

SECURITY GUARD

Defend Your **Business** Against
the Latest Cyber Threats

»





Product overview

- [Quick Start Guide](#)
- [Getting Started Guide](#)

Planning

- [Architecture and Deployment Guide](#)

Installing

- [Installation Guide](#)

Configuring & Monitoring

- [Honeypot Node Configuration Guide](#)
- [Attack Surface Monitor Configuration Guide](#)
- [Breach Data Control Configuration Guide](#)
- [Check WAF Configuration Guide](#)
- [Stress Tester](#)
- [IOC's Data Usage Guide](#)

Administration

- [User & Report Guide](#)
- [3rd Party Integration Settings](#)

Tickets



Effective Approach for Your Cyber Security with **Caspipot** Security Guard

Quick Start Guide Version 2.0

Caspipot Security Guard is an all in one SaaS security solution where you can create your honeypot services within minutes, track the attackers and gather information with attack surface monitoring & breach data control.

This guide gets you started with a typical installation and configuration. To obtain the Quick Start Guide in other languages, print the language-specific PDF from the installation media.

© Copyright CaspiPoT 2023.



Getting Started Guide

CaspiPoT Security Guard Getting Started Guide introduces you to key concepts, an overview of the installation process, and basic tasks that you perform in the user interface.

Intended audience

This information is intended for use by security administrators who are responsible for investigating and managing network security. To use this guide you must have a knowledge of your corporate network infrastructure and networking technologies.

Technical documentation for information about how to access more technical documentation, technical notes, and release notes, see CaspiPoT Security Guard Security Documentation Technical Note (<https://www.caspipot.com/support/1905>).

Contacting customer support for information about contacting customer support, see the Support and Download Technical Note (<http://caspipot.com/support/>).

Statement of good security practices IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. CaspiPoT Security Guard systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. CaspiPoT DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note: Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. CaspiPoT Security Guard may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of CaspiPoT.



Architecture and Deployment Guide

When you plan or create your CaspiPoT Security Guard deployment, it's helpful to have a good awareness of CaspiPoT architecture to assess how CaspiPoT Security Guard components might function in your network, and then to plan and create your CaspiPoT deployment. CaspiPoT processes, aggregates, and stores attack-data in real time. CaspiPoT Security Guard providing real-time information and monitoring, alerts and offenses, and responses to threats. CaspiPoT Security Guard is a modular architecture that provides real-time visibility, which you can use for threat detection and prioritization. You can scale CaspiPoT to meet your collection and WAF response. Attack Surface Monitoring systems helps to find critical issues in assets.

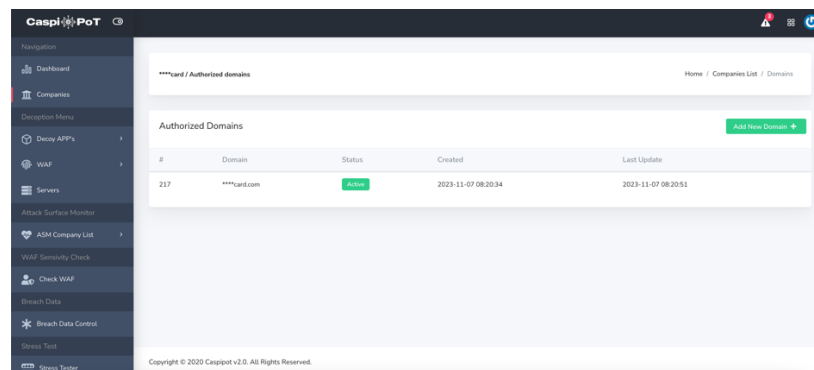
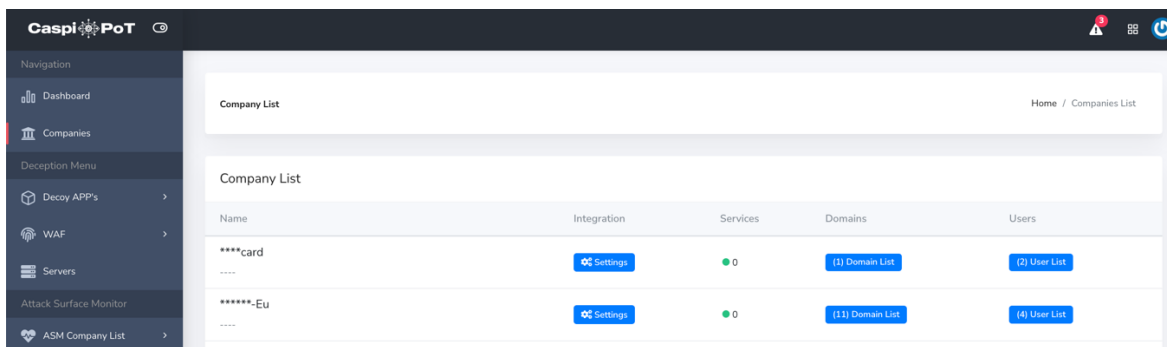
CASPIPOT COMPONENTS

CLOUD HONEYPOT	BREACH DATA CONTROL	ATTACK SURFACE MONITOR
Services Rules Waf		Vulnerability Scanner Asset Status Control Blacklist Control
Check WAF	IOC's Bad IP Pool Proxy Pool Payload Pool	Stress Tester



ALL-in-ONE DEPLOYMENT

Although the product consists of multiple modular structures, it is very easy and simple to install. First of all, in order to activate your services, you must register your domain name. You can access panel with <https://manager.caspipot.com>



After the approved registration of your **domain name** is completed, the domain name is automatically added to **Authorized Domains** list.



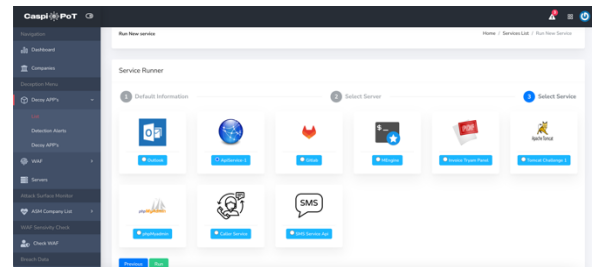
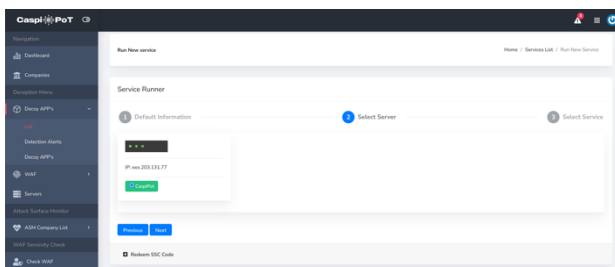
CONFIGURING

Honeypot Node Configuration Guide

To activate honeypot services via the **CaspiPot Manager Panel || Deception >> List >>> Create** field should be reached.

In order to define services, it is necessary to complete the **service name**, **domain name** and **port information** of your service completely.

With the defined information, the area where you can choose from among the servers defined in different datacenters around the world will be displayed to within the scope of the license type.



These are the things that need to be done in order to take a **service live**.



After the configurations related to the services, the manager panel shows all active and passive services. You can be viewed by following the steps of **CaspiPot Manager Panel || Deception >> Decoy APP's >>> List**

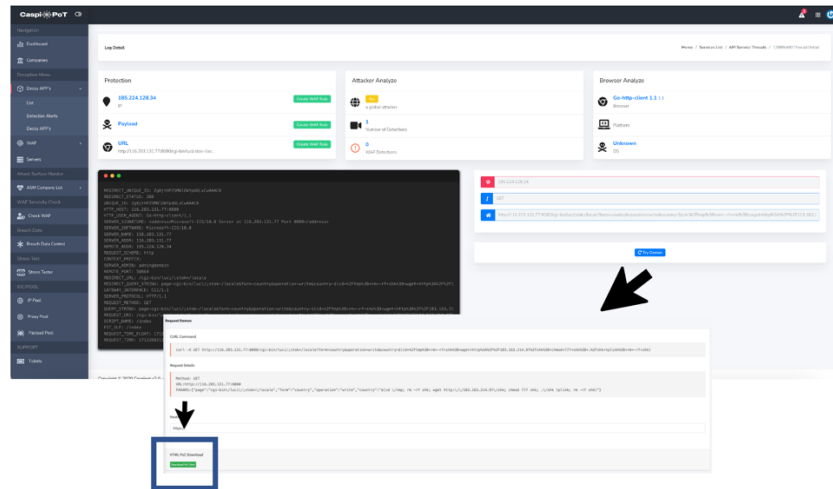
Service	Status	Domain	Server	WAF	Version/UPT	Logs	Actions
API Service ApiService-1	Active	api.caspipt.com	116.203.131.77 8080	CloudFlare	v.1	Logs	[Edit] [Delete]
phpmyadmin Demo phpMyadmin	Active Outdated	phpadmin.caspipt.com	116.203.131.77 8990	Disabled	v.1	Logs	[Edit] [Delete]
tryam Tester Invoice Tryam Panel	Active Outdated	tryam.caspipt.com	116.203.131.77 6375	Fortinet	v.4	Logs	[Edit] [Delete]

Logs field should be accessed to list the attacks on your services and write new rules

You can define your detailed **rules** for **IP, PAYLOAD AND URL.**

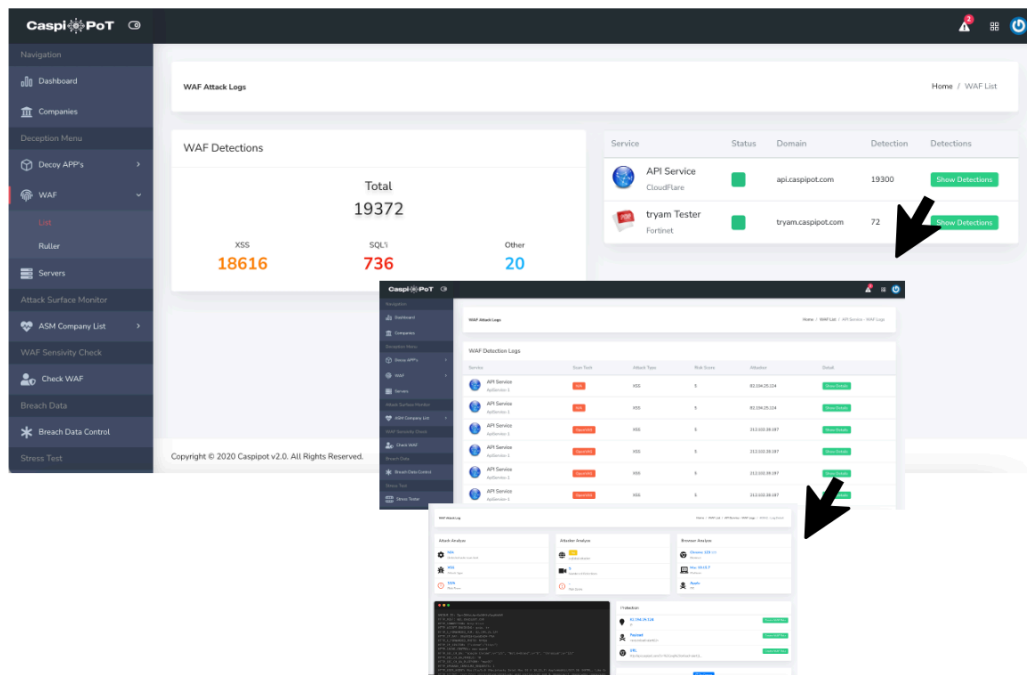


With the **TRY DEMON** button you can *simulate* an attack on your applications and with the **Download PoC** option you can test the same attack vector on your own computer..



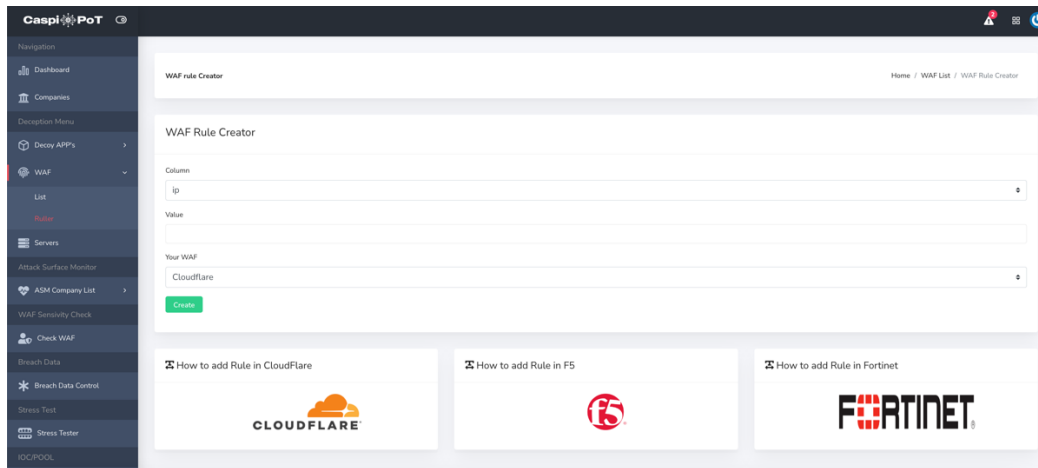
Honeypot WAF services via the **Caspiot Manager Panel || Deception >> WAF >>> List** field should be reached.

To see the statistics of the attacks and to write new rules for incoming attacks, just click on the P field.

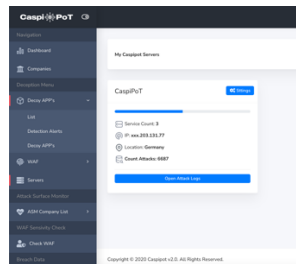




To write **new rules** for incoming attacks to HoneyPot WAF Ruller services via the **CaspiPot Manager Panel || Deception >> WAF >>> Ruller** field should be reached.



To Access your licensed servers, **CaspiPot Manager Panel || Deception >> Decoy APP's >>> Servers**



With the operations performed, attacks on services that are now defined begin to be detected. **Important rules** can be written for the listed attack types and critical situations. You can receive **hourly, daily, monthly** reports on detected attacks and automatically forward them to the relevant teams.

Attack Type	IP	Username	Password	Port	Time
SSH	69.171.78.20	root	123456	22	2023-03-30 01:20:03
SSH	14.224.169.32	admin	admin	22	2023-03-30 00:59:03
SSH	14.224.169.32	www	P@ssw0rd!	22	2023-03-30 00:55:03
SSH	38.156.73.8	root	0100123	22	2023-03-30 00:09:04
SSH	14.224.169.32	root	root	22	2023-03-29 23:58:04
SSH	14.224.169.32	admin	123456	22	2023-03-29 23:49:03
SSH	14.224.169.32	root	123456	22	2023-03-29 23:36:03
SSH	205.185.113.129	root	123456	22	2023-03-29 23:27:05



Attack Surface Monitor Configuration Guide

To activate attack surface management services via **Caspipot Manager Panel** || **Attack Surface Monitor** field should be reached.

In order to define services, it is necessary to complete at the “Total Assets” **domain name** and **IP address** service completely. CaspiPoT security guard will automatically scan and add subdomains to the system.

The screenshot shows the CaspiPoT Attack Surface Monitor dashboard. The top navigation bar includes 'Home / Attack Surface Monitor / Caspisec'. The main content area is divided into several sections:

- Total Asset:** 0 from, 13 Total, 13. Includes an 'Open List' button.
- Active Monitor:** 2. Includes an 'Open List' button.
- Black List Monitors:** 2 / 0. Includes an 'Open List' button.
- Product Inventory:** 6 / 3. Includes an 'Open List' button.
- Last Detected Ports:** A list of ports including ioc.caspipot.com:443, ioc.caspipot.com:8080, ioc.caspipot.com:80, caspisec.com:443, caspisec.com:8080, caspisec.com:80, caspipot.com:443, caspipot.com:8080, caspipot.com:80, and www.caspisec.com:443.
- Vulnerability Statistic:** A circular gauge showing 8 vulnerabilities. Below the gauge are counts for Low (5), Medium (3), and High (0).
- SSL Certificate Status:** 13 Active, 13 Less than 30 days. Includes a 'Show Certificates' button.
- Domain Status:** 4 Active, 0 Less than 30 days. Includes a 'Show Domains' button.
- Last 5 Down Detections:** A list of down detections, including ***security.com with Response Code: 200, Response Code: 2 weeks ago.
- Technology Detection:** A table with columns for Asset, Tech, and Detection. The first entry is caspipot.com, Tech: [icon], Detection: 2 weeks ago.

With the correct entry of the information, the system will automatically scan the **Technology, Port, Vulnerability** information of the added asset and display the results in a short time.

The screenshot shows the CaspiPoT Attack Surface Monitor Assets page. The page title is 'Attack Surface Monitor / Assets'. The main content area is titled 'Caspisec Asset List' and includes an 'Add New Asset' button. The table below lists the assets:

Asset	Technologies	Open PORTS	Sub Scan	Type	Location	Added	#
***.com	[Icons]	[Red] [Green] [Green]	[Toggle]	subdomain	United States	2024-01-16 15:05:58	[Icon]
***.com	[Icons]	[Green] [Green]	[Toggle]	subdomain	France	2024-01-16 15:05:56	[Icon]
***.com	[Icons]	[Green] [Green]	[Toggle]	subdomain	France	2024-01-16 15:05:56	[Icon]
***.com	[Icons]	[Green] [Green]	[Toggle]	subdomain	France	2024-01-16 15:05:56	[Icon]
***.com	[Icons]	[Red] [Green] [Green]	[Toggle]	subdomain	United States	2024-01-16 15:05:56	[Icon]
***.com	[Icons]	[Green] [Green]	[Toggle]	subdomain	Türkiye	2024-01-16 15:05:54	[Icon]
***.com	[Icons]	[Red] [Green] [Green]	[Toggle]	domain	United States	2024-01-16 14:51:02	[Icon]



Active Monitor allows you to monitor the health status of all your inventory that provides internet service that is open to the world. **Caspipot Manager Panel || Attack Surface Monitor >> Active Monitor** field should be reached.

You can add **New Assets** from here

Asset	Status	Monitor HACK	Detections	Last Control	#
***.com	200	ON (BETA)	3P	2 min ago	
caspisec.com	200	ON (BETA)	3P	1 min ago	

Copyright © 2020 Caspipot v2.0. All Rights Reserved.

Black List Monitors allows you to monitor the black list status of all your inventory. **Caspipot Manager Panel || Attack Surface Monitor >> Black List Monitors** field should be reached. You can add **New Assets** from here.

Asset	Listed	Last Control	Delete
caspipot.com	0	2024-04-03 01:28:27	
caspisec.com	0	2024-04-03 01:28:40	

Show Full Control List

Copyright © 2020 Caspipot v2.0. All Rights Reserved.



Product Inventory allows you to monitor last vulnerability and CVE status of all your inventory. **Caspipot Manager Panel || Attack Surface Monitor >> Product Inventory** field should be reached. You can add **New Assets** from here.

Product	Vendor	Detections	Show Detections
xenmobile	Citrix	0 / 0	List
broadcast server	Citrix	0 / 0	List
netscaler	Citrix	0 / 0	List
appdna	Citrix	0 / 0	List
ios	Apple	11 / 3	List
lenosp	Lenosp	0 / 0	List

Copyright © 2020 Caspipot v2.0. All Rights Reserved.

Breach Data Control Configuration Guide

To activate breach data services via the **Caspipot Manager Panel || Breach Data Control** field should be reached.

When the stolen data area is accessed, the company lists defined for you will be displayed automatically. While you access the company field you want to process, the **domain names** that have been given permissions for the company are displayed.

You can view *existing stolen* data by creating a new **Check Leaked Password**. By defining scheduled tasks and making these searches continuous, you are aware of a potential data leak.



Username	Masked Password	Hash	Sources
support@***card.com	****9130	***254a162b7691e38b0f2b02e754a7	123RF.com
@card.com	****1233	***9e405f526b03f73e1a4d40f93a06	123RF.com

Check WAF Usage Guide

To activate Check WAF services via **Caspipot manager panel** || **Check WAF** field should be reached.

Name	Status	Domain	Score	Started	Report	Result	#
card	Finished	***	148 / 148	2 weeks ago	Show Details	Show Details	1
WAF Scan ***	Finished	***	109 / 2	2 weeks ago	Show Details	Show Details	1
CF Scan	Finished	***	109 / 3	2 weeks ago	Show Details	Show Details	1
Caspipot Scan WAF	Finished	***	106 / 8	4 months ago	Show Details	Show Details	1

Use the **Start New Scan** tab to test for a new WAF.



Start New WAF Scan

caspiopot.com

Subdomain: api

Name: New Api Waf Scanner

Start

Copyright © 2020 CaspiPot v2.0. All Rights Reserved.

After the new scan you can **Download, Share** (generates a 24-hour download link) and **Show** your test details.

WAF Test Scans

Last Scans

Name	Status	Domain	Score	Started	Report	Result	#
card	Finished	***	148 / 148	2 weeks ago	Download	Show Details	#
WAF Scan ***	Finished	***	109 / 2	2 weeks ago	Download	Show Details	#
CF Scan	Finished	***	109 / 3	2 weeks ago	Download	Show Details	#
CaspiPot Scan WAF	Finished	***	106 / 8	4 months ago	Download	Show Details	#

Start New Scan

Copyright © 2020 CaspiPot v2.0. All Rights Reserved.

WAF Test Results

CF Scan - Test Results

Vector	Domain	Path	Method	Result	#
CRLF	caspiopot.com	APPENDURL	HEADER	404	bypass
CRLF	caspiopot.com	HeaderIndex	HEADER	404	bypass
CRLF	caspiopot.com	!@#%^&*~	HEADER	404	bypass
CRLF	caspiopot.com	POSTURL	GET	404	bypass

Results: 77.2% (Blocked, Bypassed)

Scan List

Attack Vector	Passed	Detected
HTML	3	0
XSS	13	0
SQI AUTH	7	1
SQI COMMANDS	9	0
SQI	15	0
NuSQL	6	0
SSRF	9	0
RCE	20	1
XXE	3	0
MISCONFIGURATION	5	1

Score Stats

Total Retries: 109

Blocked: 3, Bypassed: 106



Stress Tester Usage Guide

Stress Tester services via the **Caspipot manager panel** || **Stress Tester** field should be reached.

The Stress module is designed to measure the resilience of the current system by sending distributed **http/https requests** to a **specified target**. During the tests, a user-specified main **domain**, **subdomain** or **designated folder** can be attacked.

During the attack, it transmits **GET, POST, HEAD, OPTIONS, PUT, DELETE** sample requests.

The company domains selected to start a new test consist of a list of domains added from the company settings defined in the existing company's account.

True: caspipot.com

True: blog.caspipot.com

True: caspipot.com/blog/

False: caspipot.com/?parametre=parametre



The screenshot shows the 'Stress Test History' page in the CaspiPoT interface. It features a table titled 'Last Controls' with the following columns: Domain, METHOD, Number, URL, and Thread. The table contains 10 rows of test data.

Domain	METHOD	Number	URL	Thread
	RANDOM	10		1
	POST	10		1
	RANDOM	10		1
	POST	10	index	1
	RANDOM	10		1
	RANDOM	10		1
	POST	10		1
	RANDOM	10		1
	RANDOM	10		1
	GET	10		1

Upon completion of the stress test, you can list the **history** of all tests.

IOC's Data Usage Guide

IOC's services via the **Caspipot manager panel || IOC/POOL** field should be reached.

IOC data can be accessed under the **Caspipot manager panel || IOC Pool >> Bad Ip Pool & Proxy Pool & Payload Pool** tab.

The screenshot shows the 'WAF Attack Pool' page in the CaspiPoT interface. It displays a table titled 'CASPIPOT WAF Pool Detections' with the following columns: Preview, Attack Type, Risk Score, Masked IP, and Action. The table contains 13 rows of detection data.

Preview	Attack Type	Risk Score	Masked IP	Action
page/alerts/whitelistareabloginFL...	XSS	5	212.102.**	Copy payload
page/windows/inchtmlareabloginFL...	XSS	5	212.102.**	Copy payload
page/alerts/Web/inchtmlareablogin...	XSS	5	212.102.**	Copy payload
page/alerts/gallery.php&mpert...	XSS	5	212.102.**	Copy payload
page/alerts/gallery.php&mpert...	XSS	5	212.102.**	Copy payload
page/alerts/gallery.php&mpert...	XSS	5	212.102.**	Copy payload
page/alerts/gallery.php	XSS	5	212.102.**	Copy payload
page/alerts/category.php	XSS	5	212.102.**	Copy payload
page/windows/gallery.php&mpert...	XSS	5	212.102.**	Copy payload
page/alerts/category.php	XSS	5	212.102.**	Copy payload
page/windows/gallery.php&mpert...	XSS	5	212.102.**	Copy payload
page/alerts/gallery.php	XSS	5	212.102.**	Copy payload
page/alerts/category.php	XSS	5	212.102.**	Copy payload



Proxy List / 2024-03-31 21:24:59

These IP addresses are collected from open communities that are used for Layer 7 Stress tests and DDoS attacks and are presented to you in bulk. This list is presented after being checked 3-4 times a day.

IP	Port	Proxy Type
98.96.274.54	8118	https
95.56.254.139	3128	https
95.68.227.128	8080	https
99.56.147.242	54250	https
95.87.216.118	8080	https
82.137.244.151	8080	https
82.102.20.230	8443	https
82.147.118.164	8080	https
81.16.245.379	53281	https
81.174.11.199	61743	https

Copyright © 2020 CaspiPOT v2.0. All Rights Reserved.

Use the **Export CSV** or **API integration** to collect for a new IOC's.

ADMINISTRATION GUIDE

User & Reports

You can make arrangements for user management, adding new users and sharing of reports from the **Caspipot Manager Panel || Companies >> Users List**

Company List

Name	Integration	Services	Domains	Users
****card	[0] Settings	0	[1] Domain List	[2] User List
*****Eu	[0] Settings	0	[1] Domain List	[0] User List



Copyright © 2020 Caspipot v2.0. All Rights Reserved.

All reports are generated daily and sent to defined users via e-mail.

3rd. Party Integration

You can make 3rd party integration from the **Caspipot Manager Panel || Companies >> Integration >>> Settings**

By selecting the appropriate solution for your products, you can activate the service by entering the requested information completely.



The screenshot shows the CaspiPoT web interface. On the left is a dark sidebar with navigation items: Dashboard, Companies, Deception Menu (Decoy APPs, WAF, Servers), Attack Surface Monitor (ASM Company List, WAF Sensivity Check, Check WAF), Breach Data (Breach Data Control), Stress Test (Stress Tester), and IOC/POOL. The main content area is titled '***card Integrations' and shows a 'Logs' section with 'CloudFlare' and 'Not Configured' buttons. To the right is a configuration form for CloudFlare with fields for 'Email address', 'API Key', and 'Zone Name', and buttons for 'Get Zone Name', 'Save', and 'CloudFlare'.

Tickets

To send any support request or information via **the Caspiot Manager Panel || Usage&Support >> Tickets** field should be reached.

www.caspipot.com

Caspi  **PoT**