

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.

Epicode
Corsi di laurea
Master
Experience
About
For Business
Candidati

Fabio Garofalo

Posted under On April 23, 2025 By Chiara Clemente

< Valerio Puglisi

Andrea Secondullo >

Cerca

Cerca

Recent Posts

Epicode tra la World's Top EdTech Companies secondo il Time FT1000, EPICODE conquista la classifica del Financial Times

Epicode premiata come Leader dell'Innovazione 2025

Epicode tra i Leader della Crescita 2025

Guido Saracco Chief Advisor on Education di Epicode Institute of technology

Recent Comments

Nessun commento da mostrare.

Archives

Maggio 2025

Marzo 2025

Febbraio 2025

Gennaio 2025

Dicembre 2024

Novembre 2024

Luglio 2024

Giugno 2024

Maggio 2024

Aprile 2024

Marzo 2024

Febbraio 2024

Gennaio 2024

Dicembre 2023

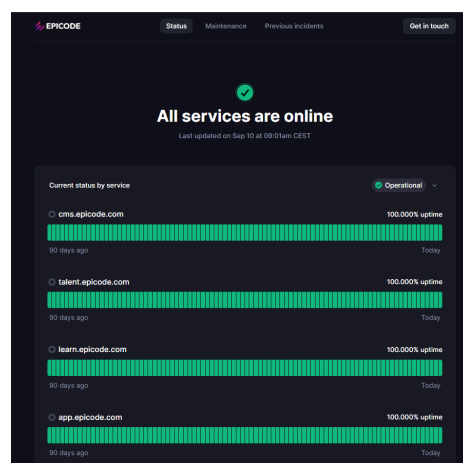
Novembre 2023

Ottobre 2023

[illegible]

```
# START YOAST BLOCK
# -----
User-agent: *
Disallow:

Sitemap: https://epicode.com/sitemap_index.xml
# -----
# END YOAST BLOCK
```

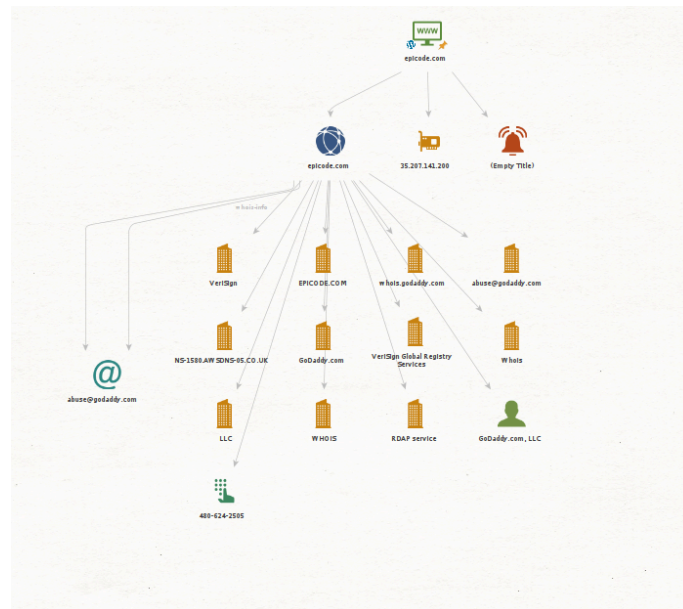


Utilizzando altri comandi di google hacking, come “`typefile:pdf site:epicode.com”` siamo riusciti a risalire ad alcuni certificati rilasciati a studenti della piattaforma, scaricabili in formato pdf, probabilmente modificabili con photoshop e riutilizzabili.

- 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: 267008881.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: 267008881.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: +1.480.624.2505
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: +1.480.624.2599
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: +1.480.624.2599
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

```
kali@kali:~$ subfinder -d epicode.com

subfinder
projectdiscovery.io

[Info] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[Info] Enumerating subdomains for epicode.com
doggen.dev.epicode.com
local-ai.epicode.com
st.epicode.com
auth.epicode.com
trigger.epicode.com
ml.epicode.com
registry.cool.epicode.com
collaudo.epicode.com
www.learn.dev.epicode.com
cert.epicode.com
notifications.dev.epicode.com
console-bucket.epicode.com
app.dev.epicode.com
www.eurolearn.epicode.com
www.learnstaging.epicode.com
ai.epicode.com
app.epicode.com
learn.dev.epicode.com
www.talent.epicode.com
www.talent-dev.epicode.com
www.cert.epicode.com
ai-dev.epicode.com
learn.main.epicode.com
www.cert-staging.epicode.com
www.epicode.com
vms.epicode.com
onboarding.epicode.com
vms-dev.epicode.com
replay.epicode.com
cert.dev.epicode.com
www.cert-dev.epicode.com
gal.epicode.com
libra.epicode.com
gta.epicode.com
linkhaus.epicode.com
www-app.epicode.com
www-dev.epicode.com
epicode.com
www-app-dev.epicode.com
kb.epicode.com
```

- 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