cloudbric
Penta SECURITY
cloud · iot · blockchain

Web Application Threat Trend Report

Trends of the Second Half of 2022

Cloudbric Corp.
Penta Security Systems Inc.

cloudbric
Penta SECURITY

Contents

I. Overview

1. Objective of report

The 2022 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 WAF+, a world-leading cloud and 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 Intelligent Customer Support (ICS) system and Cloudbric WAF+, providing an accurate representation of web attacks worldwide during the second half of 2022.

In this report, Penta Security and Cloudbric analyze these newly collected data to identify the latest web attack trends, including trends in attack type, attack pattern, commonly used malicious IPs, commonly targeted industries, and more. These analyses are then reflected in the future rules and operations of WAPPLES and Cloudbric WAF+.

This report is compiled and distributed for the sole purpose of providing information to all readers interested in web security trends, including customers and partners of WAPPLES and Cloudbric WAF+, CISOs, CSOs, 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*. 2015.

II. Executive Summary

The data presented in this report are selected based on the top 5 primary detections 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, target industries, IP addresses of major threat actors, and regional trends on where attacks occur and originate from.

During the first half of 2022, nearly 40% of attacks exploiting web vulnerabilities were aimed at either stealing or purposefully leaking sensitive information. A common attack method is **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 vulnerability is **Injection**, this is when attackers inject abnormal inputs into the website script as an attempt to alter or interfere with the request. **Identification and Authentication Failures** comes next. This is where brute force or social engineering technique is used to target accounts lacking multi-factor authentication (MFA).

Based on the top 5 detection rules of WAPPLES and Cloudbric WAF+, the most observed attack type is **SQL Injection**, where attackers inject malicious scripts into the SQL query. For many years, SQL Injection has been one of the most popular attack methods.

Below is a summary of the top 3 web attacks detected by WAPPLES and Cloudbric WAF+ from July 1 to December 31, 2022.

Rank	Attack Type	Percentage
1	SQL Injection	22.73%
2	Request Header Filtering	18.67%
3	Extension Filtering	16.94%

<Top 3 Attack Types>

Rank	Attack Objective	Percentage
1	Information Leakage	43.63%
2	Vulnerability Scanning	34.92%
3	Website Defacement	8.70%

<Top 3 Attack Objectives>

Rank	OWASP Top 3	Cases
1	Injection	23,923,836
2	Identification and Authentication Failures	22,545,164
3	Insecure Design	13,408,133

<Top 3 Attacks from OWASP Top 10>

Rank	Attack Type	Percentage
1	Request Header Filtering	61.91%
2	SQL Injection	14.68%
3	Error Handling	9.14%

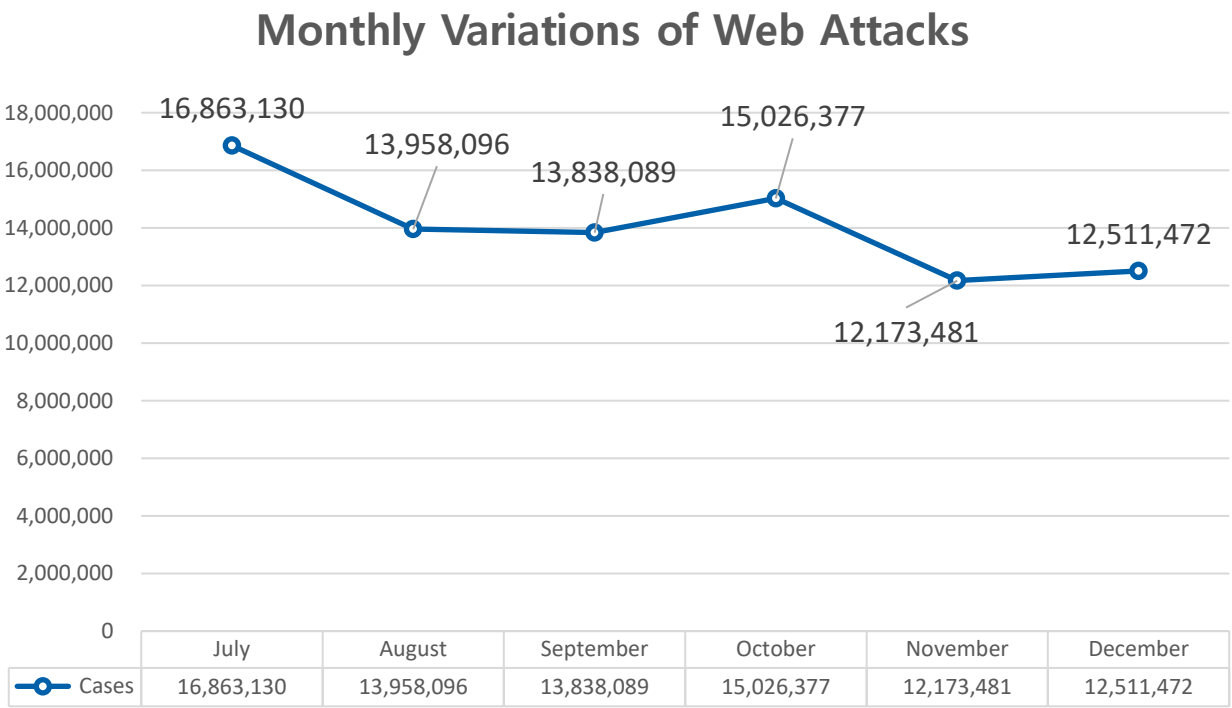
<Top 3 Picks by Major Attackers>

III. Web Attack Trends During H2 2022

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 WAF+ during the second half of 2022.



According to the data, the number of web attacks averaged at about 14.06 million per month, with over 15 million cases in July and October. The high figure in July can be related to a few major cybersecurity incidents, including the data breach of Shanghai police, which leaked 1 billion personal records,[1] as well as the discovery of Google Chrome's fourth zero-day vulnerability of the year.[2]

During the six-month period, threat actors continued to target existing vulnerabilities with new attack patterns, with many deriving new vulnerabilities from these existing vulnerabilities. This makes it crucial for organizations to continue monitoring new vulnerabilities and have their web servers and services patched as soon as one becomes available.

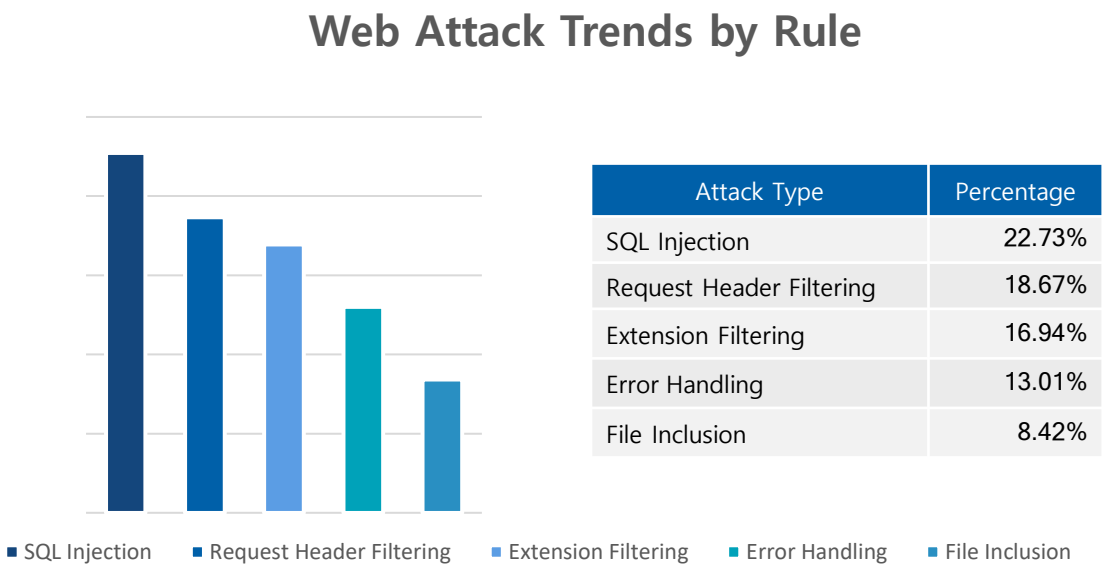
1) "A huge data leak of 1 billion records exposes China's vast surveillance state". *TechCrunch.* July 8, 2022.
2) "Google Confirms Chrome's Fourth Zero-Day Exploit in 2022". *Forbes.* July 6, 2022.

III. Web Attack Trends During H2 2022

2. Web attack trends by rule

By categorizing web attacks according to the detection rules of WAPPLES and Cloudbric WAF+, this rule-based analysis illustrates which attack types occurred the most during the second half of 2022. 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
SQL Injection	22.73%
Request Header Filtering	18.67%
Extension Filtering	16.94%
Error Handling	13.01%
File Inclusion	8.42%

Between July 1 and December 31, 2022, the top five observed attack types are **SQL Injection** (22.73%), **Request Header Filtering** (18.67%), **Extension Filtering** (16.94%), **Error Handling** (13.01%), and **File Inclusion** (8.42%).

Ranked second in the previous report, **SQL Injection** has now risen to the top spot on the list. SQL Injection 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 used for large-scale data exfiltration. A wide range of SQL Injection attack methods have been detected, making it crucial to have effective countermeasures.

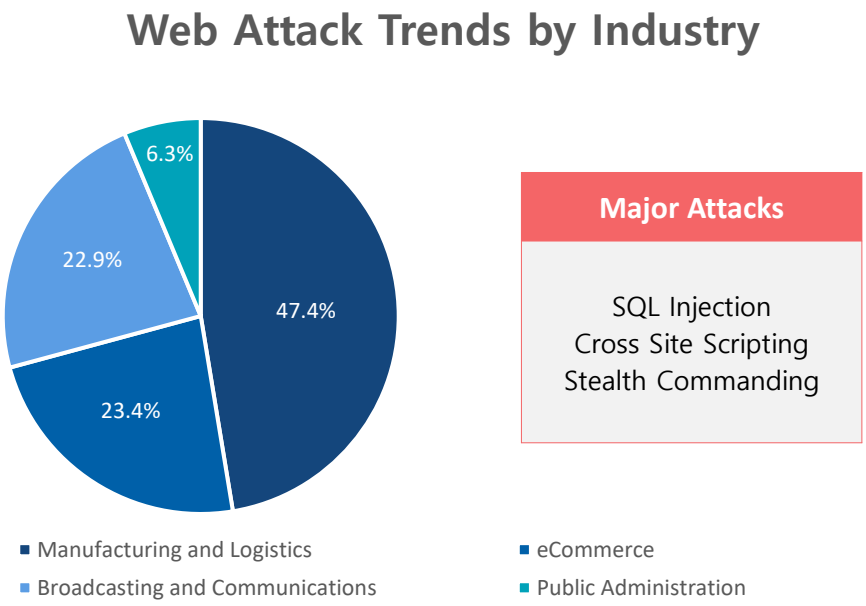
Request Header Filtering comes second on the list. This is when an attacker corrupts the HTTP requests sent from the web browser to the web server. They could do this by either removing an important element from the request header or adding scripts to the header to alter the request in favour of their attack objective. Although this type of attack does not directly lead to data exposure, it could serve as a crucial steppingstone for follow-up attacks.

Extension Filtering is the third-most common attack type. This 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.

Lastly, attacks like **Error Handling** and **File Inclusion** 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 H2 2022

3. Web attack trends by industry



The above graph shows the top 4 industries suffering the most web attacks based on the data of WAPPLES and Cloudbric WAF+ customers. A variety of attack types were observed in the analysis, providing further insights for each specific industry on how to stay prepared.

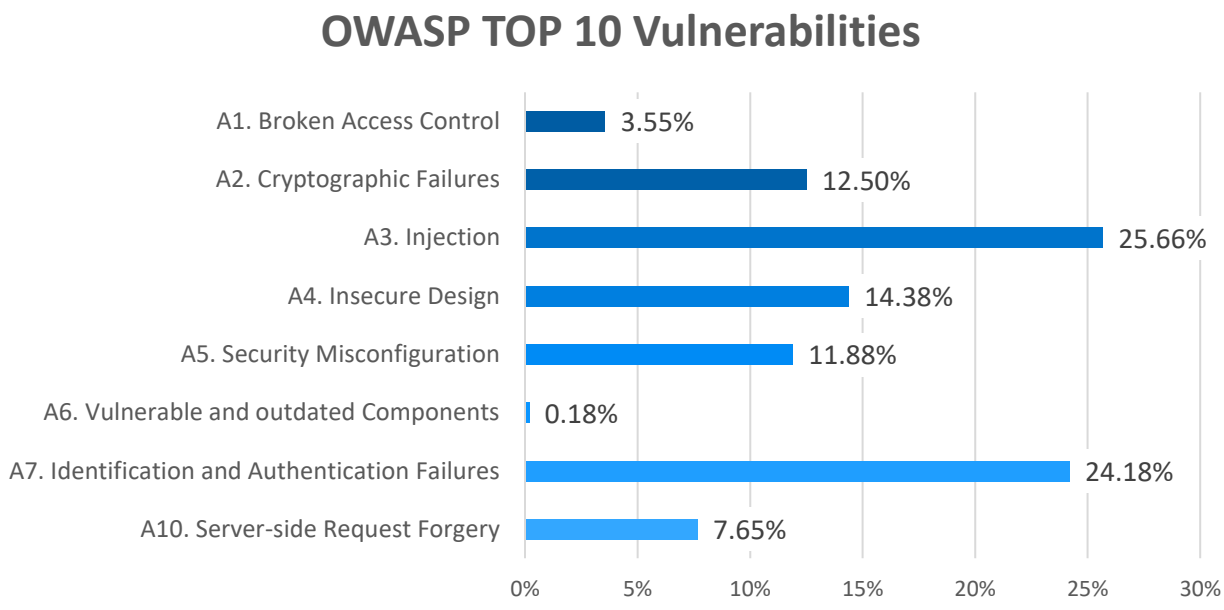
According to the graph, manufacturing and logistics, e-commerce, and broadcasting and communications are three industries suffering high loads of web attacks. A majority of attacks targeted the manufacturing and logistics industry due to the large volume of consumer data and sensitive business files it handles. Security administrators must pay special attention to protect personally identifiable information (PII).

Recently, threat actors are increasingly exploiting PII for social engineering and phishing attacks, leading to account compromise and even ransomware infection. As such, cyberattacks against critical industries not only put consumer and corporate data at risk, but also have the potential to disrupt infrastructures crucial to national security. Cybersecurity awareness and robust countermeasures must be in place to defend such threats.

III. Web Attack Trends During H2 2022

4. Web attack trends by OWASP Top 10

The following analysis categorizes all attacks detected by WAPPLES and Cloudbric WAF+ during the second half of 2022 as according to the OWASP Top 10 vulnerabilities list.



The graph above shows a breakdown of attacks in OWASP Top 10 categories between July 1 and December 31, 2022. **Injection** is the most frequently exploited vulnerability, followed by **Identification and Authentication Failures** and **Insecure Design**.

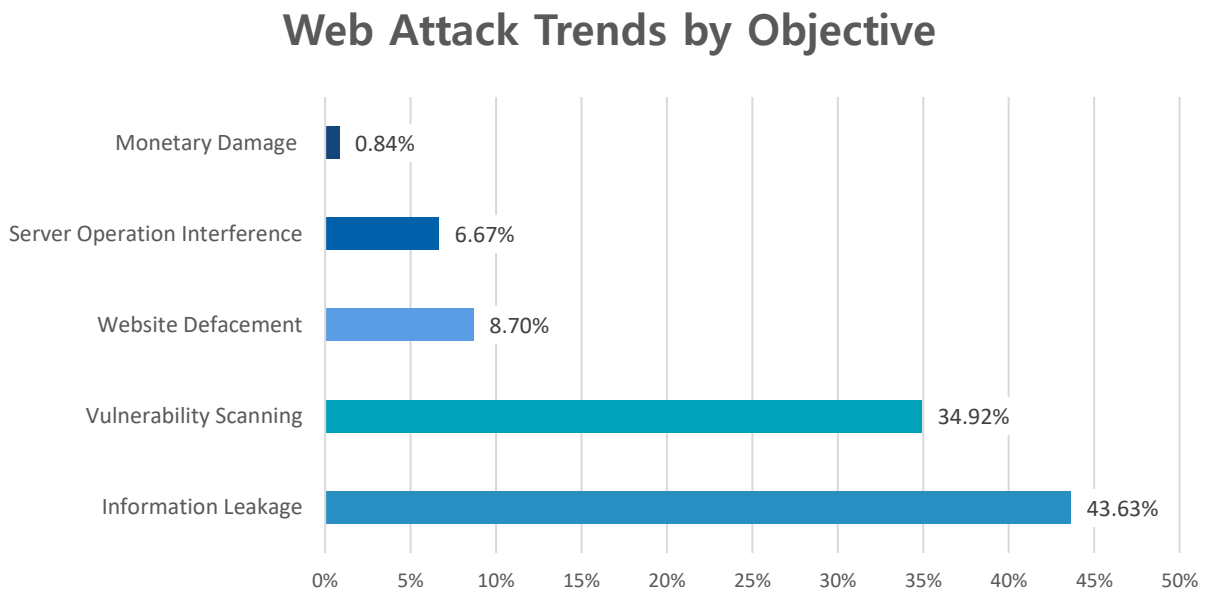
A wide range of **Injection** attack methods were discovered over this period. Hence security administrators must monitor their vulnerabilities and keep their servers and software up to date.

OWASP Top 10 (2021) Vulnerabilities	Cases
A1. Broken Access Control	3,313,383
A2. Cryptographic Failures	11,655,203
A3. Injection	23,923,836
A4. Insecure Design	13,408,133
A5. Security Misconfiguration	11,077,176
A6. Vulnerable and outdated Components	172,001
A7. Identification and Authentication Failures	22,545,164
A10. Server-side Request Forgery	7,127,649

< OWASP Top 10 Web Attack Cases>

III. Web Attack Trends During H2 2022

5. Web attack trends by objective



The above graph categorizes detected web attacks during the second half of 2022 by the attackers' objectives. The top five objectives are **Information Leakage** (43.63%), **Vulnerability Scanning** (34.92%), **Website Defacement** (8.70%), **Server Operation Interference** (6.67%), and **Monetary Damage** (0.84%).

Over 40% 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.

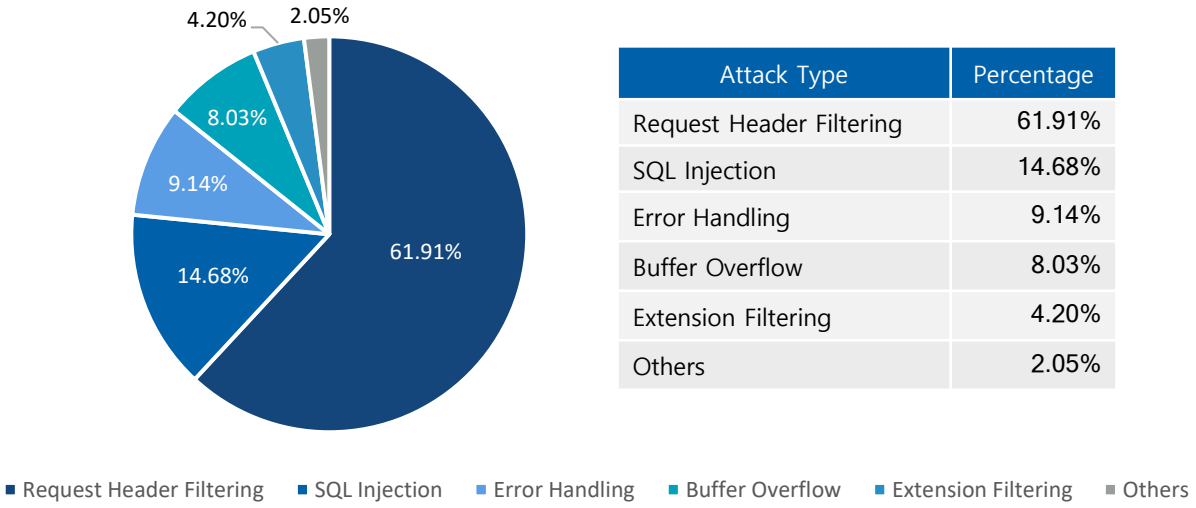
The second-most common attack objective is **Vulnerability Scanning**. This is when attackers attempt to explore potential vulnerabilities in their targeted application, usually done by using automated tools to send invalid HTTP requests or responses, to send invalid URLs that are different from the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

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

III. Web Attack Trends During H2 2022

6. Web attack trends by major attackers

Top Picks by Major Attackers



Attack Type	Percentage
Request Header Filtering	61.91%
SQL Injection	14.68%
Error Handling	9.14%
Buffer Overflow	8.03%
Extension Filtering	4.20%
Others	2.05%

This analysis demonstrates the attack patterns of the top 10 most active attackers between July 1 and December 31, 2022. 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 **Request Header Filtering** (61.91%), **SQL Injection** (14.68%), **Error Handling** (9.14%), **Buffer Overflow** (8.03%), and **Extension Filtering** (4.20%).

As the most used attack method by major attackers, **Request Header Filtering** is when an attacker corrupts the HTTP requests sent from the web browser to the web server. They could do this by either removing an important element from the request header or adding scripts to the header to alter the request in favour of their attack objective. Although this type of attack does not directly lead to data exposure, it could serve as a crucial steppingstone for secondary attacks.

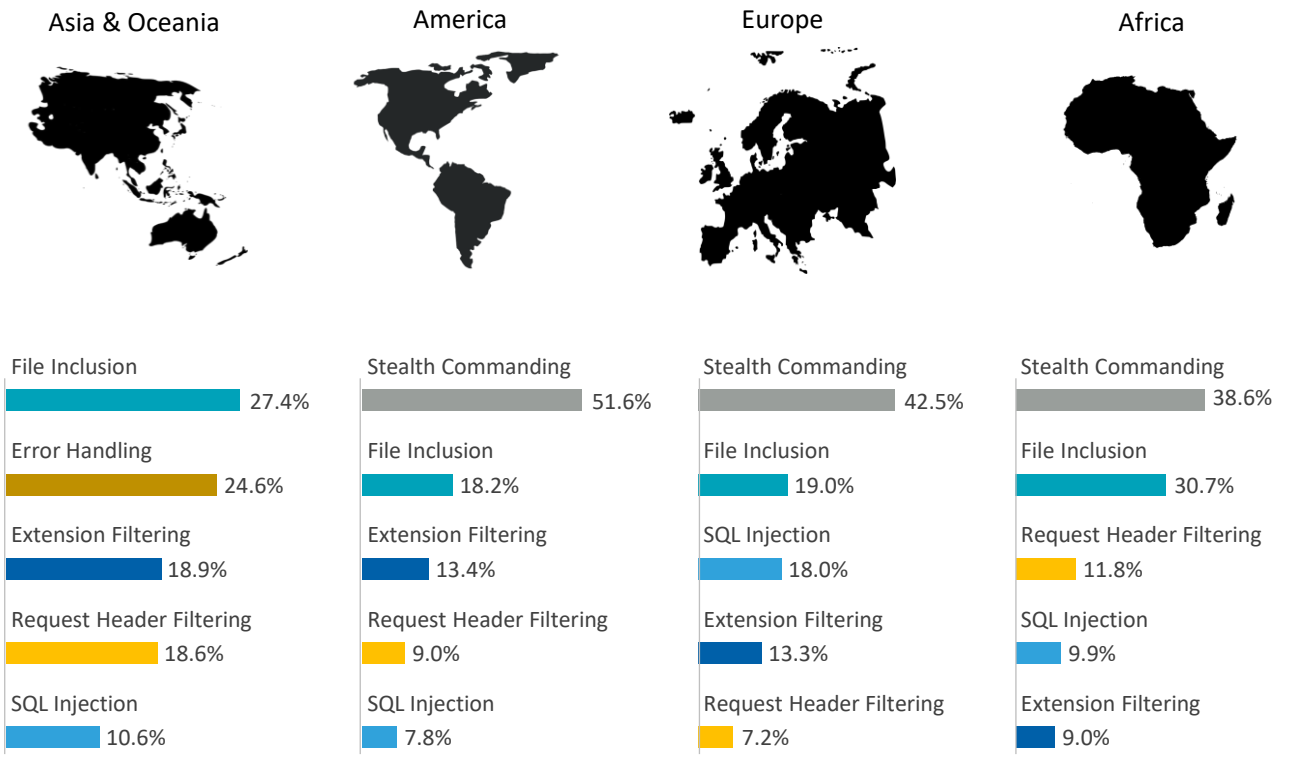
The second-most common attack method chosen by top attackers is **SQL Injection**. As mentioned earlier, this is when the attacker inserts invalid or unrelated SQL scripts to the SQL query to retrieve, modify, or delete data from the server. There are many known SQL Injection attack techniques, making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

Speaking of data breaches, one commonality across all 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 H2 2022

7. Web attack trends by continent

Web Attack Trends by Targeted Continent



The graph above depicts all detected attacks classified by their targeted continents. **File Inclusion** is the most detected attack type in Asia and Oceania, whereas **Stealth Commanding** tops the list in Europe, Africa, and the Americas.

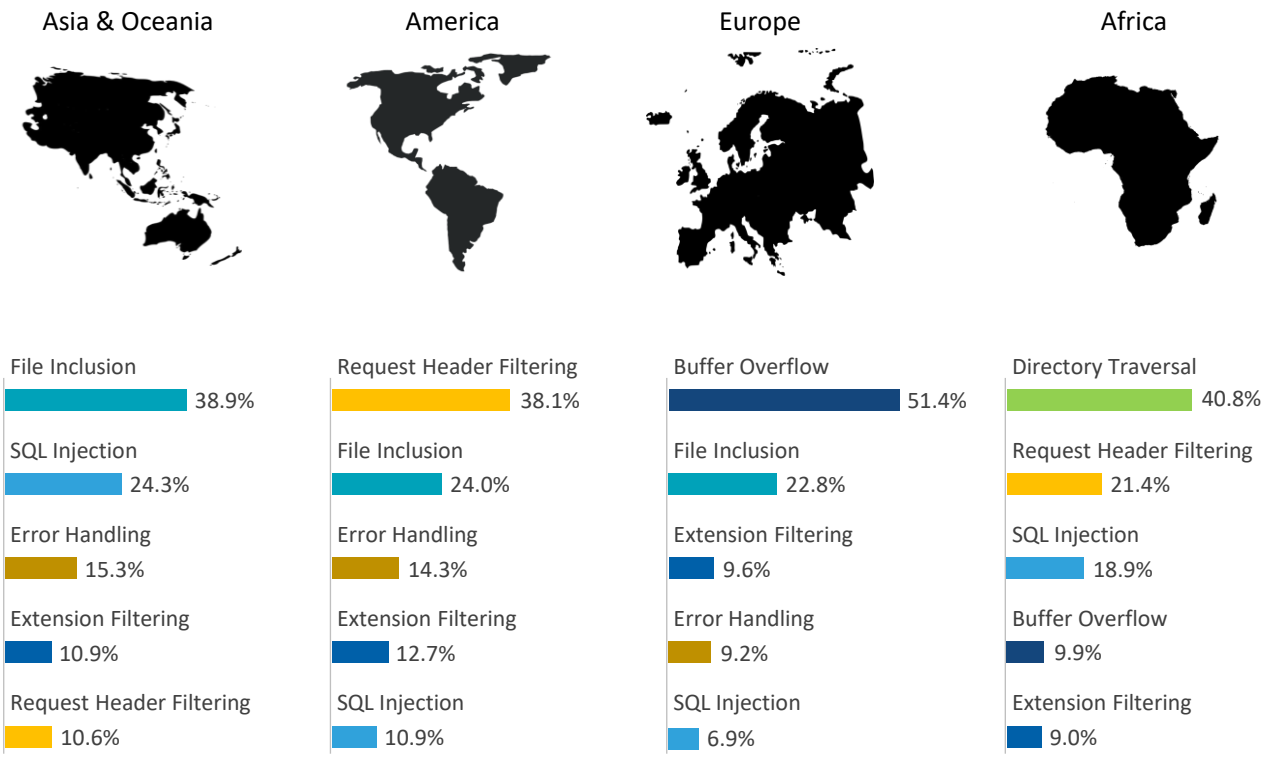
What is worth noting is that **SQL Injection**, which is ranked third on the OWASP Top 10 vulnerabilities list, is one of the top five most detected attack types on every continent of the world.

Results provide insights on which attack types security administrators from different regions of the world should prioritize on. For instance, **Stealth Commanding** should be put at the top of the priority list in Europe, Africa, and the Americas, while organizations in Asia and Oceania should pay special attention to **File Inclusion**.

III. Web Attack Trends During H2 2022

7. Web attack trends by continent

Web Attack Trends by Continent of Origin

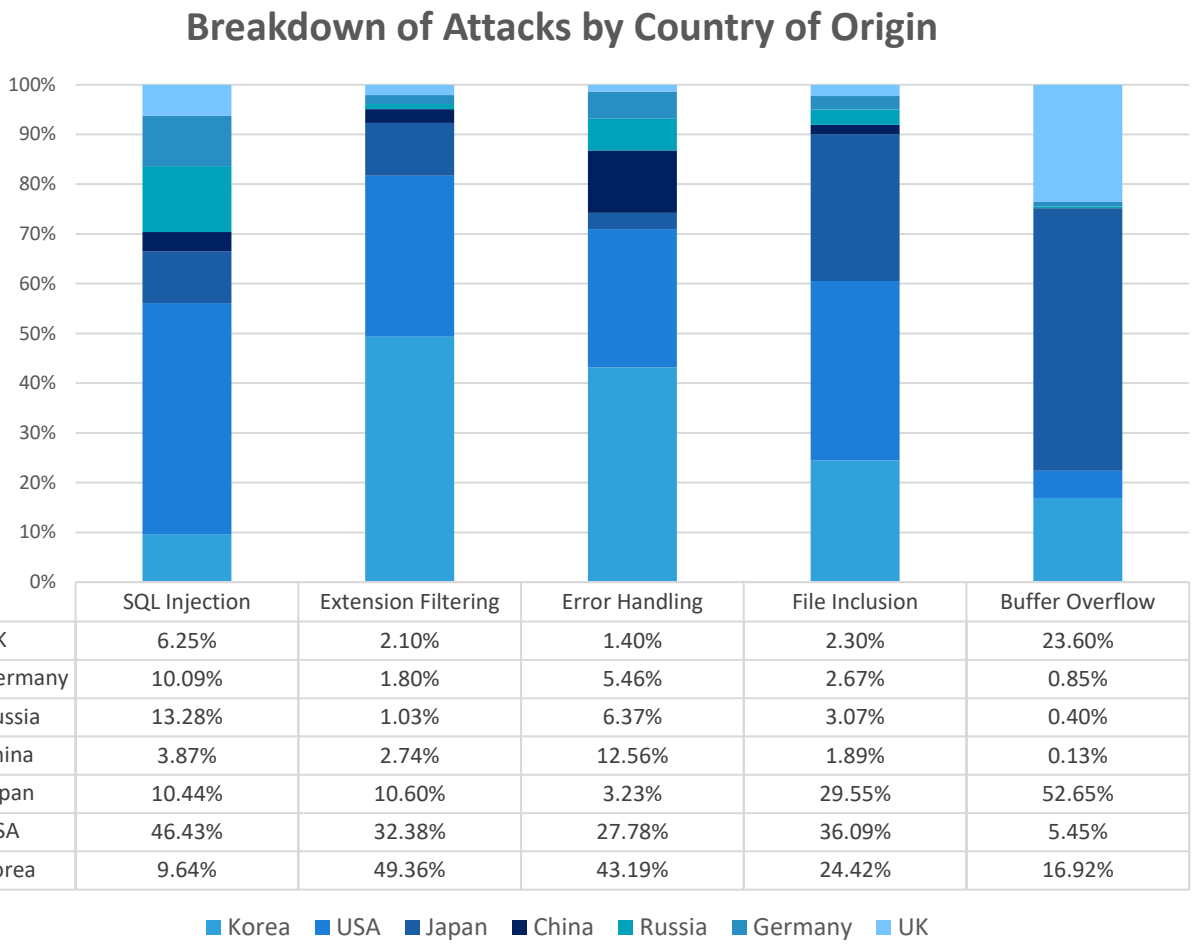


The graph above illustrates an analysis of attack origins based on their IP addresses. During this six-month period, the attack methods used by threat actors in different continents varied significantly. **File Inclusion** is the most common attack method used by attackers in Asia and Oceania. **Request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

Again, **SQL Injection** made it to the top five list in all continents, meaning that the attack method is popular among all threat actors across the globe. Also worth noting is that **File Inclusion** is highly popular everywhere except for Africa. File Inclusion is an attack method where attackers execute server scripts within a specified file. This file can either be an internal file that exists within the targeted 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.

III. Web Attack Trends During H2 2022

8. Web attack trends by country



	SQL Injection	Extension Filtering	Error Handling	File Inclusion	Buffer Overflow
UK	6.25%	2.10%	1.40%	2.30%	23.60%
Germany	10.09%	1.80%	5.46%	2.67%	0.85%
Russia	13.28%	1.03%	6.37%	3.07%	0.40%
China	3.87%	2.74%	12.56%	1.89%	0.13%
Japan	10.44%	10.60%	3.23%	29.55%	52.65%
USA	46.43%	32.38%	27.78%	36.09%	5.45%
Korea	9.64%	49.36%	43.19%	24.42%	16.92%

The graph above 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, France and South Africa no longer appear on the top 7 list, whereas Russia re-enters at the fifth spot and the UK comes in seventh.

By comparing the relative share of each attack type within each country, it can be observed that 1) **SQL Injection** is particularly popular among attackers in Germany and Russia and relatively less favoured in Korea; 2) **Buffer Overflow** is widely used by threat actors from Japan and the UK and rarely used in the US; and 3) **Error Handling** is highly popular among hackers in China.

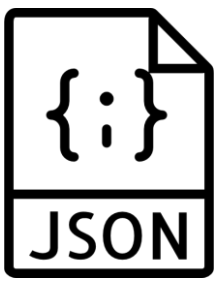
III. Web Attack Trends During H2 2022

9. Major web vulnerabilities

The most controversial web vulnerability during the second half of 2022 is JSON-based (Syntax) SQL injection[1]. JSON is an open standard file format and data interchange format that is commonly used in WebSphere Application Servers and API servers. Since JSON is compatible with many databases, this vulnerability allows attackers to exploit the JSON operators in databases to construct an SQL injection, then exfiltrate sensitive information from the databases.

JSON is compatible with a wide range of DBMS and NoSQL services. Therefore, users must either adopt a WAF or identify the payload to defend their databases from this vulnerability.

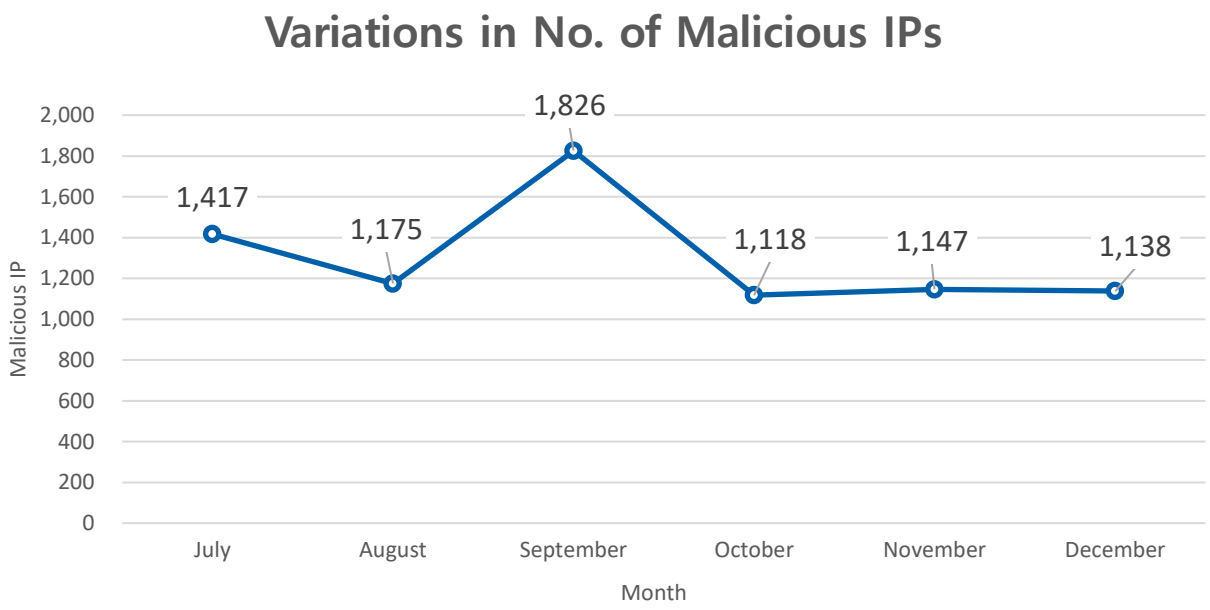
Another concerning aspect is that attackers are exploiting newer vulnerabilities based on the original vulnerability. Hence, security administrators must continue to monitor for related vulnerabilities after patching.



1) "JSON syntax hack allowed SQL injection payloads to be smuggled past WAFs". *The Daily Swig*. December 9, 2022.

III. Web Attack Trends During H2 2022

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 IPs does not necessarily indicate a lower number of attacks, since 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 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 attack patterns in the future.

Based on the data, the number of detected malicious IP addresses peaked at 1,826 in September, while averaging at 1,303 per month throughout the second half of 2022. A significant rise of nearly 700 cases in September can be related to a sudden increase in SQL injection attack vectors. 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 July 1 and December 31, 2022.

2. Key characteristics of report

The 2022 H2 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

▪ 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 number of the associated web server, application, and DBMS. This information can be used to derive the vulnerabilities of the software and conduct follow-up attacks to cause greater damage.

Potential Consequences: Data breach, secondary attacks

▪ 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: Tampered web server information, abnormal server behavior

▪ SQL Injection

SQL Injection is an attack where 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.

Potential Consequences: Unauthorized access to system and database, data breach

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.

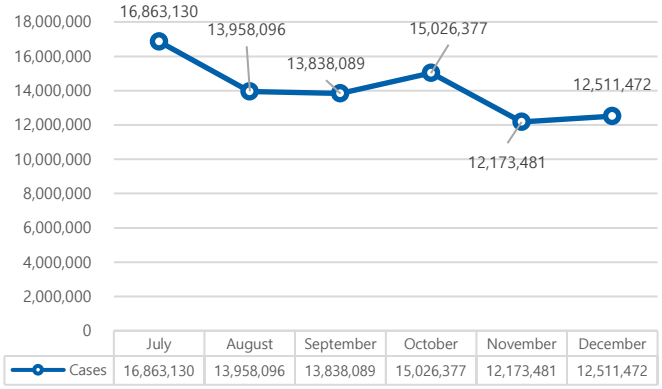
Top	OWASP Top 10	WAPPLES/Cloudbric Rules
1	Broken Access Control	Parameter Tampering
		Invalid URL
		Directory Traversal
		Url Access Control
2	Cryptographic Failures	Privacy File Filtering
		Privacy Input Filtering
		Privacy Output Filtering
		Input Content Filtering
		Response Header Filtering
		Error 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 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

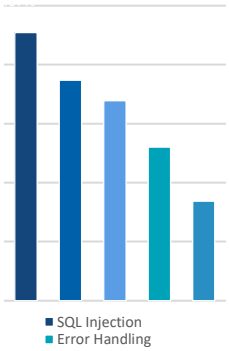
5. Summary of charts

Monthly Variations of Web Attacks



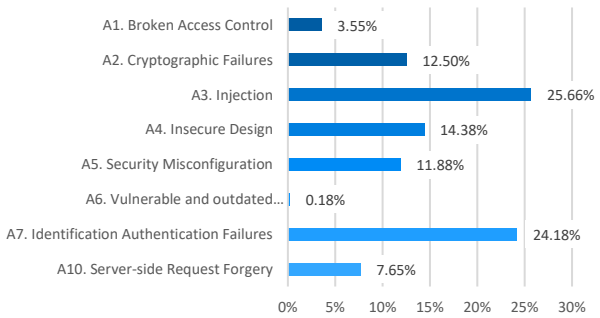
	July	August	September	October	November	December
Cases	16,863,130	13,958,096	13,838,089	15,026,377	12,173,481	12,511,472

Web Attack Trends by Rule

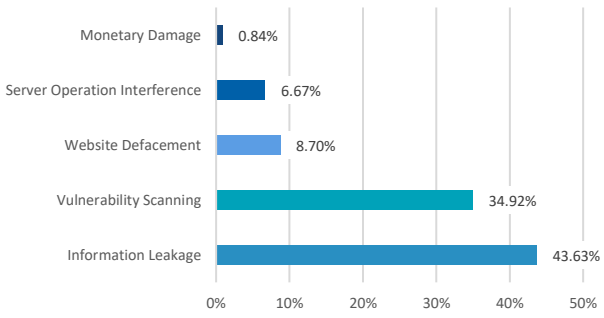


Attack Type	Percentage
SQL Injection	22.73%
Request Header Filtering	18.67%
Extension Filtering	16.94%
Error Handling	13.01%
File Inclusion	8.42%

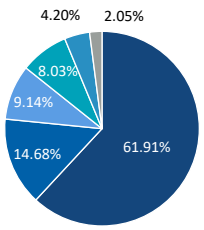
OWASP Top 10 Vulnerabilities



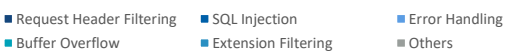
Web Attack Trends by Objective



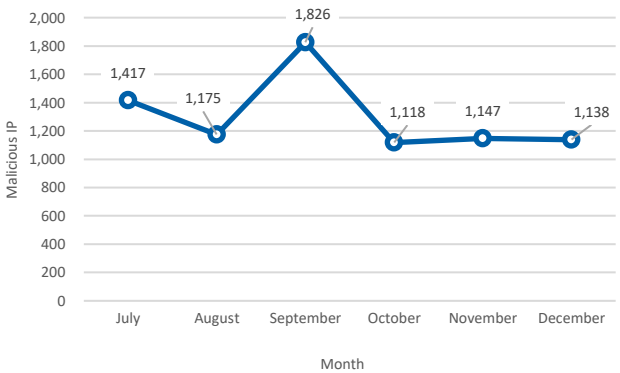
Top Picks by Major Attackers



Attack Type	Percentage
Request Header Filtering	61.91%
SQL Injection	14.68%
Error Handling	9.14%
Buffer Overflow	8.03%
Extension Filtering	4.20%
Others	2.05%



Variations in No. of Malicious IPs



IV. Appendix

6. List of top 40 attackers

Rank	IP Address	Country
1	121.131.X.X	Korea
2	211.233.X.X	Korea
3	219.240.X.X	Korea
4	115.71.X.X	Korea
5	110.45.X.X	Korea
6	1.234.X.X	Korea
7	122.199.X.X	Australia
8	20.27.X.X	USA
9	121.142.X.X	Korea
10	85.215.X.X	Germany
11	101.110.X.X	Japan
12	210.114.X.X	Korea
13	101.110.X.X	Japan
14	218.55.X.X	Korea
15	91.240.X.X	Hong Kong
16	125.7.X.X	Korea
17	106.245.X.X	Korea
18	121.142.X.X	Korea
19	94.182.X.X	Iran
20	118.151.X.X	Japan
21	95.216.X.X	Finland
22	185.7.X.X	Hong Kong
23	122.199.X.X	Australia
24	52.37.X.X	USA
25	211.114.X.X	Korea
26	121.124.X.X	Korea
27	44.241.X.X	USA
28	185.7.X.X	Hong Kong
29	185.122.X.X	UK
30	54.191.X.X	USA
31	118.151.X.X	Japan
32	61.255.X.X	Korea
33	209.141.X.X	USA
34	185.202.X.X	Unknown
35	113.52.X.X	Japan
36	20.106.X.X	USA
37	35.200.X.X	USA
38	157.90.X.X	USA
39	45.67.X.X	Unknown
40	20.13.X.X	USA

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