# SIMULAZIONE FASE DI RACCOLTA

Report a cura di Valentino Pizzi

**Obbiettivo:**

- epicode.com

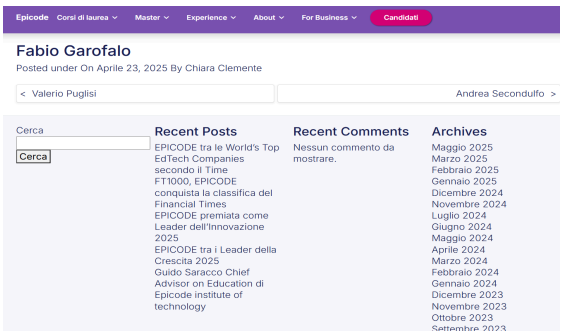
**Contenuti:**

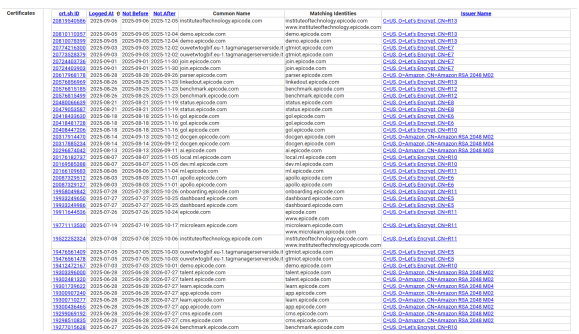
- Google Hacking
- Maltego Hacking
- Whois command line & subfinder

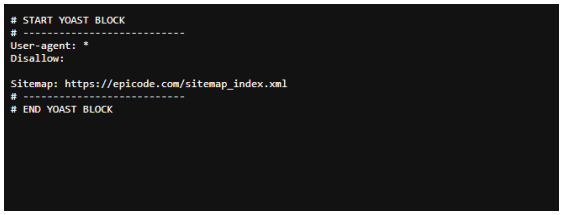
---

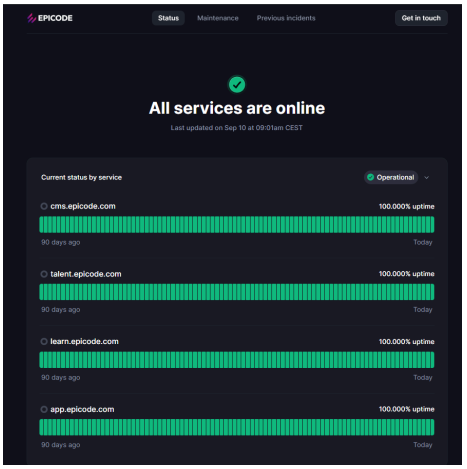
- Google Hacking

Utilizzando vari comandi di Google Hacking per la raccolta di informazioni rilevanti riguardanti il sito epicode.com siamo riusciti a risalire a vari sottodomini del sito, ai docenti, a robots.txt che non permette di trovare informazioni rilevanti utilizzando i google dorks, ed alla pagina dello status dei server epicode. Di seguito trovate screenshot dei documenti trovati in questa prima fase di ricognizione.



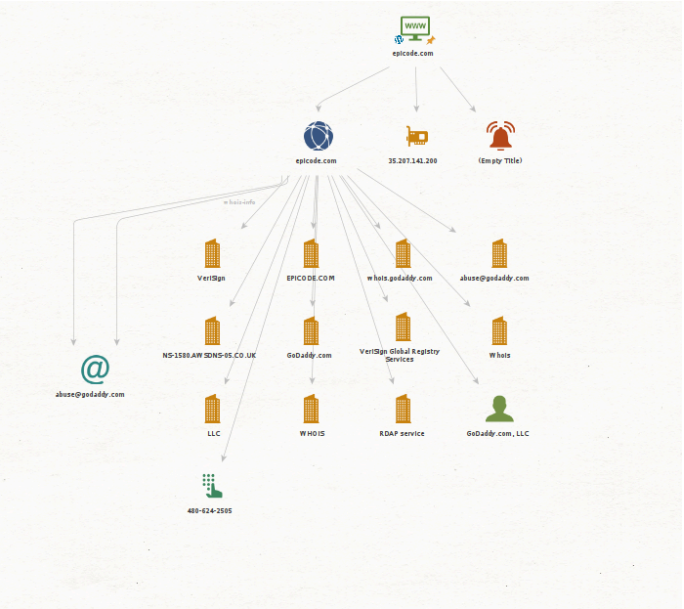




Utilizzando altri comandi di google hacking, come “typefile:pdf site:epicode.com” siamo riusciti a risalire ad alcuni certificati rilasciati a studenti della piattaforma, scaricabili in formato pdf, probabilmente modificabili con photoshop e riutilizzabili.

---

- Maltego Hacking

In questa fase di ricognizione, abbiamo sfruttato la piattaforma Maltego per cercare informazioni che ancora non siamo riusciti a reperire, ad esempio un indirizzo IP, su che piattaforma e' il sito, email collegate.
Di seguito screenshot di Maltego




Grazie a Maltego abbiamo recuperato informazioni come indirizzo IP della macchina Host, alcuni sottodomini attivi, l'hosting di 'godaddy', un numero di telefono e una mail dell'hosting.

---

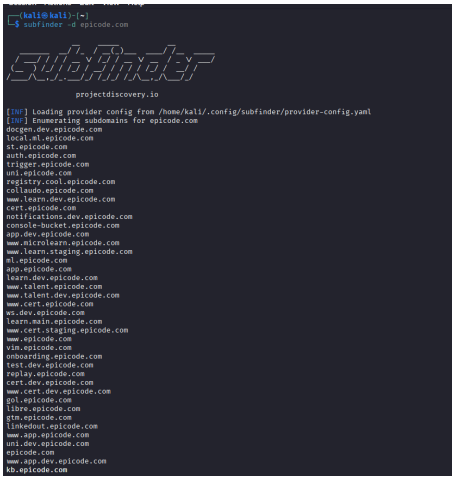
- Whois command line & subfinder

Usiamo infine il nostro terminale utilizzando la riga di comando "whois" per avere informazioni ed incrociarle con cio' che abbiamo gia' trovato per avere un quadro piu' completo.

```
┌──(kali㉿kali)-[~]
└─$ whois epicode.com
   Domain Name: EPICODE.COM
   Registry Domain ID: 26700881_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2023-05-13T05:04:09Z
   Creation Date: 2000-05-09T18:57:38Z
   Registry Expiry Date: 2031-05-09T18:57:38Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS-1492.AWSDNS-58.ORG
   Name Server: NS-1580.AWSDNS-05.CO.UK
   Name Server: NS-198.AWSDNS-24.COM
   Name Server: NS-953.AWSDNS-55.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-09-10T07:12:35Z <<<
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: epicode.com
Registry Domain ID: 26700881_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2022-12-09T12:09:46Z
Creation Date: 2000-05-09T13:57:38Z
Registrar Registration Expiration Date: 2031-05-09T13:57:38Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 100 S. Mill Ave, Suite 1600
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85281
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: https://www.godaddy.com/whois/results.aspx?domain=epicode.com&action=contactDomainOwner
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 100 S. Mill Ave, Suite 1600
Tech City: Tempe
Tech State/Province: Arizona
Tech Postal Code: 85281
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: https://www.godaddy.com/whois/results.aspx?domain=epicode.com&action=contactDomainOwner
Name Server: NS-198.AWSDNS-24.COM
Name Server: NS-953.AWSDNS-55.NET
Name Server: NS-1492.AWSDNS-58.ORG
Name Server: NS-1580.AWSDNS-05.CO.UK
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2025-09-10T07:12:48Z <<<
```

Passiamo ora a “subfinder” per cercare altri sottodomini che possono esserci sfuggiti




---

- Conclusioni

Per via di “robots.txt” i google dorks non hanno la possibilita’ di trovare vulnerabilita’ o informazioni troppo rilevanti, pero’ grazie a  “Maltego” e “Whois” invece siamo riusciti a scovare indirizzi mail, sottodomini, Hosting, indirizzo IP, numero di telefono, tutte informazioni del perimetro di epicode.com