WebStrike lab- cyber defenders

Scenario

- A suspicious file was identified on a company web server, raising alarms within the intranet. The Development team flagged the anomaly, suspecting potential malicious activity. To address the issue, the network team captured critical network traffic and prepared a PCAP file for review. Your task is to analyze the provided PCAP file to uncover how the file appeared and determine the extent of any unauthorized activity.

PCAP File: WebStrike.pcap

Category: Network Forensics

Tool Used: Wireshark

Attack Type: Web Application Compromise

Q1. From which city did the attack originate?

Answer / Tianjin, China

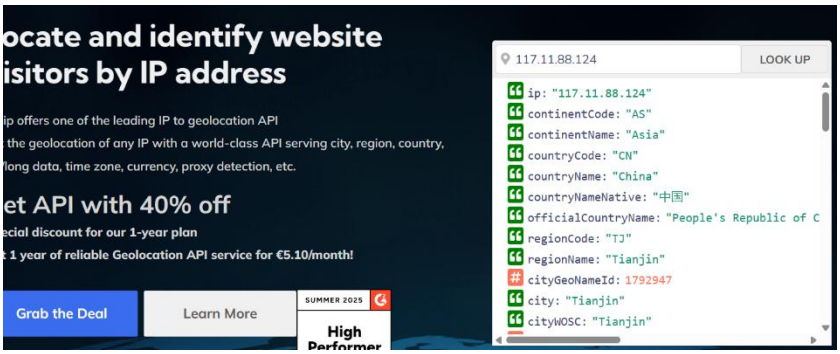
Investigation Steps

1. **Opened Statistics → Conversations → IPv4 in Wireshark.**
2. **Identified attacker IP generating the majority of traffic:**

117.11.88.124

3. **Used an external IP geolocation service outside the lab environment.**
4. **Geolocation results:**

- **Country: China**
- **City: Tianjin**

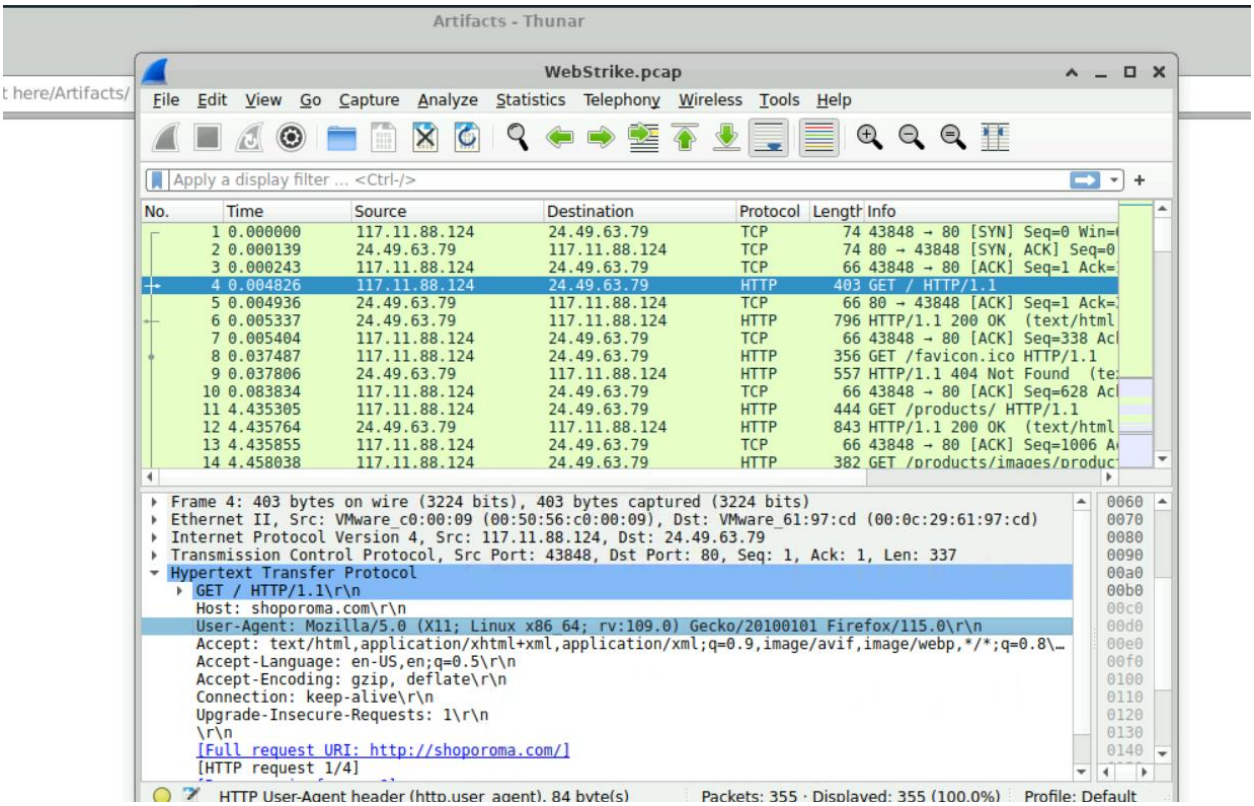


Q2. What is the attacker's full User-Agent?

Answer : Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

Investigation Steps

1. Selected HTTP GET packets in Wireshark.
2. Expanded **Hypertext Transfer Protocol** section.
3. Extracted the User-Agent header value from requests sent to the web server.



3. What malicious web shell was uploaded?

Answer/ image.jpg.php

Investigation Steps

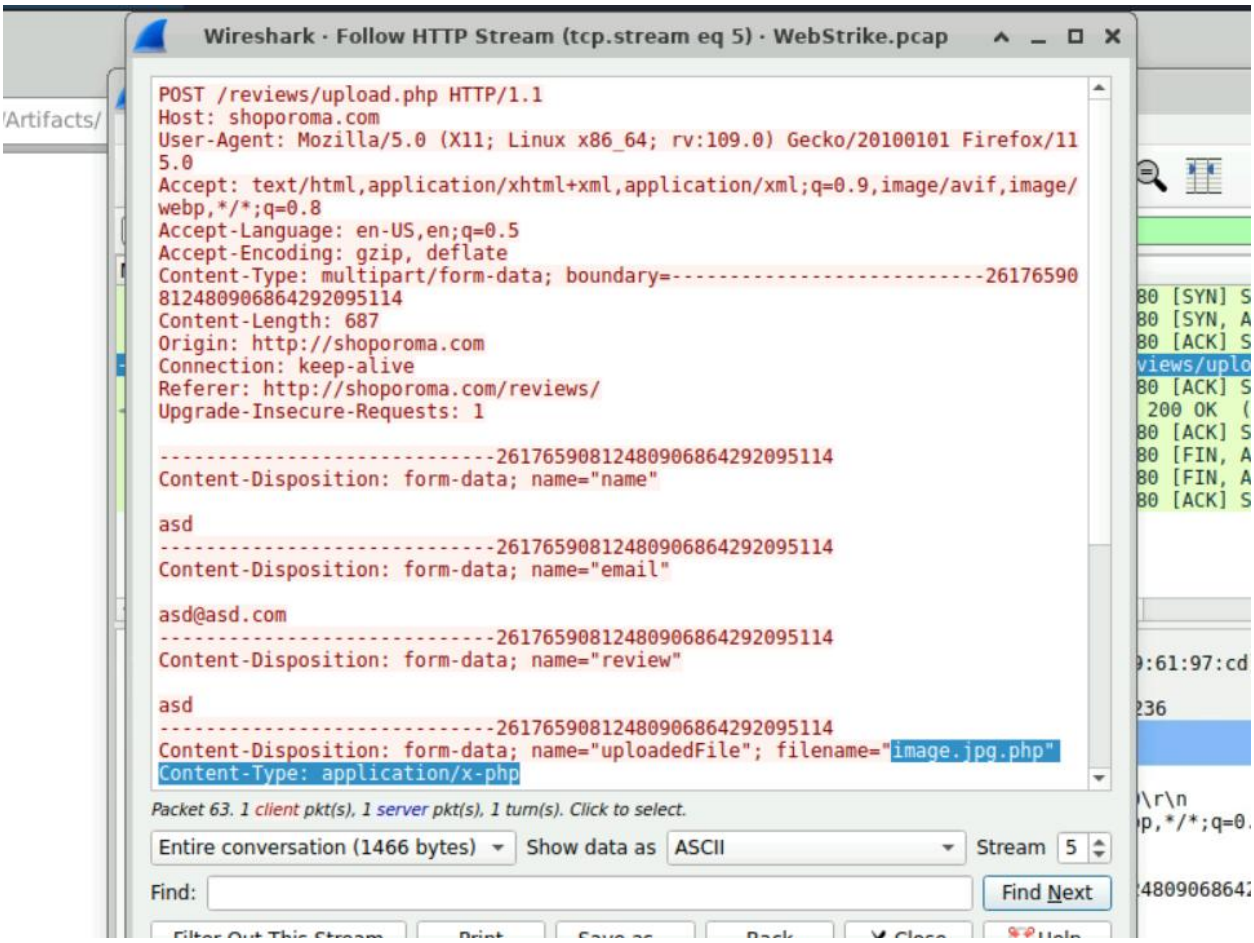
1. Applied Wireshark display filter:

http.request.method == "POST"

2.Followed the HTTP stream.

3. Observed uploaded file name:

File extension confirms PHP web shell disguised as an image.

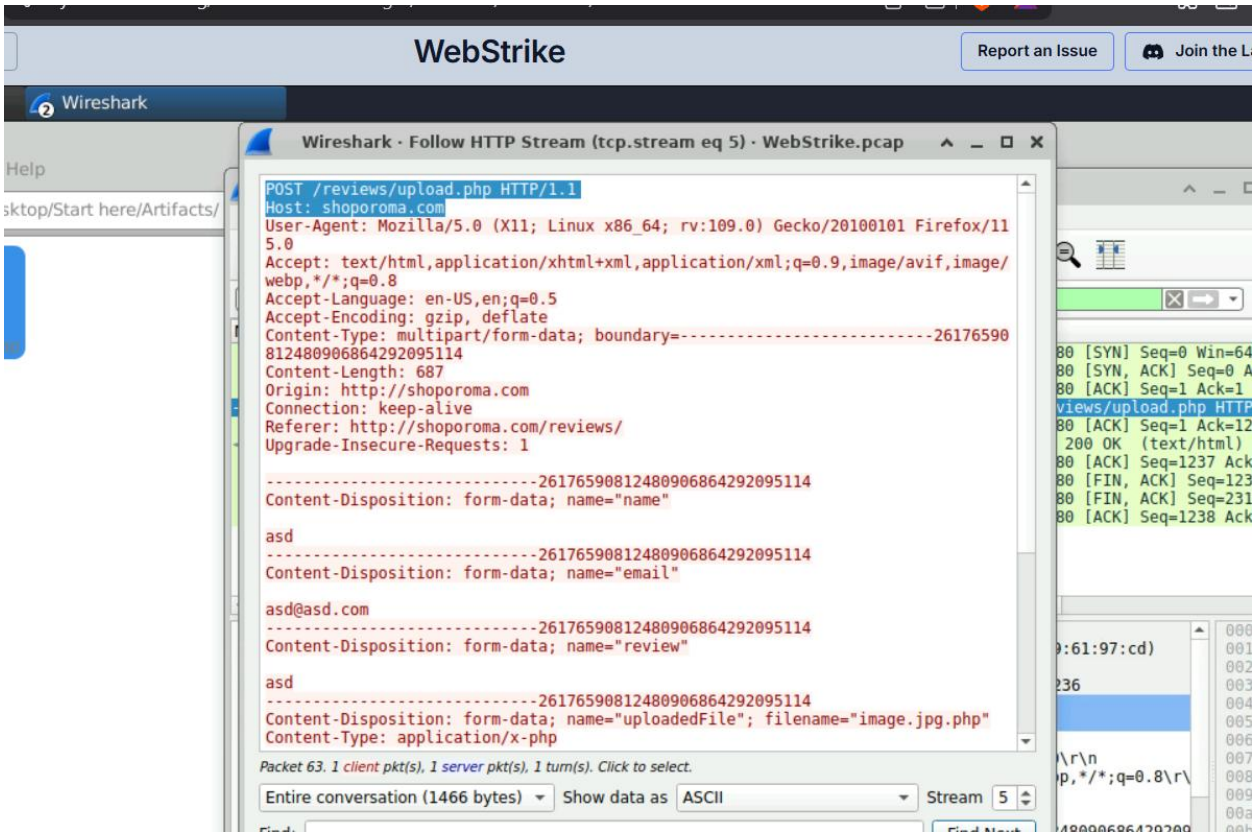


4. Which directory stores uploaded files?

Answer : /reviews/uploads/

Investigation Steps

1. Reviewed server responses after upload.
2. Observed execution path of the uploaded web shell.
3. Confirmed upload directory location within HTTP traffic.

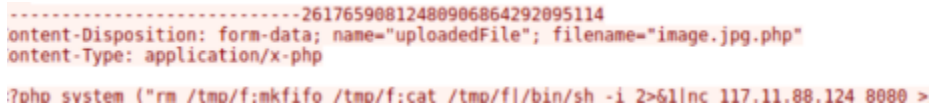


Q5. Which port on the attacker machine was targeted for outbound communication?

Answer/ 8080

Investigation Steps

1. Followed TCP stream after web shell execution.
2. Observed outbound connection attempts initiated by the compromised server.
3. Destination port identified as:8080



Q6. Which file was the attacker attempting to exfiltrate?

Answer: /etc/passwd

Investigation Steps

1. Followed interactive shell TCP stream.
2. Observed executed system commands.
3. Identified sensitive file access attempt:

Final Assessment

- **Incident Type:** Web Application Compromise
- **Root Cause:** Unrestricted file upload vulnerability
- **Impact:** Remote code execution and data exposure
- **Classification:** True Positive
- **Severity:** High