

[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?

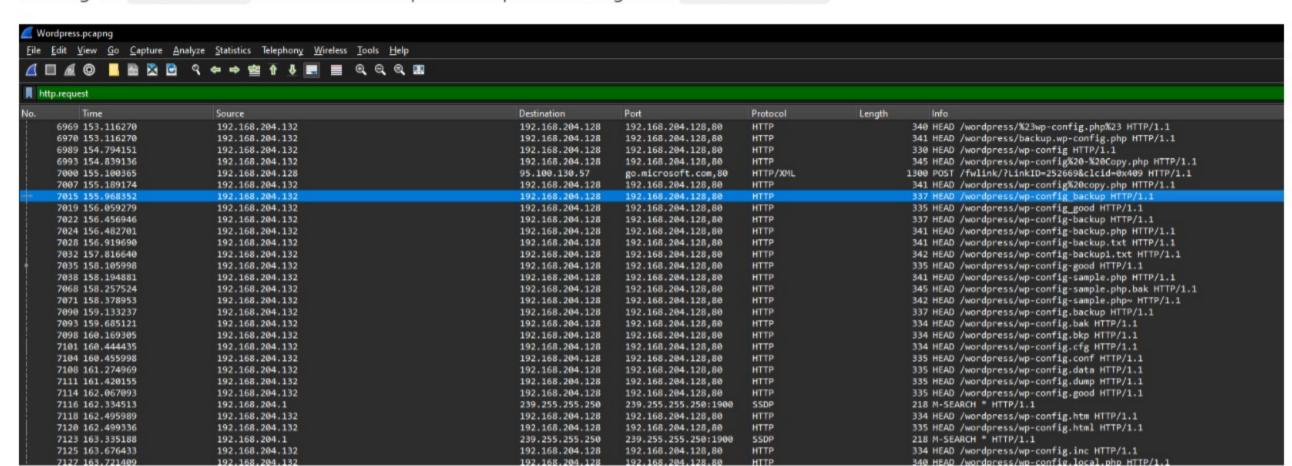
Flag Format 0xL4ugh{A1_A2}

Example: 0xL4ugh{IP1_IP2_apache1.2.3_php1.2.3}(no spaces)

Solution:

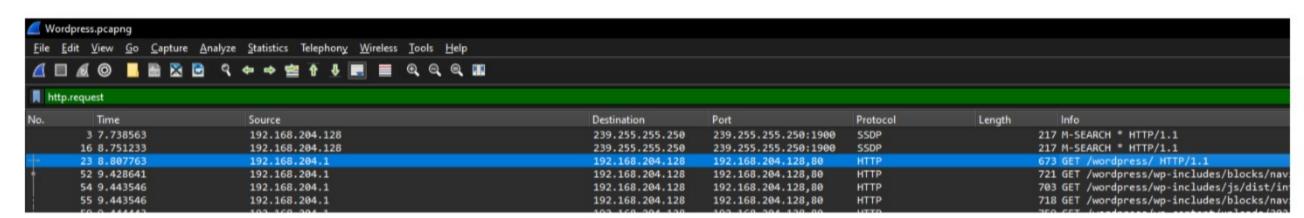
We were given a Wordpress.pcapng file.

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



So that is most likely our first attacker.

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



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
 Jser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gec
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q
 Accept-Encoding: gzip, deflate
 Accept-Language: en-US,en;q=0.9
 lookie: wordpress_test_cookie=WP%20Cookie%20check; wp-settings-1=libraryContent%3Dbrowse
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}