

pspspsps-ctf / writeups

Code

Issues

Pull requests

Actions

Projects

Security

Insights

Files

main

+

Q

Go to file

t

2024/0xL4ugh CTF 2024

Forensics/Wordpress

1

1\_1.png

1\_2.png

1\_3.png

readme.md

2

3

4

Misc/Welcome

writeups / 2024 / 0xL4ugh CTF 2024 / Forensics / Wordpress / 1 /

Add file

...

chonkyNyan

Add writeups for 0xL4ugh CTF 2024

708982 · last week

History

| Name      | Last commit message               | Last commit date |
|-----------|-----------------------------------|------------------|
| ..        |                                   |                  |
| 1_1.png   | Add writeups for 0xL4ugh CTF 2024 | last week        |
| 1_2.png   | Add writeups for 0xL4ugh CTF 2024 | last week        |
| 1_3.png   | Add writeups for 0xL4ugh CTF 2024 | last week        |
| readme.md | Add writeups for 0xL4ugh CTF 2024 | last week        |

readme.md

WordPress - 1

WordPress - 1

[Easy]

Our WordPress site has experienced a security breach, and the precise method of compromise remains undetermined at present. We need you help to investigate what actually happened.

Q1. There were two attackers attempting to compromise our environment. What is the IP address of the victim, and what is the IP address of the first attacker? Q2. What are the versions of the Apache and PHP servers deployed in our environment?

Flag Format 0xL4ugh{A1\_A2}

Example: 0xL4ugh{IP1\_IP2\_apache1.2.3\_php1.2.3}(no spaces)

Solution:

We were given a Wordpress.pcapng file.

Filtering via http.request ...we can see a suspicious requests coming from 192.168.204.132

Wordpress.pcapng

| No.  | Time       | Source          | Destination     | Port                 | Protocol | Length | Info                                              |
|------|------------|-----------------|-----------------|----------------------|----------|--------|---------------------------------------------------|
| 6969 | 153.116270 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 340    | HEAD /wordpress/%2wp-config.php%23 HTTP/1.1       |
| 6970 | 153.116270 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 341    | HEAD /wordpress/backup.wp-config.php HTTP/1.1     |
| 6989 | 154.794151 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 330    | HEAD /wordpress/wp-config HTTP/1.1                |
| 6993 | 154.839136 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 345    | HEAD /wordpress/wp-config%20-%20Copy.php HTTP/1.1 |
| 7000 | 155.100365 | 192.168.204.128 | 95.100.130.37   | 95.100.130.37        | HTTP/XSL | 1300   | POST /fullink/?linkID=25266&clcid=new09 HTTP/1.1  |
| 7007 | 155.180174 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 341    | HEAD /wordpress/wp-config%20copy.php HTTP/1.1     |
| 7015 | 155.968352 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 337    | HEAD /wordpress/wp-config_backup HTTP/1.1         |
| 7019 | 156.059279 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 335    | HEAD /wordpress/wp-config_good HTTP/1.1           |
| 7022 | 156.450946 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 337    | HEAD /wordpress/wp-config-backup HTTP/1.1         |
| 7024 | 156.482701 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 341    | HEAD /wordpress/wp-config-backup.php HTTP/1.1     |
| 7028 | 156.919690 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 341    | HEAD /wordpress/wp-config-backup.txt HTTP/1.1     |
| 7032 | 157.816640 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 342    | HEAD /wordpress/wp-config-backup1.txt HTTP/1.1    |
| 7035 | 158.105998 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 335    | HEAD /wordpress/wp-config-good HTTP/1.1           |
| 7038 | 158.194881 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 341    | HEAD /wordpress/wp-config-sample.php HTTP/1.1     |
| 7060 | 158.257524 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 345    | HEAD /wordpress/wp-config-sample.php-bak HTTP/1.1 |
| 7071 | 158.378953 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 342    | HEAD /wordpress/wp-config-sample.php- HTTP/1.1    |
| 7090 | 159.133237 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 337    | HEAD /wordpress/wp-config.backup HTTP/1.1         |
| 7093 | 159.685121 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 334    | HEAD /wordpress/wp-config.bak HTTP/1.1            |
| 7098 | 160.169366 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 334    | HEAD /wordpress/wp-config.bkp HTTP/1.1            |
| 7101 | 160.444435 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 334    | HEAD /wordpress/wp-config.cfg HTTP/1.1            |
| 7104 | 160.455998 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 335    | HEAD /wordpress/wp-config.conf HTTP/1.1           |
| 7108 | 161.274969 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 335    | HEAD /wordpress/wp-config.data HTTP/1.1           |
| 7111 | 161.420155 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 335    | HEAD /wordpress/wp-config.dump HTTP/1.1           |
| 7114 | 162.067093 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 335    | HEAD /wordpress/wp-config.good HTTP/1.1           |
| 7116 | 162.334513 | 192.168.204.1   | 239.255.255.250 | 239.255.255.250:1900 | SSDP     | 218    | M-SEARCH * HTTP/1.1                               |
| 7118 | 162.495989 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 334    | HEAD /wordpress/wp-config.htm HTTP/1.1            |
| 7120 | 162.499336 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 335    | HEAD /wordpress/wp-config.html HTTP/1.1           |
| 7123 | 163.335188 | 192.168.204.1   | 239.255.255.250 | 239.255.255.250:1900 | SSDP     | 218    | M-SEARCH * HTTP/1.1                               |
| 7125 | 163.676433 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 334    | HEAD /wordpress/wp-config.inc HTTP/1.1            |
| 7127 | 163.721489 | 192.168.204.132 | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 340    | HEAD /wordpress/wp-config.local.php HTTP/1.1      |

So that is most likely our first attacker.

Now, to answer Q2, let's scroll up a bit.

Wordpress.pcapng

| No. | Time     | Source          | Destination     | Port                 | Protocol | Length | Info                                  |
|-----|----------|-----------------|-----------------|----------------------|----------|--------|---------------------------------------|
| 3   | 7.738563 | 192.168.204.128 | 239.255.255.250 | 239.255.255.250:1900 | SSDP     | 217    | M-SEARCH * HTTP/1.1                   |
| 16  | 8.751233 | 192.168.204.128 | 239.255.255.250 | 239.255.255.250:1900 | SSDP     | 217    | M-SEARCH * HTTP/1.1                   |
| 23  | 8.607763 | 192.168.204.1   | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 573    | GET /wordpress/ HTTP/1.1              |
| 52  | 9.420641 | 192.168.204.1   | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 721    | GET /wordpress/wp-includes/blocks/nav |
| 54  | 9.443546 | 192.168.204.1   | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 703    | GET /wordpress/wp-includes/js/dist/in |
| 55  | 9.443546 | 192.168.204.1   | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 718    | GET /wordpress/wp-includes/blocks/nav |
| 56  | 9.444443 | 192.168.204.1   | 192.168.204.128 | 192.168.204.128,80   | HTTP     | 750    | GET /wordpress/wp-includes/blocks/nav |

Following the HTTP stream will give the answer that we need.

Wireshark · Follow HTTP Stream (tcp.stream eq 6) · Wordpress.pcapng

GET /wordpress/ HTTP/1.1  
Host: 192.168.204.128  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-US,en;q=0.9  
Cookie: wordpress\_test\_cookie=WP%20Cookie%20check; wp-settings-1=libraryContent%3Dbrowse; wp-settings-time=1.6582222222222222  
  
HTTP/1.1 200 OK  
Date: Wed, 17 Jan 2024 21:40:01 GMT  
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12  
X-Powered-By: PHP/8.2.12  
Link: <http://192.168.204.128/wordpress/wp-json/>; rel="https://api.w.org/"  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
Transfer-Encoding: chunked  
Content-Type: text/html; charset=UTF-8

Flag: 0xL4ugh{192.168.204.128\_192.168.204.132\_apache2.4.58\_php8.2.12}