web server or web application in order to trigger an error message, usually by entering repetitive strings, notes, or invalid IDs. The attacker then either collects the error message for future SQL injection attacks or uses the message to derive the version and release numbers of the associated web server and application.

Another attack type that has always appeared on the top five list is **SQL Injection**. This is when the attacker inserts invalid or unrelated SQL scripts to the SQL query to attack the database, making it the most common attack method used for large-scale data compromise. A wide range of SQL injection attack methods have been detected, making it crucial to have effective countermeasures.

Other attacks like **Request Header Filtering** and **Privacy Output Filtering** also tend to cause serious damages to the IT system. All organizations must take these into consideration when assigning security policies.

III. Web Attack Trends During H2 2021

3. Web attack trends by industry



The above graph shows the top four industries suffering the most web attacks, based on the industries of WAPPLES and Cloudbric customers. A variety of attack types were observed in the analysis, providing further insights for each specific industry on how to stay prepared.

According to the graph, manufacturing and logistics, broadcasting and communications, public administration, and ecommerce are four major industries suffering high loads of web attacks. The public administration industry, which includes government agencies and institutions, was targeted the most during this period, primarily due to the large quantity of sensitive personal data it handles. Security administrators must pay special attention to protect personally identifiable information (PII).

Particularly, many countries across the globe started validating COVID-19 vaccine passports during the second half of 2021. This led to an increase in hacking attempts on health administration organizations and vaccine booking websites[1)].

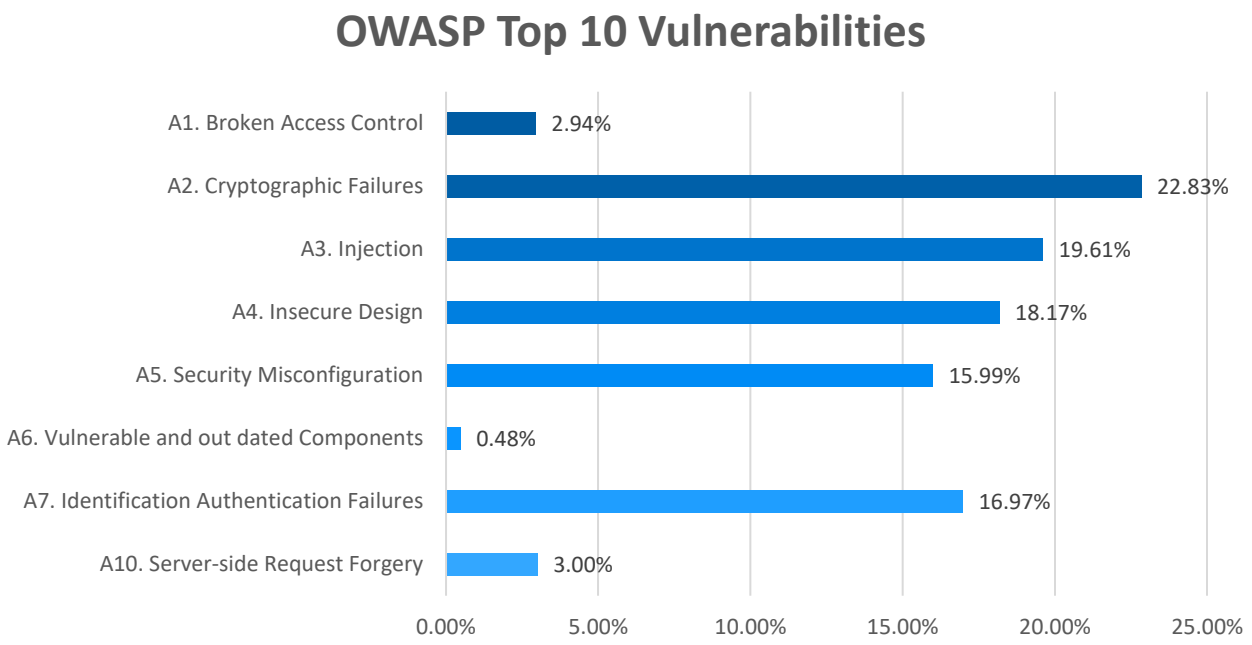
Cyberattacks on industries not only pose threats to personal information, but also sensitive corporate data and trade secrets. All organizations must have robust security measures to safeguard their data and operations.

1) *"Italian COVID-19 Vaccine Booking Portal Knocked Offline in Ransomware Attack"*, Penta Security, 2021, *https://www.pentasecurity.com/blog/security-weekly-italian-covid-19-vaccine-booking-portal-knocked-offline-in-ransomware/*

III. Web Attack Trends During H2 2021

4. Web attack trends by OWASP Top 10

The following analysis categorizes all attacks detected by WAPPLES and Cloudbric during the second half of 2021 as according to the updated OWASP Top 10 vulnerabilities list.



The graph above shows a breakdown of attacks in OWASP Top 10 categories between July 1 and December 31, 2021. **Cryptographic Failures** (previously labeled as **Sensitive data Exposure**) is the most frequently exploited vulnerability, followed by **Injection**.

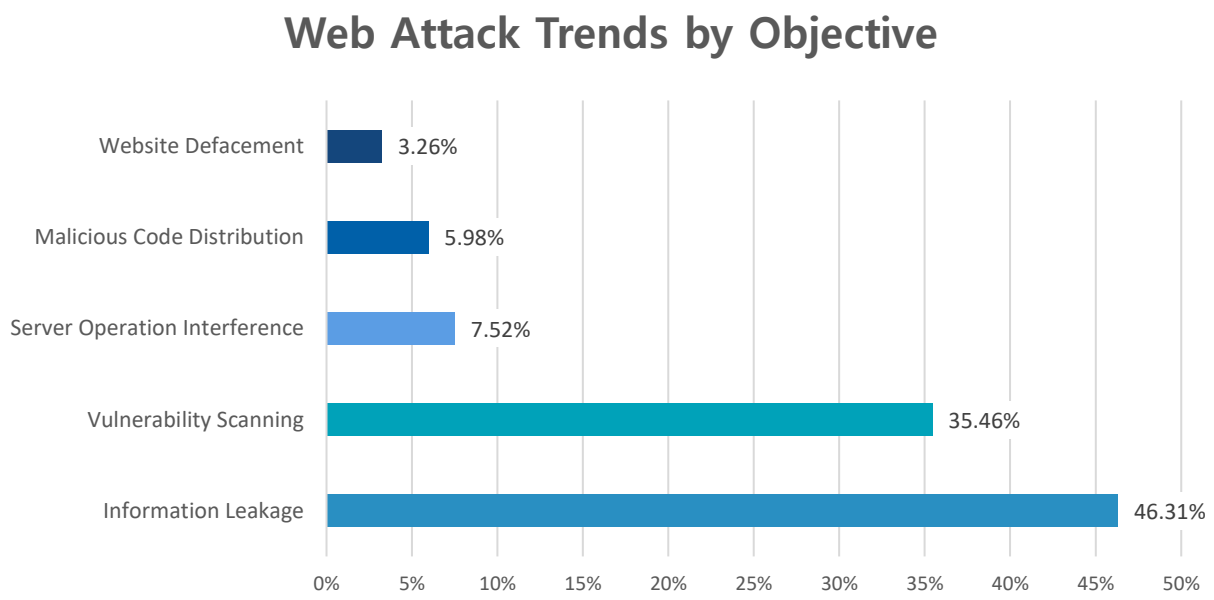
Cryptographic Failures is a common vulnerability that arises from a lack of encryption to sensitive data. To prevent such attacks, organizations must ensure that all their passwords, personal data, and sensitive corporate files are encrypted.

OWASP TOP 10 Vulnerabilities (2021)	Cases
A1. Broken Access Control	2,572,289
A2. Cryptographic Failures	19,948,457
A3. Injection	17,131,084
A4. Insecure Design	15,879,767
A5. Security Misconfiguration	13,972,481
A6. Vulnerable and outdated Components	416,489
A7. Identification Authentication Failures	14,831,675
A10. Server-side Request Forgery	2,625,034

<OWASP Top 10 Web Attack Cases>

III. Web Attack Trends During H2 2021

5. Web attack trends by objective



The above graph categorizes detected web attacks during the second half of 2021 by their objectives. By analyzing all web attacks originating from South Korea, the top five objectives are **Information Leakage** (46.31%), **Vulnerability Scanning** (35.46%), **Server Operation Interference** (7.52%), **Malicious Code Distribution** (5.98%), and **Website Defacement** (3.26%).

More than 40% of web attacks had the objective of **Information Leakage**. This can be done using a variety of attack methods. For instance, Website Defacement is when unauthorized users tamper with specific webpages and replace these with their own content. SQL Injection is when malicious code gets injected into the SQL queries to retrieve information from the SQL server. File Upload is when the attacker upload executable malicious files in EXE, JSP, and PHP formats into the server. Lastly there is Include Injection, which is when malicious scripts, files, and code are injected.

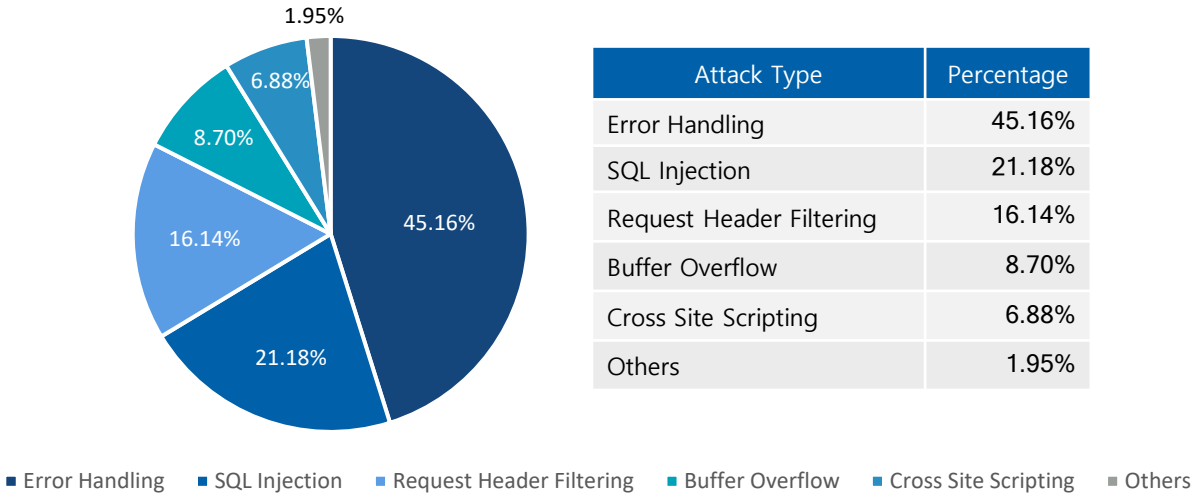
The second-most common attack objective is **Vulnerability Scanning**. This involves the use of automated tools to send invalid HTTP requests or responses, to send invalid URLs that are different from formats defined by RFC, to gain access to directory listings, or to use Error Handling to find out if any vulnerability exists.

Other objectives include **Server Operation Interference**, **Malicious Code Distribution**, and **Website Defacement**. It is important to take these objectives into account when defining security policies.

III. Web Attack Trends During H2 2021

6. Web attack trends of major attackers

Top Picks by Major Attackers



Attack Type	Percentage
Error Handling	45.16%
SQL Injection	21.18%
Request Header Filtering	16.14%
Buffer Overflow	8.70%
Cross Site Scripting	6.88%
Others	1.95%

This analysis demonstrates the attack patterns of the top ten most active attackers between July 1 and December 31, 2021. The reason to perform such an analysis is because these highly active attackers tend to be professional hackers and APTs that are likely to cause serious damage. Hence it is worth the time to look at their attack patterns separately.

The results show that the most common attack methods used by the top ten attackers are **Error Handling** (45.16%), **SQL Injection** (21.18%), **Request Header Filtering** (16.14%), **Buffer Overflow** (8.70%), and **Cross Site Scripting** (6.88%).

As the most used attack method by top attackers, **Error Handling** is an attack method where the attacker intentionally sends an invalid request to the web server or web application in order to trigger error messages, which are then used to derive the version and release numbers of the associated web server, application, and DBMS. This information can be used to understand the vulnerabilities of the software and conduct follow-up attacks to cause greater damage.

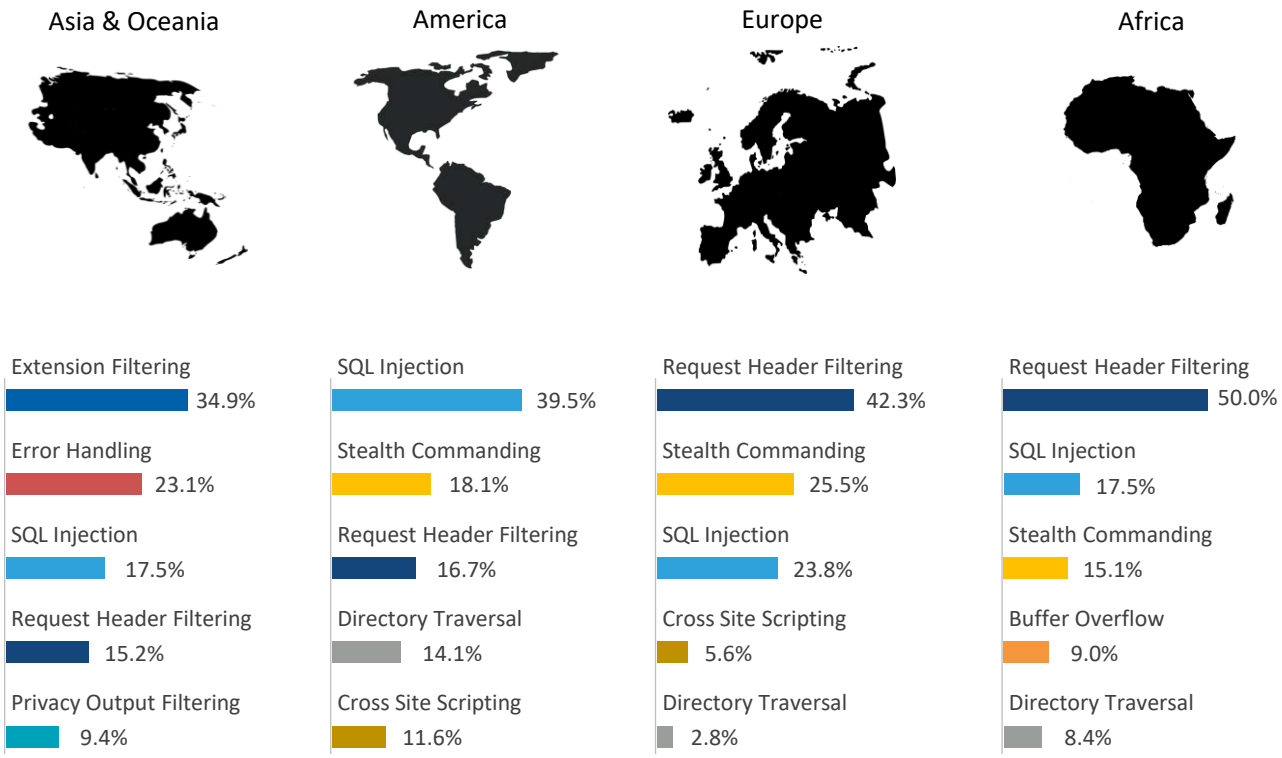
The second-most common attack method chosen by top attackers is **SQL Injection**. As mentioned earlier, this is when the attacker inserts invalid or unrelated SQL scripts to the SQL query to retrieve, modify, or delete data from the server. There are many known SQL Injection attack techniques, making security countermeasures a must. Such attacks usually lead to serious data breaches.

Speaking of data breaches, one commonality across all these five attack methods is that they all seek to gain access and control over personal and corporate data. Therefore, it is strongly recommended to have an emergency response guideline in case a data breach happens.

III. Web Attack Trends During H2 2021

7. Web attack trends by continent

Web Attack Trends by Targeted Continent



The graph above depicts all detected attacks classified by their targeted continents. **Extension Filtering** remains its top spot in Asia. In the Americas, **SQL Injection** has risen significantly from the fourth spot in the previous period to the top. **Request Header Filtering** is the most common attack type observed in both Europe and Africa.

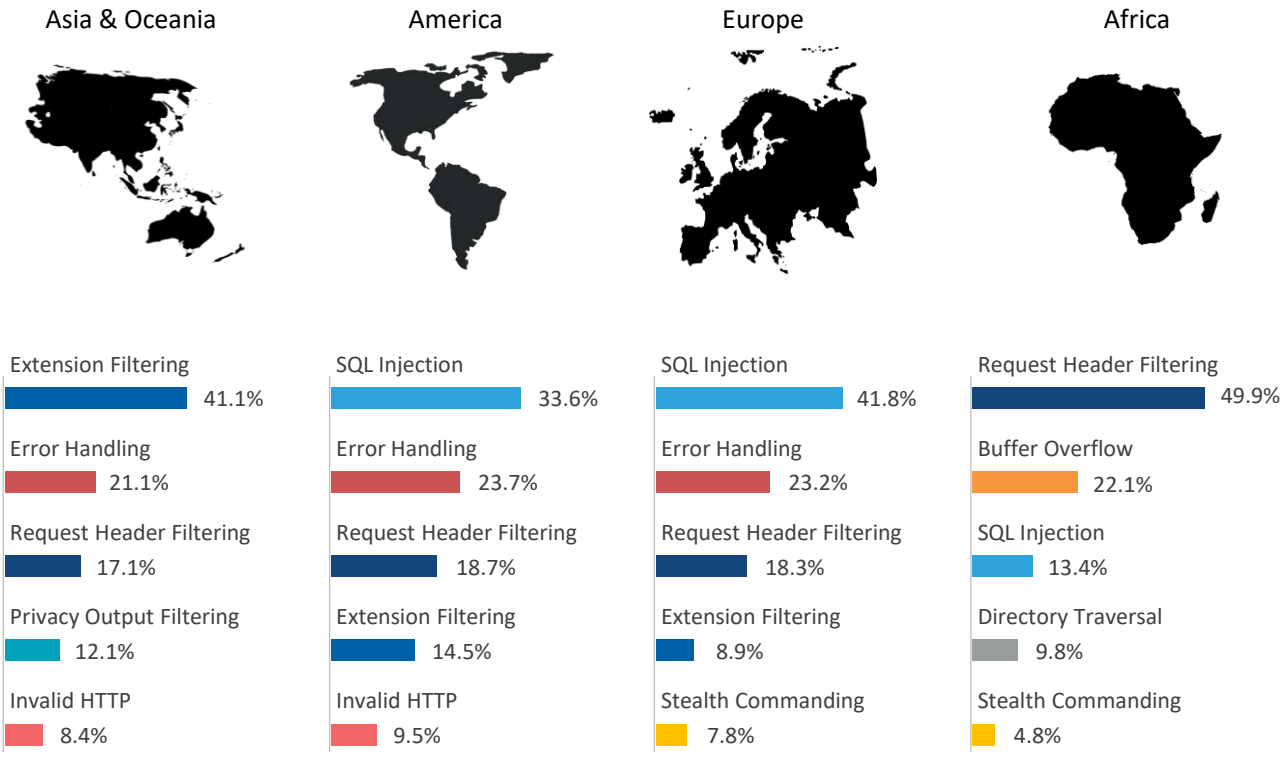
Ranked third on the OWASP Top 10 list, Injection attacks, particularly **SQL Injection**, makes it to the top three on all four continents, explaining its widespread impact worldwide.

Note that nearly half of all attacks directed at Europe and Africa are **Request Header Filtering**. This implies that organizations on these two continents must pay special attention to these attacks and establish robust countermeasures.

III. Web Attack Trends During H2 2021

7. Web attack trends by continent

Web Attack Trends by Continent of Origin



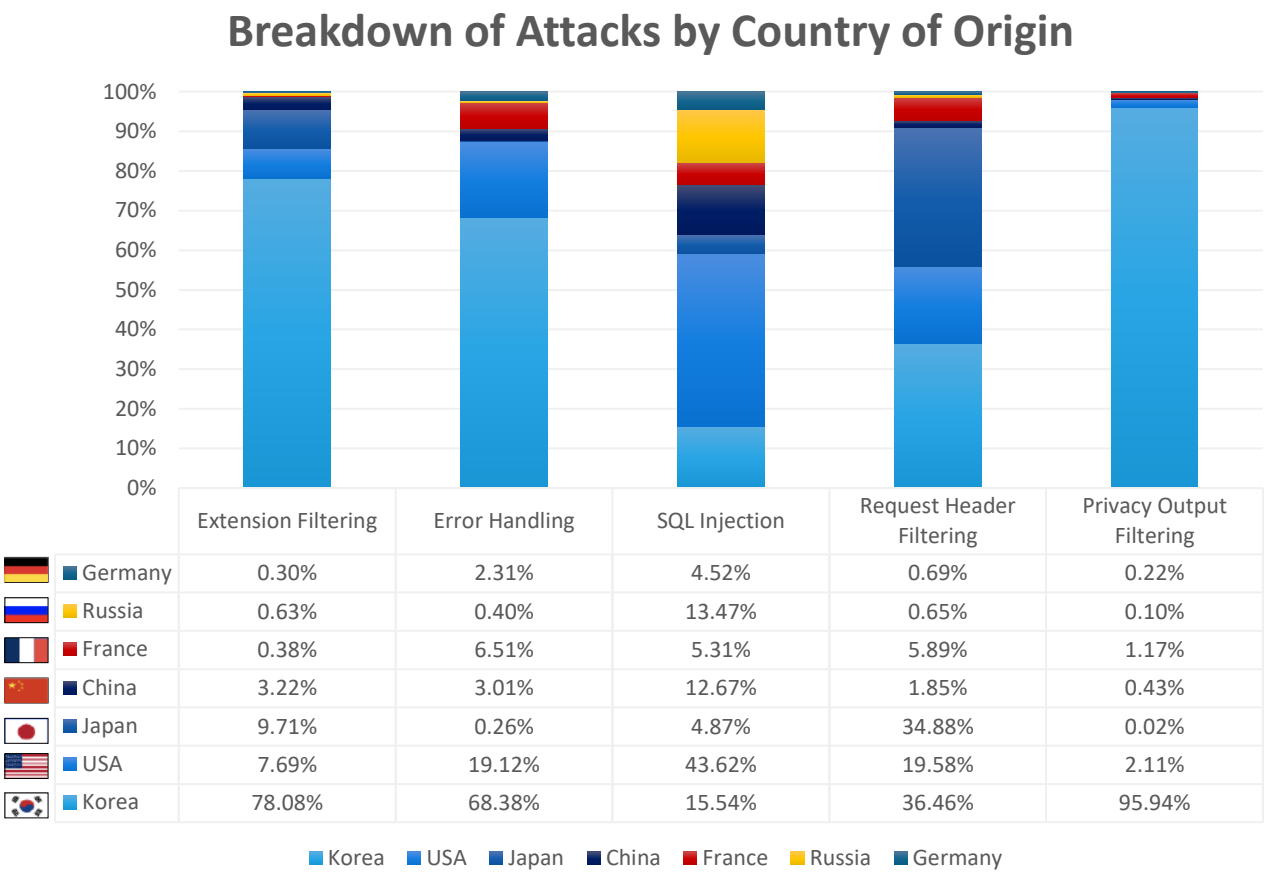
The above graph illustrates an analysis of attack origins based on their IP addresses. The most common attack type originating from Asia is **Extension Filtering**, while **SQL Injection** is most common in both the Americas and Europe. **Request Header Filtering** attempts are mostly observed in Africa.

Request Header Filtering makes it to the top five list on all four continents, showing that it is a popular choice by hackers worldwide. Also, **SQL Injection** has a significant share in attacks originating from the Americas and Europe. **Error Handling** is another popular attack method that is ranked second in Asia, the Americas, and Europe.

Comparing the targeted continents with the continents of origin, Europe receives high loads of **Request Header Filtering** attacks, but launches the most **SQL Injection** attacks, showing that a lot of web attacks in Europe are likely transcontinental attacks.

III. Web Attack Trends During H2 2021

8. Web attack trends by country



The above table illustrates the share of each attack type across their countries of origin, based on the detection data of WAPPLES and Cloudbric. The results help security administrators prepare for location-based security policies.

Note that since the locations of detected web attacks are dependent on the locations of WAPPLES and Cloudbric customers, the analysis is not a means of comparing country to country. Simply put, the above table should not be interpreted vertically but instead be read horizontally.

By comparing the relative share of each attack type within each country, it becomes apparent that **SQL Injection** is particularly popular among attackers in the US, China, and Russia, but very unpopular in Korea. Another finding is that **Request Header Filtering** is especially popular in Japan.

III. Web Attack Trends During H2 2021

9. Current status of major web vulnerabilities

The Log4j vulnerability, also known as Log4Shell or CVE-2021-44228, was reported in early December 2021 and characterized by many as the "worst vulnerability in history". Log4j is an open-source data logging package developed by Apache for the Java platform. The vulnerability occurs in a plugin called "JNDI (Java Naming and Directory Interface) Lookup", allowing hackers to launch remote code execution (RCE) attacks against web applications and install malware into the web servers[1)].

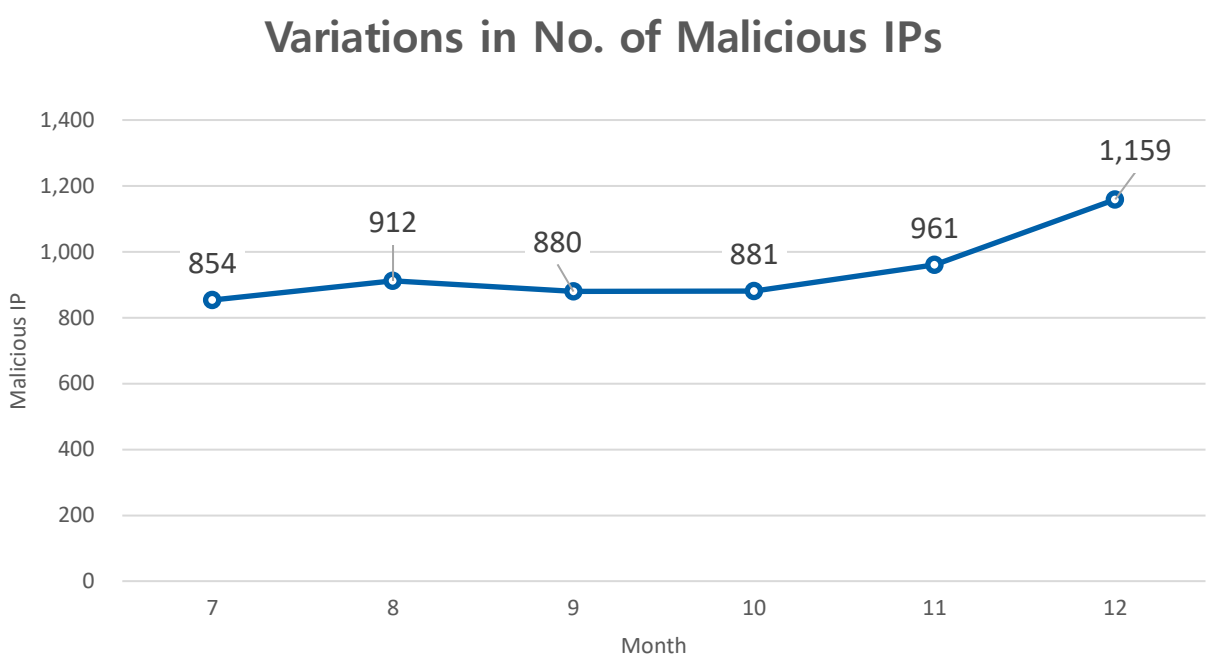
Currently, all versions of Log4j between version 2.0.beta.9 and 2.14.1 are prone to the vulnerability. Additional vulnerabilities have been discovered after Log4Shell, making it necessary for security administrators to perform follow-up patches and update their security policies.

To reduce the risk of Log4Shell, organizations should keep all their software up-to-date, including web browsers and web applications.

1) *"How WAPPLES Protects Against Log4j Vulnerability"*, Penta Security, 2021, *https://www.pentasecurity.com/blog/how-wapples-protects-against-log4j-vulnerability/*

III. Web Attack Trends During H2 2021

10. Variations in the number of malicious IPs



The graph above shows the fluctuations in the number of detected malicious IP addresses month-by-month. The analysis helps predict the frequency of web attacks. Still, a relatively low number of malicious IPs does not necessarily indicate a lower number of attacks. A single attacker can use many IP addresses to conduct an attack, while a single IP has the potential to cause tremendous damage to the target.

To classify an IP address as malicious, it must be detected at over ten destinations and be used in more than 10 attacks in a particular month. The analysis can help establish associations between attackers and their IP addresses, making it easier to predict their attack patterns in the future.

Based on the data, the number of detected malicious IP addresses peaked at 1,159 in December, while averaging at 941 per month throughout the second half of 2021. Again, the surge in attacks towards the end of the year was due to both the Log4j vulnerability and the COVID-19 Omicron variant. Organizations should continue to step up their security measures to defend against these growing threats.

IV. Appendix

1. Data collection method and duration

The data used in this WATT Report is collected from the detection 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 1 and December 31, 2021.

2. Key characteristics of report

The 2021 H2 WATT Report included detection log data from both WAPPLES and Cloudbric. Additionally, Penta Security's newly developed machine learning technology allowed for more accurate prediction of future attacks.

The report is prepared with both industry professionals and casual readers in mind. On the professional end, it provides insights for CISOs, CSOs, and security administrators, 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 will update information through continuous research and analysis and publish a report semi-annually to identify and compare the latest trends.

3. Glossary

▪ Request Header Filtering

Request Header Filtering is an attack method where the attacker modifies the header of the HTTP request sent from the web browser by inserting malicious code. This is a common technique used by automated hacking tools. Attackers can potentially modify server information.

Potential Consequences: Modify web server information, trigger abnormal server behavior

▪ Error Handling

Error Handling is an attack method where the attacker intentionally sends an invalid request to the web server or web application in order to trigger error messages, which are then used to derive the version and release numbers of the associated web server, application, and DBMS. This information can be used to understand the vulnerabilities of the software and conduct follow-up attacks to cause greater damage.

Potential Consequences: Access and expose sensitive files, prepare for follow-up attacks

▪ Directory Traversal

Directory Traversal is an attack method where the attacker gains access to the private directory or files held by the administrator as an attempt to compromise data.

Potential Consequences: Access system files by moving to parent folder, access source files

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.

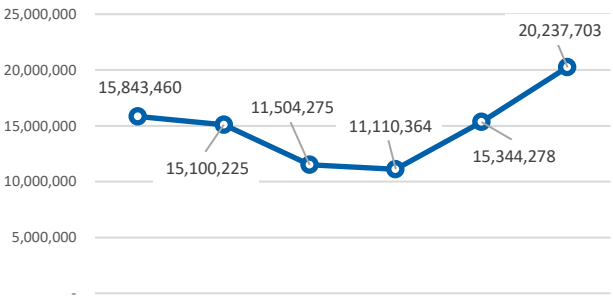
TOP	OWASP TOP 10	WAPPLES/Cloudbric Rules
1	Broken Access Control	Parameter Tampering
		Invalid URL
		Directory Traversal
		Url Access Control
2	Cryptographic Failures	Privacy File Filtering
		Privacy Input Filtering
		Privacy Output Filtering
		Input Content Filtering
		Response Header Filtering
		Error Handling
3	Injection	SQL Injection
		Stealth Commanding
		Cross Site Scripting
		NoSQL Injection
		LDAP Injection
		XPath Injection
4	Insecure Design	Error Handling
		Response Header Filtering
		Parameter Tampering
		Directory Traversal
5	Security Misconfiguration	Directory Listing
		Error Handling
		Response Header Filtering
		XXE Injection
6	Vulnerable and Outdated Components	Custom Rule
		User Defined Pattern
7	Identification Authentication Failures	Cookie Poisoning
		Authentication & Session Management
		Directory Traversal
		Cross Site Request Forgery
		SQL Injection
		NoSQL Injection
8	Software and Data Integrity Failures	Insecure Deserialization
9	Security Logging and Monitoring Failures	Detection Log Monitoring and Sync
10	Server-Side Request Forgery	File Inclusion

- One WAPPLES/Cloudbric rule may be matched to multiple OWASP Top 10 vulnerabilities.

IV. Appendix

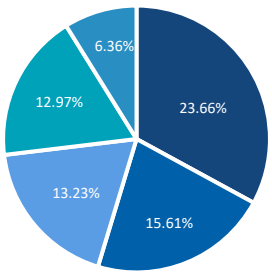
5. Summary charts

Monthly Variations of Web Attacks

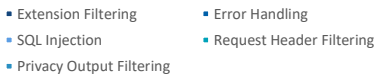


	July	August	September	October	November	December
Cases	15,843,460	15,110,225	11,504,275	11,110,364	15,344,278	20,237,703

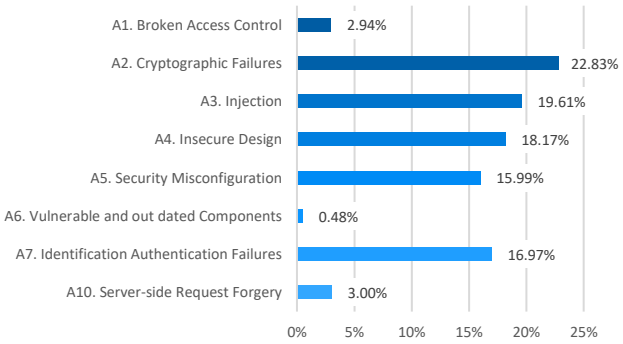
Web Attack Trends by Rule



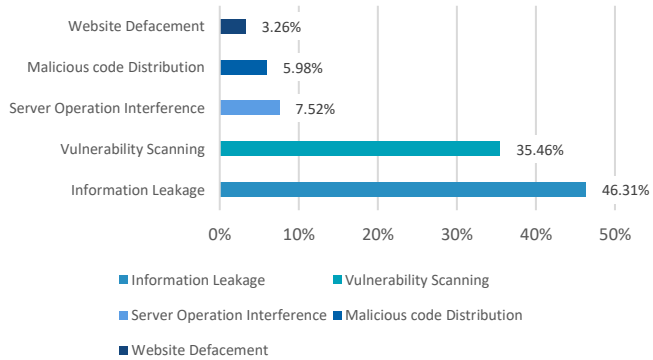
Attack Type	Percentage
Extension Filtering	23.66%
Error Handling	15.61%
SQL Injection	13.23%
Request Header Filtering	12.97%
Privacy Output Filtering	6.36%



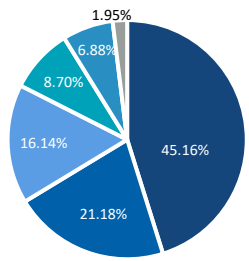
OWASP Top 10 Vulnerabilities



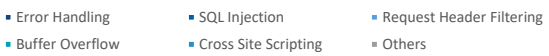
Web Attack Trends by Objective



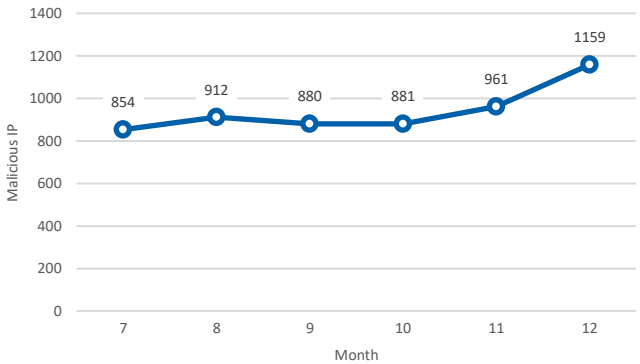
Top Picks by Major Attackers



Attack Type	Percentage
Error Handling	45.16%
SQL Injection	21.18%
Request Header Filtering	16.14%
Buffer Overflow	8.70%
Cross Site Scripting	6.88%
Others	1.95%



Variations in No. of Malicious IPs



IV. Appendix

6. List of top 40 attackers

Rank	IP Address	Country
1	203.100.X.X	Korea
2	222.229.X.X	Japan
3	113.52.X.X	Japan
4	59.26.X.X	Korea
5	13.114.X.X	United States
6	211.201.X.X	Korea
7	157.90.X.X	United States
8	110.45.X.X	Korea
9	122.52.X.X	Philippines
10	211.249.X.X	Korea
11	211.249.X.X	Korea
12	175.223.X.X	Korea
13	45.155.X.X	Unknown
14	13.115.X.X	Japan
15	150.60.X.X	Japan
16	20.194.X.X	United States
17	157.90.X.X	United States
18	59.9.253.X.X	Korea
19	211.226.X.X	Korea
20	118.71.X.X	Vietnam
21	218.38.X.X	Korea
22	154.91.X.X	Unknown
23	218.49.X.X	Korea
24	82.223.X.X	Spain
25	41.21.X.X	South Africa
26	147.46.X.X	Korea
27	157.90.X.X	United States
28	147.46.X.X	Korea
29	13.113.X.X	Japan
30	94.182.X.X	Iran
31	211.249.X.X	Korea
32	123.225.X.X	Japan
33	183.227.X.X	China
34	54.71.X.X	United States
35	91.207.X.X	Russia
36	188.127.X.X	Russia
37	54.180.X.X	United States
38	164.46.X.X	Japan
39	211.249.X.X	Korea
40	178.173.X.X	Russia

cloudbric

GROBAL	www.cloudbric.com
JAPAN	www.cloudbric.jp
KOREA	www.cloudbric.co.kr

Penta SECURITY
cloud · iot · blockchain

KOREA	www.pentasecurity.co.kr
GLOBAL	www.pentasecurity.com
JAPAN	www.pentasecurity.co.jp
CHINA	www.panqi.tech

Overall Web Security Solution Provider of the Year 2021

Web Application Security

Cyber Security Awards Application Security 2020

IoT-based Smart Security Innovation Award 2020

TU-Automotive Awards Best Auto Cybersecurity Product/Service 2019

Cybersecurity Excellence Awards Winner 2018

Hot Company in Web Application Security for 2016

SC Magazine Europe Best SME Solution

Recognized on the Gartner WAF Magic Quadrant

ICSA Labs Certified WAF


The First and Only CCEAL4 Certified WAF

PCI-DSS Compliance