

**Enhancing Digital Government and Economy**  
**Cyber Security Course**  
**Classwork-10**



**Submitted by,**  
**Name: Koushiki Devi Agarwalla**  
**Batch: JUR2B11**  
**ID: 2111271**

**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 Vulns

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

## Example: Latest Microsoft Vulnerability Details

[leakix.net/](#) →

<https://threatmap.checkpoint.com/> → live attack protocol

[LeakIX - Graph](#) → check live vulnerability

72.249.68.156 → [juniv.edu](#)

<https://www.whois.com/> → domain name, identity, ip

<https://who.is/> → inp

### Whois Online Lookup

Query the whois database online to find information about a domain name or an IP address. With the whois lookup you can find the owner of the specified domain name, the domain creation and expiration date, the company behind an IP address, the contacts of the abuse department, and much more.

<https://www.ipvoid.com/> → target ip details

72.249.68.156 [Whois Check](#)

juniv.edu	A	4612	<a href="#">72.249.68.156</a>
-----------	---	------	-------------------------------

A mean ip address → it's call A record

```
(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

Nessus installation → H.W → scan hoy policyr against e PN7W-Z9BP-KNM7-ZF5A-5NXP

SLA → service level argument

[Download Burp Suite Community Edition - PortSwigger](#)

<https://www.abuseipdb.com/> → to send a ip in black list

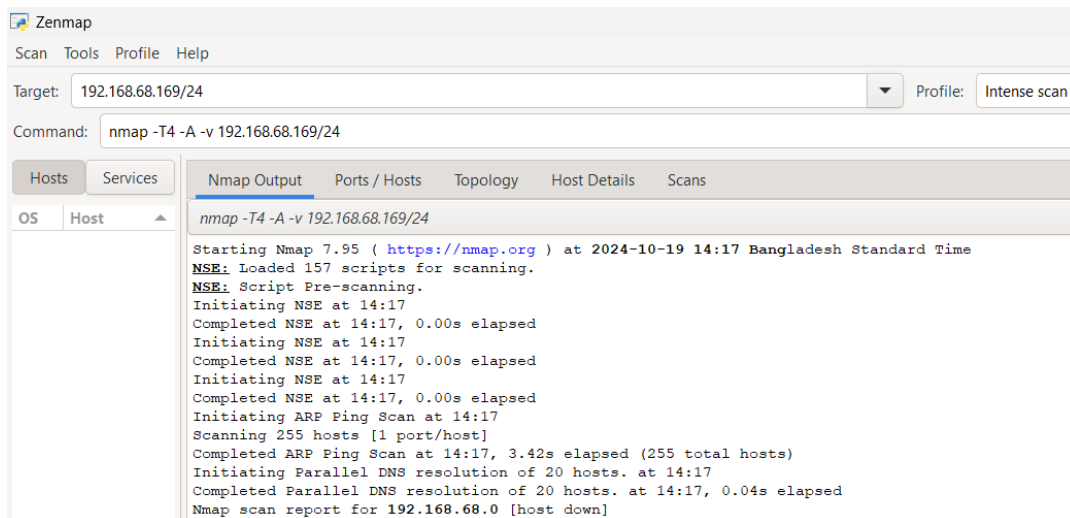
<https://any.run/>

<https://any.run/malware-reports/>

<https://app.any.run/submissions/>

<https://app.any.run/tasks/eaedffff-3e09-4c96-8bce-8f94950eaf7b>

## Information gathering:



The screenshot shows the Zenmap application interface. At the top, there's a menu bar with 'Scan', 'Tools', 'Profile', and 'Help'. Below it, the 'Target' field is set to '192.168.68.169/24' and the 'Profile' is set to 'Intense scan'. The 'Command' field shows 'nmap -T4 -A -v 192.168.68.169/24'. The main window has tabs for 'Hosts', 'Services', 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Nmap Output' tab is active, displaying the following text:

```
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]
```

