**Slingshot**

Can you retrace an attacker's steps after they enumerate and compromise a web server?

Task 1 Scenario

Slingway Inc., a leading toy company, has recently noticed suspicious activity on its e-commerce web server and potential modifications to its database. To investigate the suspicious activity, they've hired you as a SOC Analyst to look into the web server logs and uncover any instances of malicious activity.

To aid in your investigation, you've received an Elastic Stack instance containing logs from the suspected attack. Below, you'll find credentials to access the Kibana dashboard. Slingway's IT staff mentioned that the suspicious activity started on **July 26, 2023**.

By investigating and answering the questions below, we can create a timeline of events to lead the incident response activity. This will also allow us to present concise and confident findings that answer questions such as:

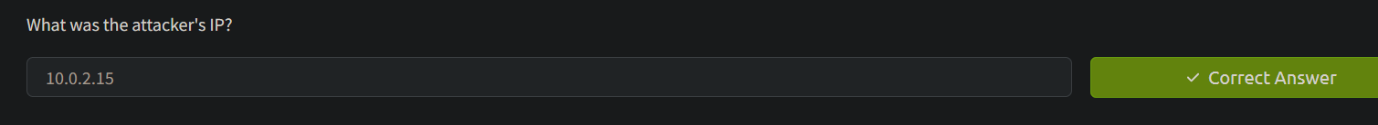
* What vulnerabilities did the attacker exploit on the web server?
* What user accounts were compromised?
* What data was exfiltrated from the server?

Instructions

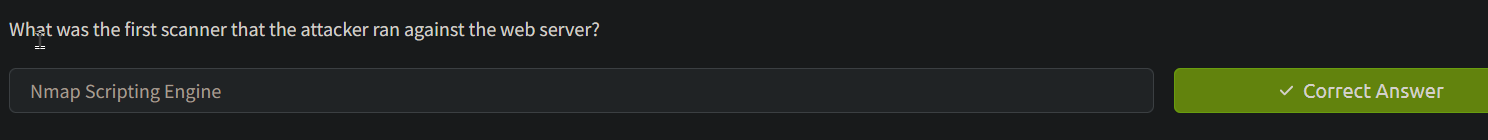
First, click **Start Machine** to start the VM attached to this task. You may access the VM using the AttackBox or your VPN connection. You can start the AttackBox by pressing the **Start AttackBox** button on the top-right of this room. **Note:** The Elastic Stack may take up to 5 minutes to fully start up. If you receive any errors, give it a few minutes and refresh the page.

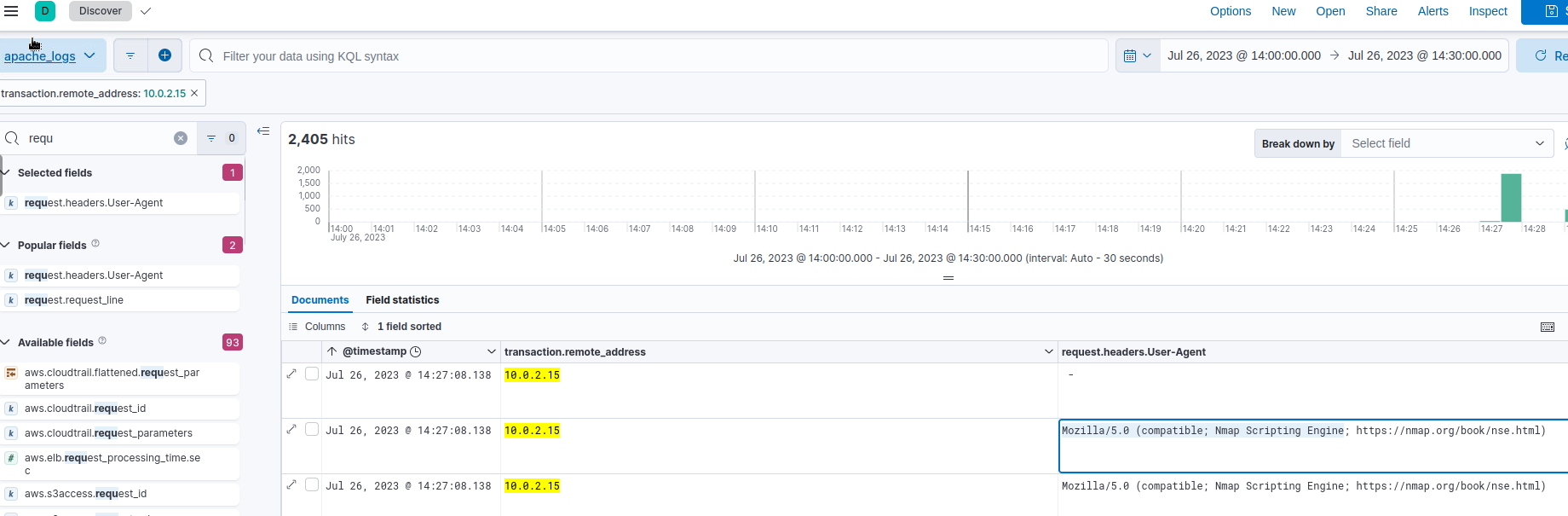
Once online, navigate to <ip>using a web browser.

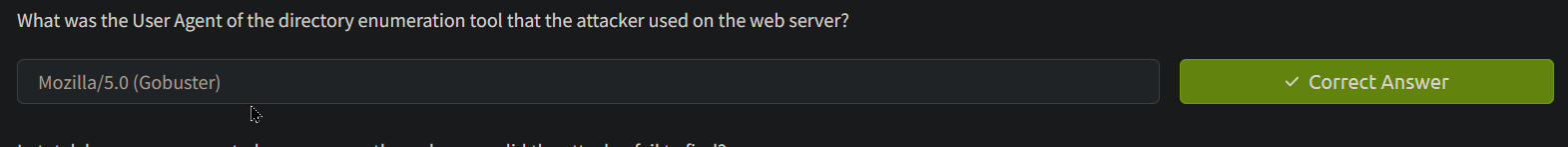
Answer the questions below:

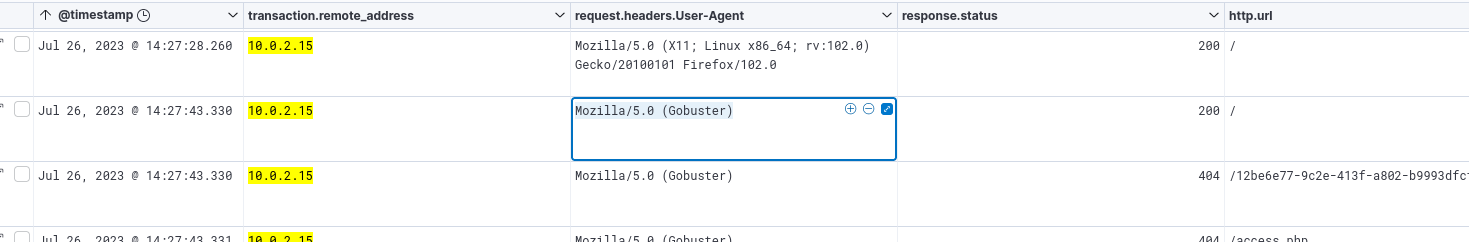


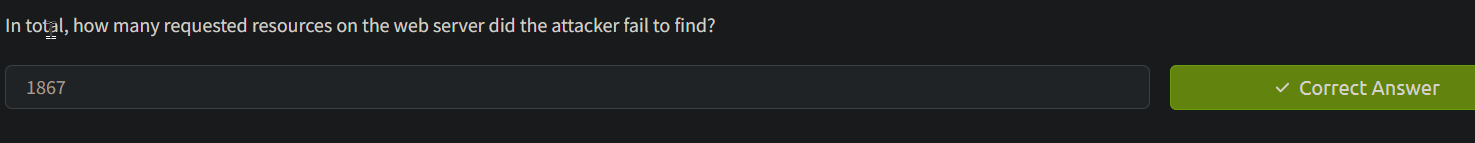
The amount of traffic is very unusual.

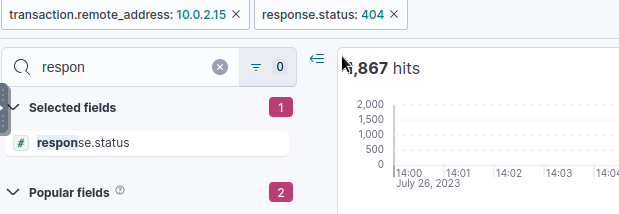


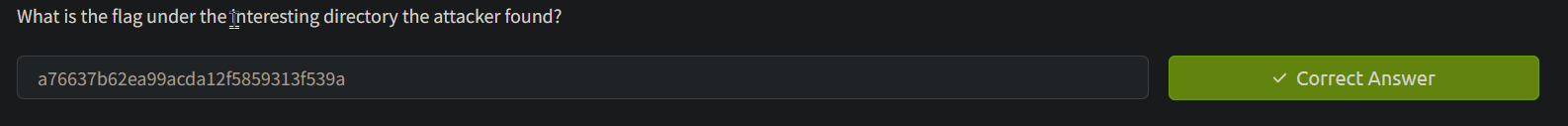


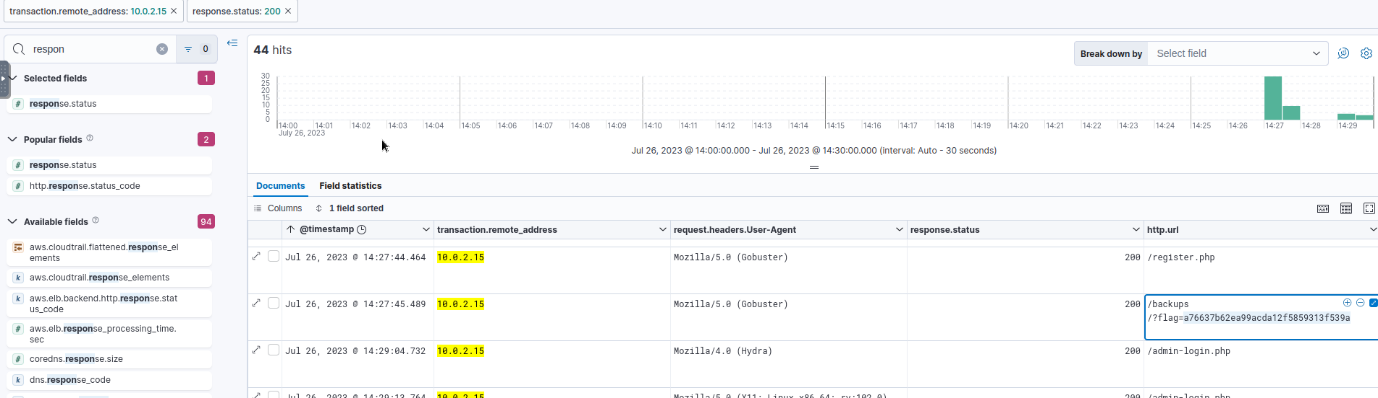


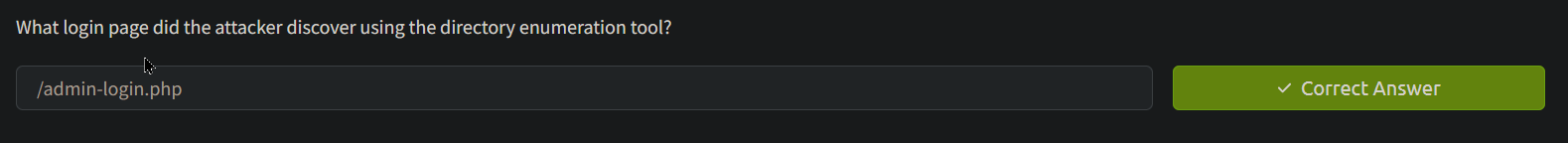




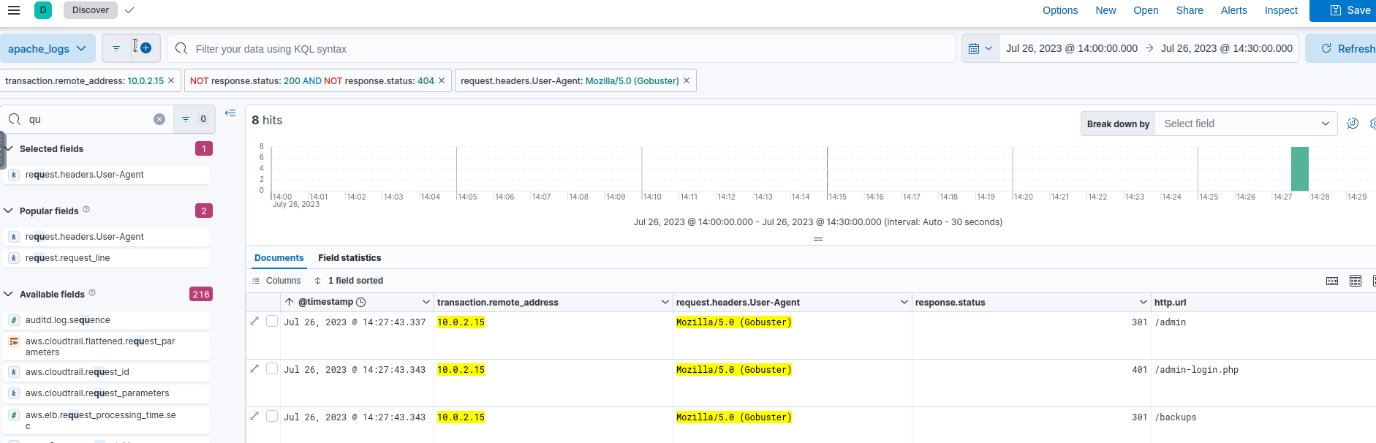


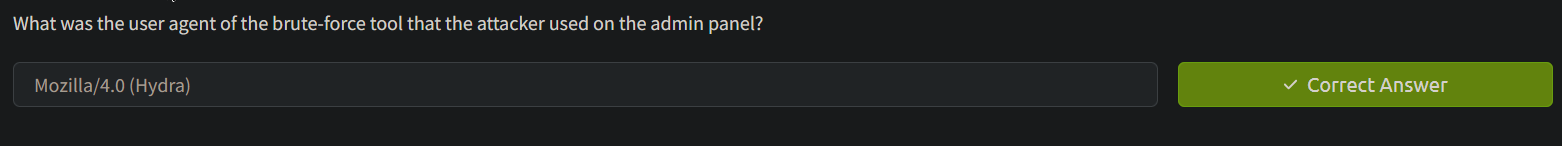




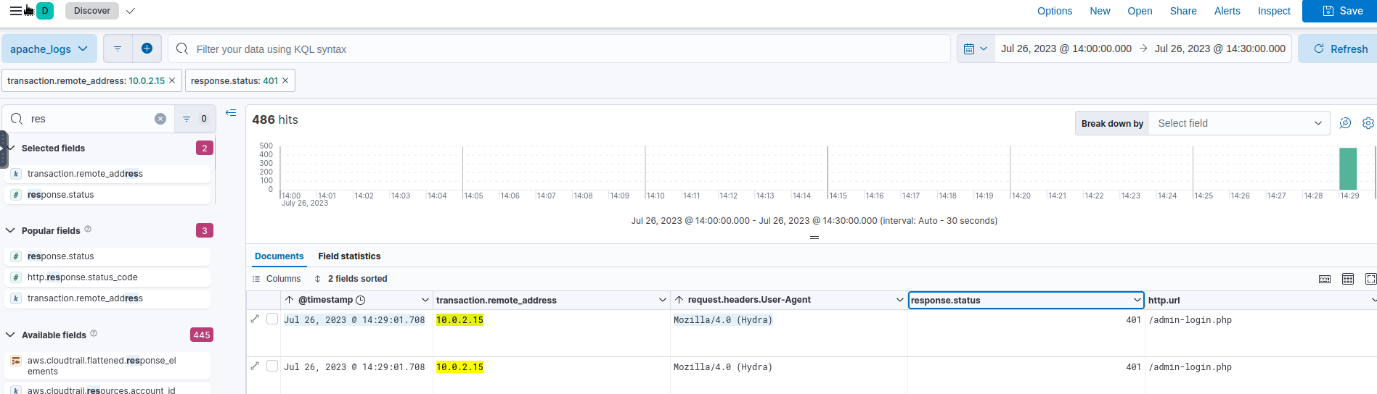


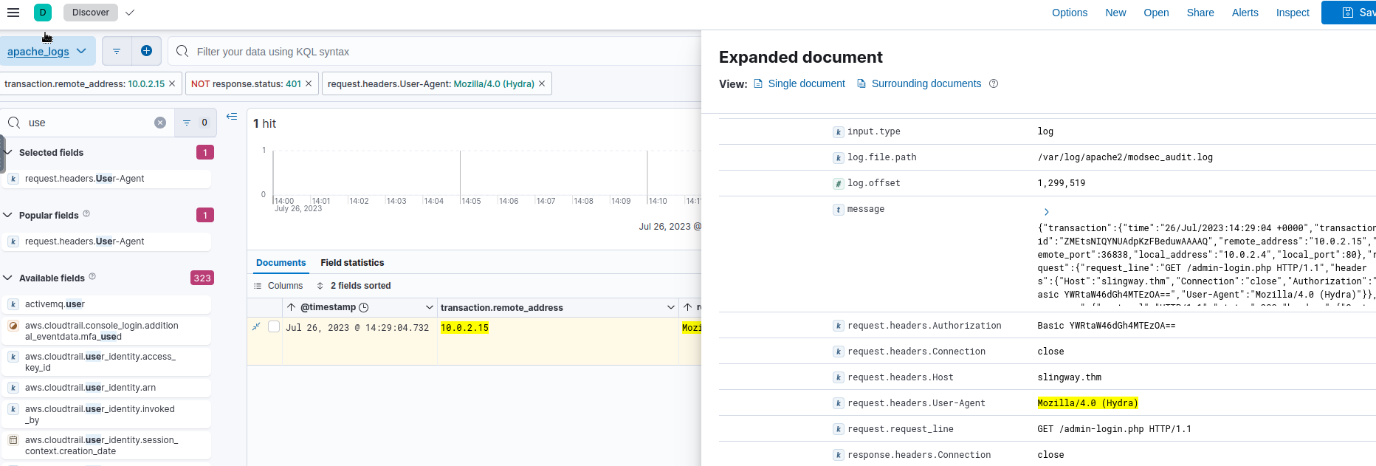
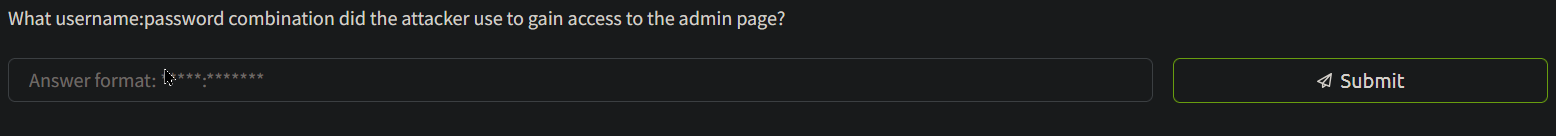
**/admin-login.php**





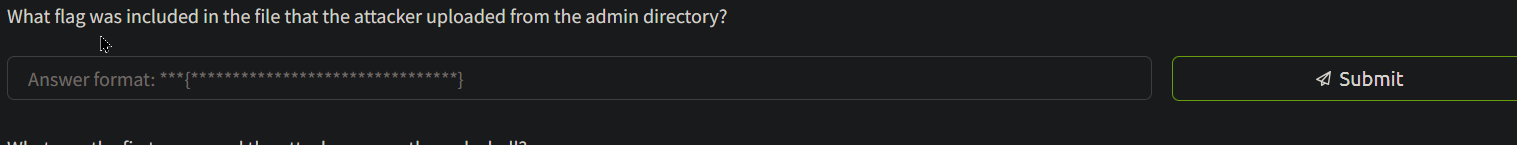
401= unauthorized



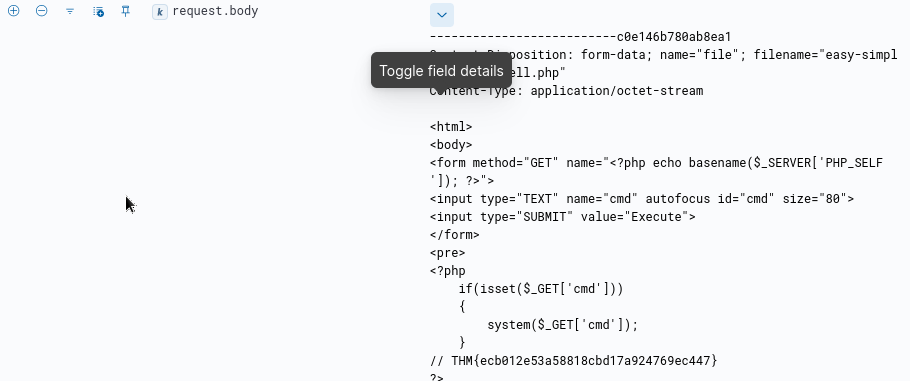


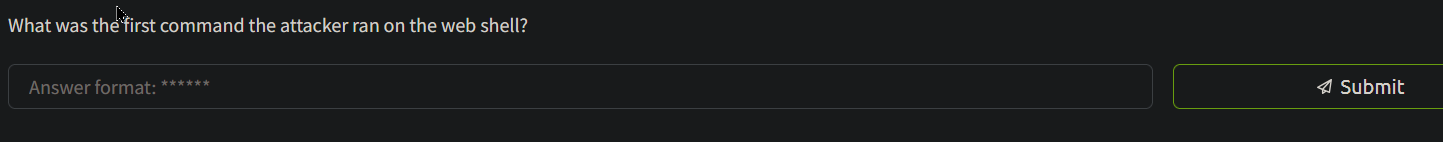
We got **YWRtaW46dGh4MTEzOA==**Which is **Base64 encoded**.

**admin:thx1138**

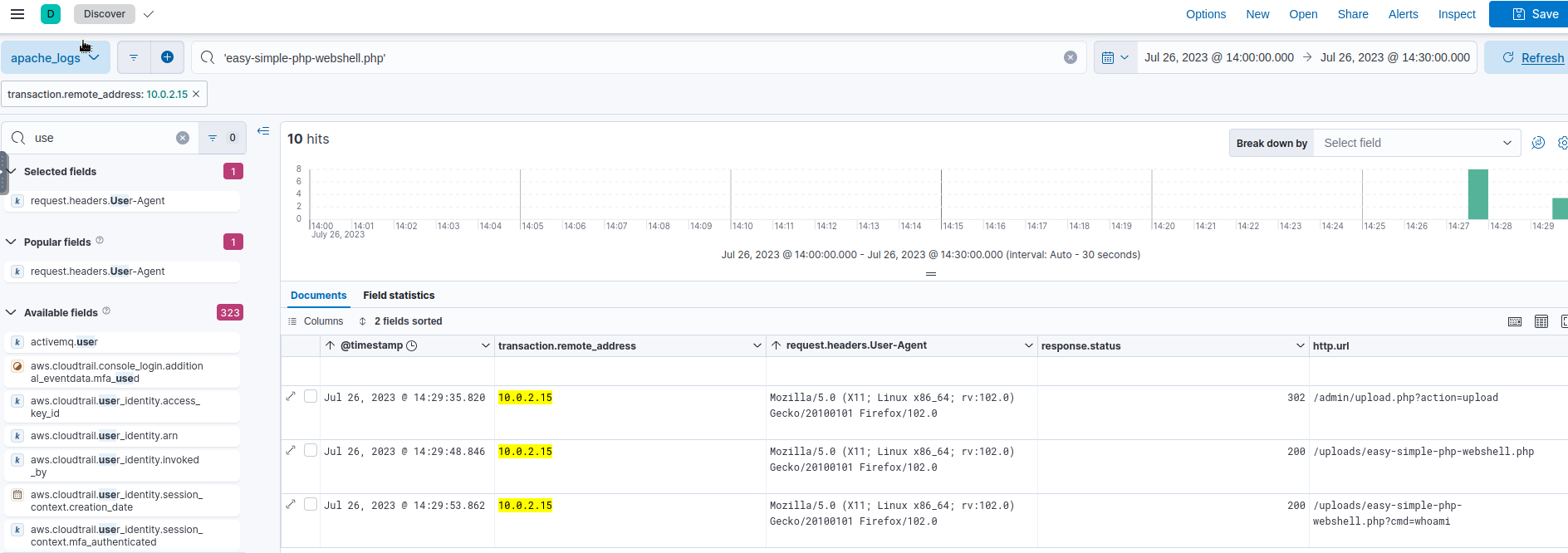
****

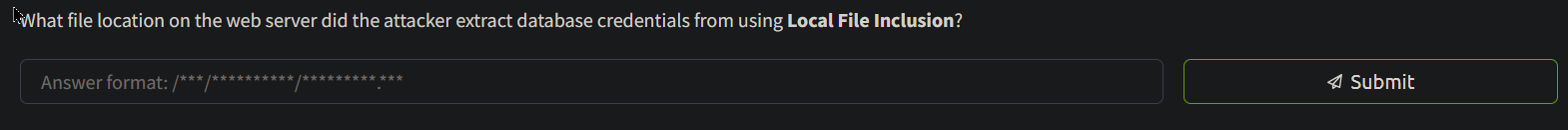


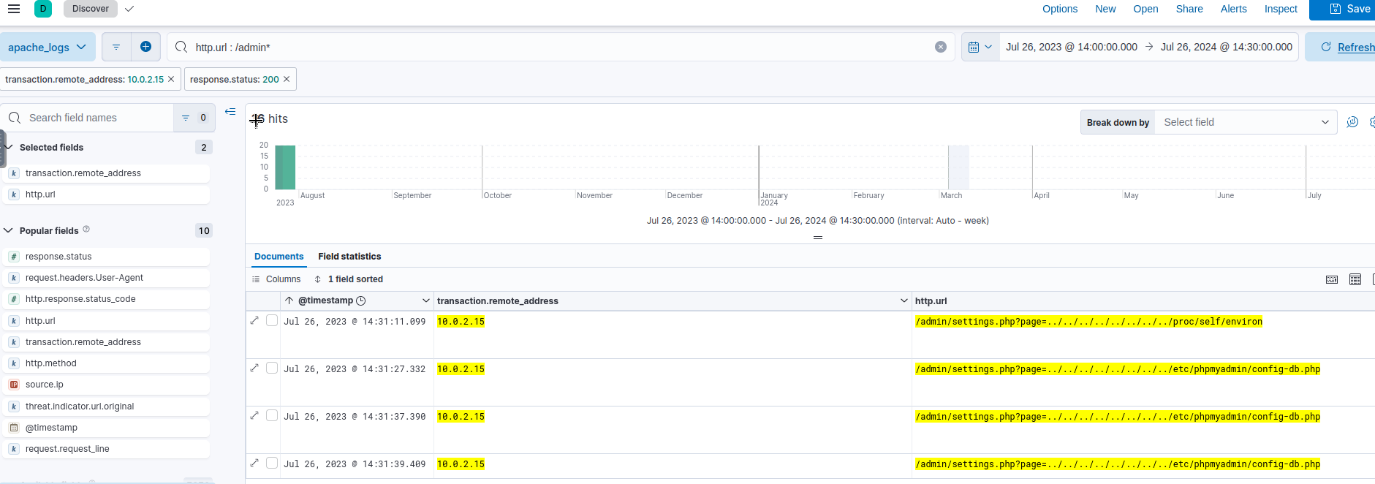


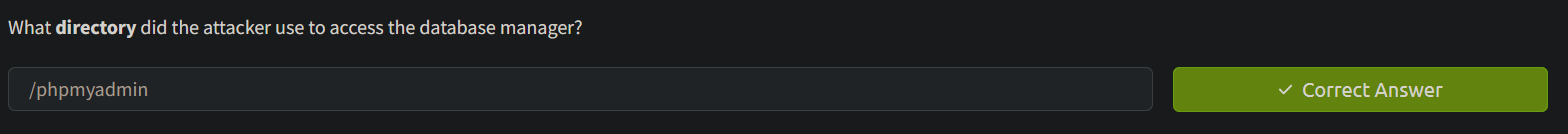




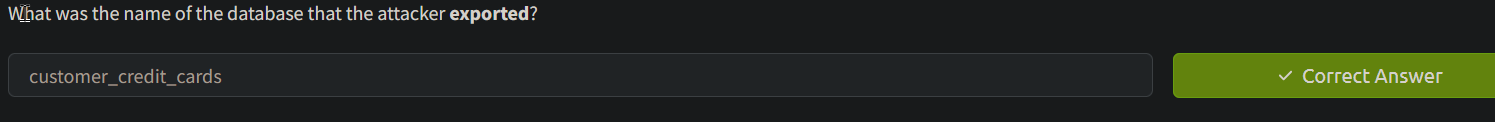




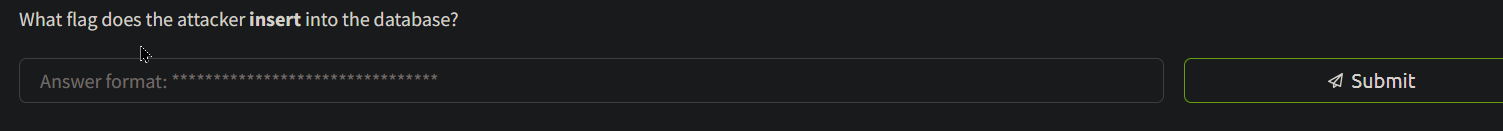




From the last answer.









Task 2Conclusion

After completing the log investigation, you can present confident findings that an attacker compromised the web server and database. You managed to follow the timeline of events, allowing for a clearer understanding of the incident and actions performed.

In response to this incident, Slingway Inc. should address the identified vulnerabilities promptly to enhance the security of its web server. Furthermore, the company should take appropriate steps to notify affected customers about the data breach and implement proactive security measures to mitigate future attacks.

Your investigation's comprehensive findings and actionable insights will enable Slingway Inc. to mitigate the damage caused by the compromised server, bolster its cyber security posture, and safeguard its customers' trust. Well done!