Q1

Understanding the geographical origin of the attack aids in geo-blocking measures and threat intelligence analysis. What city did the attack originate from?

**Tianjin**

Q2

Knowing the attacker's user-agent assists in creating robust filtering rules. What's the attacker's user agent?

**Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0**

Q3

We need to identify if there were potential vulnerabilities exploited. What's the name of the malicious web shell uploaded?

**image.jpg.php**

Q4

Knowing the directory where files uploaded are stored is important for reinforcing defenses against unauthorized access. Which directory is used by the website to store the uploaded files?

**/reviews/uploads/**

Q5

Identifying the port utilized by the web shell helps improve firewall configurations for blocking unauthorized outbound traffic. What port was used by the malicious web shell?

**8080**

Q6

Understanding the value of compromised data assists in prioritizing incident response actions. What file was the attacker trying to exfiltrate?

**passwd**