SIMULAZIONE FASE DI RACCOLTA

Report di Giuseppe Gigliotti

Target:

- epicode.com

Strumenti o Tool utilizzati:

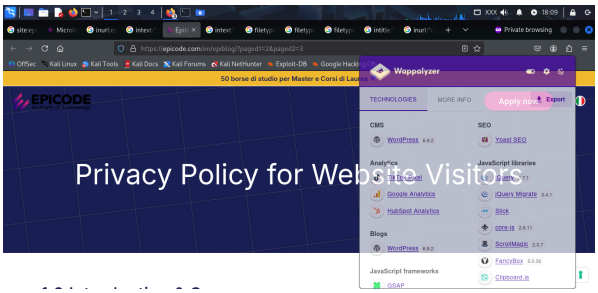
- Google Hacking (dal sito: https://www.exploit-db.com/google-hacking-database)

FALCOLTATIVO:

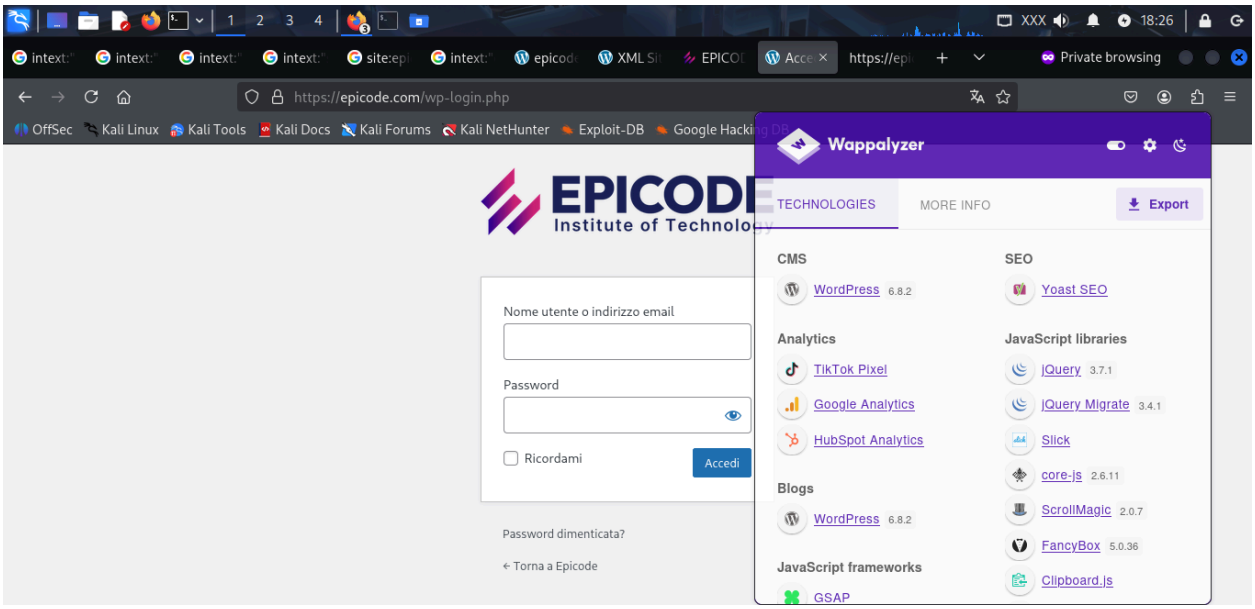
- Maltego
- Recon-ng (alternative Whois & subfinder)

Google Hacking

Usando i vari comandi di Google Hacking per la raccolta di informazioni (alcuni già indicati nella traccia dell'esercizio) sul sito target epicode.com, siamo riusciti a risalire a vari sottodomini del sito, uno in particolare era Epiblog - EPICODE Institute of Technology , che una volta analizzato con gli strumenti in nostro possesso sul browser firefox ci riporta alle informazioni che il sito è gestito con **Wordpress** quindi per conoscenze sul web scopriamo che a un file di default di nome robots.txt. Quindi avendo questa informazione possiamo andare sull'url del nostro sito target ed aggiungiamo il percorso /robots.txt (url completo: epicode.com/robots.txt) , questo non permette di trovare informazioni rilevanti utilizzando i google dorks, ma in esso possiamo trovare anche una sitemap del nostro target (url completo: https://epicode.com/sitemap_index.xml) . Di seguito possiamo trovare gli screenshot delle dei vari siti trovati in questa prima fase di ricognizione.



N.B. dalla sitemap possiamo arrivare a raggiungere anche una pagina di login.php



FACOLTATIVO:

Recon-ng:

Utilizzando il tool recon-ng e ricordando che il nostro target non permette di trovare informazioni rilevanti tramite il file robots.txt, saltiamo direttamente la possibilità di usare il modulo di ricerca di google e passiamo all'utilizzo.

- con il comando (il modulo è già stato installato in precedenza), facciamo una scansione del nostro target e dei suoi sottodomini.

```
[recon-ng][epicode] > modules load recon/domains-hosts/brute_hosts
# usando il comando info possiamo vedere che questo modulo esegue un atta
cco
# di brute forces sui nomi host utilizzando il DNS.
# Aggiorna la tabella hosts con i risultati
recon-ng][epicode][brute_hosts] > options
Manages the current context options

Usage: options <list|set|unset> [...]

[recon-ng][epicode][brute_hosts] > options list

  Name      Current Value                    Required  Description
  --------  -------------                    --------  -----------
  SOURCE    epicode.com                         yes       source of input (see 'info' f
or details)
  WORDLIST  /home/kali/.recon-ng/data/hostnames.txt  yes       path to hostna
me wordlist

[recon-ng][epicode][brute_hosts] > run
```

- L’output:

```
EPICODE.COM
-----------
"
"
```

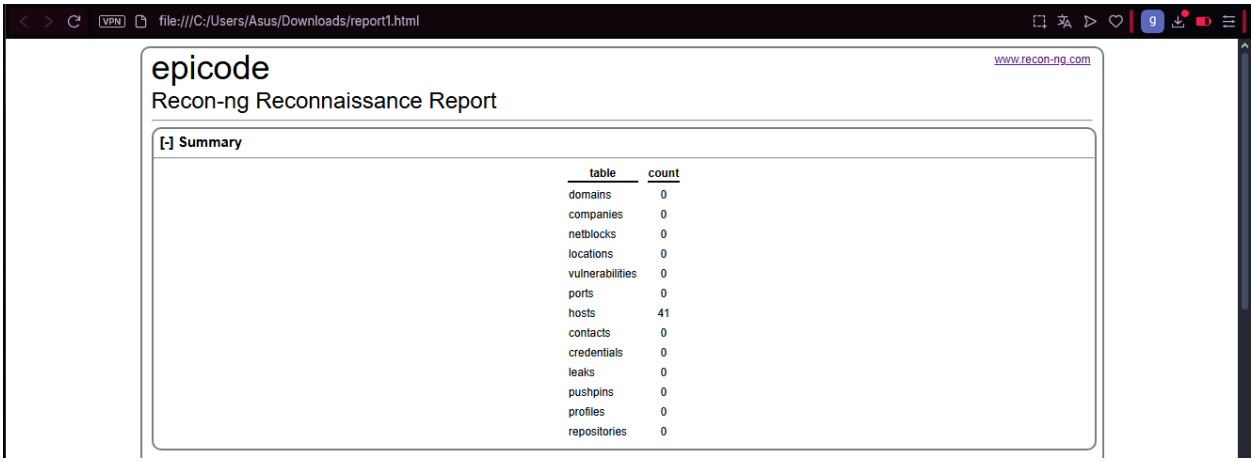
```
"
"
"
"


-------
SUMMARY
-------
[*] 36 total (4 new) hosts found.
```

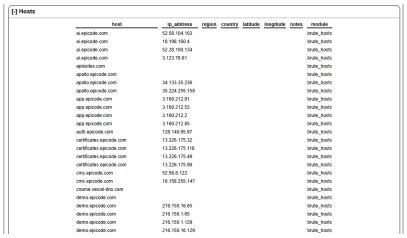
- Per creare un report dei risultati utilizziamo il modulo (già installato) :

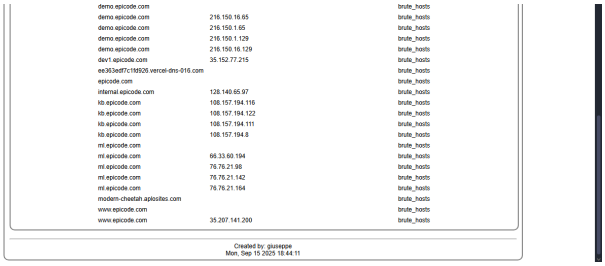
```
[recon-ng][epicode] > modules load reporting/html
[recon-ng][epicode][html] > info

      Name: HTML Report Generator
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Creates an HTML report.

Options:
  Name      Current Value           Required  Description
  --------  -------------          --------  -----------
  CREATOR   giuseppe                yes       use creator name in the report footer
  CUSTOMER  epicode                 yes       use customer name in the report hea
der
  FILENAME  /home/kali/report1.html  yes       path and filename for report outp
ut
  SANITIZE  True                    yes       mask sensitive data in the report

[recon-ng][epicode][html] > options list
```

```
  Name      Current Value          Required  Description
  --------  -------------          --------  -----------
  CREATOR   giuseppe               yes       use creator name in the report footer
  CUSTOMER  epicode                yes       use customer name in the report hea
der
  FILENAME  /home/kali/report1.html  yes       path and filename for report outp
ut
  SANITIZE  True                   yes       mask sensitive data in the report

[recon-ng][epicode][html] > run
[*] Report generated at '/home/kali/report1.html'.
```

Lascio in basso gli screen del report (che sarà lasciato completo nella repository)







Maltego: