cloudbric

Penta SECURITY

cloud · iot · blockchain

Web Application Threat Trend Report

Trends for the First Half of 2022

Cloudbric Corp.

Penta Security Systems Inc.

cloudbric
Penta SECURITY

Contents

I. Overview

1. Objective of report

The 2022 H1 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 first 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) Frost & Sullivan (2015) *"Industry Quotient"*.

II. Executive Summary

The data presented in this report are selected based on the top five most important 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.

During the first half of 2022, nearly 40% of attacks were aimed at stealing or purposefully leaking sensitive information, where attackers attempt to gain unauthorized access by exploiting web vulnerabilities. Other common intrusion objectives include vulnerability scanning and website defacement.

Putting all attacks into OWASP Top 10 categories, the most exploited vulnerability is **Identification and Authentication Failures**, which is when attackers use brute force attacks to target user accounts without multi-factor authentication (MFA). Coming second is **Insecure Design**, which is when attackers exploit flaws in application design, leading to the disclosure of sensitive information in application error messages, or the execution of unwanted actions by the servers.

Based on the top five detection rules of WAPPLES and Cloudbric WAF+, the most observed attack type is **Extension filtering**. In these attacks, attackers gain unauthorized 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 WAF+ from January 1 to June 30, 2022.

Rank	Attack Type	Percentage
1	Extension Filtering	19.53%
2	SQL Injection	13.84%
3	Request Header Filtering	13.04%

<Top 3 Attack Types>

Rank	Attack Objective	Percentage
1	Information Leakage	39.36%
2	Vulnerability Scanning	25.62%
3	Website Defacement	12.35%

<Top 3 Attack Objectives>

Rank	OWASP Top 3	Cases
1	Identification and Authentication Failures	18,335,922
2	Insecure Design	8,488,740
3	Server-side Request Forgery	10,222,908

<Top 3 Attacks from OWASP Top 10>

Rank	Attack Type	Percentage
1	Extension Filtering	17.57%
2	SQL Injection	15.05%
3	Error Handling	14.39%

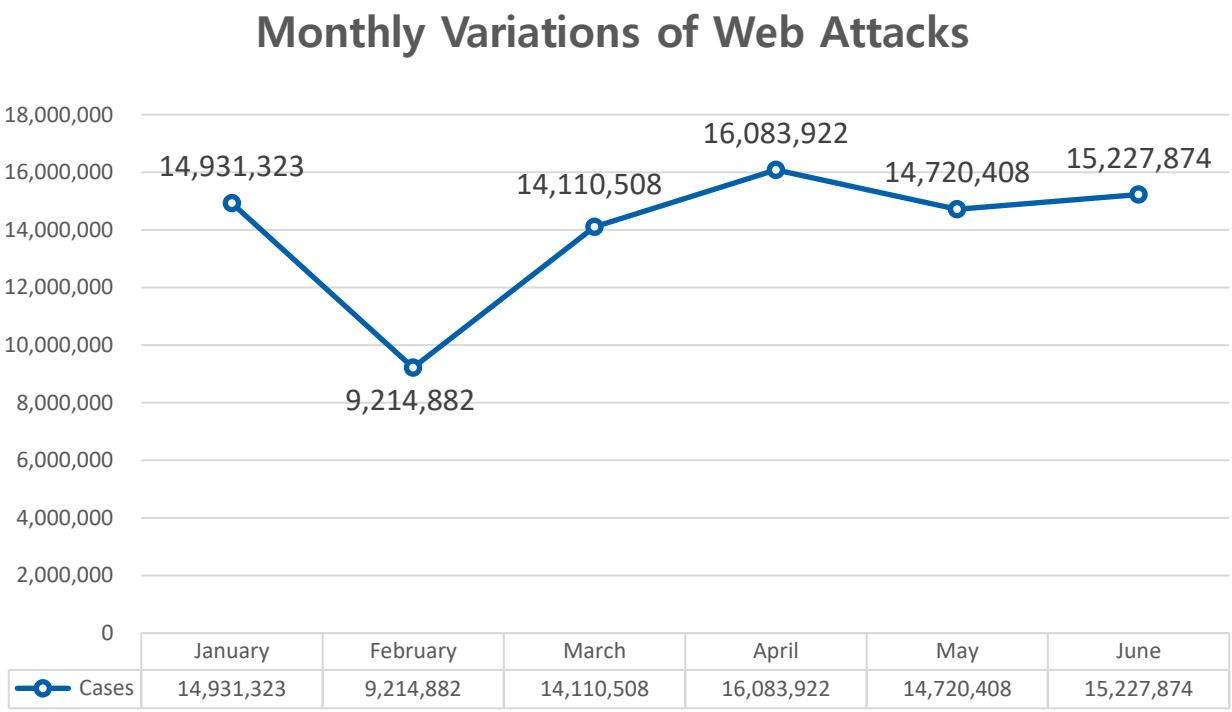
<Top 3 Picks by Major Attackers>

III. Web Attack Trends During H1 2022

1. Monthly variations

The monthly variation analysis depicts a clear view of when web attacks occur the most throughout the year, 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 first half of 2022.



According to the analysis, the number of web attack cases averaged at about 14 million per month, with over 15 million cases in April and June. Despite a drop in numbers in February, a resurgence was shown in March. Also in March, Chinese state-backed APT41 exploited the Log4j vulnerability to breach the government network of six US state governments.[1)]

With an elevated number of high-level vulnerabilities appearing during the first half of 2022, exploitation attempts are expected to continue throughout the rest of the year. Security administrators should constantly monitor these newly discovered vulnerabilities and apply security updates and patches as early as possible.

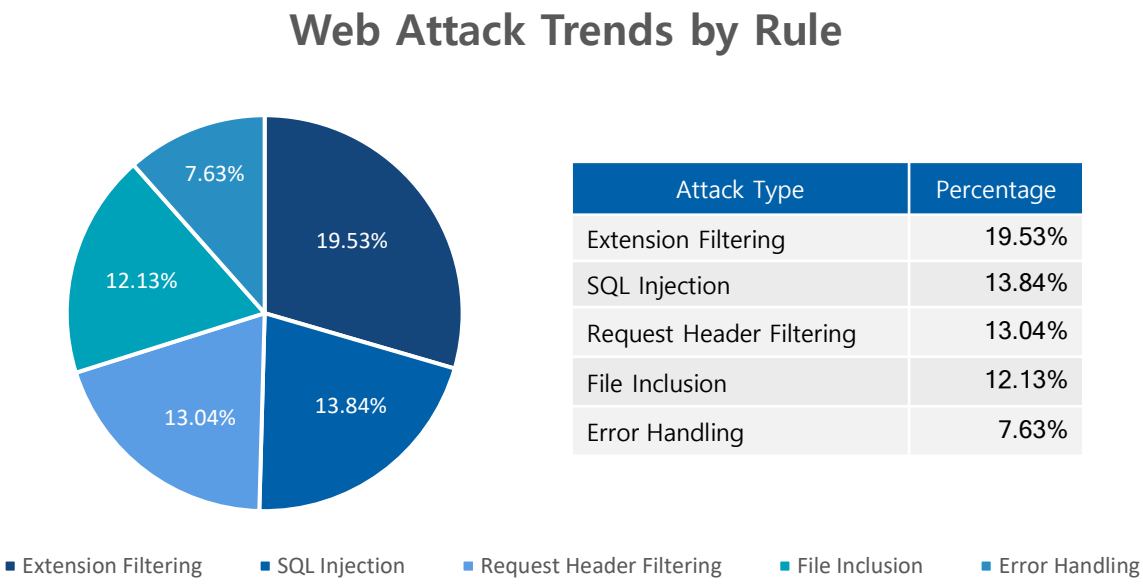
1) Mandiant (Mar 8, 2022) *"Does This Look Infected? A Summary of APT41 Targeting US State Governments".*

III. Web Attack Trends During H1 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 first 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
Extension Filtering	19.53%
SQL Injection	13.84%
Request Header Filtering	13.04%
File Inclusion	12.13%
Error Handling	7.63%

Between January 1 and June 30, 2022, the top five observed attack types are **Extension Filtering** (19.53%), **SQL Injection** (13.84%), **Request Header Filtering** (13.04%), **File Inclusion** (12.13%), **Error Handling** (7.63%).

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.

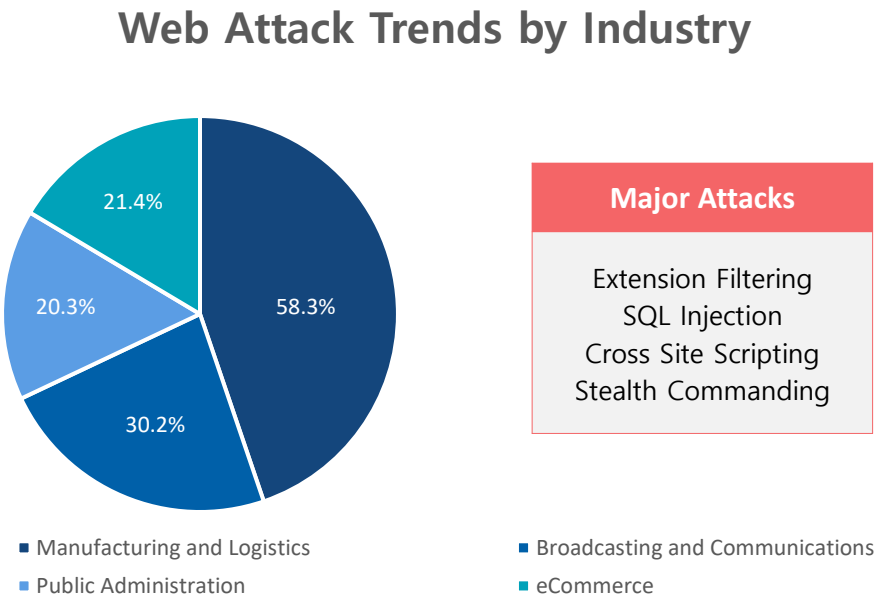
Another attack type that always appears on the top five list is **SQL Injection**. This is when the attacker inserts invalid or unrelated SQL scripts to the SQL query to attack the database, making it the most common attack method used for large-scale data compromise. A wide range of SQL Injection attack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

File Inclusion is when 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.

Lastly, attacks like **Request Head Filtering** and **Error Handling** 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 2022

3. Web attack trends by industry



The above graph shows the top four industries suffering the most web attacks based on the industries that 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, broadcasting and communications, public administration, and e-commerce are four major 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).

Examples of major cyberattacks against the manufacturing industry include the extensive hacking campaign conducted by LAPSUS$ hacker group, breaching a large number of companies from Nvidia and Microsoft to Samsung and LG. [1)] Additionally, a significant proportion of attack attempts during the first half of 2022 were politically oriented in response to the Russian invasion of Ukraine.

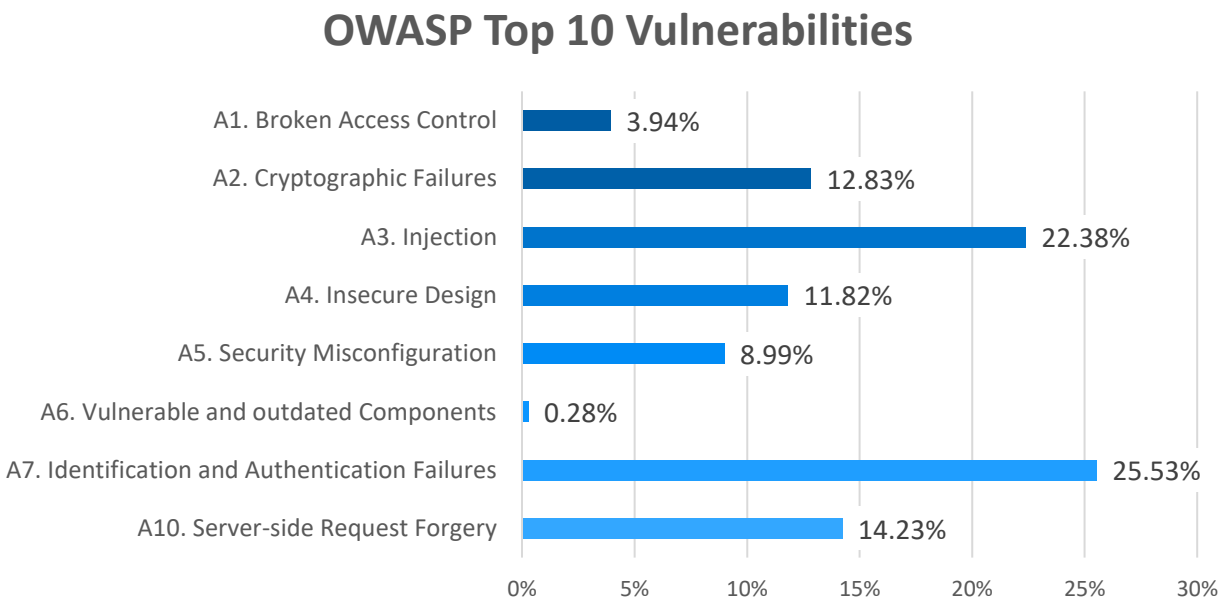
Cyberattacks against critical industries not only put consumer and business data at risk, but also have the potential to disrupt infrastructures that can be crucial to national security. Cybersecurity awareness and robust countermeasures must be in place to defend such threats.

1) Avertium (Apr 26, 2022) *"An In-Depth Look at Data Extortion Group, LAPSUS$"*.

III. Web Attack Trends During H1 2022

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 2022 as according to 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, 2022. **Identification and Authentication Failures** is the most frequently exploited vulnerability, followed by **Injection** and **Server-side Request Forgery**.

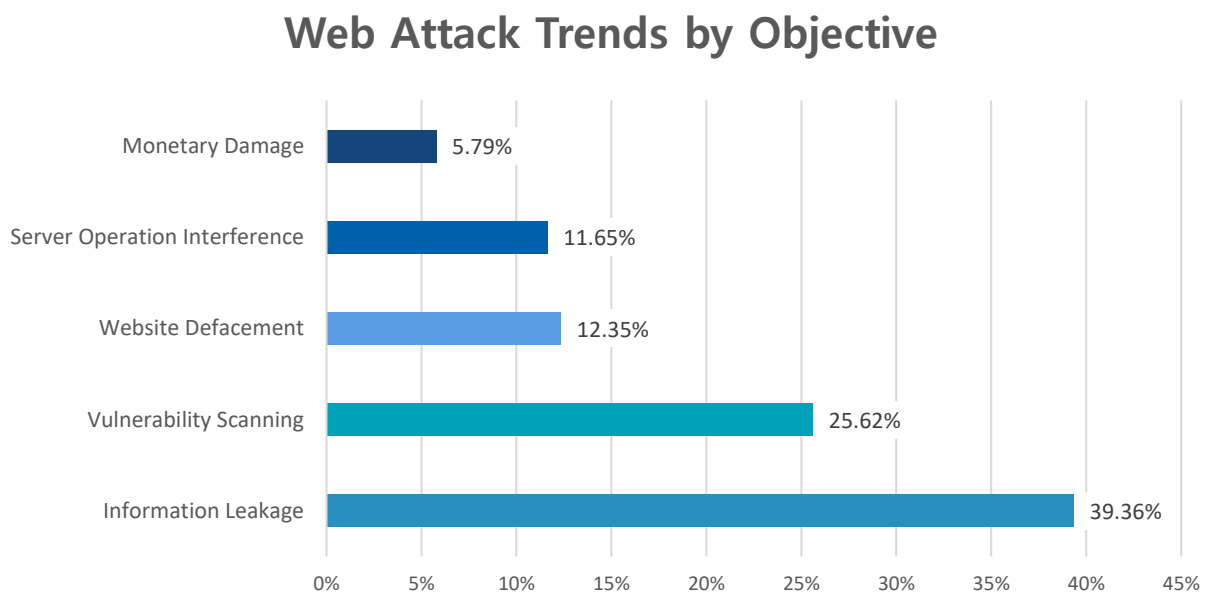
Identification and Authentication Failures (previously labeled as **Broken Authentication**) is a vulnerability that arises from the lack of multi-factor authentication (MFA) for user accounts. Threat actors target these accounts with brute force and social engineering techniques to break through authentication. To protect against these attacks, organizations should adopt a second authentication factor to control access to user accounts and servers.

OWASP Top 10 (2021) Vulnerabilities	Cases
A1. Broken Access Control	2,826,751
A2. Cryptographic Failures	9,214,349
A3. Injection	16,071,170
A4. Insecure Design	8,488,740
A5. Security Misconfiguration	6,460,364
A6. Vulnerable and outdated Components	204,162
A7. Identification and Authentication Failures	18,335,922
A10. Server-side Request Forgery	10,222,908

< OWASP Top 10 Web Attack Cases >

III. Web Attack Trends During H1 2022

5. Web attack trends by objective



The above graph categorizes detected web attacks during the first half of 2022 by the attackers' objectives. The top five objectives are **Information Leakage** (39.36%), **Vulnerability Scanning** (25.62%), **Website Defacement** (12.35%), **Server Operation Interference** (11.65%), and **Monetary Damage** (5.79%).

Nearly 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.

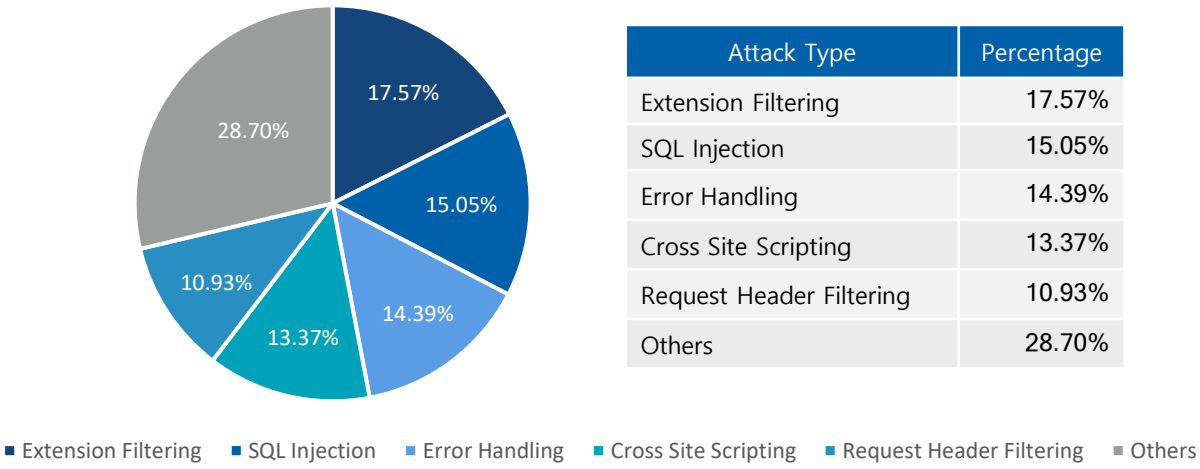
The second-most common attack objective is **Vulnerability Scanning**. This is when attackers attempt to explore potential vulnerabilities in their targeted application, usually done by using automated tools to send invalid HTTP requests or responses, to send invalid URLs that are different from the formats defined 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 H1 2022

6. Web attack trends of major attackers

Top Picks by Major Attackers



Attack Type	Percentage
Extension Filtering	17.57%
SQL Injection	15.05%
Error Handling	14.39%
Cross Site Scripting	13.37%
Request Header Filtering	10.93%
Others	28.70%

This analysis demonstrates the attack patterns of the top ten most active attackers between January 1 and June 30, 2022. Since these highly active attackers tend to be professional hackers 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 ten attackers are **Extension Filtering** (17.57%), **SQL Injection** (15.05%), **Error Handling** (14.39%), **Cross Site Scripting** (13.37%), and **Request Header Filtering** (10.93%).

As the most used attack method by major attackers, **Extension Filtering** is a type of attack where 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.

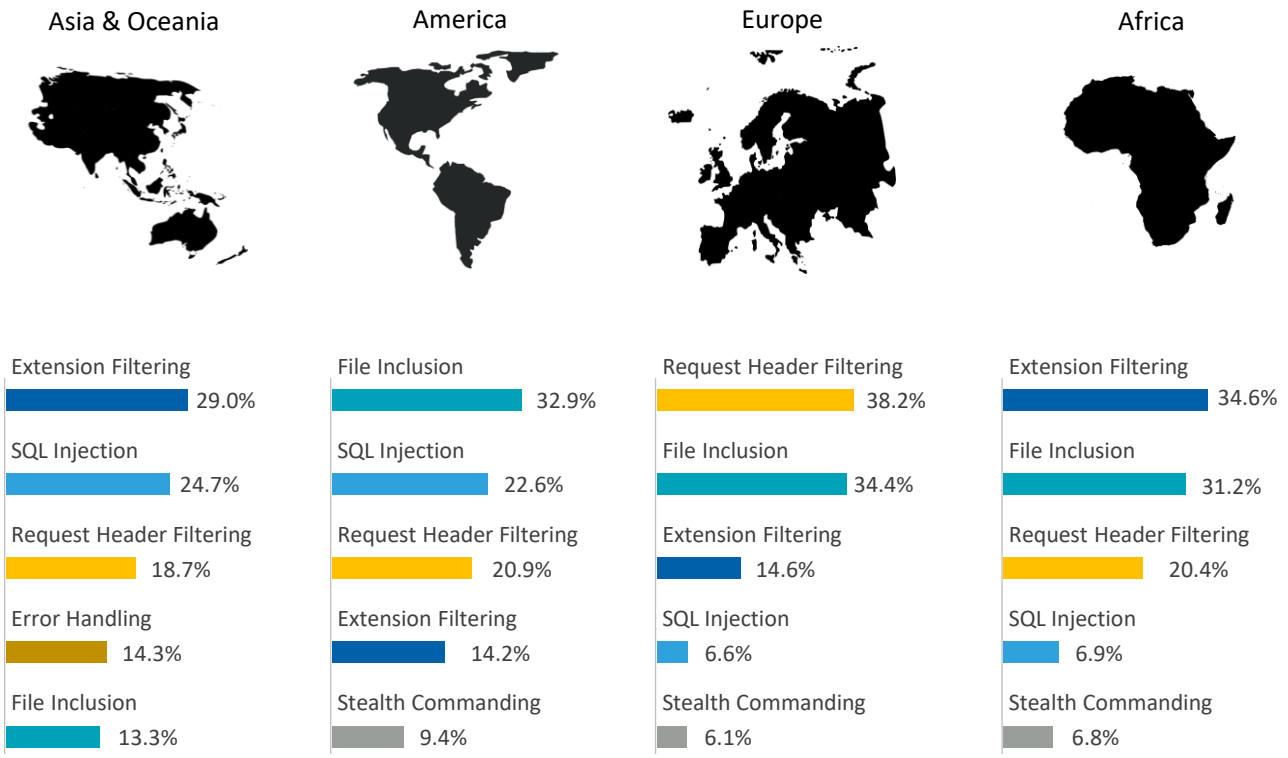
The second-most common attack method chosen by top attackers is **SQL Injection**. As mentioned earlier, this is when the attacker inserts invalid or unrelated SQL scripts to the SQL query to retrieve, modify, or delete data from the server. There are many known SQL Injection attack techniques, making 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 H1 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. Like the previous year, **Extension Filtering** remains the most detected attack type in Asia and Oceania and Africa. In the Americas, **File Inclusion** is most common, while **Request Header Filtering** tops the list in Europe.

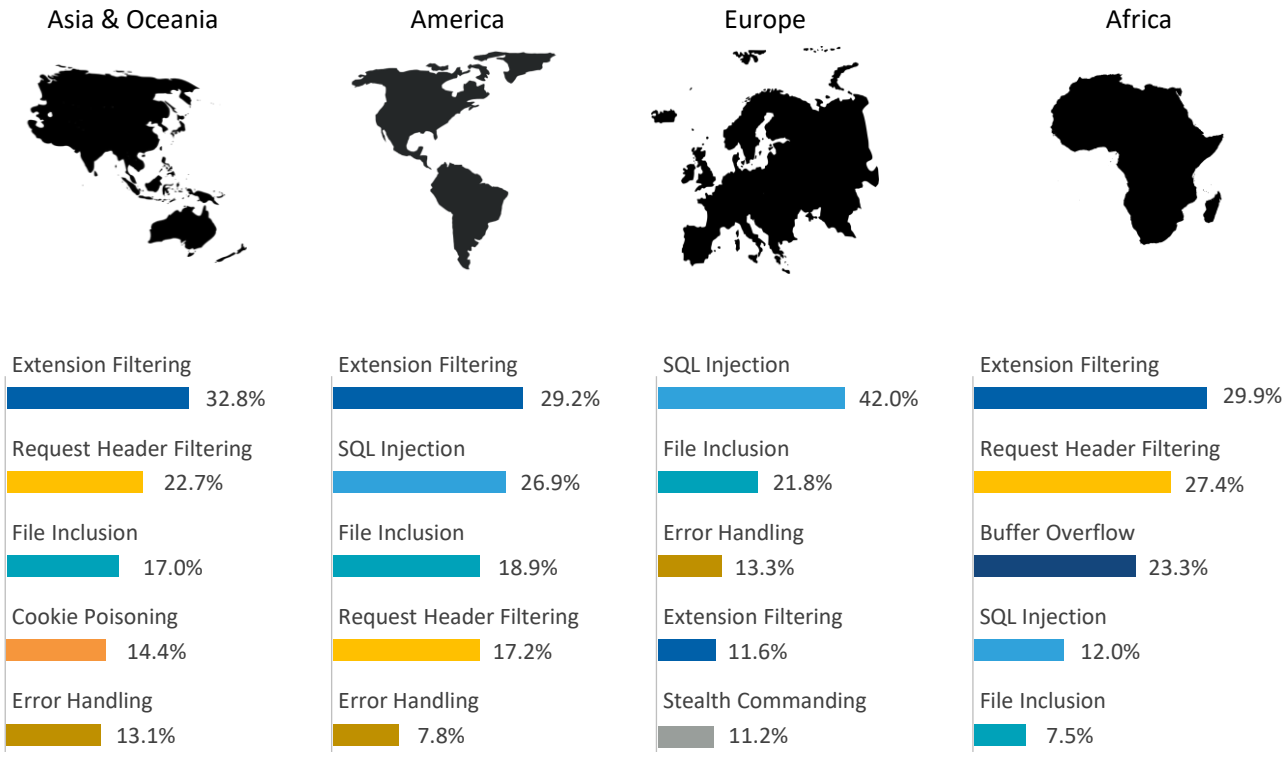
What is worth noting is that **SQL Injection**, which is ranked third on the OWASP Top 10 vulnerabilities list, is one of the top five most detected attack types on every continent of the world.

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

III. Web Attack Trends During H1 2022

7. Web attack trends by continent

Web Attack Trends by Continent of Origin



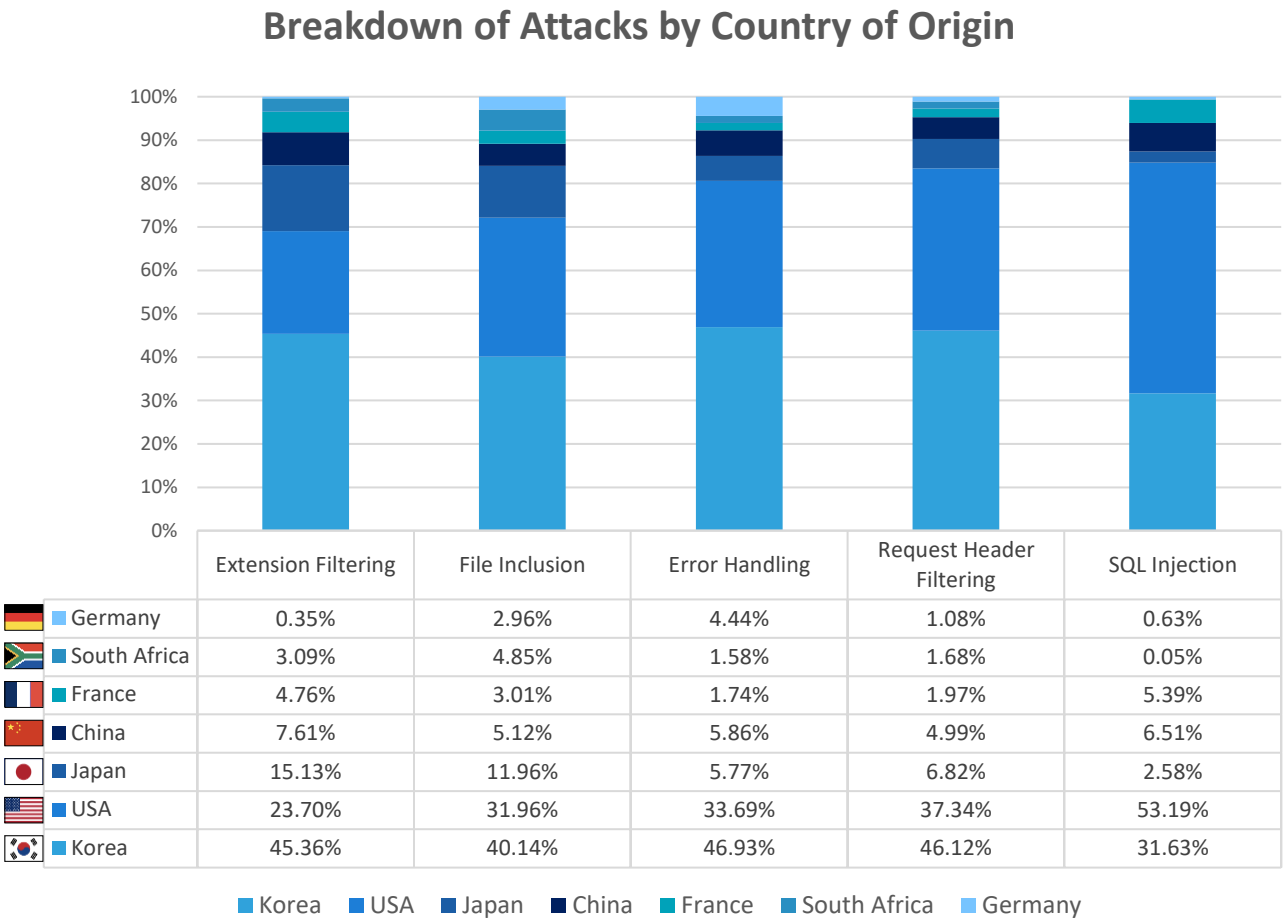
The above graph illustrates an analysis of attack origins based on their IP addresses. Among all attacks originating from Asia and Oceania, the Americas, and Africa, **Extension Filtering** was the most common type, while **SQL Injection** is by far the most used attack method by attackers in Europe.

Also worth noting is that **File Inclusion** made it to the top five list on all continents, meaning that the attack method is popular among all threat actors across the globe. As mentioned earlier, 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.

Additionally, although not commonly used by hackers in Asia and Oceania, **SQL Injection** remains one of the primary attack methods on all other continents.

III. Web Attack Trends During H1 2022

8. Web attack trends by country



	Extension Filtering	File Inclusion	Error Handling	Request Header Filtering	SQL Injection
Germany	0.35%	2.96%	4.44%	1.08%	0.63%
South Africa	3.09%	4.85%	1.58%	1.68%	0.05%
France	4.76%	3.01%	1.74%	1.97%	5.39%
China	7.61%	5.12%	5.86%	4.99%	6.51%
Japan	15.13%	11.96%	5.77%	6.82%	2.58%
USA	23.70%	31.96%	33.69%	37.34%	53.19%
Korea	45.36%	40.14%	46.93%	46.12%	31.63%

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, Russia no longer appears on the top seven countries list, with South Africa replacing it at the sixth spot.

By comparing the relative share of each attack type within each country, it can be observed that **SQL Injection** is particularly popular among attackers in the US and relatively less favored in Korea and Japan. Conversely, **Extension Filtering** is relatively less seen in the US but more commonly used by attackers in Japan and China.

III. Web Attack Trends During H1 2022

9. Current status of major web vulnerabilities

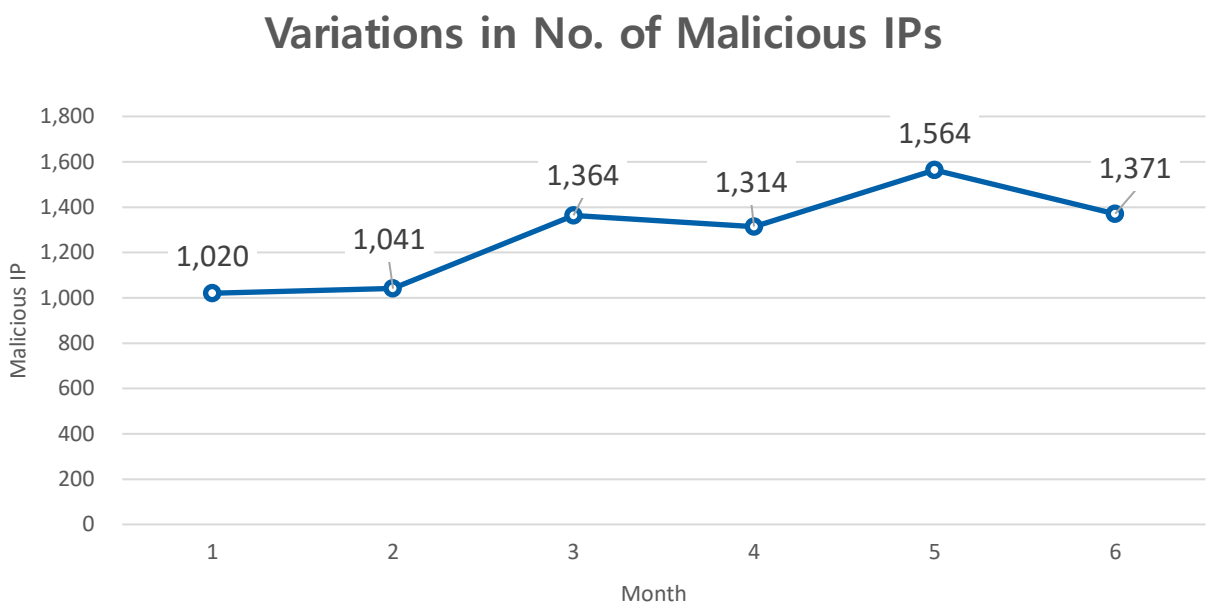
In March 2022, a severe vulnerability was discovered inside Spring Core of the Spring Java framework. Spring is an open-source application framework for the Java platform. Named Spring4Shell and tracked as CVE-2022-22965, the vulnerability gives attackers the ability to perform remote code execution (RCE).

Currently, all web servers running JDK 9 and above that use Spring Framework versions between 5.3.0 and 5.3.17, 5.2.0 and 5.2.19, or any previous version, are impacted by the vulnerability. By exploiting the vulnerability, attackers could execute code remotely on these vulnerable web servers.

Making sure that all applications are running their latest versions is of utmost importance. Besides the Spring Framework, security administrators should always ensure that the latest security patches are applied to all their hardware devices and software applications.

III. Web Attack Trends During H1 2022

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 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 1,564 in May, while averaging at 1,279 per month throughout the first half of 2022. In particular, after the disclosure of the Spring4Shell vulnerability, the number of detected malicious IPs increased by 250 from April to May. 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, 2022.

2. Key characteristics of report

The 2022 H1 WATT report included detection log data from both WAPPLES and Cloudbric WAF+. Additionally, Penta Security's proprietary 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 WAF+. 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

▪ File Inclusion

File Inclusion is when 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.

Potential Consequences: Modify web server information, trigger abnormal server behaviour, data breach

▪ 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 understand the vulnerabilities of the software and conduct follow-up attacks to cause greater damage.

Potential Consequences: Data breach, secondary attacks

▪ 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 WAF+ 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 WAF+ rules used to protect them.

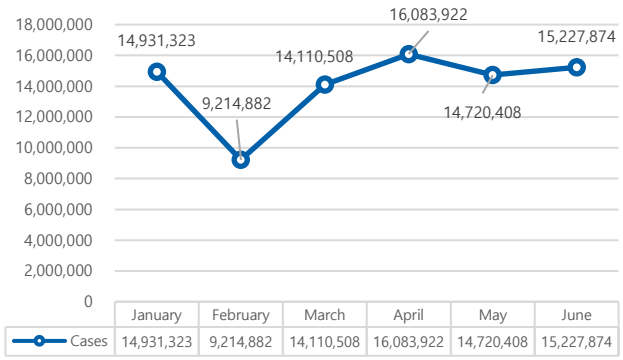
Top	OWASP Top 10	WAPPLES/Cloudbric WAF+ Rules
1	Broken Access Control	Parameter Tampering
		Invalid URL
		Directory Traversal
		Url Access Control
2	Cryptographic Failures	Privacy File Filtering
		Privacy Input Filtering
		Privacy Output Filtering
		Input Content Filtering
		Response Header Filtering
		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 Sync
10	Server-side Request Forgery	File Inclusion

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

IV. Appendix

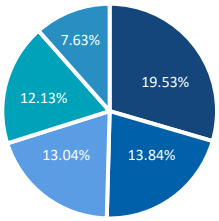
5. Summary charts

Monthly Variations of Web Attacks

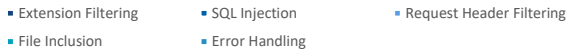


	January	February	March	April	May	June
Cases	14,931,323	9,214,882	14,110,508	16,083,922	14,720,408	15,227,874

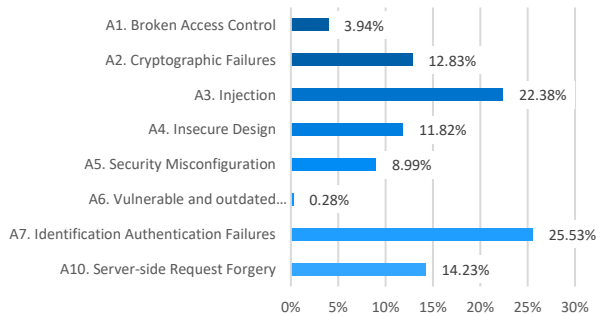
Web Attack Trends by Rule



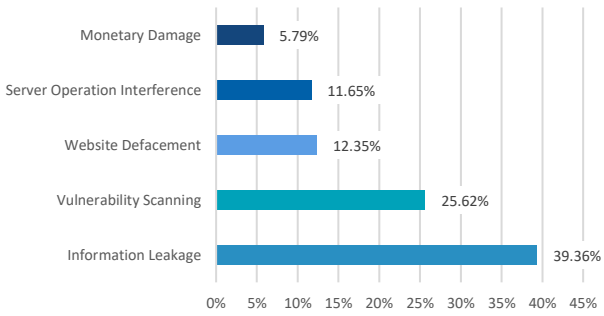
Attack Type	Percentage
Extension Filtering	19.53%
SQL Injection	13.84%
Request Header Filtering	13.04%
File Inclusion	12.13%
Error Handling	7.63%



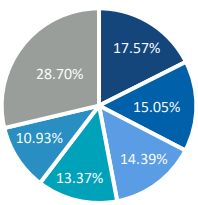
OWASP Top 10 Vulnerabilities



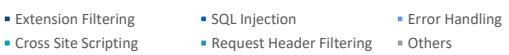
Web Attack Trends by Objective



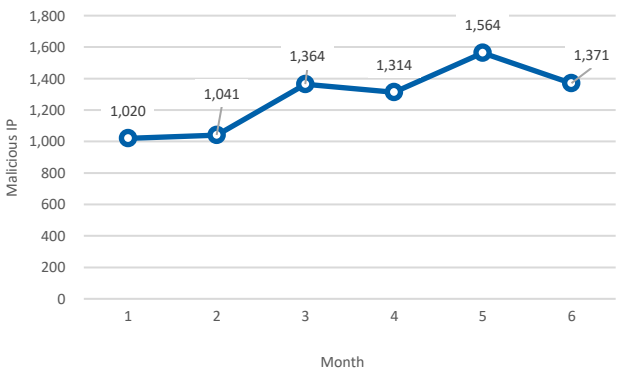
Top Picks by Major Attackers



Attack Type	Percentage
Extension Filtering	17.57%
SQL Injection	15.05%
Error Handling	14.39%
Cross Site Scripting	13.37%
Request Header Filtering	10.93%
Others	28.70%



Variations in No. of Malicious IPs



IV. Appendix

6. List of top 40 attackers

Rank	IP Address	Country
1	110.45.X.X	Korea
2	1.234.X.X	Korea
3	66.249.X.X	United States
4	171.22.X.X	Korea
5	136.243.X.X	United States
6	112.169.X.X	Unknown
7	54.71.X.X	United States
8	121.131.X.X	Korea
9	69.125.X.X	United States
10	59.26.X.X	Korea
11	45.134.X.X	Unknown
12	182.140.X.X	China
13	185.7.X.X	France
14	155.190.X.X	United States
15	155.190.X.X	United States
16	94.182.X.X	Iran
17	66.249.X.X	United States
18	221.148.X.X	Korea
19	175.125.X.X	Korea
20	185.244.X.X	Romania
21	218.55.X.X	Korea
22	203.248.X.X	Korea
23	211.226.X.X	Korea
24	185.202.X.X	Germany
25	40.78.X.X	United States
26	193.239.X.X	Unknown
27	5.226.X.X	United Kingdom
28	211.189.X.X	Korea
29	211.233.X.X	Korea
30	95.217.X.X	Ukraine
31	41.21.X.X	South Africa
32	20.213.X.X	United States
33	155.190.X.X	United States
34	35.200.X.X	United States
35	66.249.X.X	United States
36	147.46.X.X	Korea
37	175.212.X.X	Korea
38	147.46.X.X	Korea
39	94.232.X.X	Russia
40	111.75.X.X	China

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