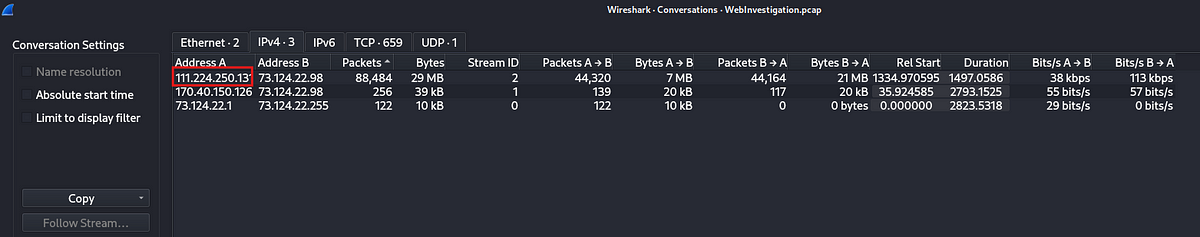
### **Web Investigation —CyberDefenders**

Scenario: You are a cybersecurity analyst working in the Security Operations Center (SOC) of BookWorld, an expansive online bookstore renowned for its vast selection of literature. BookWorld prides itself on providing a seamless and secure shopping experience for book enthusiasts around the globe. Recently, you’ve been tasked with reinforcing the company’s cybersecurity posture, monitoring network traffic, and ensuring that the digital environment remains safe from threats.  
Late one evening, an automated alert is triggered by an unusual spike in database queries and server resource usage, indicating potential malicious activity. This anomaly raises concerns about the integrity of BookWorld’s customer data and internal systems, prompting an immediate and thorough investigation.  
As the lead analyst in this case, you are required to analyze the network traffic to uncover the nature of the suspicious activity. Your objectives include identifying the attack vector, assessing the scope of any potential data breach, and determining if the attacker gained further access to BookWorld’s internal systems.

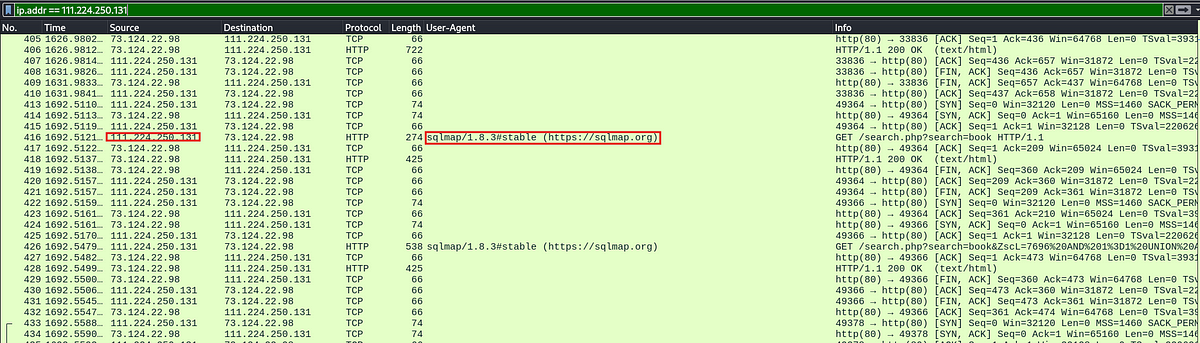
Tasks:

1. By knowing the attacker’s IP, we can analyze all logs and actions related to that IP and determine the extent of the attack, the duration of the attack, and the techniques used. Can you provide the attacker’s IP?

Let us look at the context here, the alert the SOC received is **an unusual spike in database queries and server resource usage.** Let us look at the conversations in Wireshark to see which IP address is sending the most amount of packets. Go to Statistics -> Conversations -> IPv4



We can see from the conversations tab that the IP address 111.224.250[.]131 is sending the most amount of traffic. Let us confirm if this is the malicious IP or not by looking at the packets belonging to this IP address.

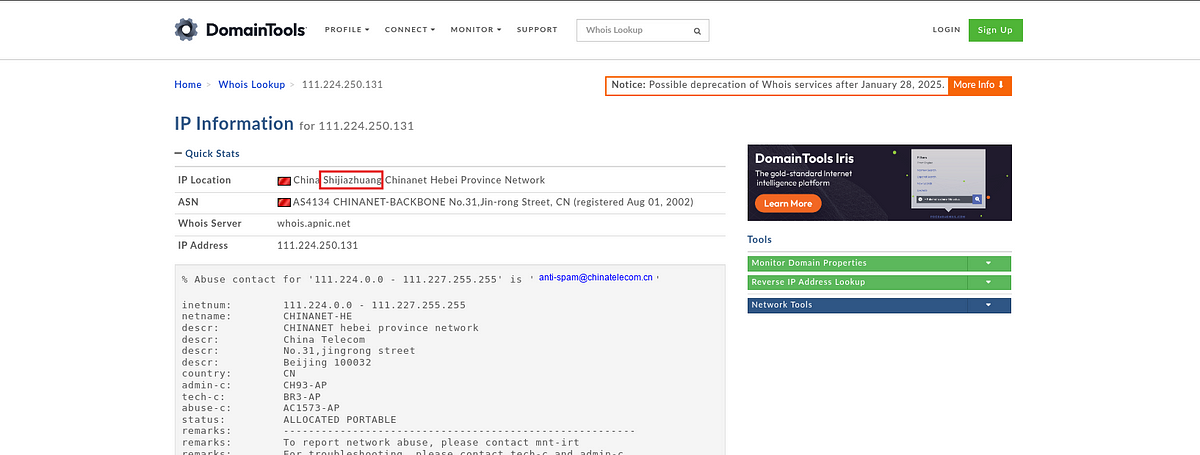


When we filter for the packets belonging to this IP we can see that it is using malicious programs to scan the server, hence we can confirm that this is the attacker IP address.

Answer: 111.224.250[.]131

2. If the geographical origin of an IP address is known to be from a region that has no business or expected traffic with our network, this can be an indicator of a targeted attack. Can you determine the origin city of the attacker?

To find out the location of the IP address we can use an online tool called Whois domain lookup.

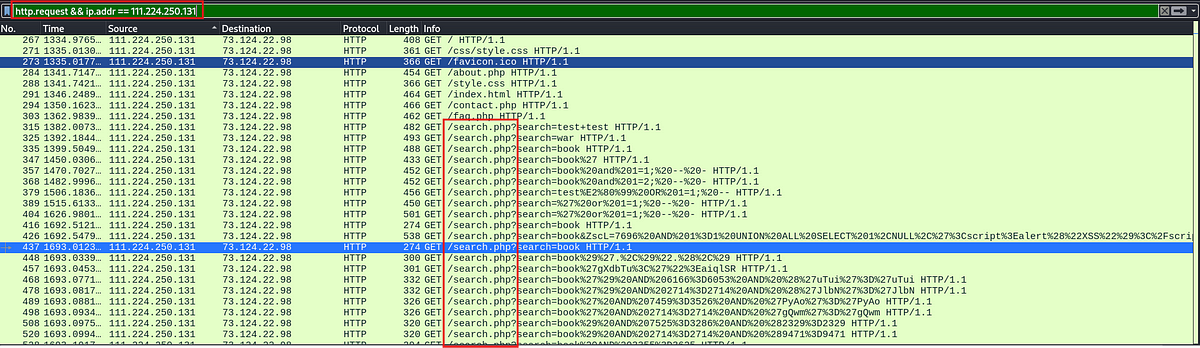


Answer: Shijiazhuang

3. Identifying the exploited script allows security teams to understand exactly which vulnerability was used in the attack. This knowledge is critical for finding the appropriate patch or workaround to close the security gap and prevent future exploitation. Can you provide the vulnerable PHP script name?

Let us look at the request the attacker is made to the server by applying the following filter.

http.request && ip.addr == 111.224.250.131

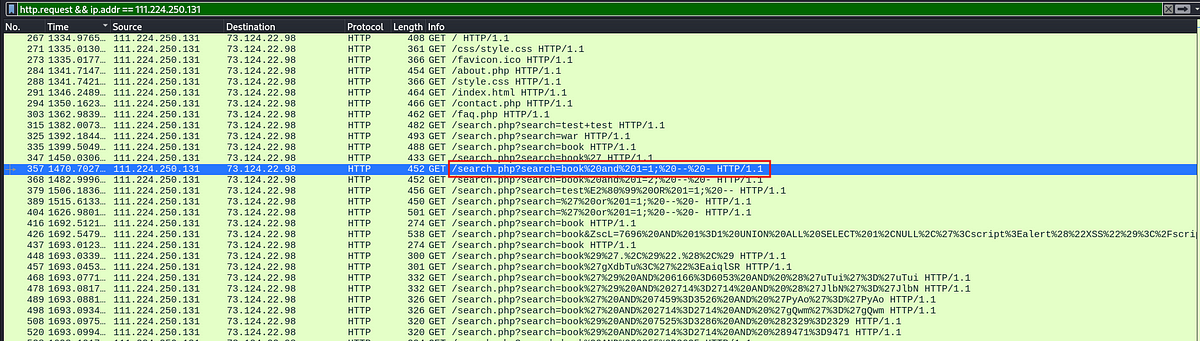


Looking at the above image it is clear that, the attacker had found a vulnerability in the search field.

Answer: search.php

4. Establishing the timeline of an attack, starting from the initial exploitation attempt, What’s the complete request URI of the first SQLi attempt by the attacker?

In the above screenshot we can see the first sqli attempt.



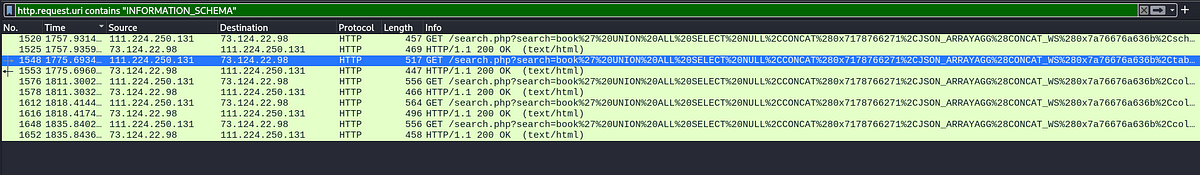
Answer: /search/php?search=book%20and%201=1;%20 — %20-

5. Can you provide the complete request URI that was used to read the web server’s available databases?

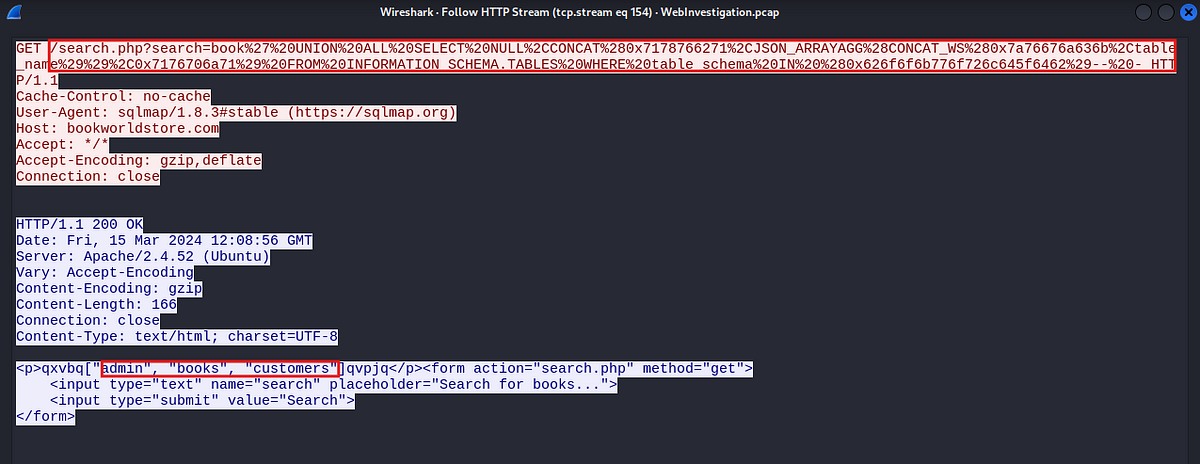
To get the information about the available tables in a database in SQL, the command to use will be

SELECT table\_name FROM INFORMATION\_SCHEMA.TABLES WHERE table\_type = ‘BASE TABLE’;

Let us check the request that have INFORMATION\_SCHEMA in their uri.



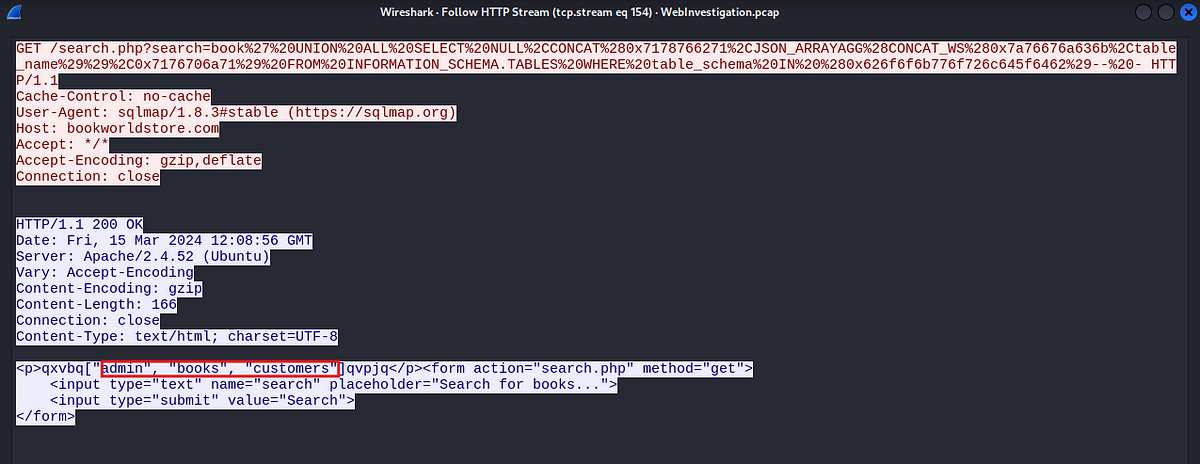
We can see above that we have 5 requests that contain “INFORMATION\_SCHEMA” in them. If we look for the responses of these requests, we can see that one of the requests actually got a response with the tables present in the database.



Answer: /search.php?search=book%27%20UNION%20ALL%20SELECT%20NULL%2CCONCAT%280x7178766271%2CJSON\_ARRAYAGG%28CONCAT\_WS%280x7a76676a636b%2Cschema\_name%29%29%2C0x7176706a71%29%20FROM%20INFORMATION\_SCHEMA.SCHEMATA — %20-

6. Assessing the impact of the breach and data access is crucial, including the potential harm to the organization’s reputation. What’s the table name containing the website users data?

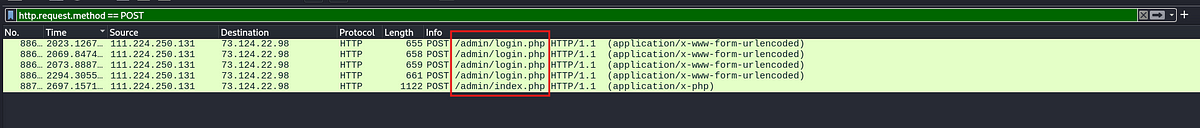
Let us check the response to the previous request. We got three tables admin, books, customers.



Answer: Customers

7. The website directories hidden from the public could serve as an unauthorized access point or contain sensitive functionalities not intended for public access. Can you provide the name of the directory discovered by the attacker?

Let us check for any post request made by the attacker.



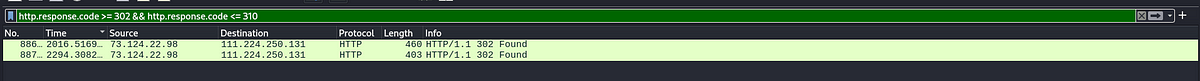
We can see above that the attacker has gained access to the admin login page.

Answer: /admin/

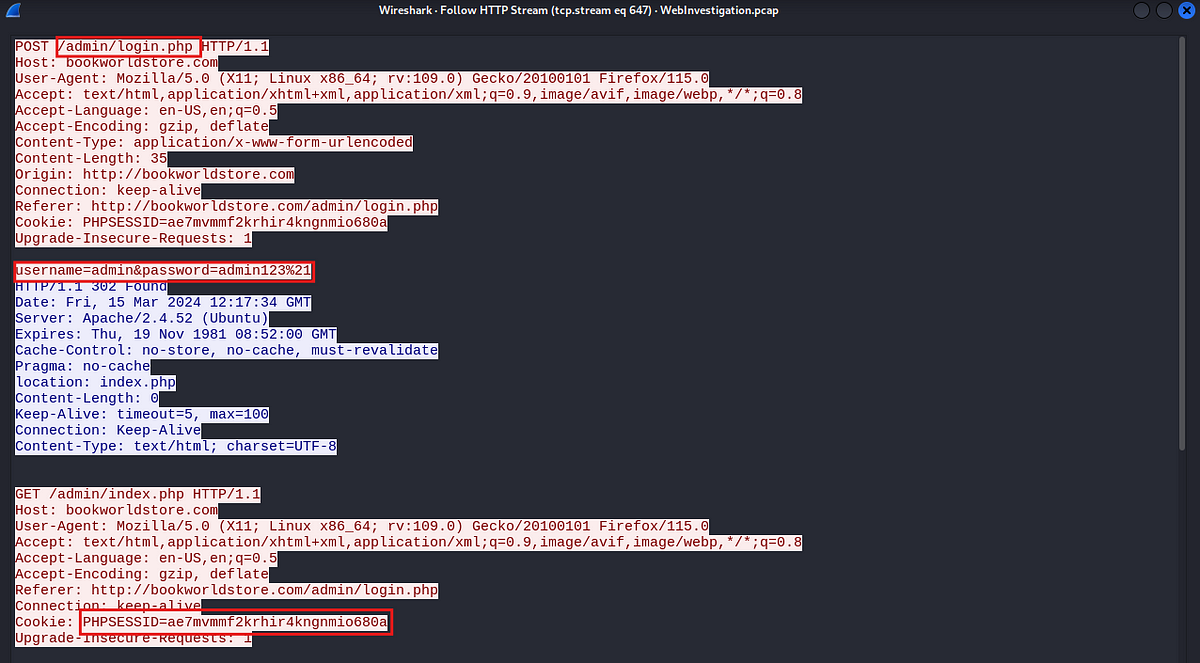
8. Knowing which credentials were used allows us to determine the extent of account compromise. What are the credentials used by the attacker for logging in?

I will usually check for any redirect codes to check for successful logins.

http.response.code ≥ 302 && http.response.code ≤ 310



We have only two packets with this code so it is easier to check if these were the successful logins from the attacker.



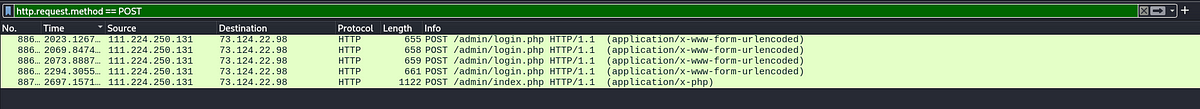
The second packet in the list was the successful login from the attacker. And we can see the username and password used which is admin:admin123!. In url encoding %21 translates to !.

Answer: admin:admin123!

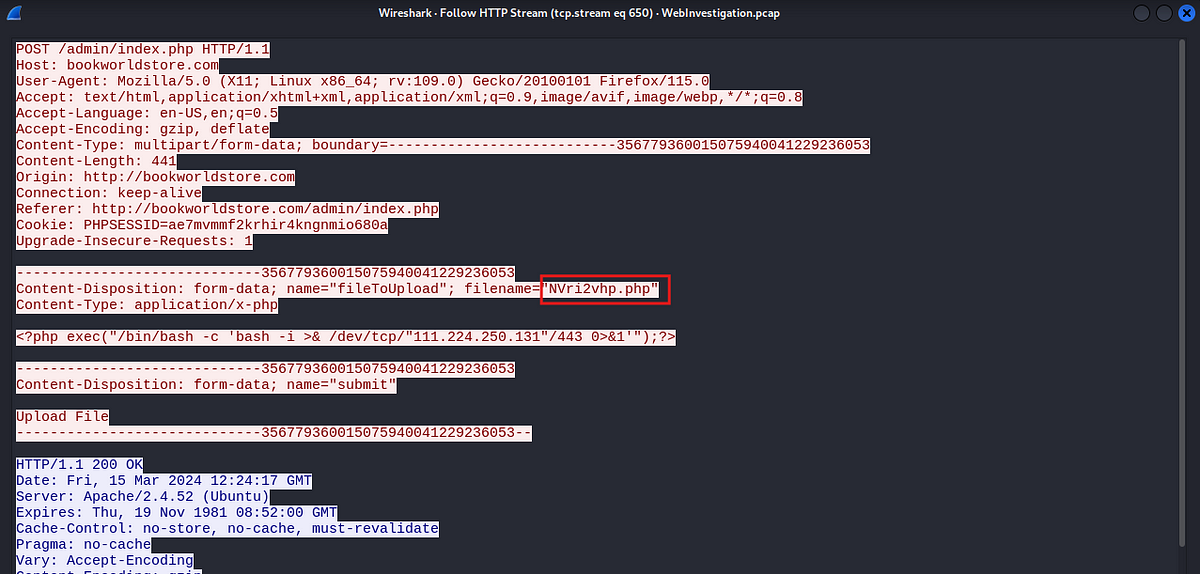
9. We need to determine if the attacker gained further access or control of our web server. What’s the name of the malicious script uploaded by the attacker?

Let us check for the POST requests from the attacker to see any malicious file uploads.

http.request.method == POST



The last packet has very high length, let us check the contents of this packet by following the HTTP stream.



It is indeed a file upload. We can see the contents of the file below the file name. By looking at the code it is clear that this is a reverse shell.

Answer: NVri2vhp.php

This is the end of the walkthrough.