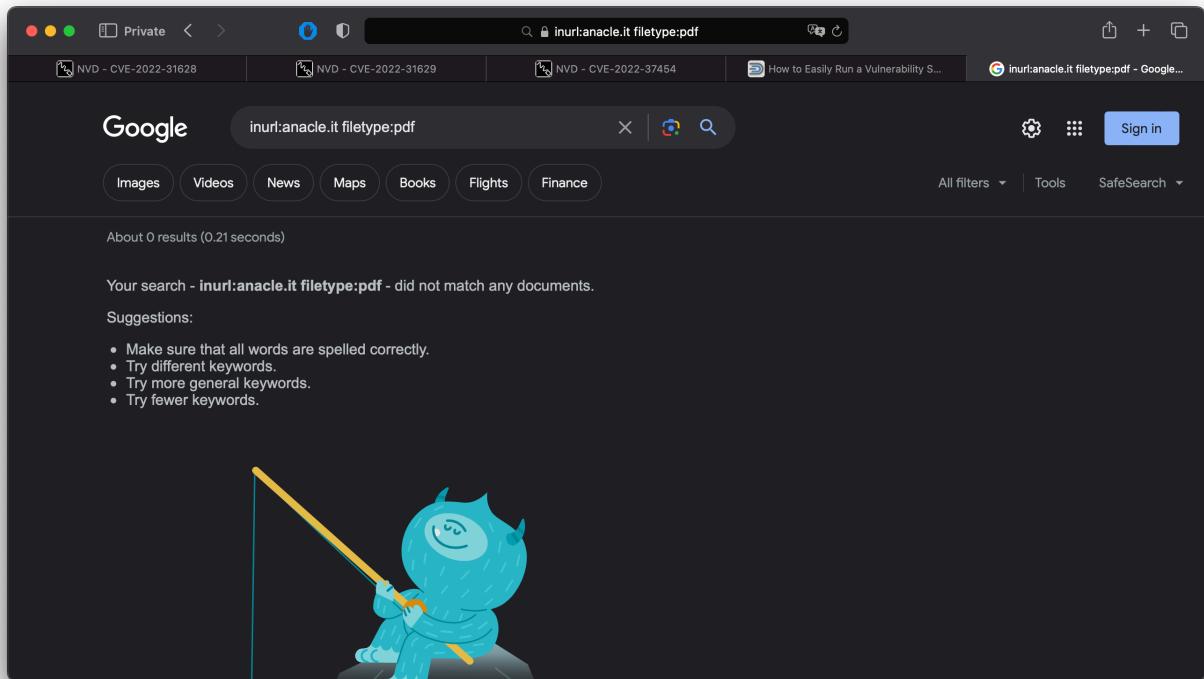


Raccolta informazioni e Google Hacking

A scopo didattico ho utilizzato come target della raccolta informazioni un piccolo brand di nome Anacle. Ho provato a utilizzare alcuni dorks come da traccia dell'esercizio senza aver trovato nessun dato particolarmente utile, tranne telefono ed email.



Sono passato dopodiché all'utilizzo dei vari tool messi a disposizione da Kali per l'information gathering.

Tool	Versione	Scopo	Note
Dmitry	—	IP e server info	—
Maltego	C.E. 4.4.1	analisi dettagliata	3 potenziali vulnerabilità trovate
Google	—	ricerca base informazioni	—

```

File Actions Edit View Help
(kali㉿kali)-[~]
$ dmitry anacle.it
Deepmagic Information Gathering Tool
"There be some deep magic going on"

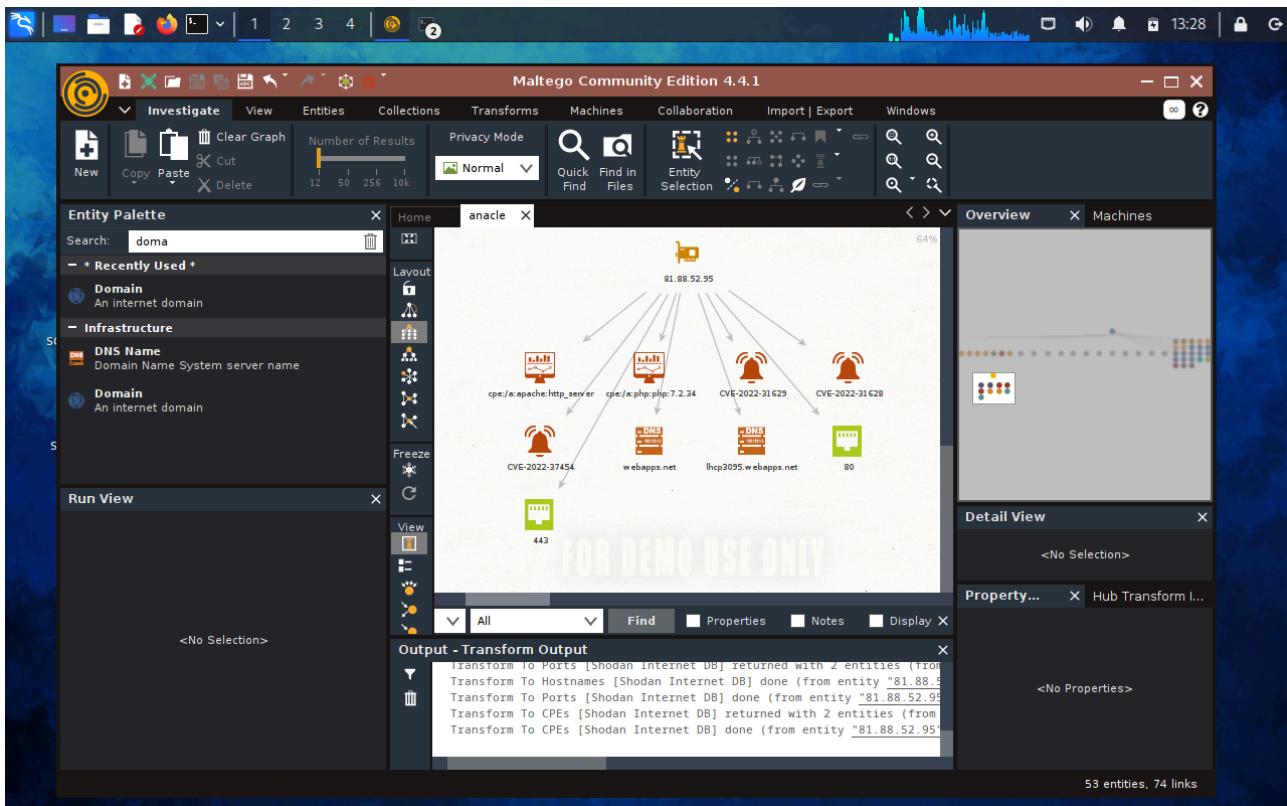
HostIP:81.88.52.95
HostName:anacle.it

Gathered Inet-whois information for 81.88.52.95

inetnum: 81.88.52.0 - 81.88.53.255
netname: REGISTERIT_HOUSING
descr: dedicated co-located servers or virtual servers
country: IT
admin-c: REGA-RIPE
tech-c: REGT-RIPE
status: ASSIGNED PA
mnt-by: MNT-REGISTER
mnt-lower: MNT-REGISTER
created: 2013-08-13T09:43:54Z
last-modified: 2013-08-13T09:43:54Z
source: RIPE

role: Register.it board - Direzione
address: Register.IT S.p.A.
address: Via Ponti, 6
address: 24126 Bergamo
address: ITALY
abuse-mailbox: abuse@register.it
admin-c: CORB3-RIPE
admin-c: CV4237-RIPE
admin-c: GOR15-RIPE
tech-c: REGT-RIPE
nic-hdl: REGA-ripe
mnt-by: MNT-REGISTER
created: 2006-04-03T16:31:22Z

```



Più precisamente con Maltego sono riuscito a trovare delle potenziali vulnerabilità sul server, due sull'utilizzo di una versione php vecchia e quindi più esposta.

Ho trovato inoltre una vulnerabilità di tipo integer overflow sull'utilizzo del algoritmo crittografico SHA3. Consigliato indagare su tale vulnerabilità per accertarne il rischio.

CVE-2022-37454 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties. This occurs in the sponge function interface.

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD	Base Score: 9.8 CRITICAL	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
------------------	---------------------------------	---

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

QUICK INFO

CVE Dictionary Entry: CVE-2022-37454
NVD Published Date: 10/21/2022
NVD Last Modified: 05/03/2023
Source: MITRE