

Cyber Security

Class no 10(Arabi Sir)

19 Oct 2024

CVEdetails.com
powered by SecurityScorecard

Vulnerabilities

- By Date
- By Type
- Known Exploited
- Assigners
- CVSS Scores
- EPSS Scores
- Search

Vulnerable Software

- Vendors
- Products
- Version Search

Vulnerability Intel.

- Newsfeed
- Open Source Vulnerabilities

Vulnerability Details : CVE-2024-49593

In Advanced Custom Fields (ACF) before 6.3.9 and Secure Custom Fields before 6.3.6.3 (plugins for WordPress), using the Field Group editor to edit one of the plugin's fields can result in execution of a stored XSS payload. NOTE: if you wish to use the WP Engine alternative update mechanism for the free version of AC then you can follow the process shown at the advancedcustomfields.com blog URL within the References section below.

Published 2024-10-17 04:15:03 Updated 2024-10-18 12:53:05 Source MITRE

View at NVD[®], CVE.

Vulnerability category: Cross site scripting (XSS)

Products affected by CVE-2024-49593

Please [log in](#) to view affected product information.

Exploit prediction scoring system (EPSS) score for CVE-2024-49593

EPSS

0.05%

Probability of exploitation activity in the next 30 days [EPSS Score History](#)

~16.4%

Percentile, the proportion of vulnerabilities that are scored at or less

Example: Latest Microsoft Vulnerability Details

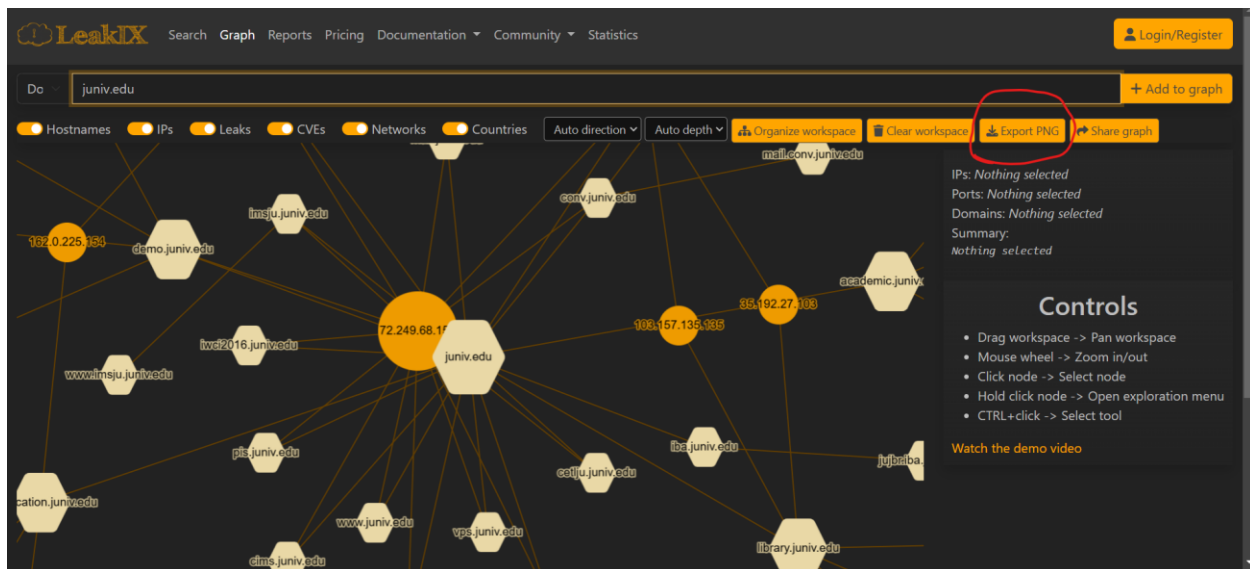
Leakix use for find ip address and all website derived from target web.

<https://leakix.net/>

<https://leakix.net/graph>

72.249.68.156 → juniv.edu

The screenshot displays the LeakIX web application interface. At the top, there is a navigation bar with links for Search, Graph, Reports, Pricing, Documentation, Community, and Statistics. A 'Login/Register' button is located in the top right corner. Below the navigation bar, a search bar contains the text 'juniv.edu'. To the right of the search bar is a '+ Add to graph' button. Below the search bar, there is a row of toggle switches for Hostnames, IPs, Leaks, CVEs, Networks, and Countries. To the right of these toggles are buttons for 'Auto direction', 'Auto depth', 'Organize workspace', 'Clear workspace', 'Export PNG', and 'Share graph'. The main content area is divided into two sections. The left section shows a list of results for 'juniv.edu', including a table with columns for IP, Port, and Domain. The right section shows a summary of the results, including a 'Controls' section with instructions for interacting with the graph.



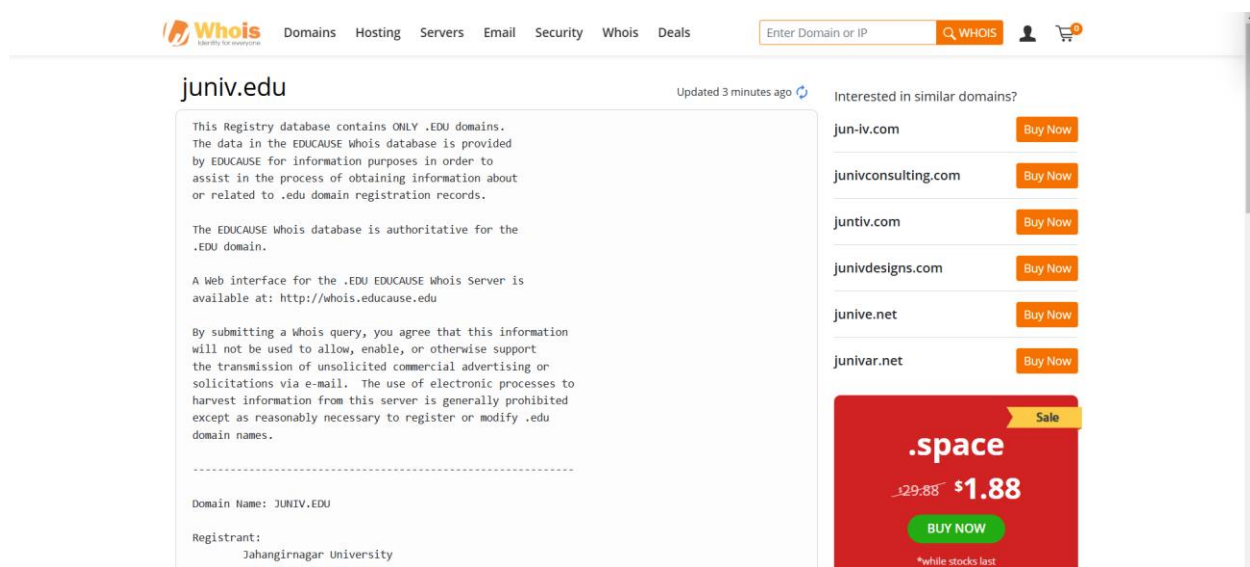
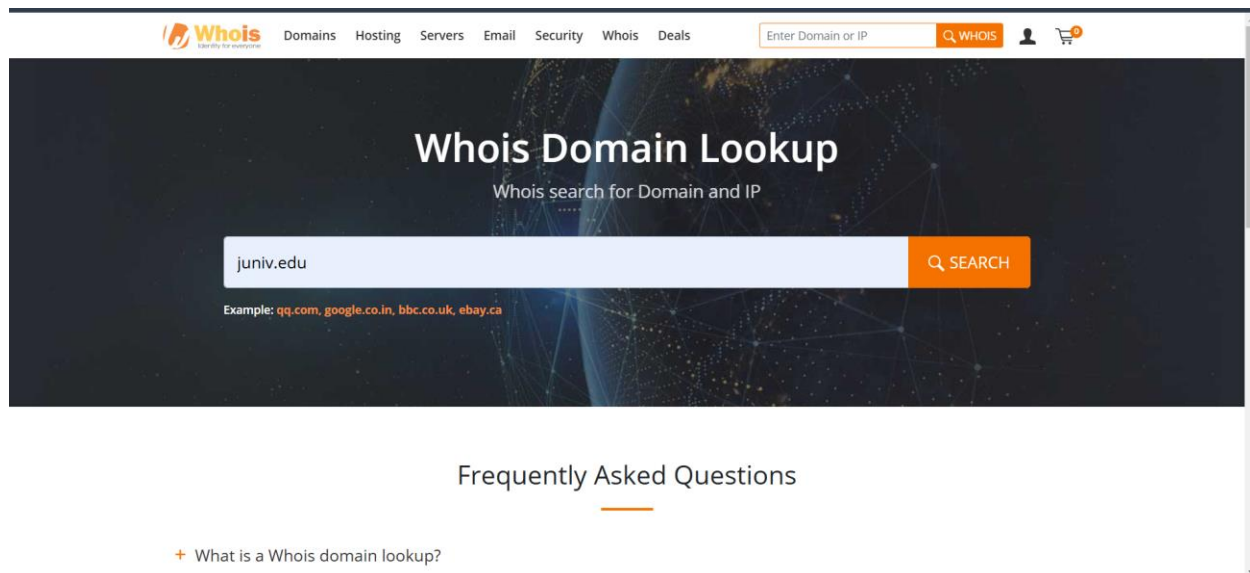
Threatmap.checkpoint show worldwide live attack

<https://threatmap.checkpoint.com/>



Whois use for find normal information

<https://www.whois.com/whois/>



Who use for find address profile

<https://who.is/>


72.249.68.156 juniv.edu ip

[Premium Domains](#) [Transfer](#) [Features](#) [Login](#) [Sign Up](#)

who.is


WHOIS Search, [Domain Name](#) Website, and IP Tools

Your IP address is [103.122.143.97](#)




See Website Information

Search the whois database, look up domain and IP owner information, and check out dozens of other statistics.



On Demand Domain Data

Get all the data you need about a domain and everything associated with that domain anytime with a single search.



Register Domain Names

Find a domain with the best domain registrar on the web. [Start your domain search at Name.com.](#)

[Transfers](#) [Premium Domains](#) [Web Hosting](#) [Website Builder](#) [Contact Us](#) [FAQs](#) [Terms of Service](#)

who.is

[Premium Domains](#) [Transfer](#) [Features](#) [Login](#) [Sign Up](#)

72.249.68.156 address profile

Whois

Diagnostics

IP Whois

NetRange: 72.249.0.0 - 72.249.191.255

CIDR: 72.249.0.0/17, 72.249.128.0/18

NetName: COL04-BLK2

NetHandle: NET-72-249-0-0-1

Parent: NET72 (NET-72-0-0-0-0)

NetType: Direct Allocation

OriginAS: AS17378

Organization: TierPoint, LLC (TL-801)

RegDate: 2006-08-25

Updated: 2024-03-19

Ref: https://rdap.arin.net/registry/ip/72.249.0.0

OrgName: TierPoint, LLC

OrgId: TL-801

Address: 12444 Powerscourt Drive Suite 450

City: St. Louis

StateProv: MO

IPVOID use for find target ip details

url: <https://www.ipvoid.com/>

Popular IP Tools

IP Blacklist Check

Check if an IP is blacklisted

Whois Lookup

Query the whois database

Ping Lookup

Ping an IPv4 address or host

IPv6 Ping Lookup

Ping an IPv6 address

IPv4 CIDR Calculator

Convert IPv4 CIDR to IP range

IPv6 CIDR Calculator

Convert IPv6 CIDR to IP range

DNS Propagation

DNS propagation checker

DiG DNS Lookup

Run a DiG DNS lookup

MX Records Lookup

View MX DNS records

real-time an IP address through more than 80 IP reputation and DNSBL services. This service is built with the IP Reputation API by APIVoid.

Check IP Address

IP Address Information

Analysis Date	2024-11-02 02:13:50
Elapsed Time	0 seconds
Detections Count	0/93
IP Address	72.249.68.156 Find Sites IP Whois
Reverse DNS	vps.juniv.edu
ASN	AS17378
ISP	TierPoint LLC
Continent	North America
Country Code	(US) United States of America
Latitude / Longitude	Google Map

Track USB Events

New Tools

Popular

Make URL Harmless

Sum of a List of Numbers

Replace Commas with New Lin

Replace New Lines with Comm

JSON Minify

TLS Checker

IP Reputation API

IPv4 CIDR Calculator

This online IPv4 CIDR calculator can convert an IPv4 CIDR address (i.e. 73.35.0.0/20) to IP range. Calculate the first and last IP address in the CIDR range, the number of IPv4 addresses contained in the CIDR, and the netmask. Just enter the IPv4 CIDR address in the form below:

Start IP: 72.249.68.156

End IP: 72.249.68.156

Number of IPs: 1

Subnet Range: 255.255.255.255

Wildcard: 0.0.0.0

- Threat Intelligence APIs
- Harden Windows 10/11
- File Lines Manipulator
- Track USB Events

- Make URL Harmless
- Sum of a List of Numbers
- Replace Commas with New Line
- Replace New Lines with Commas
- JSON Minify
- TLS Checker

juniv.edu

A

4612

72.249.68.156

A mean ip address → it's call A record

IPVOID

IP
DNS
TEXT
URL
ENC/DEC
RANDOM
EXTRACT
MORE

Find Website IP

Simple online tool to find the IP addresses associated with a website (domain or subdomain). Easily find the website IP address, get the IP address of any domain name. Convert a host to its associated IP address.

The submitted website resolves to

72.249.68.156 (vps.juniv.edu)

- Threat Intelligence APIs
- Harden Windows 10/11
- File Lines Manipulator
- Track USB Events

- Make URL Harmless
- Sum of a List of Numbers

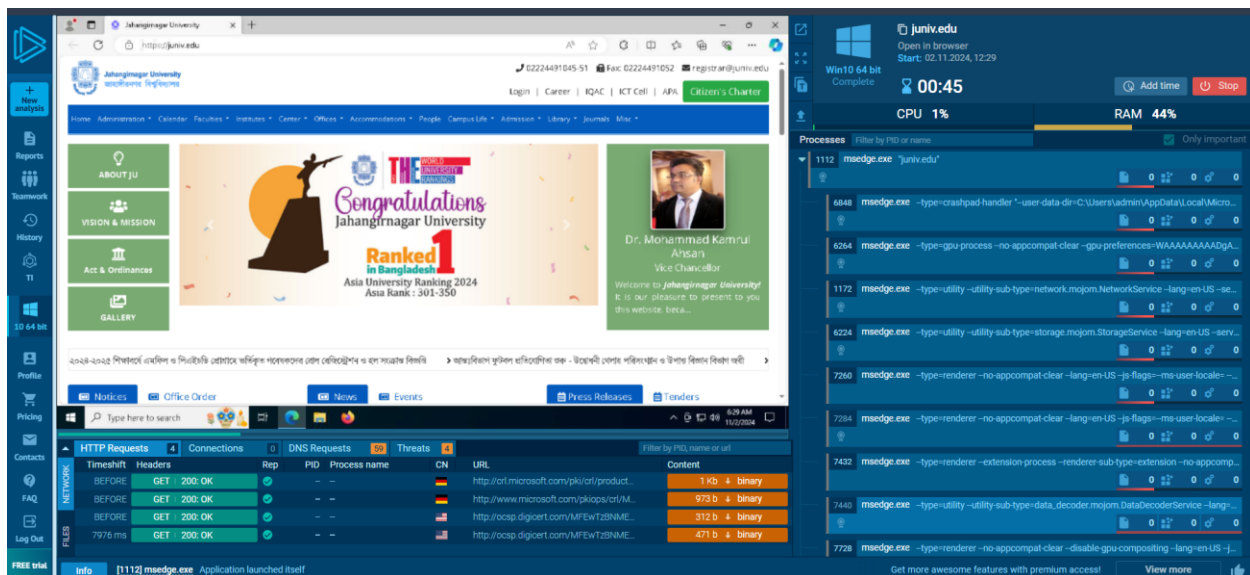
```

(root@kali)-[~]
# ping juniv.edu
PING juniv.edu (72.249.68.156) 56(84) bytes of data:
64 bytes from vps.juniv.edu (72.249.68.156): icmp_seq=3 ttl=46 time=273 ms

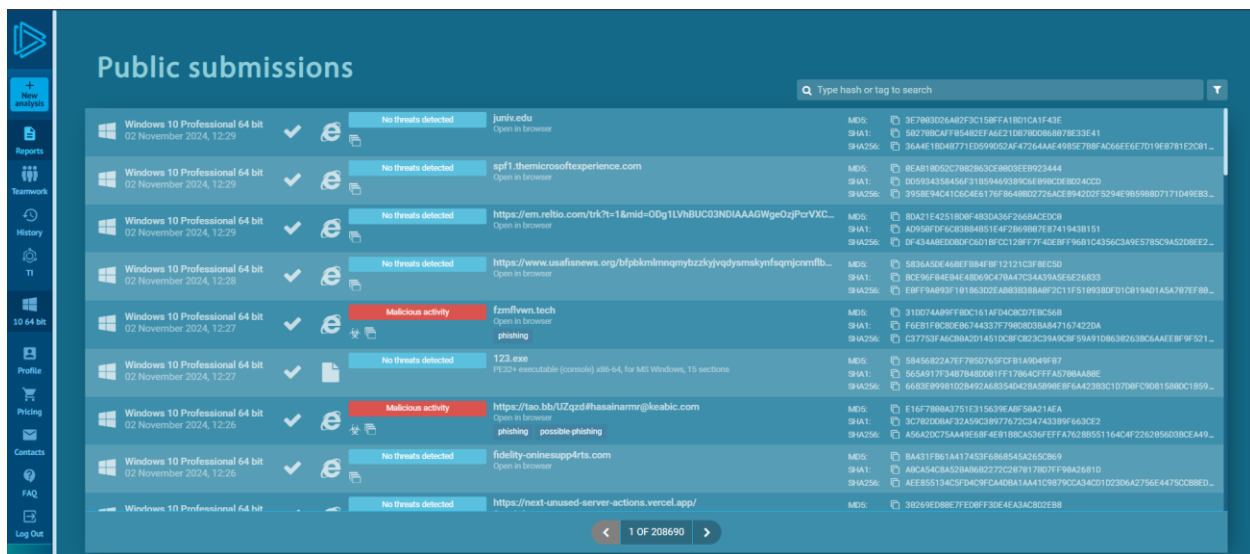
```

Nessus/tenable security center → vulnerability scanner

SLA → service level argument



Report part for find resent vulnerability:



The screenshot displays the ANY.RUN web-based malware analysis environment. On the left, a Windows 10 desktop is visible with various icons and a taskbar. The main area shows a list of processes running on the virtual machine. The process list includes:

Process Name	PID	PPID	Process Name	CN	URL	Content
conhost.exe	6736	0	conhost.exe	0x00000000	ForceV1	1 KB binary
conhost.exe	6736	0	conhost.exe	0x00000000	ForceV1	1 KB binary
powershell.exe	6780	6736	powershell.exe	0x00000000	Add-MpPreference -ExclusionPath 'C:\Users\admin\AppData\Local\Telemetry\...	973 B binary
regedit.exe	1096	6780	regedit.exe	0x00000000	ForceV1	512 B binary
wmplayer.exe	2428	6780	wmplayer.exe	0x00000000	ForceV1	953 B binary
verfault.exe	5172	6736	verfault.exe	0x00000000	ForceV1	1 KB binary

The right sidebar shows a detailed view of the selected process, 'New_Order_#070824_Order_November-2024-pdf.exe', including its MD5 hash, start time, and various indicators. The bottom section shows a list of HTTP requests and connections.

Graph part to show using all details for every part



MITRE ATT&CK Matrix											
Tactics 4 Techniques 10 Events 34				All tactics ×							
				● Danger (1) ● Warning (10) ● Other (23)							
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	C & C	Exfiltration	Impact
	Command and Scripting Interpreter (1/6) PowerShell 2			Impair Defenses (1/9) Disable or Modify Tools 1 Virtualization/Sandbox Evasion (1/3) Time Based Evasion 1		System Network Configuration Discovery (0/2) 1 Query Registry 3 16 System Information Discovery 1 6 Virtualization/Sandbox Evasion (1/3) Time Based Evasion 1 System Location Discovery (0/1) 1			Non-Standard Port 1 Application Layer Protocol (0/4) 1		

Information gathering:

Zenmap

[Scan](#)
[Tools](#)
[Profile](#)
[Help](#)

Target: 192.168.68.169/24
 ▼
 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.68.169/24

Hosts

Services

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

OS

Host

```

nmap -T4 -A -v 192.168.68.169/24

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-19 14:17 Bangladesh Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
Initiating ARP Ping Scan at 14:17
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 14:17, 3.42s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 20 hosts. at 14:17
Completed Parallel DNS resolution of 20 hosts. at 14:17, 0.04s elapsed
Nmap scan report for 192.168.68.0 [host down]

```