cloudbric

Penta SECURITY

cloud · iot · blockchain

Web Application Threat Trend Report

Trends for the First Half of 2021

Cloudbric Pte. Ltd.

Penta Security Systems Inc.

cloudbric
Penta SECURITY

Contents

I. Overview

1. Objective of Report

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

The main purpose of this report is to identify web attack patterns through detailed analyses of the latest attack trends and reflect these patterns in WAPPLES/Cloudbric operations.

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

Throughout this report, readers will be presented with various statistical data on major web attacks based on the detection rules of WAPPLES/Cloudbric. These data include information on trending attack types, trending malicious IPs used by major attackers, regional trends on where major web attacks originate, and attack trends by industry and timeframe.

1) Industry Quotient, Frost & Sullivan, 2015.

II. Executive Summary

The attack data used for analysis is collected based on the top five rules deemed most important among all detection rules of WAPPLES and Cloudbric. The report conducts analysis of web attacks based on their objectives, OWASP Top 10 vulnerability types, IPs, targeted industries, countries of origin, and more.

In the first half of 2021, more than 50% of attacks were aimed at information leakage, where unauthorized individuals try to gain access to sensitive data by exploiting website vulnerabilities. Exploitations have been carried out by injecting malicious code into the SQL queries to enable the upload of .exe, .jsp, and .php files to the server, which then allows the attackers to retrieve sensitive data from the database.

Putting all attacks into OWASP Top 10 categories, Sensitive Data Exposure came out as the most common attack type, which involves the malicious use of sensitive personal and financial information. Security Misconfiguration came second, which is when attackers exploit exposed directory listings and detailed error messages. To prevent such attacks, security measures must be taken to prevent attackers from gaining access to OS default accounts and knowing the system architecture. Such measures include periodically patching operating systems and creating customized error messages.

The most common attack detected by WAPPLES and Cloudbric is Extension Filtering. This is a very dangerous attack type where attackers attempt to access configuration files (e.g., dll, conf, ini, etc.) that contain vulnerabilities. When unauthorized individuals access these files, they could tamper with the web server to directly affect the web service.

Below is a summary of web attacks collected by WAPPLES/Cloudbric from January 1 to June 30, 2021.

Rank	Attack Type	Percentage
No. 1	Extension Filtering	28.04%
No. 2	Error Handling	13.98%
No. 3	SQL Injection	11.88%

<Top 3 Detected Attacks>

Rank	Attack Objective	Percentage
No. 1	Information Leakage	50.76%
No. 2	Vulnerability Scanning	31.76%
No. 3	Server Interference	9.39%

<Top 3 Attack Objectives>

Rank	OWASP Top 3	No. Detected
No. 1	Sensitive Data Exposure	33,823,926
No. 2	Security Misconfiguration	21,301,890
No. 3	Injection	13,182,601

<Attack Type and No. from OWASP Top 10>

Rank	Attack Type	Percentage
No. 1	Error Handling	43.35%
No. 2	Invalid HTTP	16.56%
No. 3	Extension Filtering	13.85%

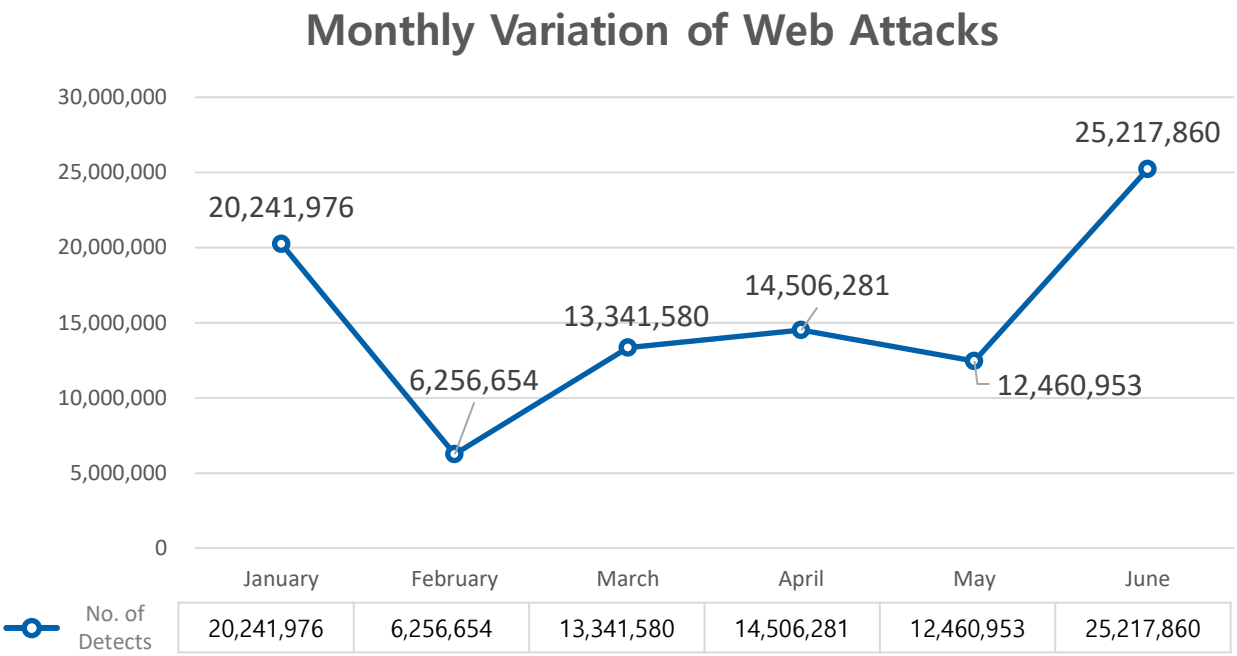
<Top 3 Picks by Major Attackers>

III. Web Attack Trends During the First Half of 2021

1. Monthly Variation

Monthly variation data provide a clear view of when web attacks are at their peak, helping to predict future attacks and prepare for countermeasures in advance.

The graph below shows an analysis of web attacks detected by WAPPLES and Cloudbric during the first half of 2021.



Based on the graph, the number of monthly attacks averaged at 15 million, with January and June exceeding 20 million.

A high number of enterprises faced security incidents in January 2021. This included major corporations in the cosmetics, automotive, and IT industries.

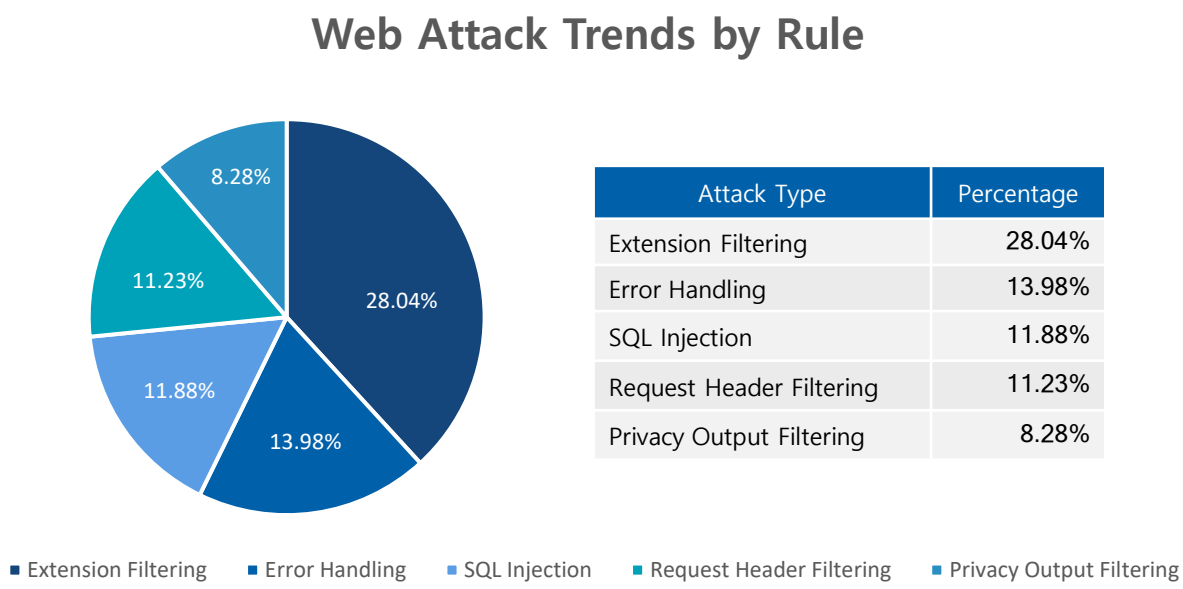
Despite a drop in the number of web attacks throughout February to May, the number of attacks in June surpassed January by 5 million. This sudden surge is due to an increase in the use of remote work and online learning services led by a new global wave of the COVID-19 pandemic. More attackers are expected target these services in the future, raising the importance of web security.

III. Web Attack Trends During the First Half of 2021

2. Web Attack Trend by Rule

The web attack trend by rule analysis shows which attacks occurred most frequently during the first half of 2021. Based on this information, response guidelines and security measures against web attacks can be established.

The graph below is an analysis of web attacks observed by WAPPLES and Cloudbric detection rules.



Attack Type	Percentage
Extension Filtering	28.04%
Error Handling	13.98%
SQL Injection	11.88%
Request Header Filtering	11.23%
Privacy Output Filtering	8.28%

Based on the number of detections, Extension Filtering (28.04%) is the most frequent attack type between January 1 and June 30, 2021. This is followed by Error Handling (13.98%), SQL Injection (11.88%), Request Header Filtering (11.23%), and Privacy Output Filtering (8.28%).

As one of the most frequent web attacks of all time, Extension Filtering refers to attempts to access configuration files (e.g., dll, conf, ini, etc.) rather than files in extension formats commonly used by websites. This is a critical attack because when unauthorized individuals access these configuration files, they could tamper with the web server and cause direct impact on the web service.

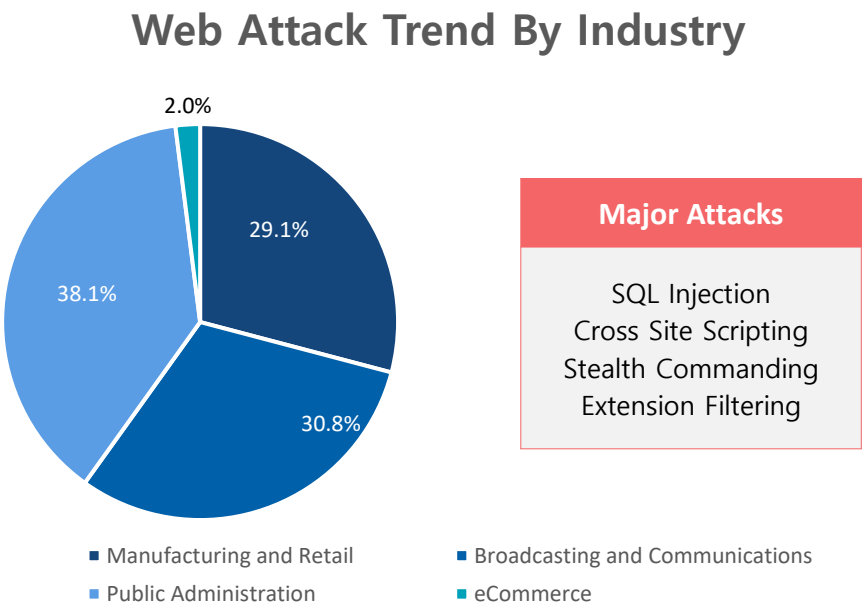
Error Handling is an attack method in which the attacker intentionally sends an invalid request to the web server or web application in order to trigger an error message, usually by entering repetitive strings, notes, or inserting wrong IDs. The attacker then either collects the error message for future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

SQL Injection has always appeared on the list. This is when the attacker insert invalid or unrelated SQL scripts to the SQL query to attack the database, making it the most common attack used for large-scale data compromise. A wide range of SQL Injection attack methods have been detected, signaling the importance of always having countermeasures.

Other attacks like Request Header Filtering and Privacy Output Filtering are also common attack methods that could cause severe damages. All organizations must have adequate security measures against them.

III. Web Attack Trends During the First Half of 2021

3. Web Attack Trend by Industry



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

According to the graph, manufacturing and retail, broadcasting and communications, public administration, and eCommerce are four major industries suffering high loads of web attacks. Public administration organizations and government agencies faced the most web attacks in this period, primarily due to the large amount of sensitive personal data they possess. Cybersecurity managers must pay special attention to protect personally identifiable information (PII).

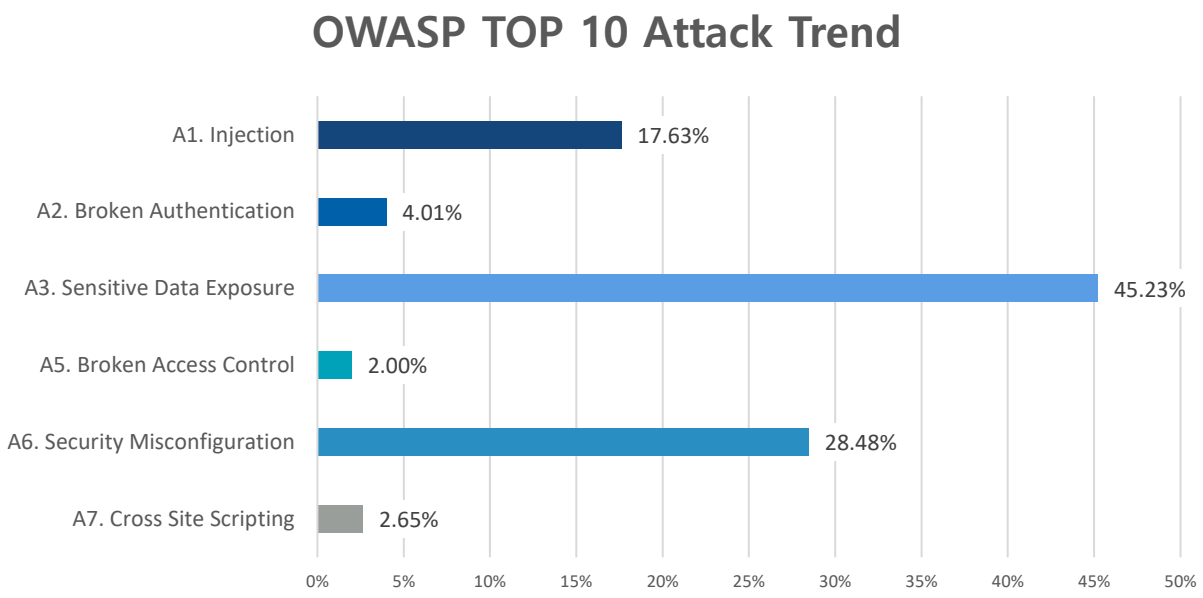
The second-most targeted industry is the broadcasting and communications industry. Due to an increase in web application usage caused by the COVID-19 pandemic, many hackers have been targeting the vulnerabilities of websites and browsers to steal sensitive data. As more and more sensitive user data get stored in remote work servers, cybersecurity managers must adopt multiple layers of security policies to prevent hackers from gaining access to these data.

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

III. Web Attack Trends During the First Half of 2021

4. OWASP Top 10 Attack Trend

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



The graph above depicts all web attacks detected by WAPPLES categorized into OWASP Top 10 web vulnerabilities. Between January 1 and June 30, 2021, Sensitive Data Exposure was the most frequently exploited vulnerability, followed by Security Misconfiguration.

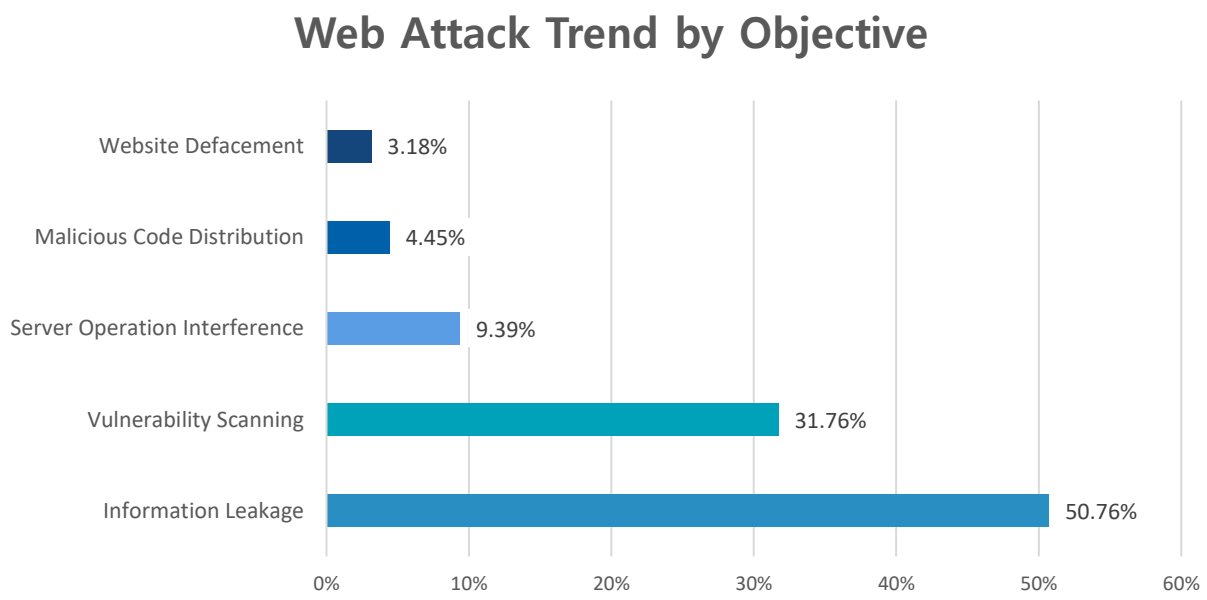
Sensitive Data Exposure only ranked fourth in the second half of 2020 but rose quickly to become the most prominent attack type. Deriving server information and system architecture through error messages or extracting directory listings from the servers can make it relatively easy to conduct such attacks. Hence, cybersecurity managers must ensure that preventative measures are in place to protect against the malicious extraction of error messages.

OWASP Top 10 Web Vulnerabilities 2017	No. Detected
A1. injection	13,182,601
A2. Broken Authentication	2,998,631
A3. Sensitive Data Exposure	33,823,926
A5. Broken Access Control	1,498,945
A6. Security Misconfiguration	21,301,890
A7. Cross Site Scripting	1,982,443

<Web Attacks Categorized into OWASP Top 10>

III. Web Attack Trends During the First Half of 2021

5. Web Attack Trend by Objective



The graph above is an analysis of web attack detection data for the first half of 2021, classified by their objectives. Among all web attacks originating from South Korea, Information Leakage (50.76%) was the most common objective, followed by Vulnerability Scanning (31.76%), Server Operation Interference (9.39%), Malicious Code Distribution (4.45%), and Website Defacement (3.18%).

More than 50% of web attacks had the objective of Information Leakage (50.76%). 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.

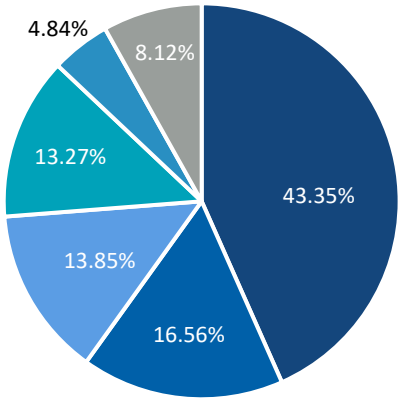
The second-most common attack objective is Vulnerability Scanning (31.76%). This involves the use of automated tools to send invalid HTTP requests or responses, to send invalid URLs that are different from formats defined by RFC, to gain access to directory listings, or to use error handling to find 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.

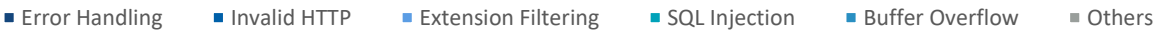
III. Web Attack Trends During the First Half of 2021

6. Major Attacker Trend

Top Picks by Major Attackers



Attack Type	Percentage
Error Handling	43.35%
Invalid HTTP	16.56%
Extension Filtering	13.85%
SQL Injection	13.27%
Buffer Overflow	4.84%
Others	8.12%



This analysis was done by first selecting the top 10 major attackers based on the number of web attacks each initiated in the first half of 2021, then looking at the most common attack methods these 10 attackers used. The reason to perform such an analysis is because these top attackers tend to be the ones that cause the most damage. Hence it is worth the time to study the attack patterns of these attackers separately.

Based on this analysis method, the most common attack initiated by the top 10 major attackers were, in descending order, Error Handling (43.35%), Invalid HTTP (16.56%), Extension Filtering (13.85%), SQL Injection (13.27%), and Buffer Overflow (4.84%).

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 inserting wrong 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.

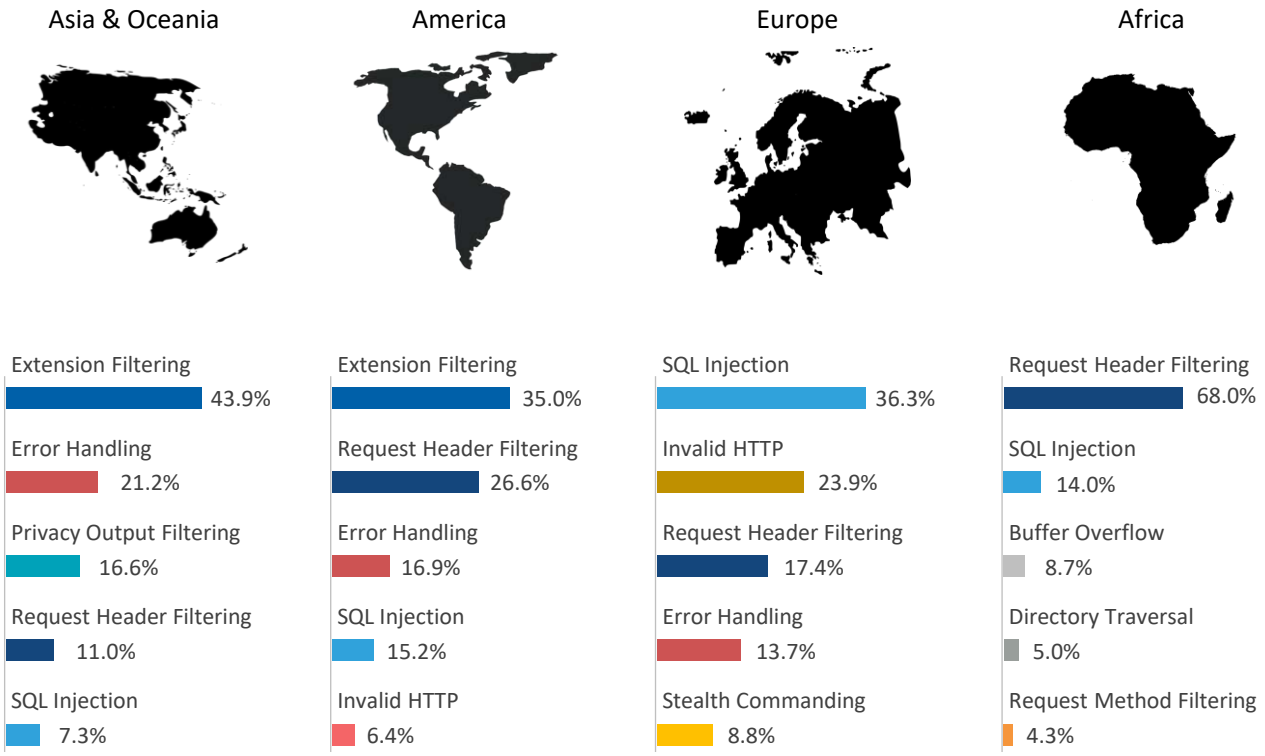
The second-most common attack method, Invalid HTTP, is when the attacker sends requests or responses for non-existent websites using invalid HTTP formats as an attempt to trigger abnormal traffic. This is usually conducted by attack tools such as worms. Such invalid HTTP traffic is not shown in regular web browsers, thus is good at hiding behind normal traffic.

One commonality among all these five attack methods is that they all seek to exploit vulnerabilities to gain access to personal and corporate data. Therefore, it is strongly recommended to not just having security measures to prevent them, but to prepare an emergency response guideline in case a data breach happens.

III. Web Attack Trends During the First Half of 2021

7. Web Attack Trend by Continent

Web Attack Trend by Continent of Arrival



The graph above analyzes all detected attacks classified by their continent of arrival. Like the previous period, Extension Filtering was the most detected attack in both Asia and America. SQL Injection was most common in Europe, whereas Request Header Filtering was most common in Africa.

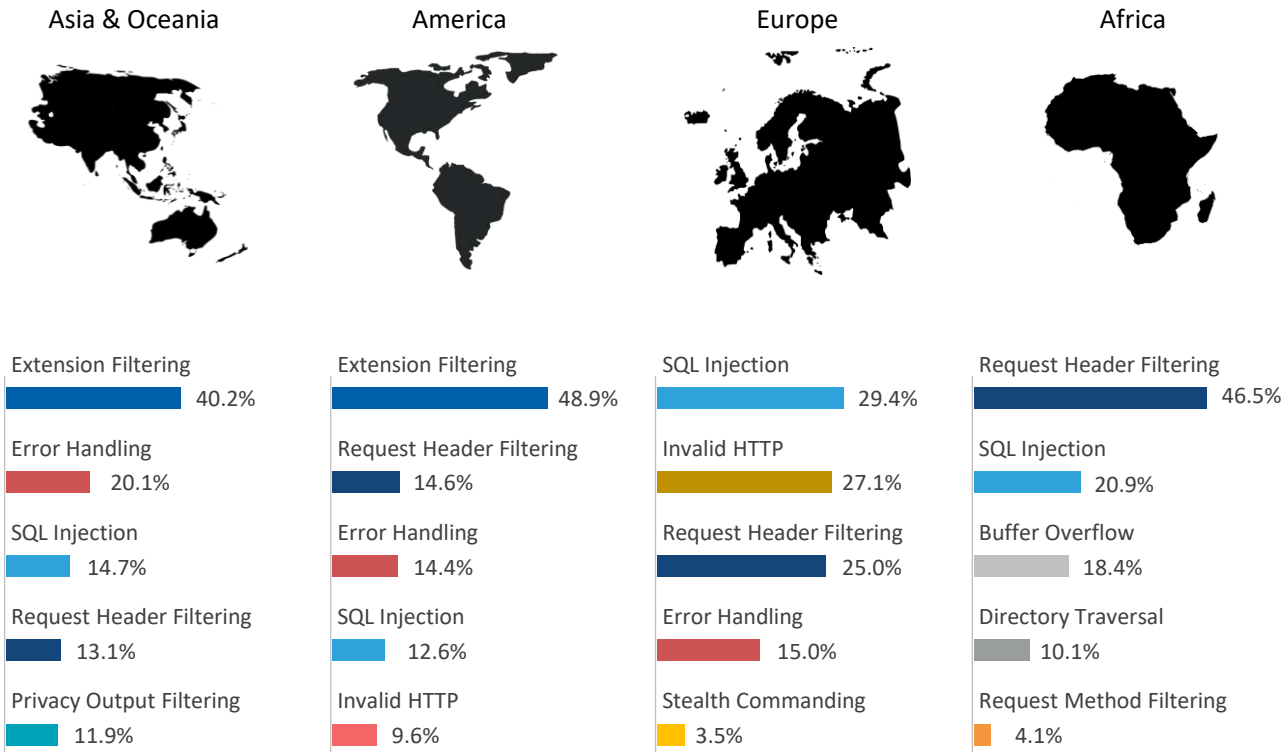
Note that SQL Injection made the list for all four continent. Being ranked first on the OWASP Top 10 web vulnerabilities list, Injection attacks were proven to be widespread all across the globe.

Also note that both Asia and America suffered a significant amount of Extension Filtering attempts. Especially in Asia, the percentage of Extension Filtering reached nearly 44%. Organizations in Asia must stay on high alert against Extension Filtering attacks.

III. Web Attack Trends During the First Half of 2021

7. Web Attack Trend by Continent

Web Attack Trend by Continent of Origin



The graph above analyzes the originating continent of all web attacks based on their IP addresses. Extension Filtering was the most common attack originating from both Asia and America. SQL Injection most originated in Europe, whereas Request Header Filtering was most common in Africa.

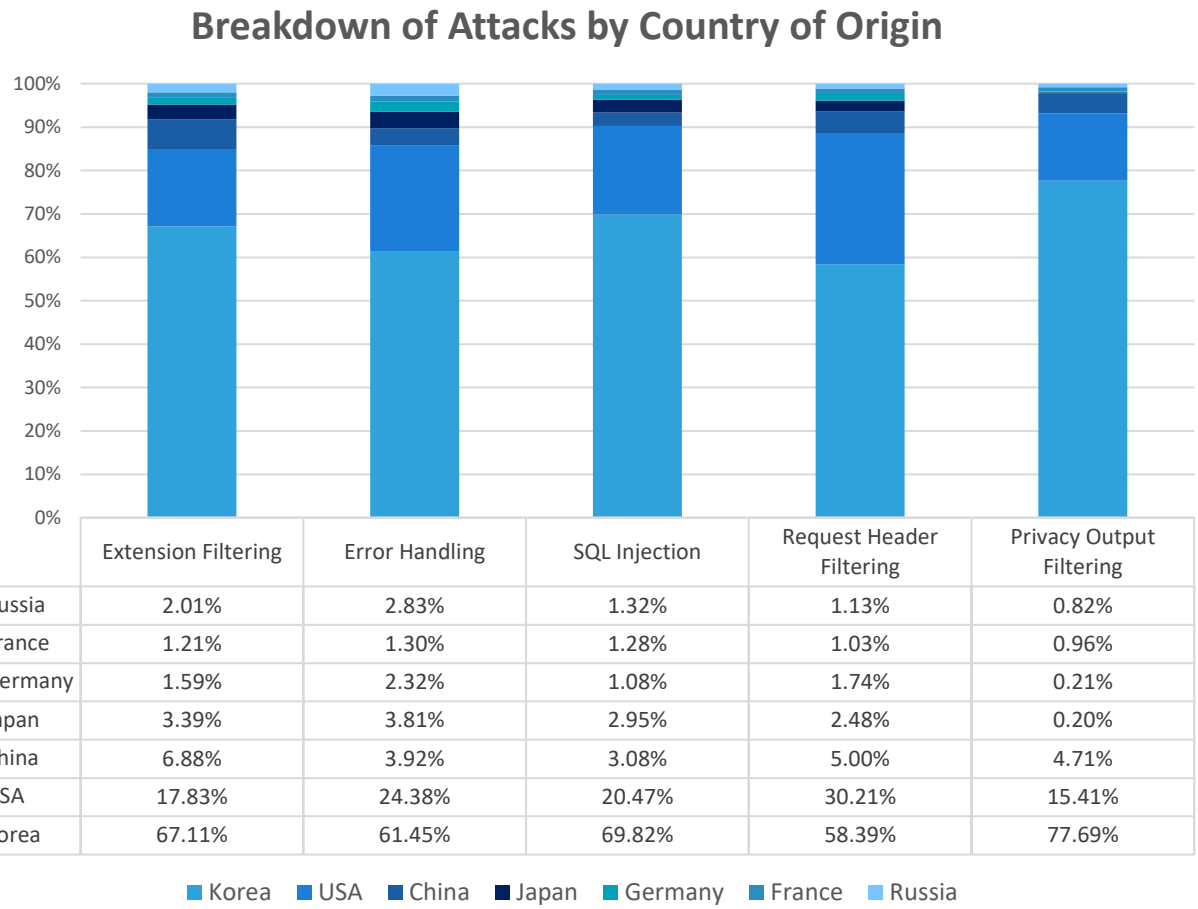
Note that both SQL Injection and Request Header Filtering made the top 5 list on all continents. All cybersecurity managers around the world must pay special attention to such attacks.

Request Header Filtering was especially common in Africa, with 46.5% of all web attacks originating from Africa being Request Header Filtering. This is an attack that exploits HTTP requests sent to web browsers. Different from a regular HTTP request, the attacker corrupts the header of the request by removing necessary elements or injecting malicious code to achieve their goal. Even though Request Header Filtering might only cause limited damage to the server, it can be leveraged for follow-up attacks.

Other attacks like Error Handling are also highly disruptive, all of which should be taken account for by cybersecurity managers.

III. Web Attack Trends During the First Half of 2021

8. Web Attack Trend by Country



	Extension Filtering	Error Handling	SQL Injection	Request Header Filtering	Privacy Output Filtering
Russia	2.01%	2.83%	1.32%	1.13%	0.82%
France	1.21%	1.30%	1.28%	1.03%	0.96%
Germany	1.59%	2.32%	1.08%	1.74%	0.21%
Japan	3.39%	3.81%	2.95%	2.48%	0.20%
China	6.88%	3.92%	3.08%	5.00%	4.71%
USA	17.83%	24.38%	20.47%	30.21%	15.41%
Korea	67.11%	61.45%	69.82%	58.39%	77.69%

The graph above illustrates the top seven countries where the highest proportions of web attacks originated from. The analysis helps depict a clear view of which attacks come from which countries, allowing cybersecurity managers to prepare based on their locations.

Compared to the previous report, France surpassed Germany to take the second spot. Korea, USA, China, and Japan all remained on the top 7 list. Despite small changes, all countries on the list remained to be top web attack origins.

According to the graph, intensive Extension Filtering and Error Handling attacks originated from all these major countries. Economic powerhouses like the USA, Korea, and China remained as popular web attack origins. Hence web attack prevention measures should be dedicated to attacks originating from these countries..

In addition, Error Handling was the most common web attack during the first half of 2021, cybersecurity managers should dedicate special effort towards preventing Error Handling.

III. Web Attack Trends During the First Half of 2021

9. Current Status of Major Web Vulnerabilities

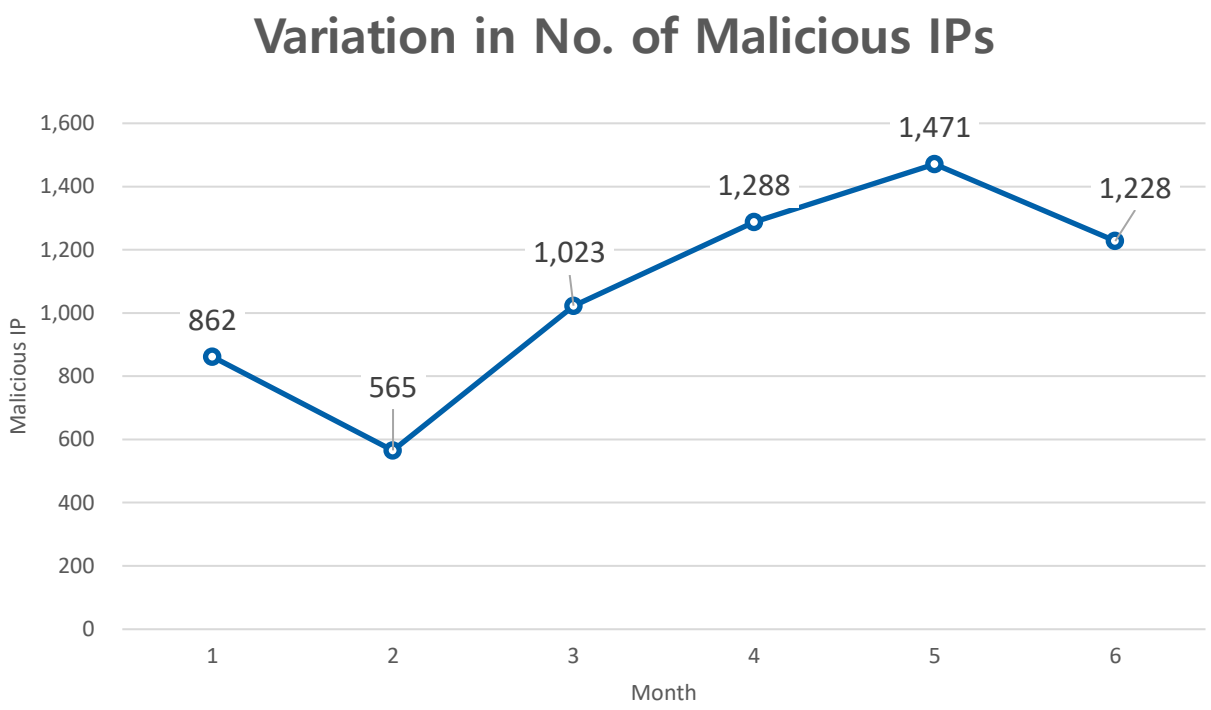
Some of the major web vulnerabilities in the first half of 2021 include CVE-2021-3449 and CVE-2021-3450. One of them is a denial-of-service vulnerability caused by dereferencing a NULL pointer when handling extended fields of a manipulated signature algorithm in a TLS server. Another is a 'security function bypass' vulnerability that allows the attacker to bypass the certificate validation process.

The vulnerabilities do not affect Open SSL versions 1.0.2 and 1.1.1k and above. All web services using Open SSL versions 1.1.1k and below are advised to upgrade to newer versions to prevent attacks that exploit these vulnerabilities.

Having the latest security patches is always helpful for all organizations. It is crucial to frequently check for security updates and keep track of the versions of all web browsers and software programs. One of the easiest ways to prevent web attacks is to stay on top of all updates.

III. Web Attack Trends During the First Half of 2021

10. Variation in No. of Malicious IPs



The graph above shows the fluctuations in the number of detected malicious IPs. The analysis helps predict the frequency of web attacks. Nevertheless, a lower number of malicious IPs does not necessarily mean a lower number of attacks. A single attacker can use many IP addresses to conduct attacks, while a single IP address can cause tremendous damage.

To classify an IP address as malicious, it must be detected at over 10 destinations and 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 IPs varied between 1,471 in May and 565 in February, with an average of 1,073 over the first half of 2021. Due to the third and fourth waves of the COVID-19 pandemic in many countries, a near-doubling surge in the number of malicious IP addresses was discovered in March. Therefore, organizations must always stay prepared for such significant surges in attacks and have emergency manuals to guide them through an attack.

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 January 1 and June 30, 2021.

2. Key Characteristics of Report

The 2021 H1 WATT Report included data from Cloudbric, a cloud-based web application firewall distributed around the world. Additionally, Penta Security's newly developed machine learning technology allowed for more accurate prediction of future attacks.

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

3. Glossary

▪ SQL Injection

SQL Injection is the injection of SQL scripts into the queries of the web application in order to deliver malicious command to the database server.

Potential Consequences: Unauthorized data access, manipulation, and defacement, authorization bypass, information leakage

▪ Stealth Commanding

Stealth Commanding is when the attacker inject malicious command as part of the data packet. When the web application sends to packet to outside programs, the malicious command gets executed.

Potential Consequences: Injection of Trojan virus, execution of malicious code, data compromise

▪ 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

1. OWASP & WAPPLES/Cloudbric Rules

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

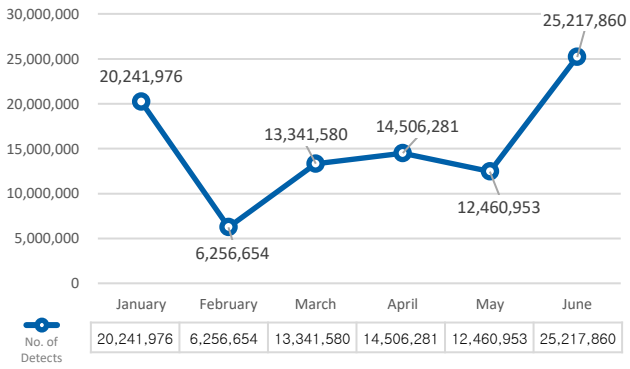
TOP	OWASP TOP 10	WAPPLES/Cloudbric Rules
1	injection	SQL Injection
		Stealth Commanding
		Cross Site Scripting
2	Broken Authentication	Cookie Poisoning
		Directory Traversal
		Cross Site Request Forgery
		SQL Injection
3	Sensitive Data Exposure	Privacy File Filtering
		Privacy Input Filtering
		Privacy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

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

IV. Appendix

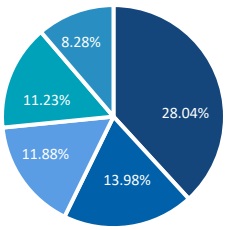
2. Summary Charts

Monthly Variation of Web Attacks



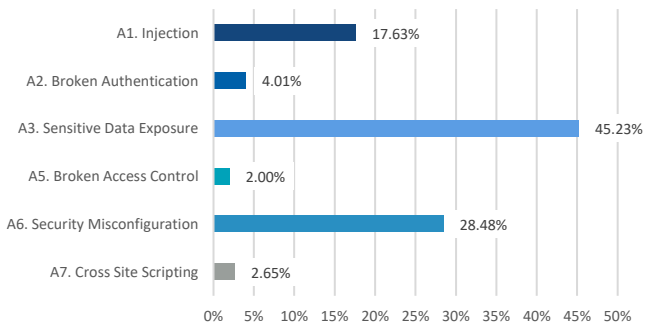
	January	February	March	April	May	June
No. of Detects	20,241,976	6,256,654	13,341,580	14,506,281	12,460,953	25,217,860

Web Attack Trends by Rule

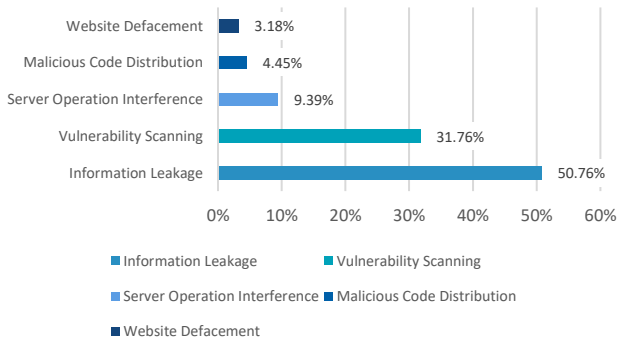


Attack Type	Percentage
Extension Filtering	28.04%
Error Handling	13.98%
SQL Injection	11.88%
Request Header Filtering	11.23%
Privacy Output Filtering	8.28%

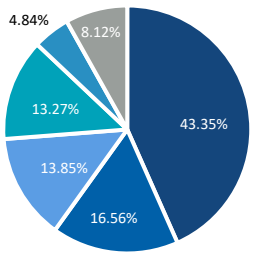
OWASP TOP 10 Attack Trend



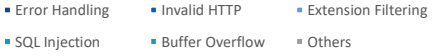
Web Attack Trend by Objective



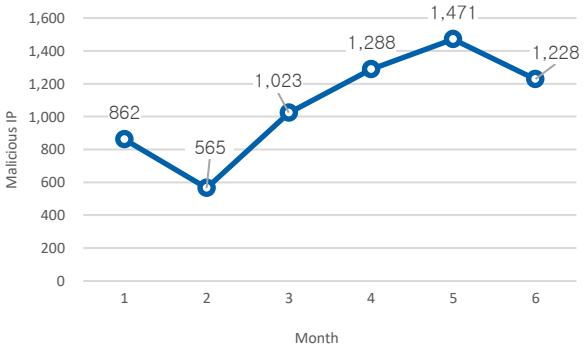
Top Picks by Major Attackers



Attack Type	Percentage
Error Handling	43.35%
Invalid HTTP	16.56%
Extension Filtering	13.85%
SQL Injection	13.27%
Buffer Overflow	4.84%
Others	8.12%



Variation in No. of Malicious IPs



IV. Appendix

6. List of Top 40 Attackers

Rank	Attacker IP	Country
1	5.188.X.X	Russia
2	193.42.X.X	Italy
3	199.195.X.X	United States
4	172.105.X.X	United States
5	39.101.X.X	China
6	172.104.X.X	United States
7	39.104.X.X	China
8	60.191.X.X	China
9	193.174.X.X	Germany
10	80.82.X.X	Netherlands
11	39.103.X.X	China
12	39.101.X.X	China
13	137.135.X.X	United States
14	121.42.X.X	China
15	80.82.X.X	Seychelles
16	129.146.X.X	United States
17	47.113.X.X	China
18	91.199.X.X	United Kingdom
19	112.124.X.X	China
20	80.82.X.X	Netherlands
21	89.40.X.X	Romania
22	5.188.X.X	Russia
23	61.160.X.X	China
24	167.248.X.X	United States
25	60.191.X.X	China
26	185.202.X.X	France
27	39.99.X.X	China
28	134.19.X.X	Azerbaijan
29	129.146.X.X	United States
30	223.105.X.X	China
31	94.102.X.X	Netherlands
32	192.35.X.X	United States
33	123.56.X.X	China
34	71.6.199.X.X	United States
35	167.248.X.X	United States
36	93.174.X.X	Netherlands
37	190.128.X.X	Paraguay
38	5.188.X.X	Russia
39	66.240.X.X	United States
40	167.248.X.X	United States

cloudbric

GROBAL www.cloudbric.com

JAPAN www.cloudbric.jp

Penta SECURITY
cloud · iot · blockchain

KOREA www.pentasecurity.co.kr

GLOBAL www.pentasecurity.com

JAPAN www.pentasecurity.co.jp

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