

08/04/2024
MONDAY

DAY - 7

Don't judge a Book by

PATH TRAVERSAL [File inclusion] its cover.

→ Cyber Chef

* Base64 algorithm - Encoder Not a Hash.

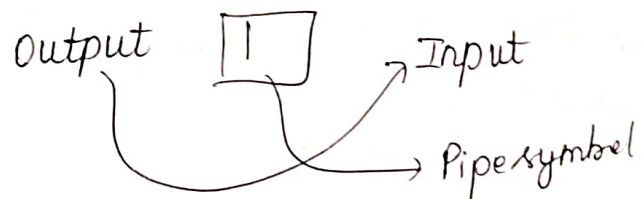
→ etc/passwd - Contains username

bin/bash - terminal

filename = .../etc/passwd #HTTP/2

→ Book hack tricks - guide.

cmd: cat /etc/passwd | grep /bin/bash
/zsh



&& → Compare both side Content and it's independent.

mkdir MKCE && cd MKCE && touch test

* Within single line multiple Commands can be Combined together.

File Upload

web shell - Browser

Bind shell - process, service, port Combine

Reverse shell - User interaction.

Raw shell. Com

cmd : nc -lvp 8080
netcraft

Arduino {
MID
USB

* Bat, ps1, exe.

Accessing terminal through kali

* Antivirus
* Antimalware }

→ Top view (System internals)

→ Process utilities - Process explorer.

_____ x _____
File upload
vulnerability. } Cable changed as command
line injection.

* Vulnerability Combining -

→ Content-type validation

_____ x _____ x _____
Cross site scripting.

→ cloudflare - WAF

→ Cookie - stealer

→ Canary tokens Tracking purpose (7)

→ URL shortener.