cloudbric
Penta SECURITY
enterprise · iot · blockchain

Web Application Threat Trend Report

Trends for the First Half of 2023

Cloudbric Corp.
Penta Security Systems Inc.

cloudbric
Penta SECURITY

Contents

I. Overview

1. Objective of report

The 2023 H1 Web Application Threat Trend (WATT) Report is compiled based on detection log data from both Penta Security's WAPPLES, a next-gen web application firewall with leading market share in the Asia Pacific,[1)] and Cloudbric WAF+, a world-leading cloud and edge-computing security solution. All reported data are collected by Penta Security's Intelligent Customer Support (ICS) system and Cloudbric, providing an accurate representation of web attack trends worldwide.

In this report, Penta Security and Cloudbric analyze these detection log data to identify any latest web attack trends and patterns, including common attack methods, IP addresses, commonly targeted industries, and more. The results of these analyses are then used to enhance the detection rules and operations of both WAPPLES and Cloudbric WAF+.

The data and analyses provided in this report are for informational purpose only, serving all readers interested in web security trends, including customers and partners of Penta Security and Cloudbric, CISOs, security administrators at enterprises and government agencies, and researchers at academic institutions. All data are handled and disclosed in accordance with the terms agreed upon by the customers.

1) Industry Quotient, Frost & Sullivan, 2023.

II. Executive Summary

The data presented in this report are selected based on the top 5 primary detection rules of WAPPLES and Cloudbric WAF+. 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 from.

During the first half of 2023, over 40% of all web attacks were aimed at either stealing or purposefully leaking sensitive information. Information leakage can be a result of SQL Injection, where attackers inject malicious scripts into the SQL query, or File Upload, where unauthorized users upload corrupted files in EXE, JSP, and PHP extensions to the web server.

Putting all attacks into OWASP Top 10 categories, the most exploited vulnerabilities following Injection is Identification and Authentication Failures. A common type of such failure is having no multi-factor authentication (MFA) in place to stop brute force attacks. Coming at the third place is Insecure Design, described as a lack of security integration during application development. This could result in the exposure of sensitive server information in an error message or the execution of commands that are different from the server's intention.

Based on the top 5 detection rules of WAPPLES and Cloudbric WAF+, the most observed attack type is File Inclusion. This is an attack method where attackers execute malicious server scripts within a specified file to run commands on a targeted server. This file can either be an internal file that exists within the server or a remote file that fetches a file on the server. Both can be highly destructive towards the web service and lead to sensitive data exposure.

Below is a summary of the top web attacks detected by WAPPLES and Cloudbric from January 1 to June 30, 2023.

Rank	Attack Type	Percentage
1	File Inclusion	25.14%
2	SQL Injection	18.64%
3	Error Handling	16.74%

<Top 3 Attack Types>

Rank	Attack Objective	Percentage
1	Information Leakage	38.66%
2	Vulnerability Scanning	25.93%
3	Website Defacement	25.41%

<Top 3 Attack Objectives>

Rank	OWASP Top 3	Cases
1	Server-Side Request Forgery	27,648,549
2	Injection	26,660,631
3	Identification and Authentication Failures	25,352,564

<Top 3 Attacks from OWASP Top 10>

Rank	Attack Type	Percentage
1	File Inclusion	45.98%
2	SQL Injection	23.16%
3	Error Handling	10.77%

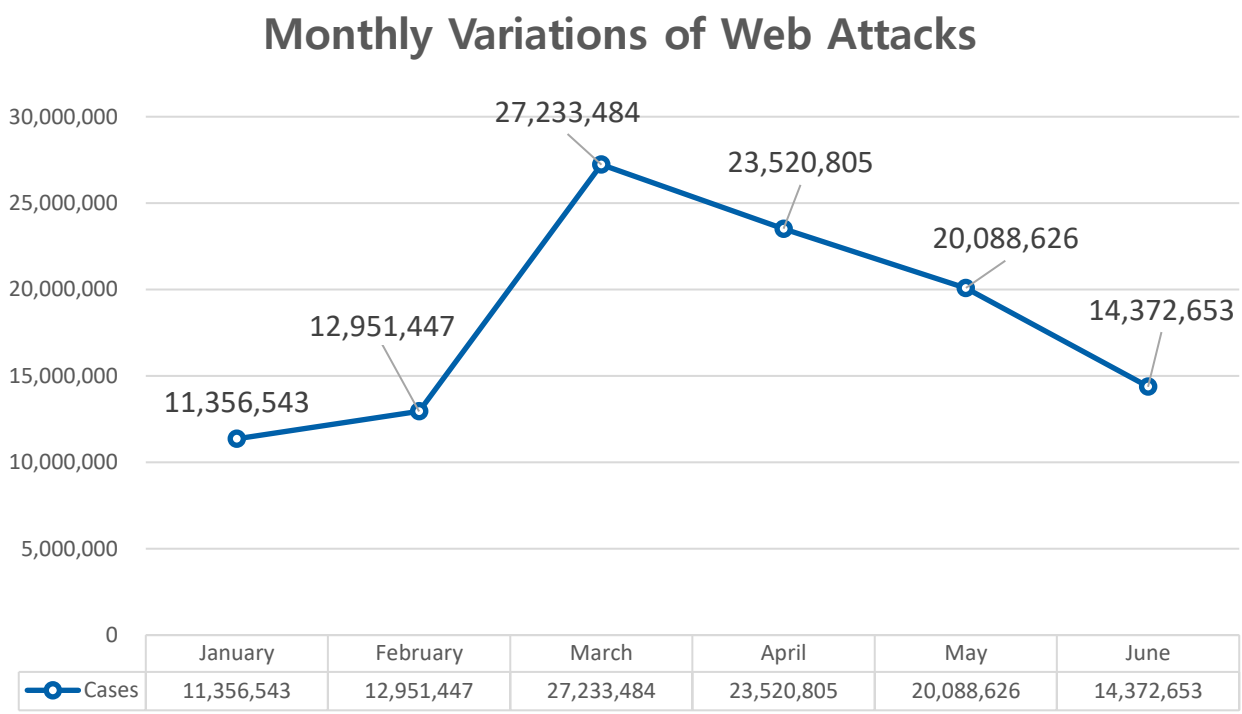
<Top 3 Picks by Major Attackers>

III. Web Attack Trends During H1 2023

1. Monthly variations

The monthly variation analysis depicts a clear view of when web attacks occur the most throughout the six-month period, helping organizations 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 first half of 2023.



There are an average of 18.25 million cases of web attacks per month throughout the period. A significant peak is seen in March and April, reporting over 27 and 23 million cases, respectively.

The rise in attack numbers throughout March and April can be attributed to a few actively exploited vulnerabilities, including the critically severe flaw in the Control Web Panel (CVE-2022-44877) leading to unauthorized remote access,[1] as well as the WordPress Advanced Custom Fields plugin flaw that impacted over 2 million websites.[2]

Threat actors are continuing to target high severity vulnerabilities with new attack patterns. This makes it crucial for organizations to continue to monitor new vulnerabilities and have their servers and systems patched as soon as one becomes available.

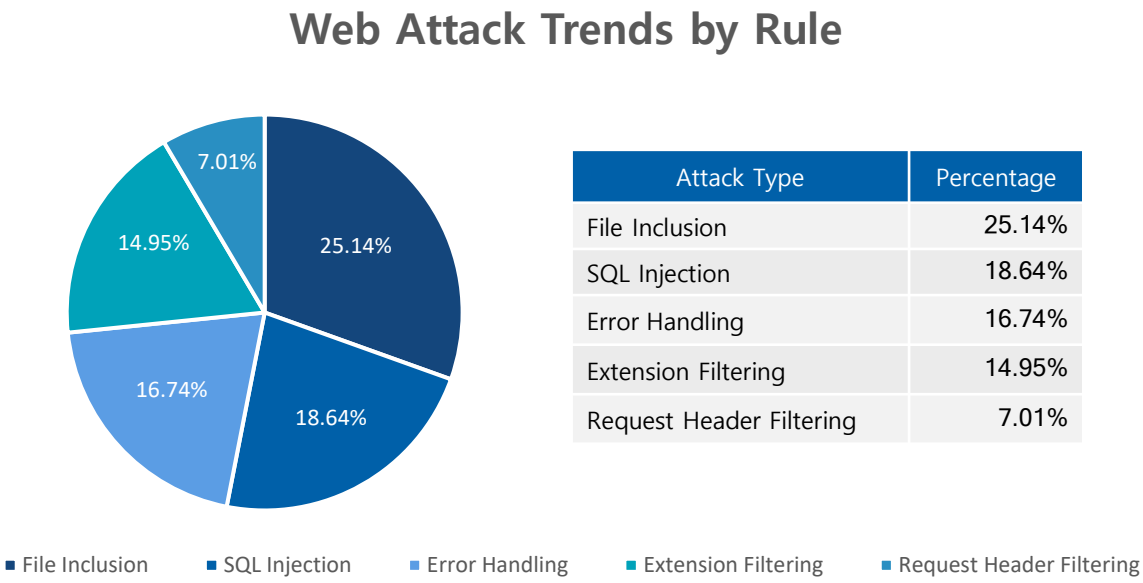
1) "Hackers exploit Control Web Panel flaw to open reverse shells." *Bleeping Computer.* January 12, 2023.
2) "WordPress plugin hole puts 2 million websites at risk." *The Register.* May 8, 2023.

III. Web Attack Trends During H1 2023

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 first half of 2023. 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
File Inclusion	25.14%
SQL Injection	18.64%
Error Handling	16.74%
Extension Filtering	14.95%
Request Header Filtering	7.01%

Between January 1 and June 30, 2023, the top five observed attack types are File Inclusion (25.14%), SQL Injection (18.64%), Error Handling (16.74%), Extension Filtering (14.95%), and Request Header Filtering (7.01%).

As the most observed attack type, **File Inclusion** is when attackers execute malicious server scripts within a specified file to run commands on a targeted server. This file can either be an internal file within the server (i.e. local file inclusion, LFI) or a remote file that fetches a file on the targeted server (i.e. remote file inclusion, RFI). Both can be highly destructive towards the web service and lead to sensitive data exposure.

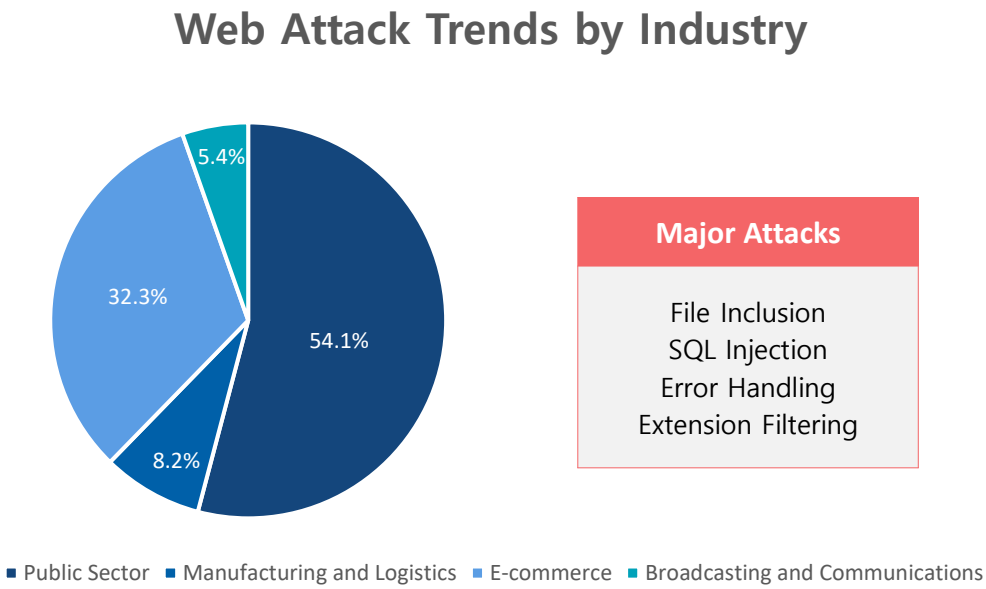
SQL Injection comes second on the list. This is when an attacker inserts invalid or unrelated SQL scripts to the SQL query to attack the database, making it the most common attack method for large-scale data exfiltration. A wide range of SQL Injection attack methods have been detected, making it crucial to establish effective countermeasures.

Error Handling vulnerabilities occur when an error message contains details that might be useful to an attacker, such as software version details and file locations. Such details could also be exposed in an implicit manner, such as when an error message behaves differently when a user identifier exists than when it does not. Attackers exploiting Error Handling vulnerabilities often send large amounts of invalid inputs purposefully to trigger error messages.

Lastly, attacks like Extension Filtering and Request Header Filtering also have the potential to cause serious damage to the IT system. All organizations must take these into consideration when assigning security policies.

III. Web Attack Trends During H1 2023

3. Web attack trends by industry



The above graph shows the distribution of major attacks detected among the four major industries of WAPPLES and Cloudbric customers. A wide range of attack types were observed in the analysis, providing further insights for each specific industry on how to stay prepared.

According to the graph, most web attacks targeted either the public sector or the e-commerce industry, of which over half of all attacks targeted the public sector. The likely reason attackers concentrate on the public sector is that these organizations contain large volumes of data on citizens, businesses, and public infrastructure. Security administrators of the public sector must take effective actions to protect these data.

Due to political tensions, Chinese state-linked hackers have been particularly active during this period. In January, a Chinese hacker group attacked 12 South Korean academic institutions.[1] In June, the email accounts of the US Department of State and the Department of Commerce were accessed.[2]

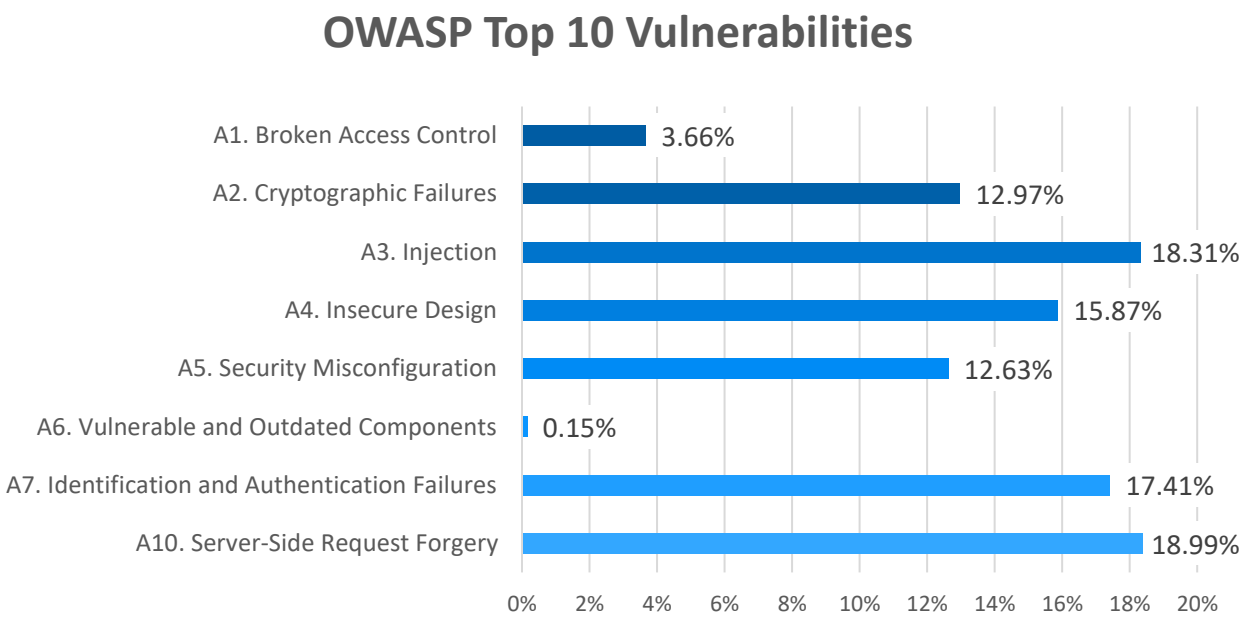
Cyberattacks against these critical industries not only put consumer and corporate data at risk, but also have the potential to disrupt infrastructures that are crucial to national security. Cybersecurity awareness and robust countermeasures must be in place to defend such threats.

1) "Chinese hackers attack 12 S. Korean academic institutions: KISA." *Yonhap News Agency.* January 25, 2023.
2) "Chinese hackers breached State, Commerce Depts, Microsoft and US say." *Reuters. July* 13, 2023.

III. Web Attack Trends During H1 2023

4. Web attack trends by OWASP Top 10

The following analysis categorizes all attacks detected by WAPPLES and Cloudbric WAF+ during the first half of 2023, based on the categories defined in the OWASP Top 10 vulnerabilities list.



The graph above shows a breakdown of attacks in OWASP Top 10 categories between January 1 and June 30, 2023. Server-Side Request Forgery is the most frequently exploited vulnerability, followed by Injection and Identification and Authentication Failures.

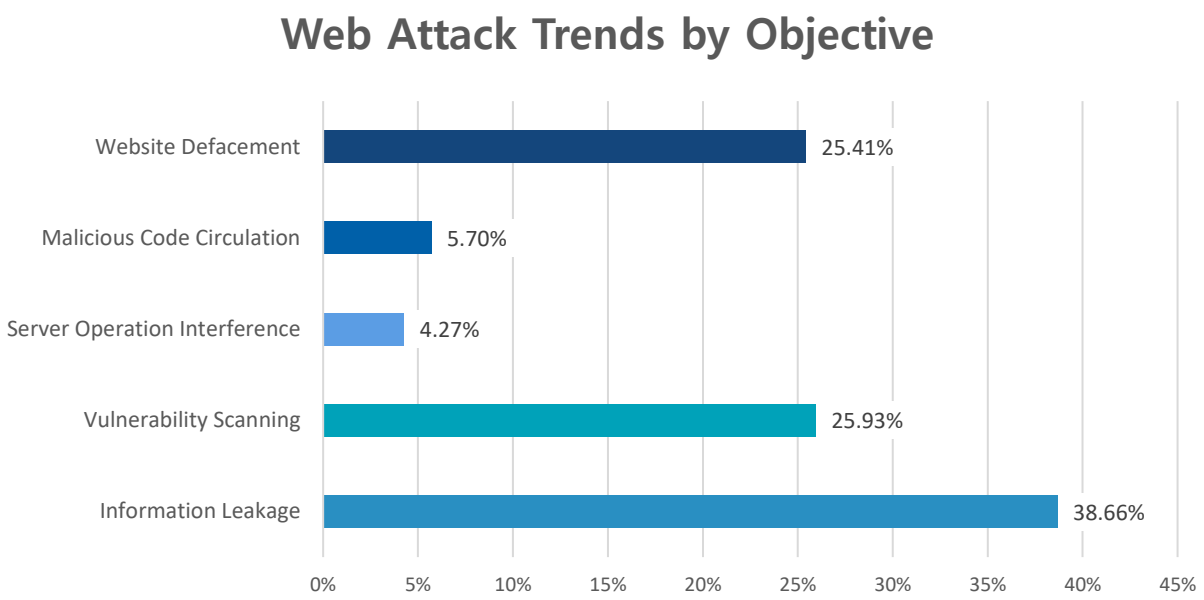
Server-Side Request Forgery is the same type of vulnerability as file inclusion. It happens when attackers execute malicious server scripts within a specified file to run commands on a targeted server. This file can either be an internal file within the server (i.e. local file inclusion, LFI) or a remote file that fetches a file on the targeted server (i.e. remote file inclusion, RFI). Both can be highly destructive towards the web service and lead to sensitive data exposure.

OWASP Top 10 (2021) Vulnerabilities	Cases
A1. Broken Access Control	5,321,489
A2. Cryptographic Failures	18,880,708
A3. Injection	26,660,631
A4. Insecure Design	23,108,770
A5. Security Misconfiguration	18,391,649
A6. Vulnerable and Outdated Components	219,963
A7. Identification and Authentication Failures	25,352,564
A10. Server-Side Request Forgery	27,648,549

< OWASP Top 10 Web Attack Cases>

III. Web Attack Trends During H1 2023

5. Web attack trends by objective



The above graph categorizes detected web attacks during the first half of 2023 by the attackers' objectives. The top five objectives are Information Leakage (38.66%), Vulnerability Scanning (25.93%), Website Defacement (25.41%), Malicious Code Circulation (5.70%), and Server Operation Interference (4.27%).

About 38% of web attacks had the objective of **Information Leakage**. This can be done using a variety of attack methods, such as website defacement, SQL injection, and file inclusion. A website defacement attack 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 inclusion is when malicious scripts are injected into files in the targeted system.

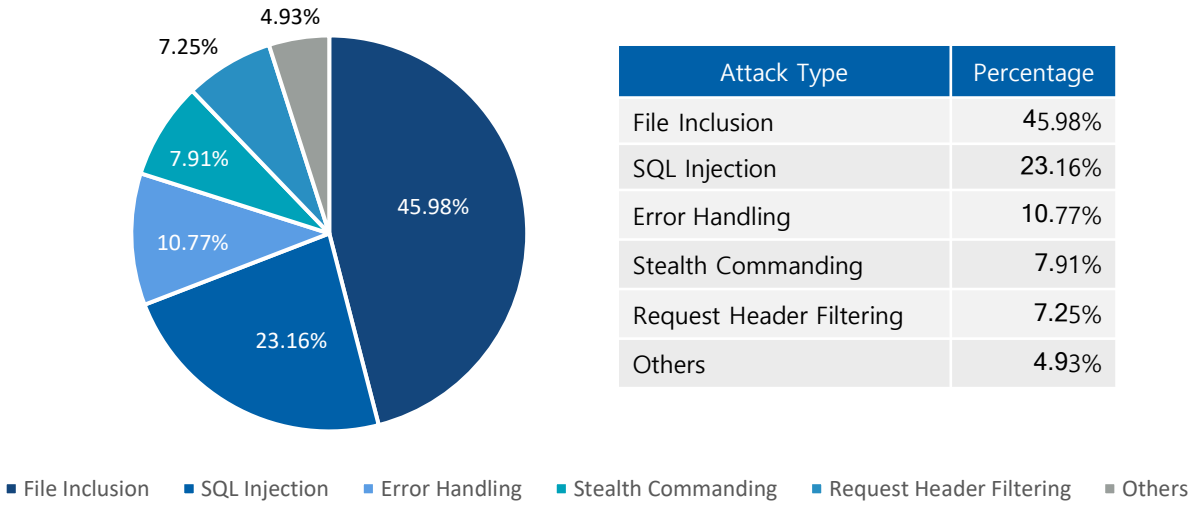
The second-most common attack objective is **Vulnerability Scanning**. This is when attackers attempt to explore potential vulnerabilities in their targeted application, usually done by using automated tools to send invalid HTTP requests or responses, to send invalid URLs that are different from the formats defined by RFC, to gain access to directory listings, or by error handling.

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

III. Web Attack Trends During H1 2023

6. Web attack trends by major attackers

Top Picks by Major Attackers



Attack Type	Percentage
File Inclusion	45.98%
SQL Injection	23.16%
Error Handling	10.77%
Stealth Commanding	7.91%
Request Header Filtering	7.25%
Others	4.93%

This analysis demonstrates the attack patterns of the top 10 most active attackers between January 1 and June 30, 2023. Since these highly active attackers tend to be professional threat actors and APTs that are more likely to cause serious damage, it is worth the time to analyze their attack patterns separately.

Results show that the most common attack methods used by the top 10 attackers are File Inclusion (45.98%), SQL Injection (23.16%), Error Handling (10.77%), Stealth Commanding (7.91%) , and Request Header Filtering (7.25).

As the most used attack method by major attackers, **File Inclusion** is when attackers execute malicious server scripts within a specified file to run commands on a targeted server. This can be highly destructive towards the web service and lead to sensitive data exposure, making it crucial to establish sufficient countermeasures.

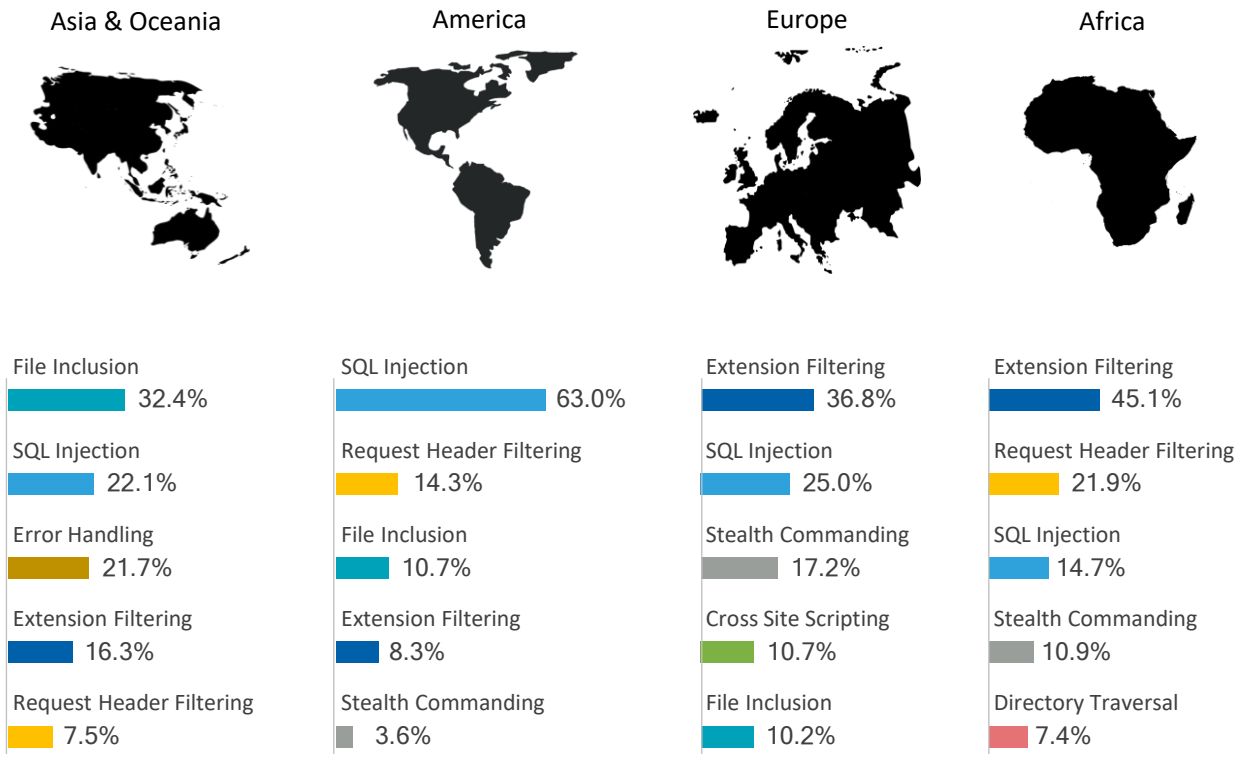
The second-most common attack method chosen by top attackers is **SQL Injection**. As mentioned earlier, this is when the attacker inserts invalid or unrelated SQL scripts to the SQL query to retrieve, modify, or delete data from the server. There are many known SQL Injection attack techniques, making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

Speaking of data breaches, one commonality across all major attackers 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 manual in case a data breach happens.

III. Web Attack Trends During H1 2023

7. Web attack trends by continent

Web Attack Trends by Targeted Continent



The graph above depicts all detected attacks classified by their targeted continents. Consistent with last year, **File Inclusion** is the most detected attack type in Asia and Oceania. **SQL Injection** is most detected in the Americas. **Extension Filtering** tops the list in Europe and Africa.

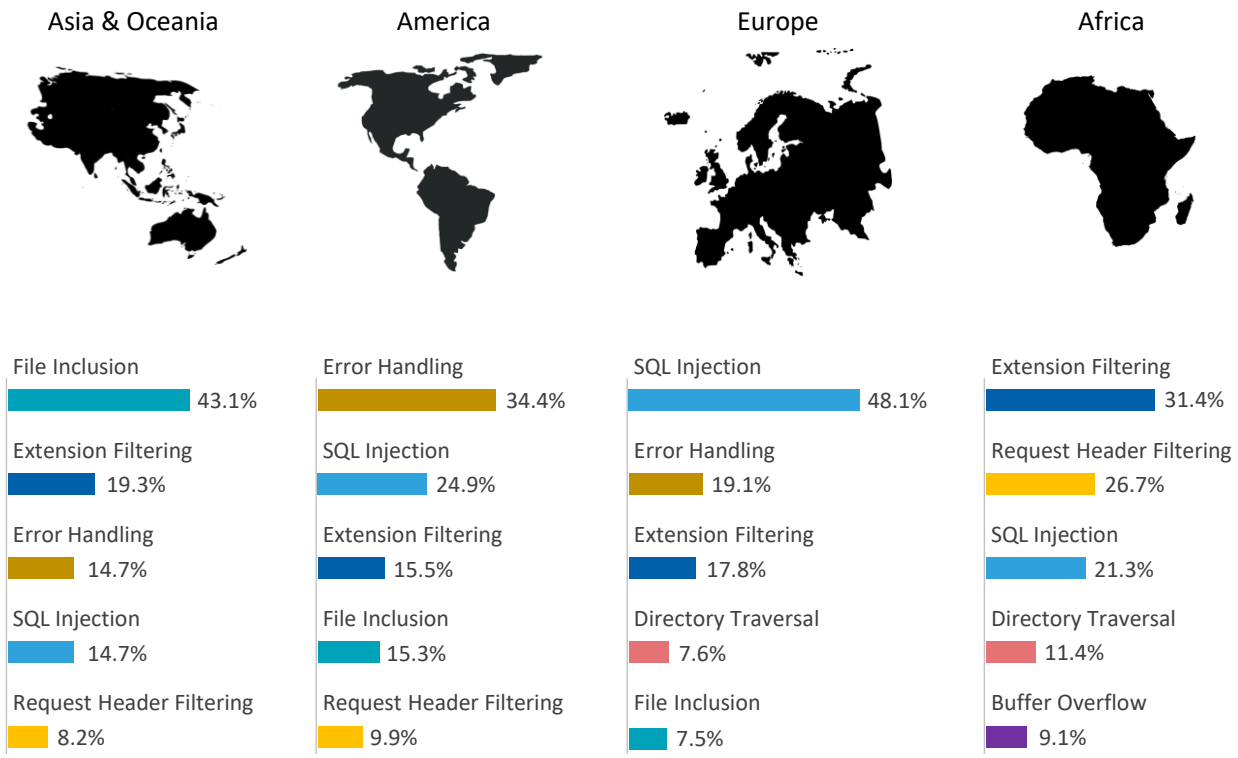
What is worth noting is that **SQL Injection**, which is ranked third on the OWASP Top 10 vulnerabilities list, is one of the top three most detected attack types on every continent of the world.

Results provide insights on which attack types security administrators from different regions of the world should prioritize on. For instance, **Extension Filtering** should be put at the top of the priority list in Europe and Africa, while organizations in the Americas should pay special attention to **SQL Injection**.

III. Web Attack Trends During H1 2023

7. Web attack trends by continent

Web Attack Trends by Continent of Origin

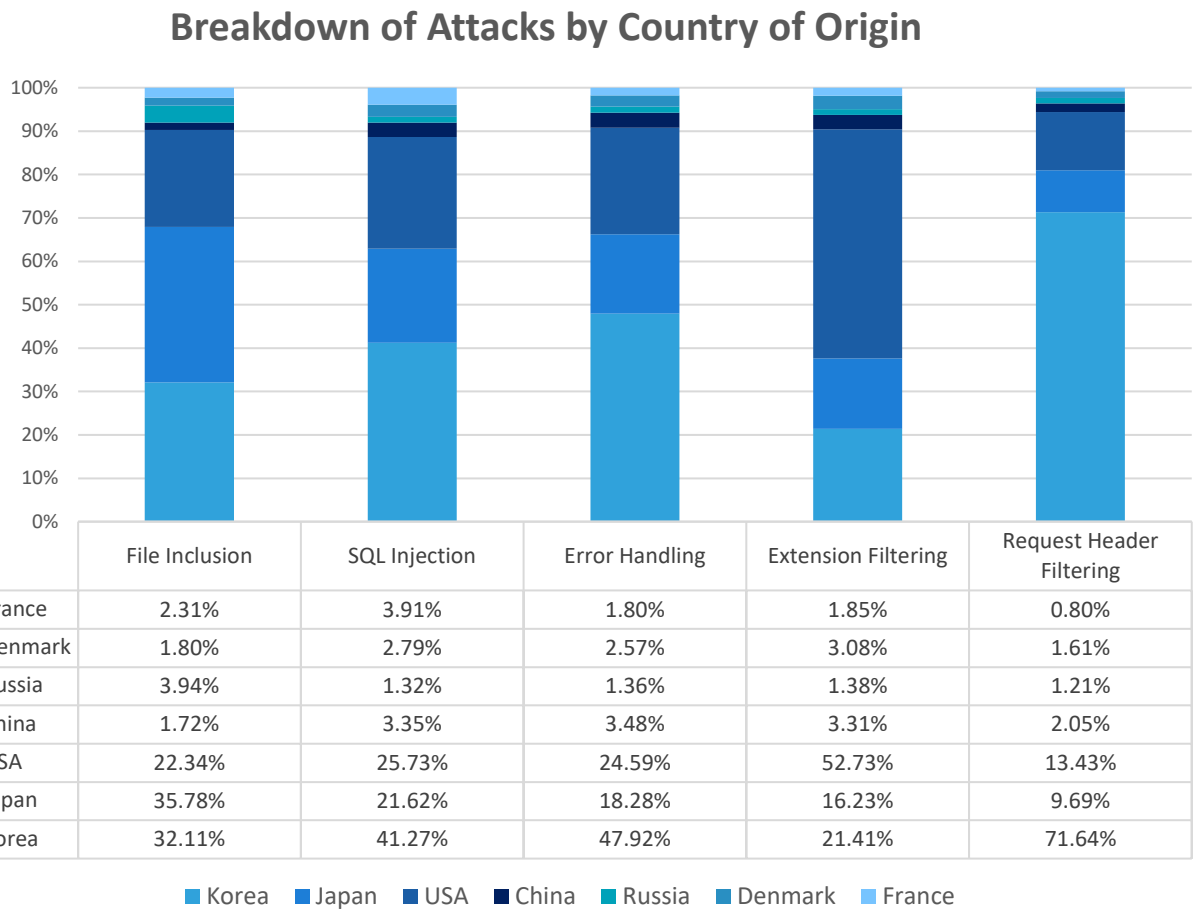


The graph above illustrates an analysis of attack origins based on their IP addresses. During the six-month period, the attack methods used by threat actors in different continents varied significantly. **File Inclusion** is the most common attack method used by attackers in Asia and Oceania. **Error Handling** is popular among attackers in the Americas. Nearly 50% of all attacks originating from Europe are **SQL Injection**, Lastly, **Extension Filtering** is most common among attacks originating from Africa.

What is worth noting is that both **SQL Injection** and **Extension Filtering** made it to the top four on all continents, meaning that these two attack methods are popular among all threat actors across the globe. Extension Filtering happens when attackers attempt to access configuration files (e.g. DLL, CONF, INI, etc.) that are prone to vulnerabilities. These attacks can be highly destructive because when unauthorized individuals access these configuration files, they could tamper with the web server and directly control the web service.

III. Web Attack Trends During H1 2023

8. Web attack trends by country



	File Inclusion	SQL Injection	Error Handling	Extension Filtering	Request Header Filtering
France	2.31%	3.91%	1.80%	1.85%	0.80%
Denmark	1.80%	2.79%	2.57%	3.08%	1.61%
Russia	3.94%	1.32%	1.36%	1.38%	1.21%
China	1.72%	3.35%	3.48%	3.31%	2.05%
USA	22.34%	25.73%	24.59%	52.73%	13.43%
Japan	35.78%	21.62%	18.28%	16.23%	9.69%
Korea	32.11%	41.27%	47.92%	21.41%	71.64%

The above graph illustrates the share of each attack type across their countries of origin, based on the detected attack attempts by WAPPLES and Cloudbric WAF+. The seven countries included in the analysis are the countries where the most attacks originated from. Results help security administrators prepare for location-based security policies.

Compared to the previous period, the UK and Germany no longer appear on the top 7 list, whereas Denmark and France enter the list at the sixth and seventh spots, respectively.

By comparing the relative share of each attack type within each country, it can be observed that 1) **Extension Filtering** is particularly popular among attackers in the US; 2) **File Inclusion** is widely used by threat actors from Russia; and 3) **SQL Injection** is relatively popular among hackers in France.

III. Web Attack Trends During H1 2023

9. Major web vulnerabilities

The most controversial web vulnerability during the first half of 2023 is the reflected cross site scripting (XSS) vulnerability (CVE-2023-30777) found in WordPress plugins **"WP Engine Advanced Custom Fields"** and **"WP Engine Advanced Custom Fields Pro".**[1] Reflected XSS, also known as a non-persistent attack, occurs when a malicious script is reflected off a web application to the victim's browser.

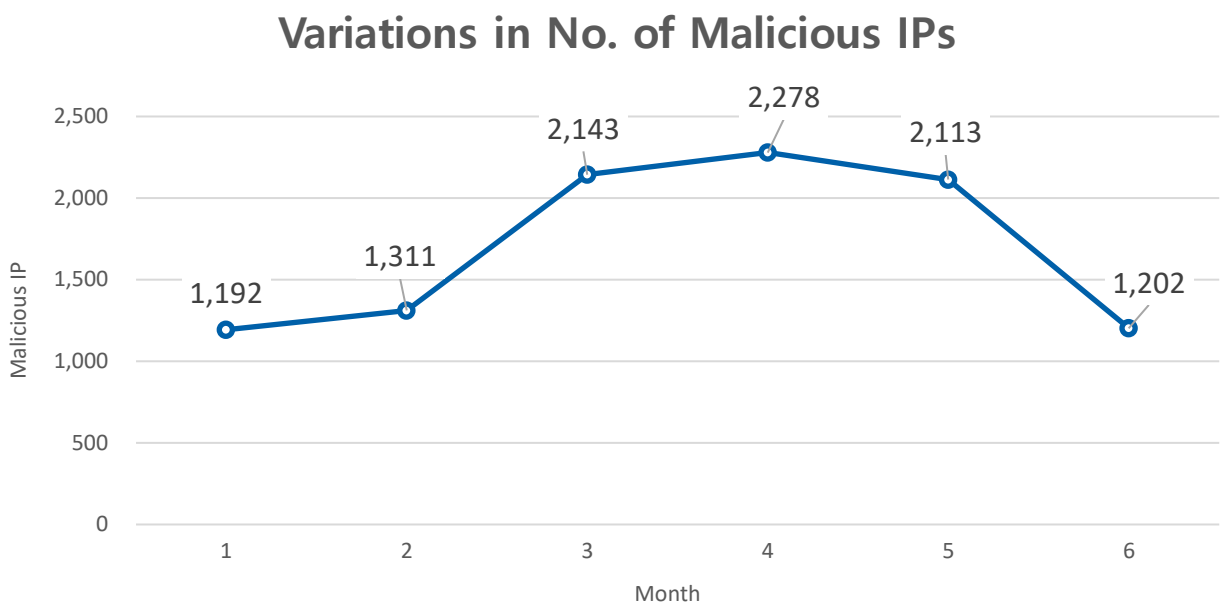
Reported on May 15, 2023, the vulnerability impacts all versions up to 6.1.5. Given an CVSS rating of 6.1 by NVD and 7.1 by Patchstack, the exploitation of this vulnerability could result in privilege escalation. To secure this vulnerability, administrators must either upgrade the plugin to the latest version or set up strict access control.

To minimize the potential impacts of zero-day vulnerabilities, it is recommended to update all plugins, browsers, and software programs to their latest versions.

1) "National Vulnerability Database: CVE-2023-30777 Detail." *National Institute of Standards and Technology.* May 10, 2023.

III. Web Attack Trends During H1 2023

10. Variations in 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 IP addresses does not necessarily indicate a lower number of attacks, as a single attacker can use many IP addresses to conduct an attack, and 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 ten attacks in a particular month. The analysis can help establish associations between specific attackers and their IP addresses, making it easier to predict their patterns in the future.

Based on the data, the number of detected malicious IP addresses peaked at 2,278 in April, while averaging at 1,706 per month throughout the first half of 2023. A significant rise of over 800 cases in March can be related to the WordPress plugin vulnerability. Organizations should continue to step up their security measures to defend against these growing threats and have emergency response manuals prepared in advance.

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 WAF+, a cloud and edge computing-based web service distributed worldwide. The data collection duration is between January 1 and June 30, 2023.

2. Key characteristics of report

The 2023 H1 WATT report included detection log data from both WAPPLES and Cloudbric WAF+. This data is used by Penta Security's proprietary machine learning technology to allow 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 WAF+. On the casual end, it is an easy read for general readers, including those involved in research on cybersecurity 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

▪ 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

▪ Cross Site Scripting (XSS)

A type of injection, XSS happens when malicious scripts are injected into trusted websites, usually in forums and emails. For instance, the attacker could inject a malicious script into a web page, usually in the form of a browser-side script. End-users landing on the page will be triggered to execute the malicious code.

Potential Consequences: access user cookies, access user sessions, execute malicious code

▪ Extension Filtering

The "extension" refers to file extensions. These attacks happen when attackers attempt to use abnormal extensions to trigger file download, code execution, and other malicious actions.

Potential Consequences: execute malicious code

IV. Appendix

4. OWASP and WAPPLES/Cloudbric Rules

OWASP (Open Web Application Security Project) creates a list every three years on 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.

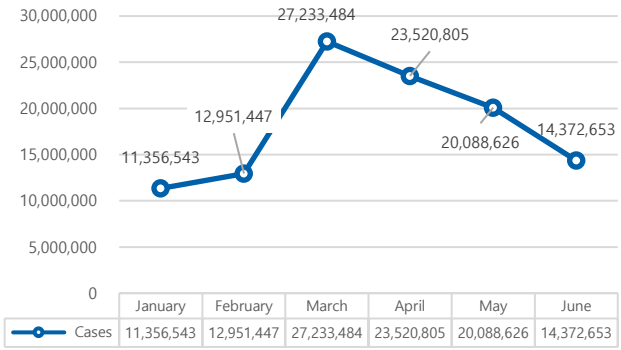
Rank	OWASP Top 10	WAPPLES/Cloudbric Rules
1	Broken Access Control	Parameter Tampering
		Invalid URL
		Directory Traversal
		Url Access Control
2	Cryptographic Failures	Privacy File Filtering
		Privacy Input Filtering
		Privacy Output Filtering
		Input Content Filtering
		Response Header Filtering
		Error 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 and 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 Synchronization
10	Server-Side Request Forgery	File Inclusion

- One WAPPLES/Cloudbric rule may match multiple OWASP Top 10 vulnerabilities.

IV. Appendix

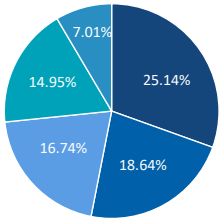
5. Summary of charts

Monthly Variations of Web Attacks

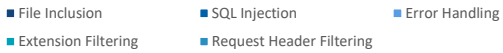


	January	February	March	April	May	June
Cases	11,356,543	12,951,447	27,233,484	23,520,805	20,088,626	14,372,653

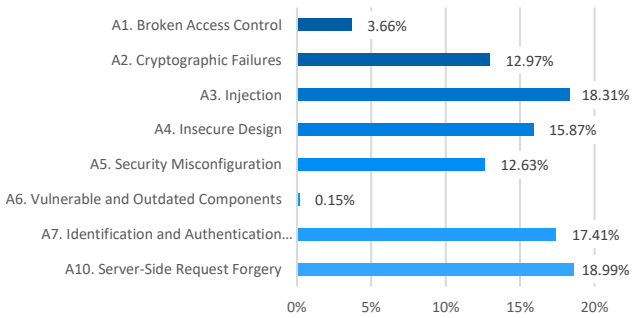
Web Attack Trends by Rule



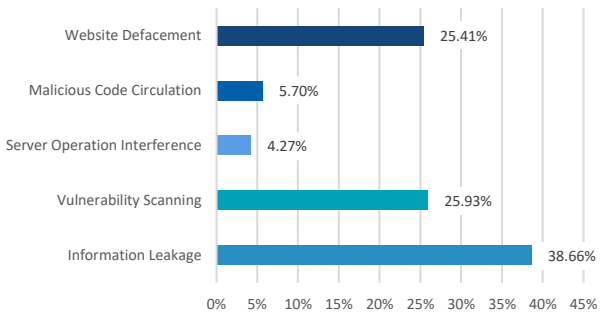
Attack Type	Percentage
File Inclusion	25.14%
SQL Injection	18.64%
Error Handling	16.74%
Extension Filtering	14.95%
Request Header Filtering	7.01%



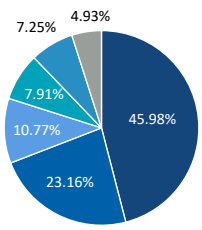
OWASP Top 10 Vulnerabilities



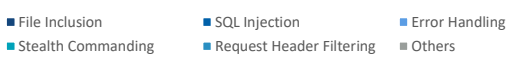
Web Attack Trends by Objective



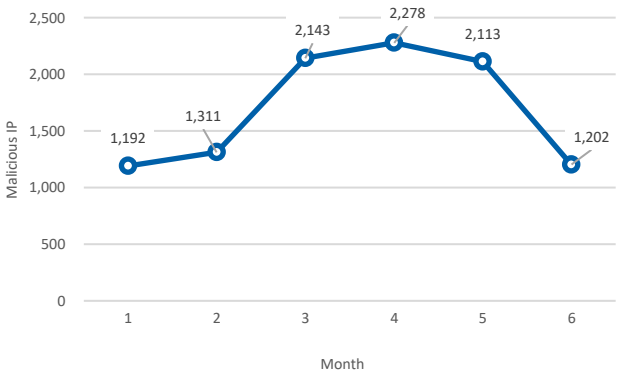
Top Picks by Major Attackers



Attack Type	Percentage
File Inclusion	45.98%
SQL Injection	23.16%
Error Handling	10.77%
Stealth Commanding	7.91%
Request Header Filtering	7.25%
Others	4.93%



Variations in No. of Malicious IPs



IV. Appendix

6. List of top 40 attackers

Rank	IP Address	Country
1	192.169.X.X	United States
2	218.200.X.X	China
3	66.11.X.X	Japan
4	23.106.X.X	Singapore
5	211.253.X.X	Korea
6	110.45.X.X	Korea
7	66.249.X.X	United States
8	183.96.X.X	Korea
9	66.249.X.X	United States
10	52.193.X.X	Japan
11	193.107.X.X	Hong Kong
12	52.167.X.X	United States
13	103.86.X.X	Korea
14	37.187.X.X	France
15	40.77.X.X	United States
16	211.253.X.X	Korea
17	121.254.X.X	Korea
18	34.98.X.X	Japan
19	218.55.X.X	Korea
20	154.47.X.X	Japan
21	118.151.X.X	Japan
22	118.151.X.X	Japan
23	91.240.X.X	Netherlands
24	220.93.X.X	Korea
25	211.253.X.X	Korea
26	103.252.X.X	Hong Kong
27	45.147.X.X	Germany
28	45.93.X.X	Russian Federation
29	157.55.X.X	United States
30	207.148.X.X	Japan
31	46.3.199.X.X	Russian Federation
32	40.77.X.X	United States
33	66.249.X.X	United States
34	34.98.X.X	Japan
35	3.226.X.X	United States
36	157.55.X.X	United States
37	137.135.X.X	United States
38	113.39.X.X	Japan
39	66.249.X.X	United States
40	52.37.X.X	United States

cloudbric

GLOBAL www.cloudbric.com

JAPAN www.cloudbric.jp

Penta SECURITY
enterprise · iot · blockchain

KOREA www.pentasecurity.co.kr

GLOBAL www.pentasecurity.com

JAPAN www.pentasecurity.co.jp

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