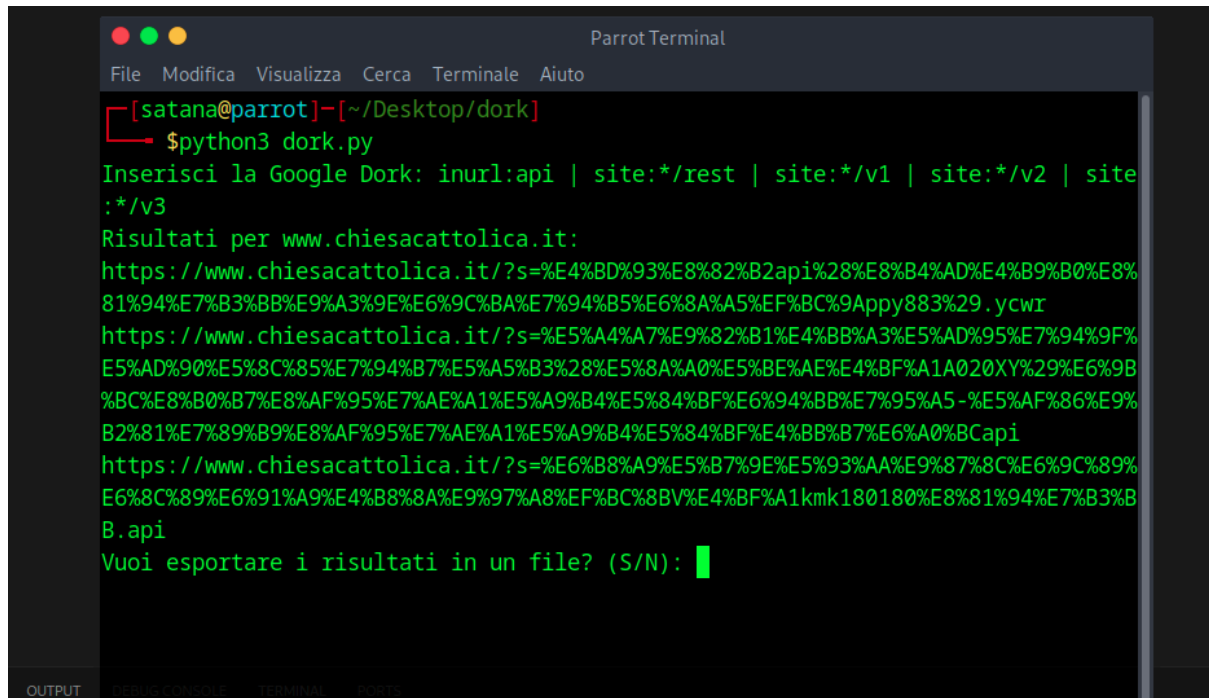


Information gathering

Consegna S5/L2

Obiettivi: Identificazione di vari domini potenzialmente vulnerabili ad attacchi web-based. Ho condotto la ricerca utilizzando le google dorks e automatizzando alcuni task tramite un piccolo script Python che ho sviluppato.



```
Parrot Terminal
File Modifica Visualizza Cerca Terminale Aiuto
[satana@parrot] - [~/Desktop/dork]
$python3 dork.py
Inserisci la Google Dork: inurl:api | site:*/rest | site:*/v1 | site:*/v2 | site:*/v3
Risultati per www.chiesacattolica.it:
https://www.chiesacattolica.it/?s=%E4%BD%93%E8%82%B2api%28%E8%B4%AD%E4%B9%B0%E8%81%94%E7%B3%BB%E9%A3%9E%E6%9C%BA%E7%94%B5%E6%8A%A5%EF%BC%9Apy883%29.ycwr
https://www.chiesacattolica.it/?s=%E5%A4%A7%E9%82%B1%E4%BB%A3%E5%AD%95%E7%94%9F%E5%AD%90%E5%8C%85%E7%94%B7%E5%A5%B3%28%E5%8A%A0%E5%BE%AE%E4%BF%A1A020XY%29%E6%9B%BC%E8%B0%B7%E8%AF%95%E7%AE%A1%E5%A9%B4%E5%84%BF%E6%94%BB%E7%95%A5-%E5%AF%86%E9%B2%81%E7%89%B9%E8%AF%95%E7%AE%A1%E5%A9%B4%E5%84%BF%E4%BB%B7%E6%A0%BCapi
https://www.chiesacattolica.it/?s=%E6%B8%A9%E5%B7%9E%E5%93%AA%E9%87%8C%E6%9C%89%E6%8C%89%E6%91%A9%E4%B8%8A%E9%97%A8%EF%BC%8BV%E4%BF%A1kmk180180%E8%81%94%E7%B3%B.B.api
Vuoi esportare i risultati in un file? (S/N):
```

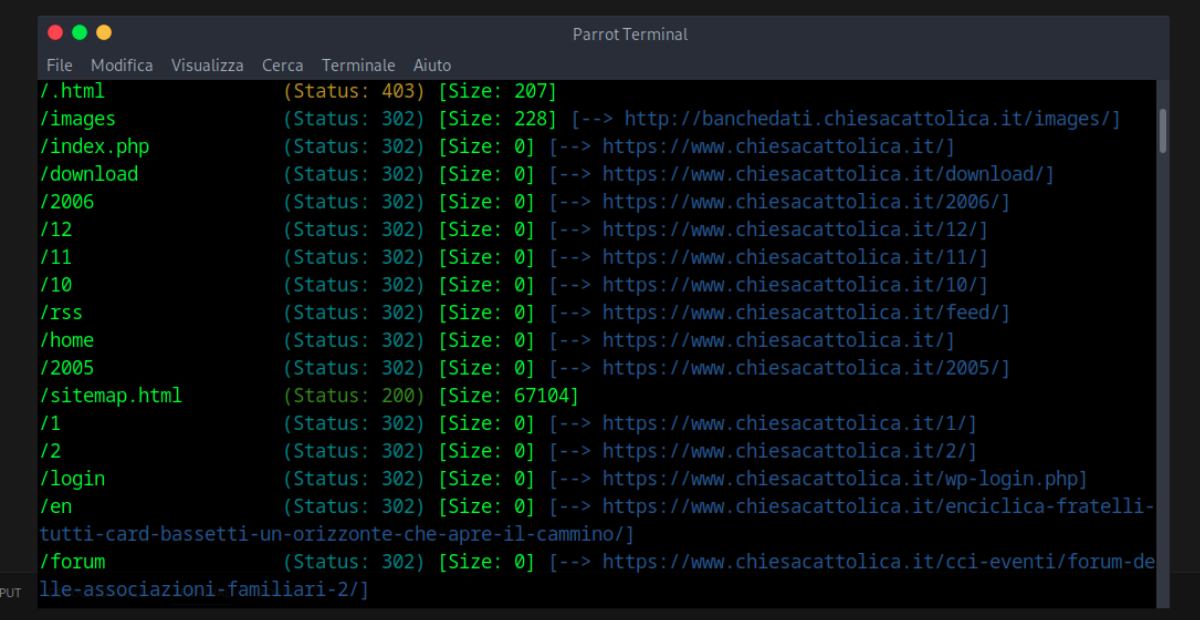
Lo script accetta in input una dork, e si aspetta nella stessa directory un file .txt contenente i domini di interesse. La lista di domini può essere personalizzata a nostro piacimento, oppure è possibile utilizzare liste di domini reperibili online. I risultati sono esportabili in un file di testo nella stessa directory dello script.

Gli screenshot sono a titolo illustrativo. Una ricerca è stata effettuata con la dork:

```
site:www.chiesacattolica.it inurl:api | site:*/rest | site:*/v1 | site:*/v2 | site:*/v3
```

mirata ad individuare pagine del sito www.chiesacattolica.it contenenti "api" nell'URL, e su qualsiasi dominio con percorsi /rest, /v1, /v2 o /v3.

Le dorks, spesso, come anche in questo caso, non restituiscono i risultati attesi. Ma possono invitare ad effettuare ulteriori ricerche, come in questo caso. Ho limitato l'analisi dei domini utilizzando Gobuster e alcuni parametri.



```
Parrot Terminal
File Modifica Visualizza Cerca Terminale Aiuto
/.html (Status: 403) [Size: 207]
/images (Status: 302) [Size: 228] [--> http://banchedati.chiesacattolica.it/images/]
/index.php (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/]
/download (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/download/]
/2006 (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/2006/]
/12 (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/12/]
/11 (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/11/]
/10 (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/10/]
/rss (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/feed/]
/home (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/]
/2005 (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/2005/]
/sitemap.html (Status: 200) [Size: 67104]
/1 (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/1/]
/2 (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/2/]
/login (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/wp-login.php]
/en (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/enciclica-fratelli-tutti-card-bassetti-un-orizzonte-che-apre-il-cammino/]
/forum (Status: 302) [Size: 0] [--> https://www.chiesacattolica.it/ccj-eventi/forum-de-
lle-associazioni-familiari-2/]
```

Gobuster viene utilizzato per individuare file o directory potenzialmente interessanti tramite tecniche di bruteforce.

Utilizzando altre google dorks, ho individuato diversi siti potenzialmente vulnerabili a **SQL injection** e **XSS reflected**. Tuttavia, essendo limitato dai permessi e non essendo questo lo scopo del compito, ho interrotto l'analisi.

Le dorks spesso non richiedono complessità elevate, come dimostrato in questo caso:

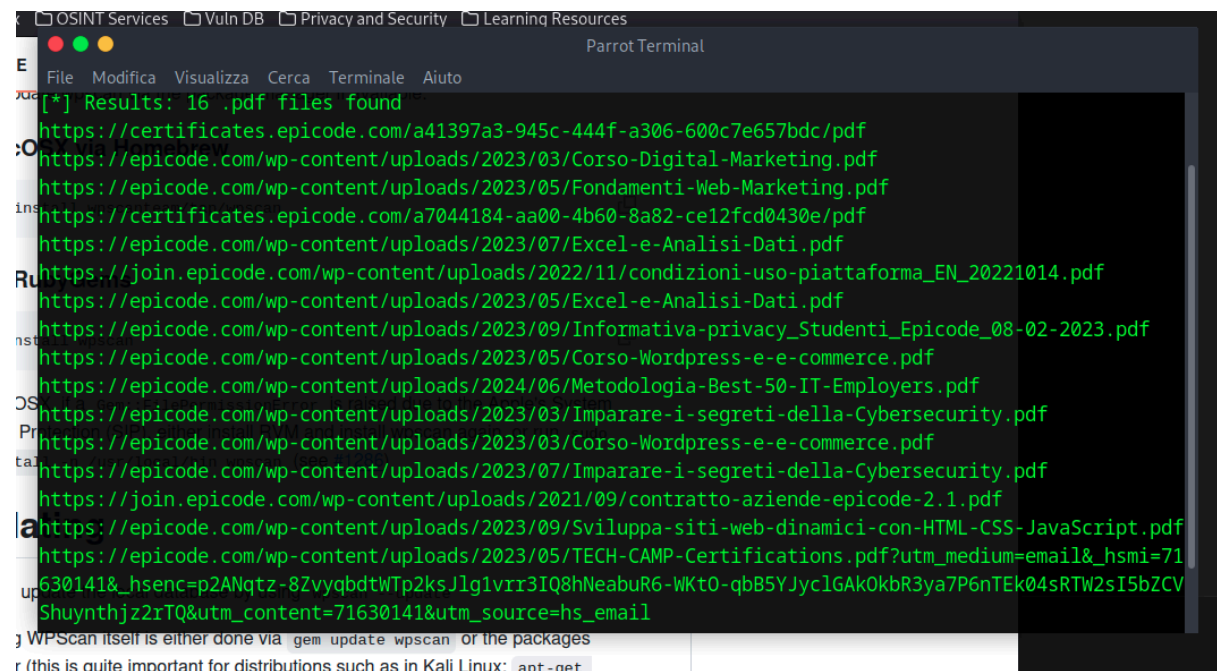
```
bradleycoscd.com
Parrot Terminal
File Modifica Visualizza Cerca Terminale Aiuto
[satana@parrot]-[~/Desktop/dork]
$python3 dork.py
Inserisci la Google Dork: "powered by joomla 3.2" OR "powered by joomla 3.3" OR "powered by joomla 3.4"
Risultati per bradleycoscd.com:
http://bradleycoscd.com/index.php/about-us
http://bradleycoscd.com/index.php/m-contactus
http://bradleycoscd.com/index.php/programs-and-services/programs
http://bradleycoscd.com/index.php/2-uncategorised/43-client-gateway
http://bradleycoscd.com/index.php/value-of-ag
http://bradleycoscd.com/index.php/board-and-staff
http://bradleycoscd.com/index.php/programs-and-services/programs/arcf
http://bradleycoscd.com/index.php/programs-and-services
http://bradleycoscd.com/index.php/programs-and-services/programs/equip
http://bradleycoscd.com/index.php/2-uncategorised/23-burn-permits
Vuoi esportare i risultati in un file? (S/N):
```

L'esempio del dominio è illustrativo. Avrei potuto analizzare migliaia di domini con installazioni Joomla potenzialmente vulnerabili. In questo caso, dopo l'output delle dorks, ho eseguito una semplice enumerazione:

```
Parrot Terminal
File Modifica Visualizza Cerca Terminale Aiuto
[+] Checking robots.txt existing
[++] robots.txt is found
path : http://bradleycoscd.com/robots.txt

Interesting path found from robots.txt
http://bradleycoscd.com/joomla/administrator/
http://bradleycoscd.com/administrator/
http://bradleycoscd.com/bin/
http://bradleycoscd.com/cache/
http://bradleycoscd.com/cli/
http://bradleycoscd.com/components/
http://bradleycoscd.com/images/
http://bradleycoscd.com/includes/
http://bradleycoscd.com/installation/
http://bradleycoscd.com/language/
http://bradleycoscd.com/layouts/
http://bradleycoscd.com/libraries/
http://bradleycoscd.com/logs/
http://bradleycoscd.com/media/
```

Un altro strumento interessante nell'ambito dell'OSINT è Metagoofil, utilizzato per la ricerca di file e metadati su specifici domini. Ad esempio:



```
OSINT Services  Vuln DB  Privacy and Security  Learning Resources
Parrot Terminal
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
[*] Results: 16 .pdf files found
https://certificates.epicode.com/a41397a3-945c-444f-a306-600c7e657bdc/pdf
https://epicode.com/wp-content/uploads/2023/03/Corso-Digital-Marketing.pdf
https://epicode.com/wp-content/uploads/2023/05/Fondamenti-Web-Marketing.pdf
https://certificates.epicode.com/a7044184-aa00-4b60-8a82-ce12fcd0430e/pdf
https://epicode.com/wp-content/uploads/2023/07/Excel-e-Analisi-Dati.pdf
https://join.epicode.com/wp-content/uploads/2022/11/condizioni-uso-piattaforma_EN_20221014.pdf
https://epicode.com/wp-content/uploads/2023/05/Excel-e-Analisi-Dati.pdf
https://epicode.com/wp-content/uploads/2023/09/Informativa-privacy_Studenti_Epicode_08-02-2023.pdf
https://epicode.com/wp-content/uploads/2023/05/Corso-Wordpress-e-e-commerce.pdf
https://epicode.com/wp-content/uploads/2024/06/Metodologia-Best-50-IT-Employers.pdf
https://epicode.com/wp-content/uploads/2023/03/Imparare-i-segreti-della-Cybersecurity.pdf
https://epicode.com/wp-content/uploads/2023/03/Corso-Wordpress-e-e-commerce.pdf
https://epicode.com/wp-content/uploads/2023/07/Imparare-i-segreti-della-Cybersecurity.pdf
https://join.epicode.com/wp-content/uploads/2021/09/contratto-aziende-epicode-2.1.pdf
https://epicode.com/wp-content/uploads/2023/09/Sviluppa-siti-web-dinamici-con-HTML-CSS-JavaScript.pdf
https://epicode.com/wp-content/uploads/2023/05/TECH-CAMP-Certifications.pdf?utm_medium=email&_hsmi=71630141&_hsenc=p2ANqtz-8ZvyqbdTWp2ksJlglvrr3IQ8hNeabuR6-WKt0-qbB5YJyclGAk0kbr3ya7P6nTEk04sRTW2sI5bZCVShuynthjz2rTQ&utm_content=71630141&utm_source=hs_email
WPScan itself is either done via  gem update wpscan  or the packages
r (this is quite important for distributions such as in Kali Linux:  apt-get
```

Infine, la tana del bianconiglio mi ha portato nell'ambito dei data leaks. Grazie alle varie tecniche di osint, ho trovato un vecchio DB di facebook risalente al 2019 circa, contenente migliaia di informazioni sensibili di utenti facebook.

Il solo archivio italiano pesa circa 4gb, nello screen un esempio di dati esfiltrati dal leak utilizzando il tool grep:

```
Italy - zsh - 90x28
flavio@Italy % grep "Mario:Rossi" *.txt
0.txt:39330276930:100002249935139:Mario:Rossi:male:Cincinnati:Carbonia, Italy::::
0.txt:39330458533:100000312481067:Mario:Rossi:::::1/1/0001 12:00:00 AM::
0.txt:39330604426:1533497780:Mario:Rossi:male:Turin, Italy:Milan, Italy:Engaged:::02/08/1980
0.txt:39330665029:100000686555502:Mario:Rossi:male:::::
0.txt:39335201800:100015915527592:Mario:Rossi:male:::::1/1/0001 12:00:00 AM::
0.txt:39335222841:100003819684638:Mario:Rossi:female:Abbiategrosso:Abbiategrosso::B&B La Ginibissa strada Ginibissa 13 ::
0.txt:39335232540:100009908689112:Mario:Rossi:male:::::1/1/0001 12:00:00 AM::
0.txt:39335250260:100029256403644:Mario:Rossi:male:::::1/1/0001 12:00:00 AM::
0.txt:39335250510:1463538386:Mario:Rossi:male:::::3/3/2018 12:00:00 AM::
0.txt:39335252550:100009723966636:Mario:Rossi:male:::::9/23/2016 12:00:00 AM::
0.txt:39335259341:1661096472:Mario:Rossi:::::
0.txt:39335275076:1565382661:Mario:Rossi:male:::::1/9/2018 12:00:00 AM::
0.txt:39335283944:100007680633766:Mario:Rossi:male:::::
0.txt:39335287195:100011241675787:Mario:Rossi:female::Haiti, El Seibo, Dominican Republic::::
0.txt:39335292602:100012332535581:Mario:Rossi:female:::::
0.txt:39335294072:100013659490612:Mario:Rossi:male:::::1/1/0001 12:00:00 AM::
0.txt:39335294345:100014090565225:Mario:Rossi:male:::::
0.txt:39335298314:100022540566258:Mario:Rossi:male::Milan, Italy::::
0.txt:39335308667:100009610664918:Mario:Rossi:male:::::
0.txt:39335348337:1464012922:Mario:Rossini:male:::::1/1/0001 12:00:00 AM::
0.txt:39335360885:100013414128776:Mario:Rossi:male:::::1/1/0001 12:00:00 AM::
0.txt:39335360888:100010876892263:Mario:Rossi:male:New York, New York:New York, New York:::12/7/2015 12:00:00 AM::
```

Con specifiche tecniche di DARKINT e l'ausilio di vari tools, ho individuato ulteriori data breach nel dark web. Tuttavia ci tengo a sottolineare che queste ricerche esulano dagli obiettivi etici e pratici dell'esercizio svolto.

Grazie

Flavio Scognamiglio