Incident Analysis Report: Web Server Compromise (WebStrike)

Date: January 31, 2026

Analyst: Mduduzi Radebe

Case ID: 2026-WS-001

Severity: High (Data Exfiltration Confirmed)

1. Executive Summary

On January 31, 2026, an investigation was conducted into a suspicious file upload on a company web server (24.49.63.79). The analysis confirmed that an external attacker (117.11.88.124) exploited a file upload vulnerability to deploy a PHP web shell. Following the compromise, the attacker established a reverse shell, performed system reconnaissance, and successfully exfiltrated the /etc/passwd file.

2. Technical Timeline & Findings

Time (UTC)	Event Type	Source IP	Destination IP	Description
T1	Initial Access	117.11.88.124	24.49.63.79	Malicious file image.jpg.php uploaded via /reviews/upload.php.
T2	Execution	117.11.88.124	24.49.63.79	Attacker triggered shell via GET request to /reviews/uploads/image.jpg.php.
T3	Persistence /C2	24.49.63.79	117.11.88.124	Reverse shell established on TCP Port 8080.

T4	Reconnaissance	24.49.63.79	117.11.88.124	Execution of whoami and uname -a commands.
T5	Exfiltration	24.49.63.79	117.11.88.124	/etc/passwd file exfiltrated via HTTP POST on Port 443.

3. Detailed Workflow & Methodology

Phase 1: Identification of Initial Access

To identify how the file arrived, I filtered for HTTP POST requests to find data being sent to the server.

- **Wireshark Filter:** http.request.method == "POST"
- **Observation:** I identified a POST request to /reviews/upload.php. Upon inspecting the **MIME Multipart Media**, I found the parameter filename="image.jpg.php". This indicates a bypass of file-extension filtering (Double Extension Attack).

Phase 2: Confirming Execution

I searched for the moment the attacker "activated" the uploaded script.

- **Wireshark Filter:** http.request.uri contains "image.jpg.php"
- **Observation:** A GET request (Packet 138) returned an **HTTP 200 OK**, confirming the web shell was successfully executed by the server.

Phase 3: Command and Control (C2) Analysis

Post-execution, I looked for non-standard traffic departing the server.

- **Wireshark Filter:** tcp.port == 8080
- **Action:** I utilized **Follow > TCP Stream**.
- **Findings:** The stream revealed a raw terminal session. The attacker was confirmed as the user www-data. I observed the attacker navigating the file system and reading the /etc/passwd file.

Phase 4: Data Exfiltration Discovery

I investigated how the stolen data left the network.

- **Wireshark Filter:** ip.dst == 117.11.88.124 && http.request.method == "POST"
- **Action:** Followed HTTP Stream on Port 443.
- **Findings:** I found a curl command exfiltrating the contents of /etc/passwd to the attacker's listener.

4. Forensic Evidence & Threat Intelligence

4.1 Attacker Attribution & Geolocation

A geolocation audit of the source IP (**117.11.88.124**) was conducted to identify the origin of the threat. The infrastructure is tied to **China Unicom (AS4837)**, specifically originating from **Tianjin, China**.

- **Significance:** Identifying the geographical origin allows for the implementation of geo-blocking at the firewall level to mitigate future reconnaissance from this specific backbone.

4.2 Adversary Fingerprinting (User-Agent Analysis)

By analyzing the `HTTP` header in Packet 53, the attacker's browser fingerprint was extracted.

- **Full User-Agent:** `Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0`
- **Analyst Note:** The use of a Linux-based Firefox agent suggests the attacker was likely utilizing a penetration testing distribution (e.g., Kali Linux). This fingerprint can be used to create WAF (Web Application Firewall) rules to flag similar session signatures.

4.3 Exploit Breakdown: Web Shell Deployment

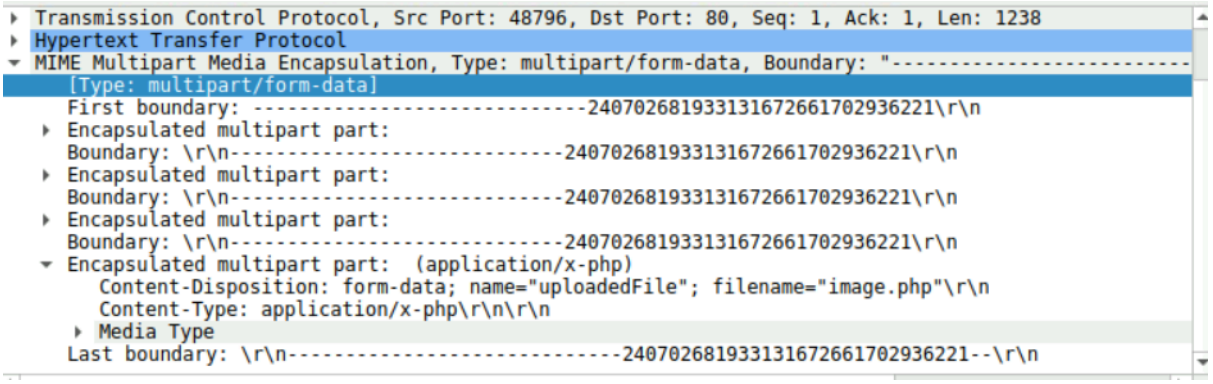
The investigation confirmed a successful **Broken Access Control** exploit on the `/reviews/upload.php` endpoint.

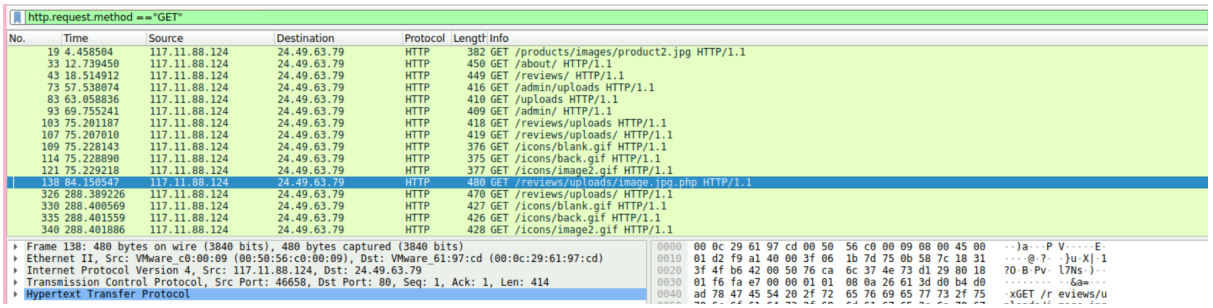
- **Malicious Payload:** `image.jpg.php`
- **Storage Directory:** `/reviews/uploads/`
- **Bypass Technique:** The attacker utilized a "Double Extension" bypass. The server was configured to trust the `.jpg` prefix but failed to sanitize the final `.php` suffix, allowing the server's engine to execute the script rather than treating it as a static image.

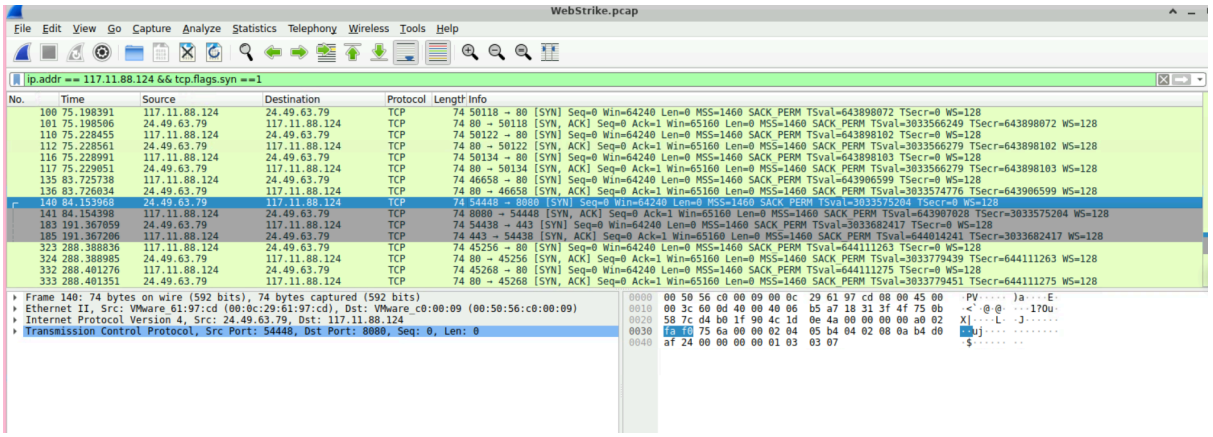
4.4 Command & Control (C2) Identification

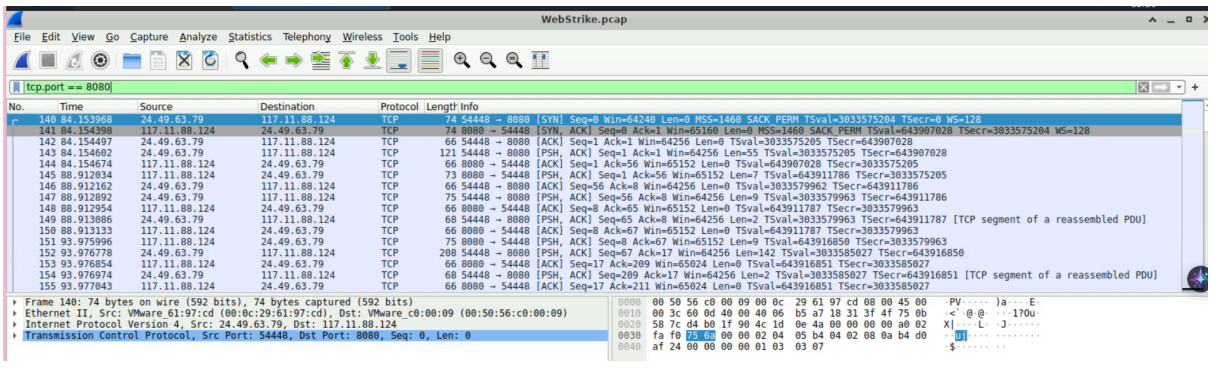
Immediately following the execution of the web shell (Packet 138), the server initiated a **SYN** packet to the attacker's IP.

- **C2 Callback Port:** `8080` (TCP)
- **Protocol:** Raw TCP (Reverse Shell)
- **Exfiltrated Target:** `/etc/passwd`
- **Exfiltration Method:** Data was tunneled out via an unencrypted `HTTP POST` request to the attacker's listener on port `443`.


Transmission Control Protocol, Src Port: 48796, Dst Port: 80, Seq: 1, Ack: 1, Len: 1238
Hypertext Transfer Protocol
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "--------------------------
[Type: multipart/form-data]
First boundary: ----------------------------240702681933131672661702936221\r\n
Encapsulated multipart part:
Boundary: \r\n----------------------------240702681933131672661702936221\r\n
Encapsulated multipart part:
Boundary: \r\n----------------------------240702681933131672661702936221\r\n
Encapsulated multipart part:
Boundary: \r\n----------------------------240702681933131672661702936221\r\n
Encapsulated multipart part: (application/x-php)
Content-Disposition: form-data; name="uploadedFile"; filename="image.php"\r\n
Content-Type: application/x-php\r\n\r\n
Media Type
Last boundary: \r\n----------------------------240702681933131672661702936221--\r\n


http.request.method =="GET"
No. Time Source Destination Protocol Length Info
19 4.458504 117.11.88.124 24.49.63.79 HTTP 382 GET /products/images/product2.jpg HTTP/1.1
33 12.739450 117.11.88.124 24.49.63.79 HTTP 450 GET /about/ HTTP/1.1
43 18.514912 117.11.88.124 24.49.63.79 HTTP 449 GET /reviews/ HTTP/1.1
73 57.538074 117.11.88.124 24.49.63.79 HTTP 416 GET /admin/uploads HTTP/1.1
83 63.058836 117.11.88.124 24.49.63.79 HTTP 410 GET /uploads HTTP/1.1
93 69.755241 117.11.88.124 24.49.63.79 HTTP 409 GET /admin/ HTTP/1.1
103 75.201187 117.11.88.124 24.49.63.79 HTTP 418 GET /reviews/uploads HTTP/1.1
107 75.207010 117.11.88.124 24.49.63.79 HTTP 419 GET /reviews/uploads/ HTTP/1.1
109 75.228143 117.11.88.124 24.49.63.79 HTTP 376 GET /icons/blank.gif HTTP/1.1
114 75.228890 117.11.88.124 24.49.63.79 HTTP 375 GET /icons/back.gif HTTP/1.1
121 75.229218 117.11.88.124 24.49.63.79 HTTP 377 GET /icons/image2.gif HTTP/1.1
138 84.150547 117.11.88.124 24.49.63.79 HTTP 480 GET /reviews/uploads/image.jpg.php HTTP/1.1
326 288.389226 117.11.88.124 24.49.63.79 HTTP 470 GET /reviews/uploads/ HTTP/1.1
330 288.400569 117.11.88.124 24.49.63.79 HTTP 427 GET /icons/blank.gif HTTP/1.1
335 288.401559 117.11.88.124 24.49.63.79 HTTP 426 GET /icons/back.gif HTTP/1.1
340 288.401886 117.11.88.124 24.49.63.79 HTTP 428 GET /icons/image2.gif HTTP/1.1
Frame 138: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits)
Ethernet II, Src: VMware_c0:00:09 (00:50:56:c0:00:09), Dst: VMware_61:97:cd (00:0c:29:61:97:cd)
Internet Protocol Version 4, Src: 117.11.88.124, Dst: 24.49.63.79
Transmission Control Protocol, Src Port: 46658, Dst Port: 80, Seq: 1, Ack: 1, Len: 414
Hypertext Transfer Protocol


WebStrike.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 117.11.88.124 && tcp.flags.syn ==1
No. Time Source Destination Protocol Length Info
100 75.198391 117.11.88.124 24.49.63.79 TCP 74 50118 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=643898072 TSecr=0 WS=128
101 75.198506 24.49.63.79 117.11.88.124 TCP 74 80 → 50118 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3033566249 TSecr=643898072 WS=128
110 75.228455 117.11.88.124 24.49.63.79 TCP 74 50122 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=643898102 TSecr=0 WS=128
112 75.228561 24.49.63.79 117.11.88.124 TCP 74 80 → 50122 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3033566279 TSecr=643898102 WS=128
116 75.228991 117.11.88.124 24.49.63.79 TCP 74 50134 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=643898103 TSecr=0 WS=128
117 75.229051 24.49.63.79 117.11.88.124 TCP 74 80 → 50134 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3033566279 TSecr=643898103 WS=128
135 83.725738 117.11.88.124 24.49.63.79 TCP 74 46658 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=643906599 TSecr=0 WS=128
136 83.726034 24.49.63.79 117.11.88.124 TCP 74 80 → 46658 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3033574776 TSecr=643906599 WS=128
140 84.153968 24.49.63.79 117.11.88.124 TCP 74 54448 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3033575204 TSecr=0 WS=128
141 84.154398 117.11.88.124 24.49.63.79 TCP 74 8080 → 54448 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=643907028 TSecr=3033575204 WS=128
183 191.367059 24.49.63.79 117.11.88.124 TCP 74 54438 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3033682417 TSecr=0 WS=128
185 191.367206 117.11.88.124 24.49.63.79 TCP 74 443 → 54438 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=644014241 TSecr=3033682417 WS=128
323 288.388836 117.11.88.124 24.49.63.79 TCP 74 45256 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=644111263 TSecr=0 WS=128
324 288.388985 24.49.63.79 117.11.88.124 TCP 74 80 → 45256 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3033779439 TSecr=644111263 WS=128
332 288.401276 117.11.88.124 24.49.63.79 TCP 74 45268 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=644111275 TSecr=0 WS=128
333 288.401351 24.49.63.79 117.11.88.124 TCP 74 80 → 45268 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3033779451 TSecr=644111275 WS=128
Frame 140: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: VMware_61:97:cd (00:0c:29:61:97:cd), Dst: VMware_c0:00:09 (00:50:56:c0:00:09)
Internet Protocol Version 4, Src: 24.49.63.79, Dst: 117.11.88.124
Transmission Control Protocol, Src Port: 54448, Dst Port: 8080, Seq: 0, Len: 0


WebStrike.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 8080
No. Time Source Destination Protocol Length Info
140 84.153968 24.49.63.79 117.11.88.124 TCP 74 54448 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3033575204 TSecr=0 WS=128
141 84.154398 117.11.88.124 24.49.63.79 TCP 74 8080 → 54448 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=643907028 TSecr=3033575204 WS=128
142 84.154497 24.49.63.79 117.11.88.124 TCP 66 54448 → 8080 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3033575205 TSecr=643907028
143 84.154602 24.49.63.79 117.11.88.124 TCP 121 54448 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=55 TSval=3033575205 TSecr=643907028
144 84.154674 117.11.88.124 24.49.63.79 TCP 66 8080 → 54448 [ACK] Seq=1 Ack=56 Win=65152 Len=0 TSval=643907028 TSecr=3033575205
145 88.912034 117.11.88.124 24.49.63.79 TCP 73 8080 → 54448 [PSH, ACK] Seq=1 Ack=56 Win=65152 Len=7 TSval=643911786 TSecr=3033575205
146 88.912162 24.49.63.79 117.11.88.124 TCP 66 54448 → 8080 [ACK] Seq=56 Ack=8 Win=64256 Len=0 TSval=3033579962 TSecr=643911786
147 88.912892 24.49.63.79 117.11.88.124 TCP 75 54448 → 8080 [PSH, ACK] Seq=56 Ack=8 Win=64256 Len=9 TSval=3033579963 TSecr=643911786
148 88.912954 117.11.88.124 24.49.63.79 TCP 66 8080 → 54448 [ACK] Seq=8 Ack=65 Win=65152 Len=0 TSval=643911787 TSecr=3033579963
149 88.913086 24.49.63.79 117.11.88.124 TCP 68 54448 → 8080 [PSH, ACK] Seq=65 Ack=8 Win=64256 Len=2 TSval=3033579963 TSecr=643911787 [TCP segment of a reassembled PDU]
150 88.913133 117.11.88.124 24.49.63.79 TCP 66 8080 → 54448 [ACK] Seq=8 Ack=67 Win=65152 Len=0 TSval=643911787 TSecr=3033579963
151 93.975996 117.11.88.124 24.49.63.79 TCP 75 8080 → 54448 [PSH, ACK] Seq=8 Ack=67 Win=65152 Len=9 TSval=643916850 TSecr=3033579963
152 93.976778 24.49.63.79 117.11.88.124 TCP 208 54448 → 8080 [PSH, ACK] Seq=67 Ack=17 Win=64256 Len=142 TSval=3033585027 TSecr=643916850
153 93.976854 117.11.88.124 24.49.63.79 TCP 66 8080 → 54448 [ACK] Seq=17 Ack=209 Win=65024 Len=0 TSval=643916851 TSecr=3033585027
154 93.976974 24.49.63.79 117.11.88.124 TCP 68 54448 → 8080 [PSH, ACK] Seq=209 Ack=17 Win=64256 Len=2 TSval=3033585027 TSecr=643916851 [TCP segment of a reassembled PDU]
155 93.977043 117.11.88.124 24.49.63.79 TCP 66 8080 → 54448 [ACK] Seq=17 Ack=211 Win=65024 Len=0 TSval=643916851 TSecr=3033585027
Frame 140: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: VMware_61:97:cd (00:0c:29:61:97:cd), Dst: VMware_c0:00:09 (00:50:56:c0:00:09)
Internet Protocol Version 4, Src: 24.49.63.79, Dst: 117.11.88.124
Transmission Control Protocol, Src Port: 54448, Dst Port: 8080, Seq: 0, Len: 0

```
/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 18:01:13 UTC 2 x86_64 x86_64 x86_64 GN
U/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:/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
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
```

---

5. Indicators of Compromise (IoCs)

(Keep your existing table here, it's great!)

4. Indicators of Compromise (IoCs)

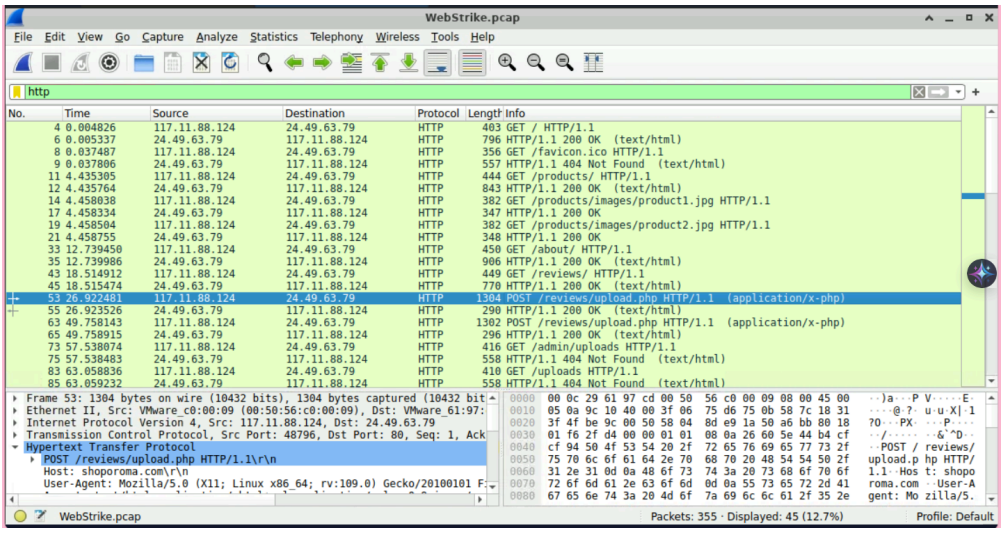
Type	Value	Description
IP Address	117.11.88.124	Attacker Command & Control Server
Filename	image.jpg.php	Malicious PHP Web Shell
URL Path	/reviews/uploads/	Unauthorized File Storage Path
Port	8080	Reverse Shell Listener Port
User Agent	Mozilla/5.0...Firefox/115.0	Attacker Browser Fingerprint

5. Recommendations (Remediation)

1. **Immediate Action:** Block the Attacker IP (117.11.88.124) at the edge firewall.
2. **Short-term:** Implement strict file-upload validation. Files should be renamed upon upload, and extensions should be validated against a whitelist (e.g., only .jpg, .png).
3. **Long-term:** Disable execution permissions on the /uploads/ directory (e.g., using .htaccess or server config) to prevent scripts from running even if uploaded.
4. **Security Monitoring:** Configure SIEM alerts for any outbound traffic from web servers on non-standard ports (like 8080).

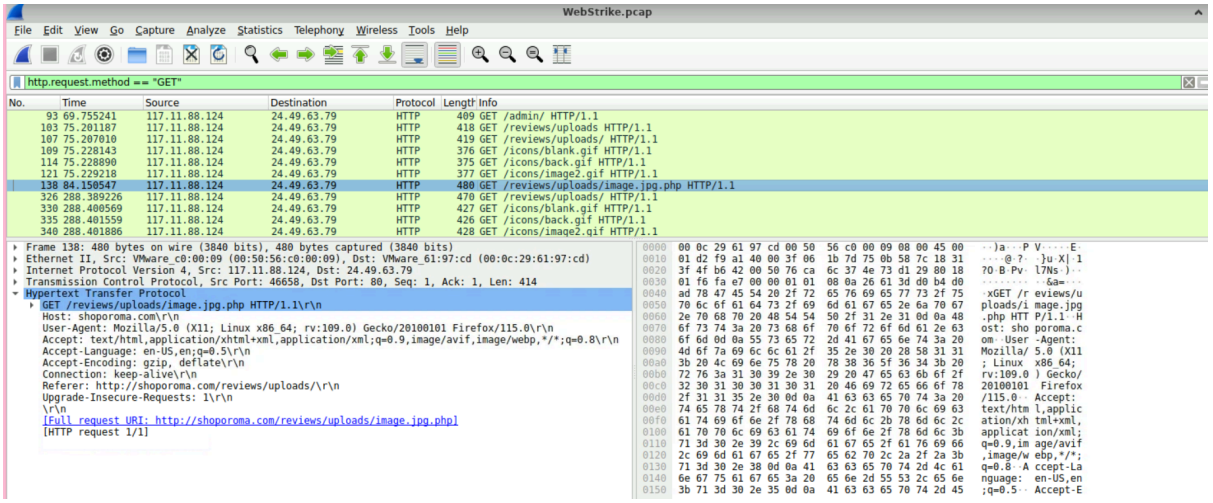
Screenshots :

Delivery" phase of the attack.

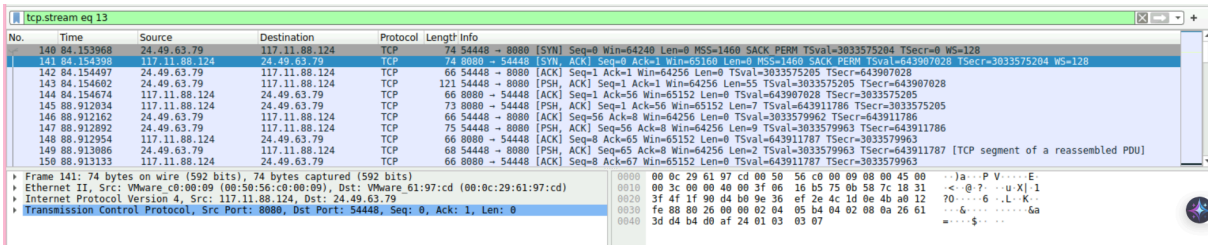


Finding the Execution Request

`http.request.method == "GET"`



Searching for traffic going **from** the server (`24.49.63.79`) **to** the attacker (`117.11.88.124`) on a non-web port.



`ip.addr == 117.11.88.124 && tcp.port != 80`.