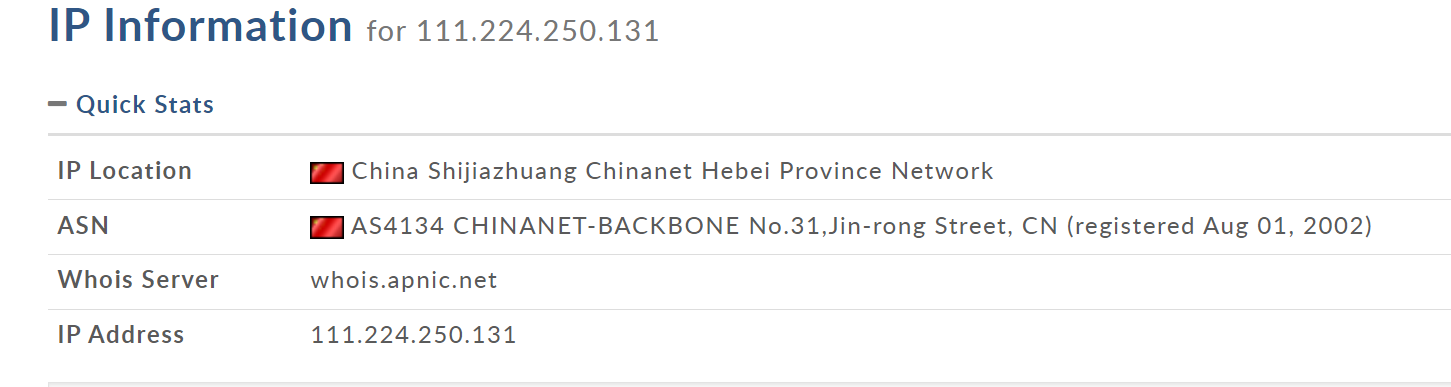
1. By knowing the attacker's IP, we can analyze all logs and actions related to that IP and determine the extent of the attack, the duration of the attack, and the techniques used. Can you provide the attacker's IP?

**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?

**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 script name?

**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?

**/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 available databases?

**/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?

**customers**



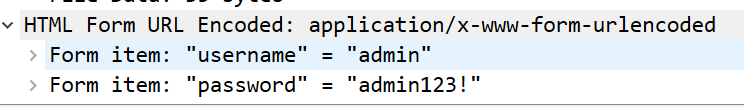
7. The website directories hidden from the public could serve as an unauthorized access point or contain sensitive functionalities not intended for public access. Can you provide name of the directory discovered by the attacker?

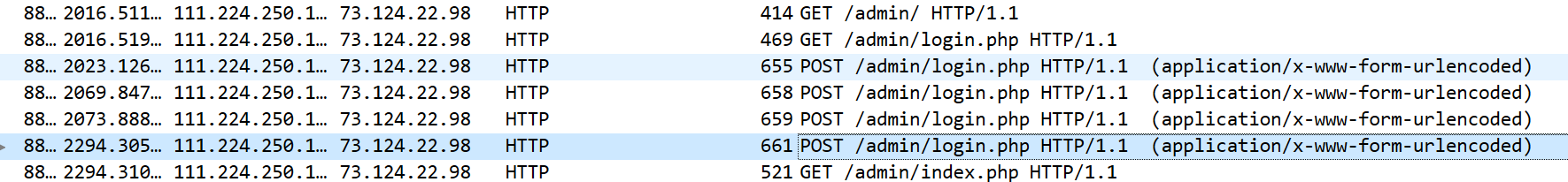
**/admin/**



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

**admin:admin123!**

****



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

**NVri2vhp.php**

