

Output dei Comandi e degli Strumenti

OWASP Juice Shop

[Caroli Sofia](#) - [Passini Anna](#) - [Ricci Gabriele](#)

Comandi.....	2
docker inspect juice-shop.....	2
whatweb http://127.0.0.1:3000.....	3
wafw00f.....	3
nslookup https://juice-shop.herokuapp.com.....	3
nmap -sV localhost -p 3000.....	4
nmap -sn localhost.....	4
nikto -h http://172.17.0.2:3000.....	20
Strumenti.....	21
https://dnschecker.org/.....	21
www.shodan.io.....	22
bgp.he.net.....	23
https://jwt.io.....	23
https://webhook.site.....	24
htmledit.squarefree.com.....	24
Postman - http://localhost:3000/api/Users (enumerazione utenti).....	25
Postman - http://localhost:3000/rest/products/search (enumerazione prodotti).....	26
Burp Suite.....	27

docker inspect juice-shop

Funzionamento: il comando restituisce in formato JSON tutte le informazioni relative al container selezionato, viene effettuata una lettura diretta dei metadati archiviati da Docker Engine.

[illegible]

whatweb http://127.0.0.1:3000

Scopo: identificare automaticamente le tecnologie web utilizzate; capire con quali stack tecnologici è stato costruito OWASP Juice Shop per cercare eventuali vulnerabilità note associate a quei componenti.

Funzionamento: WhatWeb invia richieste HTTP e analizza i metadati, gli header HTTP e le risposte per confrontarli con firme note nel proprio database che identificano le diverse tecnologie.

Output:

```
http://127.0.0.1:3000 [200 OK] Country[RESERVED][ZZ], HTML5, IP[127.0.0.1], JQuery[2.2.4], Script[module],
Title[OWASP Juice Shop],
UncommonHeaders[access-control-allow-origin,x-content-type-options,feature-policy,x-recruiting],
X-Frame-Options[SAMEORIGIN]
```

wafw00f

Scopo: identificare la presenza di WAF noti, analizzando le risposte del server e confrontandole con firme conosciute.

Funzionamento: invia richieste HTTP e analizza i metadati, gli header HTTP e le risposte per identificare la presenza di WAF.

Output:

```

      /_____\
      ( Woof! )
      \_____/
        )
        ) (
        "
        .-
        0" ; |==|
        / (      /\
        ( / )    /\
        \_ ) )   / | \

```

~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit

```
[*] Checking http://juice-shop.herokuapp.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

nslookup https://juice-shop.herokuapp.com

Scopo: risolvere un nome a dominio e scoprire gli indirizzi IP pubblici associati. Ottenere gli IP dietro la demo pubblica Juice Shop e usarli nelle scansioni successive (Nmap, Shodan, ecc.).

Funzionamento: nslookup effettua una query DNS (Domain Name System) al resolver predefinito (es. 127.0.0.53) per risolvere il dominio specificato nell'indirizzo IP.

Fornisce anche alias e nomi alternativi (CNAME/A/AAAA records).

Output:

Server:	127.0.0.53	Name:	ie02.ingress.herokuapp.com
Address:	127.0.0.53#53	Address:	54.220.192.176
		Name:	ie02.ingress.herokuapp.com
		Address:	46.137.15.86
Non-authoritative answer:		Name:	ie02.ingress.herokuapp.com
https://juice-shop.herokuapp.com canonical name =		Address:	54.73.53.13
ie02.ingress.herokuapp.com.			

[illegible][illegible][illegible]

[illegible][illegible][illegible]

[illegible][illegible][illegible]

[illegible][illegible][illegible]

[illegible][illegible][illegible]

[illegible]

```

Nmap scan report for ec2-46-137-45-192.eu-west-1.compute.amazonaws.com
(46.137.45.192)
Host is up (0.18s latency).
Nmap scan report for ec2-46-137-45-194.eu-west-1.compute.amazonaws.com
(46.137.45.194)
Host is up (0.095s latency).
Nmap scan report for ec2-46-137-45-203.eu-west-1.compute.amazonaws.com
(46.137.45.203)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-45-219.eu-west-1.compute.amazonaws.com
(46.137.45.219)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-45-235.eu-west-1.compute.amazonaws.com
(46.137.45.235)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-45-245.eu-west-1.compute.amazonaws.com
(46.137.45.245)
Host is up (0.14s latency).
Nmap scan report for ec2-46-137-46-2.eu-west-1.compute.amazonaws.com
(46.137.46.2)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-46-4.eu-west-1.compute.amazonaws.com
(46.137.46.4)
Host is up (0.092s latency).
Nmap scan report for ec2-46-137-46-15.eu-west-1.compute.amazonaws.com
(46.137.46.15)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-46-17.eu-west-1.compute.amazonaws.com
(46.137.46.17)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-46-23.eu-west-1.compute.amazonaws.com
(46.137.46.23)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-46-25.eu-west-1.compute.amazonaws.com
(46.137.46.25)
Host is up (0.095s latency).
Nmap scan report for ec2-46-137-46-31.eu-west-1.compute.amazonaws.com
(46.137.46.31)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-46-54.eu-west-1.compute.amazonaws.com
(46.137.46.54)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-46-55.eu-west-1.compute.amazonaws.com
(46.137.46.55)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-46-74.eu-west-1.compute.amazonaws.com
(46.137.46.74)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-46-90.eu-west-1.compute.amazonaws.com
(46.137.46.90)
Host is up (0.31s latency).
Nmap scan report for ec2-46-137-46-113.eu-west-1.compute.amazonaws.com
(46.137.46.113)
Host is up (0.19s latency).
Nmap scan report for ec2-46-137-46-170.eu-west-1.compute.amazonaws.com
(46.137.46.170)
Host is up (0.095s latency).
Nmap scan report for ec2-46-137-46-175.eu-west-1.compute.amazonaws.com
(46.137.46.175)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-46-204.eu-west-1.compute.amazonaws.com
(46.137.46.204)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-46-226.eu-west-1.compute.amazonaws.com
(46.137.46.226)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-46-233.eu-west-1.compute.amazonaws.com
(46.137.46.233)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-46-238.eu-west-1.compute.amazonaws.com
(46.137.46.238)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-46-255.eu-west-1.compute.amazonaws.com
(46.137.46.255)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-47-14.eu-west-1.compute.amazonaws.com
(46.137.47.14)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-47-15.eu-west-1.compute.amazonaws.com
(46.137.47.15)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-47-34.eu-west-1.compute.amazonaws.com
(46.137.47.34)
Host is up (0.079s latency).
Nmap scan report for ec2-46-137-47-46.eu-west-1.compute.amazonaws.com
(46.137.47.46)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-47-47.eu-west-1.compute.amazonaws.com
(46.137.47.47)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-47-70.eu-west-1.compute.amazonaws.com
(46.137.47.70)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-47-134.eu-west-1.compute.amazonaws.com
(46.137.47.134)
Host is up (0.19s latency).
Nmap scan report for ec2-46-137-47-136.eu-west-1.compute.amazonaws.com
(46.137.47.136)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-47-150.eu-west-1.compute.amazonaws.com
(46.137.47.150)
Host is up (0.14s latency).
Nmap scan report for ec2-46-137-47-152.eu-west-1.compute.amazonaws.com
(46.137.47.152)
Host is up (0.098s latency).
Nmap scan report for ec2-46-137-47-166.eu-west-1.compute.amazonaws.com
(46.137.47.166)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-47-173.eu-west-1.compute.amazonaws.com
(46.137.47.173)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-47-186.eu-west-1.compute.amazonaws.com
(46.137.47.186)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-47-189.eu-west-1.compute.amazonaws.com
(46.137.47.189)
Host is up (0.10s latency).
Stats: 0.31-36 elapsed; 12288 hosts completed (1038 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 64.12% done; ETC: 10.59 (0.02-00 remaining)
Stats: 0.34-31 elapsed, 12288 hosts completed (1038 up), 4096 undergoing Ping Scan
Parallel DNS resolution of 4096 hosts. Timing: About 4.66% done; ETC: 11.46
(0.39-32 remaining)
Nmap scan report for ec2-46-137-48-3.eu-west-1.compute.amazonaws.com
(46.137.48.3)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-48-8.eu-west-1.compute.amazonaws.com
(46.137.48.8)
Host is up (0.098s latency).
Nmap scan report for ec2-46-137-48-13.eu-west-1.compute.amazonaws.com
(46.137.48.13)
Host is up (0.099s latency).
Nmap scan report for ec2-46-137-48-26.eu-west-1.compute.amazonaws.com
(46.137.48.26)
Host is up (0.52s latency).
Nmap scan report for ec2-46-137-48-41.eu-west-1.compute.amazonaws.com
(46.137.48.41)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-48-50.eu-west-1.compute.amazonaws.com
(46.137.48.50)

```

[illegible]

(at 0.11 s latency)
Nmap scan report for ec2-46-137-50-218.eu-west-1.compute.amazonaws.com (46.137.50.218)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-50-222.eu-west-1.compute.amazonaws.com (46.137.50.222)
Host is up (0.099s latency).
Nmap scan report for ec2-46-137-50-231.eu-west-1.compute.amazonaws.com (46.137.50.231)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-51-10.eu-west-1.compute.amazonaws.com (46.137.51.10)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-51-26.eu-west-1.compute.amazonaws.com (46.137.51.26)
Host is up (0.52s latency).
Nmap scan report for ec2-46-137-51-92.eu-west-1.compute.amazonaws.com (46.137.51.92)
Host is up (0.14s latency).
Nmap scan report for ec2-46-137-51-95.eu-west-1.compute.amazonaws.com (46.137.51.95)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-51-103.eu-west-1.compute.amazonaws.com (46.137.51.103)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-51-106.eu-west-1.compute.amazonaws.com (46.137.51.106)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-51-124.eu-west-1.compute.amazonaws.com (46.137.51.124)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-51-131.eu-west-1.compute.amazonaws.com (46.137.51.131)
Host is up (0.17s latency).
Nmap scan report for ec2-46-137-51-151.eu-west-1.compute.amazonaws.com (46.137.51.151)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-51-158.eu-west-1.compute.amazonaws.com (46.137.51.158)
Host is up (0.099s latency).
Nmap scan report for ec2-46-137-51-167.eu-west-1.compute.amazonaws.com (46.137.51.167)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-51-201.eu-west-1.compute.amazonaws.com (46.137.51.201)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-51-205.eu-west-1.compute.amazonaws.com (46.137.51.205)
Host is up (0.099s latency).
Nmap scan report for ec2-46-137-51-208.eu-west-1.compute.amazonaws.com (46.137.51.208)
Host is up (0.099s latency).
Nmap scan report for ec2-46-137-51-209.eu-west-1.compute.amazonaws.com (46.137.51.209)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-51-212.eu-west-1.compute.amazonaws.com (46.137.51.212)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-51-216.eu-west-1.compute.amazonaws.com (46.137.51.216)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-51-219.eu-west-1.compute.amazonaws.com (46.137.51.219)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-51-239.eu-west-1.compute.amazonaws.com (46.137.51.239)
Host is up (0.097s latency).
Nmap scan report for ec2-46-137-51-246.eu-west-1.compute.amazonaws.com (46.137.51.246)
Host is up (0.18s latency).
Nmap scan report for ec2-46-137-51-248.eu-west-1.compute.amazonaws.com (46.137.51.248)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-51-252.eu-west-1.compute.amazonaws.com (46.137.51.252)
Host is up (0.15s latency).
Nmap scan report for ec2-46-137-51-255.eu-west-1.compute.amazonaws.com (46.137.51.255)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-52-2.eu-west-1.compute.amazonaws.com (46.137.52.2)
Host is up (0.11s latency).
Nmap scan report for www.payments.onyxresourcesource.com (46.137.52.9)
Host is up (0.14s latency).
Nmap scan report for ec2-46-137-52-27.eu-west-1.compute.amazonaws.com (46.137.52.27)
Host is up (0.14s latency).
Nmap scan report for ec2-46-137-52-30.eu-west-1.compute.amazonaws.com (46.137.52.30)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-52-35.eu-west-1.compute.amazonaws.com (46.137.52.35)
Host is up (0.095s latency).
Nmap scan report for ec2-46-137-52-48.eu-west-1.compute.amazonaws.com (46.137.52.48)
Host is up (0.099s latency).
Nmap scan report for ec2-46-137-52-56.eu-west-1.compute.amazonaws.com (46.137.52.56)
Host is up (0.20s latency).
Nmap scan report for ec2-46-137-52-60.eu-west-1.compute.amazonaws.com (46.137.52.60)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-52-83.eu-west-1.compute.amazonaws.com (46.137.52.83)
Host is up (0.14s latency).
Nmap scan report for ec2-46-137-52-92.eu-west-1.compute.amazonaws.com (46.137.52.92)
Host is up (0.14s latency).
Nmap scan report for ec2-46-137-52-118.eu-west-1.compute.amazonaws.com (46.137.52.118)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-52-143.eu-west-1.compute.amazonaws.com (46.137.52.143)
Nmap scan report for ec2-46-137-52-152.eu-west-1.compute.amazonaws.com (46.137.52.152)
Host is up (0.15s latency).
Nmap scan report for ec2-46-137-52-153.eu-west-1.compute.amazonaws.com (46.137.52.153)
Host is up (0.092s latency).
Nmap scan report for ec2-46-137-52-159.eu-west-1.compute.amazonaws.com (46.137.52.159)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-52-164.eu-west-1.compute.amazonaws.com (46.137.52.164)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-52-179.eu-west-1.compute.amazonaws.com (46.137.52.179)
Host is up (0.11s latency).
Nmap report for ec2-46-137-52-182.eu-west-1.compute.amazonaws.com (46.137.52.182)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-52-188.eu-west-1.compute.amazonaws.com (46.137.52.188)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-52-203.eu-west-1.compute.amazonaws.com (46.137.52.203)
Host is up (0.098s latency).
Nmap scan report for ec2-46-137-52-204.eu-west-1.compute.amazonaws.com (46.137.52.204)
Host is up (0.094s latency).

[illegible][illegible]

[illegible][illegible]

```

Nmap scan report for ec2-46-137-62-220.eu-west-1.compute.amazonaws.com
(46.137.62.220)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-62-221.eu-west-1.compute.amazonaws.com
(46.137.62.221)
Host is up (0.099s latency).
Nmap scan report for ec2-46-137-62-225.eu-west-1.compute.amazonaws.com
(46.137.62.225)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-62-239.eu-west-1.compute.amazonaws.com
(46.137.62.239)
Host is up (0.098s latency).
Nmap scan report for ec2-46-137-63-8.eu-west-1.compute.amazonaws.com
(46.137.63.8)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-63-16.eu-west-1.compute.amazonaws.com
(46.137.63.16)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-63-33.eu-west-1.compute.amazonaws.com
(46.137.63.33)
Host is up (0.67s latency).
Nmap scan report for ec2-46-137-63-45.eu-west-1.compute.amazonaws.com
(46.137.63.45)
Host is up (0.094s latency).
Nmap scan report for ec2-46-137-63-61.eu-west-1.compute.amazonaws.com
(46.137.63.61)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-63-78.eu-west-1.compute.amazonaws.com
(46.137.63.78)
Host is up (0.22s latency).
Nmap scan report for ec2-46-137-63-83.eu-west-1.compute.amazonaws.com
(46.137.63.83)
Host is up (0.14s latency).
Nmap scan report for ec2-46-137-63-106.eu-west-1.compute.amazonaws.com
(46.137.63.106)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-63-110.eu-west-1.compute.amazonaws.com
(46.137.63.110)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-63-120.eu-west-1.compute.amazonaws.com
(46.137.63.120)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-63-136.eu-west-1.compute.amazonaws.com
(46.137.63.136)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-63-146.eu-west-1.compute.amazonaws.com
(46.137.63.146)
Host is up (0.097s latency).
Nmap scan report for ec2-46-137-63-148.eu-west-1.compute.amazonaws.com
(46.137.63.148)
Host is up (0.16s latency).
Nmap scan report for ec2-46-137-63-150.eu-west-1.compute.amazonaws.com
(46.137.63.150)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-63-155.eu-west-1.compute.amazonaws.com
(46.137.63.155)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-63-157.eu-west-1.compute.amazonaws.com
(46.137.63.157)
Host is up (0.095s latency).
Nmap scan report for ec2-46-137-63-180.eu-west-1.compute.amazonaws.com
(46.137.63.180)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-63-182.eu-west-1.compute.amazonaws.com
(46.137.63.182)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-63-193.eu-west-1.compute.amazonaws.com
(46.137.63.193)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-63-208.eu-west-1.compute.amazonaws.com
(46.137.63.208)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-63-221.eu-west-1.compute.amazonaws.com
(46.137.63.221)
Host is up (0.19s latency).
Nmap scan report for ec2-46-137-63-231.eu-west-1.compute.amazonaws.com
(46.137.63.231)
Host is up (0.20s latency).
Nmap scan report for ec2-46-137-63-234.eu-west-1.compute.amazonaws.com
(46.137.63.234)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-63-242.eu-west-1.compute.amazonaws.com
(46.137.63.242)
Host is up (0.30s latency).
Nmap scan report for ec2-46-137-63-249.eu-west-1.compute.amazonaws.com
(46.137.63.249)
Host is up (0.10s latency).
Stats: 0:42:11 elapsed; 16384 hosts completed (1355 up), 4096 undergoing Ping
Ping Scan Timing: About 58.58% done; ETC: 11:11 (40.36 remaining)
Stats: 0:42:33 elapsed; 16384 hosts completed (1355 up), 4096 undergoing Ping
Parallel DNS resolution of 4096 hosts. Timing: About 7.47% done; ETC: 11:50
(0:44:11 remaining)
Nmap scan report for ec2-46-137-64-6.eu-west-1.compute.amazonaws.com
(46.137.64.6)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-64-18.eu-west-1.compute.amazonaws.com
(46.137.64.18)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-64-22.eu-west-1.compute.amazonaws.com
(46.137.64.22)
Host is up (0.15s latency).
Nmap scan report for ec2-46-137-64-27.eu-west-1.compute.amazonaws.com
(46.137.64.27)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-64-39.eu-west-1.compute.amazonaws.com
(46.137.64.39)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-64-49.eu-west-1.compute.amazonaws.com
(46.137.64.49)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-64-63.eu-west-1.compute.amazonaws.com
(46.137.64.63)
Host is up (0.089s latency).
Nmap scan report for ec2-46-137-64-75.eu-west-1.compute.amazonaws.com
(46.137.64.75)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-64-87.eu-west-1.compute.amazonaws.com
(46.137.64.87)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-64-99.eu-west-1.compute.amazonaws.com
(46.137.64.99)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-64-100.eu-west-1.compute.amazonaws.com
(46.137.64.100)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-64-107.eu-west-1.compute.amazonaws.com
(46.137.64.107)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-64-130.eu-west-1.compute.amazonaws.com
(46.137.64.130)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-64-163.eu-west-1.compute.amazonaws.com
(46.137.64.163)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-64-165.eu-west-1.compute.amazonaws.com
(46.137.64.165)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-64-166.eu-west-1.compute.amazonaws.com
(46.137.64.166)

```

[illegible][illegible][illegible]

[illegible]

Nmap scan report for ec2-46-137-82-59 eu-west-1.compute.amazonaws.com
 (46.137.82.59)
 Host is up (0.095s latency).
 Nmap scan report for ec2-46-137-82-61 eu-west-1.compute.amazonaws.com
 (46.137.82.61)
 Host is up (0.14s latency).
 Nmap scan report for ec2-46-137-82-100 eu-west-1.compute.amazonaws.com
 (46.137.82.100)
 Host is up (0.099s latency).
 Nmap scan report for ec2-46-137-82-111 eu-west-1.compute.amazonaws.com
 (46.137.82.111)
 Host is up (0.16s latency).
 Nmap scan report for ec2-46-137-82-230 eu-west-1.compute.amazonaws.com
 (46.137.82.230)
 Host is up (0.17s latency).
 Nmap scan report for ec2-46-137-82-240 eu-west-1.compute.amazonaws.com
 (46.137.82.240)
 Host is up (0.097s latency).
 Nmap scan report for ec2-46-137-82-245 eu-west-1.compute.amazonaws.com
 (46.137.82.245)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-82-251 eu-west-1.compute.amazonaws.com
 (46.137.82.251)
 Host is up (0.15s latency).
 Nmap scan report for ec2-46-137-82-255 eu-west-1.compute.amazonaws.com
 (46.137.82.255)
 Host is up (0.097s latency).
 Nmap scan report for ec2-46-137-83-12 eu-west-1.compute.amazonaws.com
 (46.137.83.12)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-83-13 eu-west-1.compute.amazonaws.com
 (46.137.83.13)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-83-14 eu-west-1.compute.amazonaws.com
 (46.137.83.14)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-83-47 eu-west-1.compute.amazonaws.com
 (46.137.83.47)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-83-54 eu-west-1.compute.amazonaws.com
 (46.137.83.54)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-83-61 eu-west-1.compute.amazonaws.com
 (46.137.83.61)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-83-83 eu-west-1.compute.amazonaws.com
 (46.137.83.83)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-83-144 eu-west-1.compute.amazonaws.com
 (46.137.83.144)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-83-196 eu-west-1.compute.amazonaws.com
 (46.137.83.196)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-83-202 eu-west-1.compute.amazonaws.com
 (46.137.83.202)
 Host is up (0.089s latency).
 Nmap scan report for ec2-46-137-83-214 eu-west-1.compute.amazonaws.com
 (46.137.83.214)
 Host is up (0.14s latency).
 Nmap scan report for ec2-46-137-83-249 eu-west-1.compute.amazonaws.com
 (46.137.83.249)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-83-253 eu-west-1.compute.amazonaws.com
 (46.137.83.253)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-84-28 eu-west-1.compute.amazonaws.com
 (46.137.84.28)
 Host is up (0.093s latency).
 Nmap scan report for ec2-46-137-84-40 eu-west-1.compute.amazonaws.com
 (46.137.84.40)
 Host is up (0.095s latency).
 Nmap scan report for ec2-46-137-84-46 eu-west-1.compute.amazonaws.com
 (46.137.84.46)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-84-50 eu-west-1.compute.amazonaws.com
 (46.137.84.50)
 Host is up (0.13s latency).
 Nmap scan report for ec2-46-137-84-57 eu-west-1.compute.amazonaws.com
 (46.137.84.57)
 Host is up (0.16s latency).
 Nmap scan report for ec2-46-137-84-78 eu-west-1.compute.amazonaws.com
 (46.137.84.78)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-85-17 eu-west-1.compute.amazonaws.com
 (46.137.85.17)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-85-23 eu-west-1.compute.amazonaws.com
 (46.137.85.23)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-85-48 eu-west-1.compute.amazonaws.com
 (46.137.85.48)
 Host is up (0.15s latency).
 Nmap scan report for ec2-46-137-85-78 eu-west-1.compute.amazonaws.com
 (46.137.85.78)
 Host is up (0.10s latency).
 Nmap scan report for ec2-46-137-85-87 eu-west-1.compute.amazonaws.com
 (46.137.85.87)
 Host is up (0.095s latency).
 Nmap scan report for ec2-46-137-85-97 eu-west-1.compute.amazonaws.com
 (46.137.85.97)
 Host is up (0.10s latency).
 Nmap scan report for www.dnsmip.pl (46.137.85.101)
 Host is up (0.32s latency).
 Nmap scan report for ec2-46-137-85-130 eu-west-1.compute.amazonaws.com
 (46.137.85.130)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-85-219 eu-west-1.compute.amazonaws.com
 (46.137.85.219)
 Host is up (0.097s latency).
 Nmap scan report for ec2-46-137-85-237 eu-west-1.compute.amazonaws.com
 (46.137.85.237)
 Host is up (0.099s latency).
 Nmap scan report for ec2-46-137-85-252 eu-west-1.compute.amazonaws.com
 (46.137.85.252)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-86-17 eu-west-1.compute.amazonaws.com
 (46.137.86.17)
 Host is up (0.098s latency).
 Nmap scan report for ec2-46-137-86-38 eu-west-1.compute.amazonaws.com
 (46.137.86.38)
 Host is up (0.094s latency).
 Nmap scan report for ec2-46-137-86-51 eu-west-1.compute.amazonaws.com
 (46.137.86.51)
 Host is up (0.086s latency).
 Nmap scan report for ec2-46-137-86-85 eu-west-1.compute.amazonaws.com
 (46.137.86.85)
 Host is up (0.095s latency).
 Nmap scan report for ec2-46-137-86-101 eu-west-1.compute.amazonaws.com
 (46.137.86.101)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-86-187 eu-west-1.compute.amazonaws.com
 (46.137.86.187)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-86-234 eu-west-1.compute.amazonaws.com
 (46.137.86.234)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-86-242 eu-west-1.compute.amazonaws.com
 (46.137.86.242)
 Host is up (0.11s latency).

[illegible]

[illegible][illegible][illegible]

Nmap scan report for ec2-46-137-108-14.eu-west-1.compute.amazonaws.com (46.137.108.14)
 Host is up (0.0993s latency).
 Nmap scan report for ec2-46-137-108-17.eu-west-1.compute.amazonaws.com (46.137.108.17)
 Host is up (0.14s latency).
 Nmap scan report for ec2-46-137-108-19.eu-west-1.compute.amazonaws.com (46.137.108.19)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-108-21.eu-west-1.compute.amazonaws.com (46.137.108.21)
 Host is up (0.14s latency).
 Nmap scan report for ec2-46-137-108-46.eu-west-1.compute.amazonaws.com (46.137.108.46)
 Host is up (0.10s latency).
 Nmap scan report for ec2-46-137-108-56.eu-west-1.compute.amazonaws.com (46.137.108.56)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-108-93.eu-west-1.compute.amazonaws.com (46.137.108.93)
 Host is up (0.0998s latency).
 Nmap scan report for ec2-46-137-108-97.eu-west-1.compute.amazonaws.com (46.137.108.97)
 Host is up (0.0966s latency).
 Nmap scan report for ec2-46-137-108-100.eu-west-1.compute.amazonaws.com (46.137.108.100)
 Host is up (0.10s latency).
 Nmap scan report for ec2-46-137-108-102.eu-west-1.compute.amazonaws.com (46.137.108.102)
 Host is up (0.0933s latency).
 Nmap scan report for ec2-46-137-108-111.eu-west-1.compute.amazonaws.com (46.137.108.111)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-108-118.eu-west-1.compute.amazonaws.com (46.137.108.118)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-108-121.eu-west-1.compute.amazonaws.com (46.137.108.121)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-108-126.eu-west-1.compute.amazonaws.com (46.137.108.126)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-108-137.eu-west-1.compute.amazonaws.com (46.137.108.137)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-108-148.eu-west-1.compute.amazonaws.com (46.137.108.148)
 Host is up (0.0966s latency).
 Nmap scan report for ec2-46-137-108-167.eu-west-1.compute.amazonaws.com (46.137.108.167)
 Host is up (0.17s latency).
 Nmap scan report for ec2-46-137-108-199.eu-west-1.compute.amazonaws.com (46.137.108.199)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-108-248.eu-west-1.compute.amazonaws.com (46.137.108.248)
 Host is up (0.10s latency).
 Nmap scan report for ec2-46-137-109-3.eu-west-1.compute.amazonaws.com (46.137.109.3)
 Host is up (0.15s latency).
 Nmap scan report for ec2-46-137-109-4.eu-west-1.compute.amazonaws.com (46.137.109.4)
 Host is up (0.16s latency).
 Nmap scan report for ec2-46-137-109-7.eu-west-1.compute.amazonaws.com (46.137.109.7)
 Host is up (0.18s latency).
 Nmap scan report for ec2-46-137-109-12.eu-west-1.compute.amazonaws.com (46.137.109.12)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-109-15.eu-west-1.compute.amazonaws.com (46.137.109.15)
 Host is up (0.10s latency).
 Nmap scan report for ec2-46-137-109-16.eu-west-1.compute.amazonaws.com (46.137.109.16)
 Host is up (0.16s latency).
 Nmap scan report for ec2-46-137-109-23.eu-west-1.compute.amazonaws.com (46.137.109.23)
 Host is up (0.0933s latency).
 Nmap scan report for ec2-46-137-109-48.eu-west-1.compute.amazonaws.com (46.137.109.48)
 Host is up (0.0998s latency).
 Nmap scan report for ec2-46-137-109-51.eu-west-1.compute.amazonaws.com (46.137.109.51)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-109-62.eu-west-1.compute.amazonaws.com (46.137.109.62)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-109-71.eu-west-1.compute.amazonaws.com (46.137.109.71)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-109-76.eu-west-1.compute.amazonaws.com (46.137.109.76)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-109-109.eu-west-1.compute.amazonaws.com (46.137.109.109)
 Host is up (0.47s latency).
 Nmap scan report for ec2-46-137-109-145.eu-west-1.compute.amazonaws.com (46.137.109.145)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-109-148.eu-west-1.compute.amazonaws.com (46.137.109.148)
 Host is up (0.18s latency).
 Nmap scan report for ec2-46-137-109-184.eu-west-1.compute.amazonaws.com (46.137.109.184)
 Nmap scan report for ec2-46-137-109-189.eu-west-1.compute.amazonaws.com (46.137.109.189)
 Host is up (0.13s latency).
 Nmap scan report for ec2-46-137-109-198.eu-west-1.compute.amazonaws.com (46.137.109.198)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-109-210.eu-west-1.compute.amazonaws.com (46.137.109.210)
 Host is up (0.10s latency).
 Nmap scan report for ec2-46-137-109-217.eu-west-1.compute.amazonaws.com (46.137.109.217)
 Host is up (0.10s latency).
 Nmap scan report for ec2-46-137-109-220.eu-west-1.compute.amazonaws.com (46.137.109.220)
 Host is up (0.0999s latency).
 Nmap scan report for ec2-46-137-109-240.eu-west-1.compute.amazonaws.com (46.137.109.240)
 Host is up (0.16s latency).
 Nmap scan report for ec2-46-137-109-245.eu-west-1.compute.amazonaws.com (46.137.109.245)
 Host is up (0.11s latency).
 Nmap scan report for www.nobleprog.be (46.137.109.249)
 Host is up (0.15s latency).
 Nmap scan report for ec2-46-137-110-0.eu-west-1.compute.amazonaws.com (46.137.110.0)
 Host is up (0.16s latency).
 Nmap scan report for ec2-46-137-110-5.eu-west-1.compute.amazonaws.com (46.137.110.5)
 Host is up (0.14s latency).
 Nmap scan report for app.fernepi.net (46.137.110.7)
 Host is up (0.13s latency).
 Nmap scan report for ec2-46-137-110-18.eu-west-1.compute.amazonaws.com (46.137.110.18)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-110-28.eu-west-1.compute.amazonaws.com (46.137.110.28)

[illegible][illegible]

[illegible][illegible]

Nmap scan report for ec2-46-137-121-10.eu-west-1.compute.amazonaws.com (46.137.121.10)
 Host is up (0.13s latency).
 Nmap scan report for ec2-46-137-121-38.eu-west-1.compute.amazonaws.com (46.137.121.38)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-121-44.eu-west-1.compute.amazonaws.com (46.137.121.44)
 Host is up (0.095s latency).
 Nmap scan report for ec2-46-137-121-94.eu-west-1.compute.amazonaws.com (46.137.121.94)
 Host is up (0.18s latency).
 Nmap scan report for ec2-46-137-121-100.eu-west-1.compute.amazonaws.com (46.137.121.100)
 Host is up (0.19s latency).
 Nmap scan report for ec2-46-137-121-119.eu-west-1.compute.amazonaws.com (46.137.121.119)
 Host is up (0.091s latency).
 Nmap scan report for ec2-46-137-121-143.eu-west-1.compute.amazonaws.com (46.137.121.143)
 Host is up (0.29s latency).
 Nmap scan report for ec2-46-137-121-155.eu-west-1.compute.amazonaws.com (46.137.121.155)
 Host is up (0.13s latency).
 Nmap scan report for ec2-46-137-121-162.eu-west-1.compute.amazonaws.com (46.137.121.162)
 Host is up (0.097s latency).
 Nmap scan report for ec2-46-137-121-165.eu-west-1.compute.amazonaws.com (46.137.121.165)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-121-179.eu-west-1.compute.amazonaws.com (46.137.121.179)
 Host is up (0.16s latency).
 Nmap scan report for ec2-46-137-121-227.eu-west-1.compute.amazonaws.com (46.137.121.227)
 Host is up (0.13s latency).
 Nmap scan report for ec2-46-137-121-237.eu-west-1.compute.amazonaws.com (46.137.121.237)
 Host is up (0.14s latency).
 Nmap scan report for ec2-46-137-121-255.eu-west-1.compute.amazonaws.com (46.137.121.255)
 Host is up (0.094s latency).
 Nmap scan report for ec2-46-137-122-0.eu-west-1.compute.amazonaws.com (46.137.122.0)
 Host is up (0.13s latency).
 Nmap scan report for ec2-46-137-122-14.eu-west-1.compute.amazonaws.com (46.137.122.14)
 Host is up (0.10s latency).
 Nmap scan report for ec2-46-137-122-16.eu-west-1.compute.amazonaws.com (46.137.122.16)
 Host is up (0.14s latency).
 Nmap scan report for ec2-46-137-122-51.eu-west-1.compute.amazonaws.com (46.137.122.51)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-122-81.eu-west-1.compute.amazonaws.com (46.137.122.81)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-122-93.eu-west-1.compute.amazonaws.com (46.137.122.93)
 Host is up (0.13s latency).
 Nmap scan report for ec2-46-137-122-96.eu-west-1.compute.amazonaws.com (46.137.122.96)
 Host is up (0.17s latency).
 Nmap scan report for ec2-46-137-122-111.eu-west-1.compute.amazonaws.com (46.137.122.111)
 Host is up (0.11s latency).
 Nmap scan report for nagios.apptus.co.uk (46.137.122.132)
 Host is up (0.11s latency).
 Nmap scan report for travel-swift.com (46.137.122.144)
 Host is up (0.14s latency).
 Nmap scan report for ec2-46-137-122-147.eu-west-1.compute.amazonaws.com (46.137.122.147)
 Host is up (0.097s latency).
 Nmap scan report for ec2-46-137-122-149.eu-west-1.compute.amazonaws.com (46.137.122.149)
 Host is up (0.35s latency).
 Nmap scan report for ec2-46-137-122-168.eu-west-1.compute.amazonaws.com (46.137.122.168)
 Host is up (0.33s latency).
 Nmap scan report for ec2-46-137-122-243.eu-west-1.compute.amazonaws.com (46.137.122.243)
 Host is up (0.10s latency).
 Nmap scan report for ec2-46-137-123-3.eu-west-1.compute.amazonaws.com (46.137.123.3)
 Host is up (0.13s latency).
 Nmap scan report for ec2-46-137-123-10.eu-west-1.compute.amazonaws.com (46.137.123.10)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-123-11.eu-west-1.compute.amazonaws.com (46.137.123.11)
 Host is up (0.13s latency).
 Nmap scan report for ec2-46-137-123-15.eu-west-1.compute.amazonaws.com (46.137.123.15)
 Host is up (0.13s latency).
 Nmap scan report for ec2-46-137-123-30.eu-west-1.compute.amazonaws.com (46.137.123.30)
 Host is up (0.093s latency).
 Nmap scan report for ec2-46-137-123-88.eu-west-1.compute.amazonaws.com (46.137.123.88)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-123-97.eu-west-1.compute.amazonaws.com (46.137.123.97)
 Host is up (0.18s latency).
 Nmap scan report for ec2-46-137-123-98.eu-west-1.compute.amazonaws.com (46.137.123.98)
 Host is up (0.19s latency).
 Nmap scan report for ec2-46-137-123-135.eu-west-1.compute.amazonaws.com (46.137.123.135)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-123-143.eu-west-1.compute.amazonaws.com (46.137.123.143)
 Host is up (0.29s latency).
 Nmap scan report for ec2-46-137-123-144.eu-west-1.compute.amazonaws.com (46.137.123.144)
 Host is up (0.28s latency).
 Nmap scan report for ec2-46-137-123-163.eu-west-1.compute.amazonaws.com (46.137.123.163)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-123-168.eu-west-1.compute.amazonaws.com (46.137.123.168)
 Host is up (0.33s latency).
 Nmap scan report for ec2-46-137-123-201.eu-west-1.compute.amazonaws.com (46.137.123.201)
 Host is up (0.14s latency).
 Nmap scan report for ec2-46-137-123-203.eu-west-1.compute.amazonaws.com (46.137.123.203)
 Host is up (0.44s latency).
 Nmap scan report for ec2-46-137-123-236.eu-west-1.compute.amazonaws.com (46.137.123.236)
 Host is up (0.14s latency).
 Nmap scan report for ec2-46-137-124-18.eu-west-1.compute.amazonaws.com (46.137.124.18)
 Host is up (0.12s latency).
 Nmap scan report for ec2-46-137-124-19.eu-west-1.compute.amazonaws.com (46.137.124.19)
 Host is up (0.26s latency).
 Nmap scan report for ec2-46-137-124-29.eu-west-1.compute.amazonaws.com (46.137.124.29)
 Host is up (0.11s latency).
 Nmap scan report for ec2-46-137-124-49.eu-west-1.compute.amazonaws.com (46.137.124.49)

Host is up (0.13s latency).
Nmap scan report for ec2-46-137-124-72.eu-west-1.compute.amazonaws.com (46.137.124.72)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-124-83.eu-west-1.compute.amazonaws.com (46.137.124.83)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-124-94.eu-west-1.compute.amazonaws.com (46.137.124.94)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-124-95.eu-west-1.compute.amazonaws.com (46.137.124.95)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-124-101.eu-west-1.compute.amazonaws.com (46.137.124.101)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-124-103.eu-west-1.compute.amazonaws.com (46.137.124.103)
Host is up (0.16s latency).
Nmap scan report for ec2-46-137-124-121.eu-west-1.compute.amazonaws.com (46.137.124.121)
Host is up (0.097s latency).
Nmap scan report for ec2-46-137-124-126.eu-west-1.compute.amazonaws.com (46.137.124.126)
Host is up (0.099s latency).
Nmap scan report for ec2-46-137-124-132.eu-west-1.compute.amazonaws.com (46.137.124.132)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-124-142.eu-west-1.compute.amazonaws.com (46.137.124.142)
Host is up (0.31s latency).
Nmap scan report for ec2-46-137-124-148.eu-west-1.compute.amazonaws.com (46.137.124.148)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-124-152.eu-west-1.compute.amazonaws.com (46.137.124.152)
Host is up (0.30s latency).
Nmap scan report for ec2-46-137-124-155.eu-west-1.compute.amazonaws.com (46.137.124.155)
Host is up (0.16s latency).
Nmap scan report for ec2-46-137-124-162.eu-west-1.compute.amazonaws.com (46.137.124.162)
Host is up (0.42s latency).
Nmap scan report for ec2-46-137-124-169.eu-west-1.compute.amazonaws.com (46.137.124.169)
Host is up (0.17s latency).
Nmap scan report for mail.hypermatrix.com (46.137.124.173)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-124-176.eu-west-1.compute.amazonaws.com (46.137.124.176)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-124-185.eu-west-1.compute.amazonaws.com (46.137.124.185)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-124-190.eu-west-1.compute.amazonaws.com (46.137.124.190)
Host is up (0.19s latency).
Nmap scan report for ec2-46-137-124-194.eu-west-1.compute.amazonaws.com (46.137.124.194)
Host is up (0.091s latency).
Nmap scan report for ec2-46-137-124-233.eu-west-1.compute.amazonaws.com (46.137.124.233)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-124-236.eu-west-1.compute.amazonaws.com (46.137.124.236)
Host is up (0.14s latency).
Nmap scan report for ec2-46-137-124-252.eu-west-1.compute.amazonaws.com (46.137.124.252)
Host is up (0.11s latency).

Nmap scan report for ec2-46-137-125-10.eu-west-1.compute.amazonaws.com (46.137.125.10)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-125-22.eu-west-1.compute.amazonaws.com (46.137.125.22)
Host is up (0.14s latency).
Nmap scan report for ec2-46-137-125-81.eu-west-1.compute.amazonaws.com (46.137.125.81)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-125-104.eu-west-1.compute.amazonaws.com (46.137.125.104)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-125-106.eu-west-1.compute.amazonaws.com (46.137.125.106)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-125-132.eu-west-1.compute.amazonaws.com (46.137.125.132)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-125-139.eu-west-1.compute.amazonaws.com (46.137.125.139)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-125-146.eu-west-1.compute.amazonaws.com (46.137.125.146)
Host is up (0.098s latency).
Nmap scan report for ec2-46-137-125-150.eu-west-1.compute.amazonaws.com (46.137.125.150)
Host is up (0.34s latency).
Nmap scan report for ec2-46-137-125-153.eu-west-1.compute.amazonaws.com (46.137.125.153)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-125-164.eu-west-1.compute.amazonaws.com (46.137.125.164)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-125-214.eu-west-1.compute.amazonaws.com (46.137.125.214)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-125-235.eu-west-1.compute.amazonaws.com (46.137.125.235)
Host is up (0.11s latency).
Nmap scan report for www1.1c-bitrix.ru (46.137.125.240)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-126-8.eu-west-1.compute.amazonaws.com (46.137.126.8)
Host is up (0.15s latency).
Nmap scan report for ec2-46-137-126-83.eu-west-1.compute.amazonaws.com (46.137.126.83)
Host is up (0.14s latency).
Nmap scan report for ec2-46-137-126-94.eu-west-1.compute.amazonaws.com (46.137.126.94)
Host is up (0.14s latency).
Nmap scan report for ec2-46-137-126-101.eu-west-1.compute.amazonaws.com (46.137.126.101)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-126-110.eu-west-1.compute.amazonaws.com (46.137.126.110)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-126-128.eu-west-1.compute.amazonaws.com (46.137.126.128)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-126-130.eu-west-1.compute.amazonaws.com (46.137.126.130)
Host is up (0.16s latency).
Nmap scan report for ec2-46-137-126-137.eu-west-1.compute.amazonaws.com (46.137.126.137)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-126-144.eu-west-1.compute.amazonaws.com (46.137.126.144)
Host is up (0.28s latency).
Nmap scan report for ec2-46-137-126-166.eu-west-1.compute.amazonaws.com (46.137.126.166)

Host is up (0.11s latency).
Nmap scan report for ec2-46-137-126-169.eu-west-1.compute.amazonaws.com (46.137.126.169)
Host is up (0.29s latency).
Nmap scan report for ec2-46-137-126-185.eu-west-1.compute.amazonaws.com (46.137.126.185)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-126-189.eu-west-1.compute.amazonaws.com (46.137.126.189)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-126-204.eu-west-1.compute.amazonaws.com (46.137.126.204)
Host is up (0.10s latency).
Nmap scan report for ec2-46-137-126-226.eu-west-1.compute.amazonaws.com (46.137.126.226)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-126-244.eu-west-1.compute.amazonaws.com (46.137.126.244)
Host is up (0.18s latency).
Nmap scan report for ec2-46-137-126-248.eu-west-1.compute.amazonaws.com (46.137.126.248)
Host is up (0.098s latency).
Nmap scan report for ec2-46-137-127-1.eu-west-1.compute.amazonaws.com (46.137.127.1)
Host is up (0.14s latency).
Nmap scan report for ec2-46-137-127-16.eu-west-1.compute.amazonaws.com (46.137.127.16)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-127-27.eu-west-1.compute.amazonaws.com (46.137.127.27)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-127-60.eu-west-1.compute.amazonaws.com (46.137.127.60)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-127-99.eu-west-1.compute.amazonaws.com (46.137.127.99)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-127-118.eu-west-1.compute.amazonaws.com (46.137.127.118)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-127-122.eu-west-1.compute.amazonaws.com (46.137.127.122)
Host is up (0.099s latency).
Nmap scan report for ec2-46-137-127-131.eu-west-1.compute.amazonaws.com (46.137.127.131)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-127-149.eu-west-1.compute.amazonaws.com (46.137.127.149)
Host is up (0.35s latency).
Nmap scan report for ec2-46-137-127-150.eu-west-1.compute.amazonaws.com (46.137.127.150)
Host is up (0.13s latency).
Nmap scan report for ec2-46-137-127-167.eu-west-1.compute.amazonaws.com (46.137.127.167)
Host is up (0.34s latency).
Nmap scan report for ec2-46-137-127-173.eu-west-1.compute.amazonaws.com (46.137.127.173)
Host is up (0.11s latency).
Nmap scan report for ec2-46-137-127-209.eu-west-1.compute.amazonaws.com (46.137.127.209)
Host is up (0.12s latency).
Nmap scan report for ec2-46-137-127-234.eu-west-1.compute.amazonaws.com (46.137.127.234)
Host is up (0.089s latency).
Nmap scan report for ec2-46-137-127-247.eu-west-1.compute.amazonaws.com (46.137.127.247)
Host is up (0.10s latency).
Nmap done: 32768 IP addresses (2428 hosts up) scanned in 4660.61 seconds

nikto -h http://172.17.0.2:3000

Scopo: identificare configurazioni pericolose, file nascosti, vulnerabilità note del web server Juice Shop; trovare directory esposte, header HTTP informativi e possibili fughe di informazioni.

Funzionamento: Nikto effettua richieste HTTP con numerose firme note, verifica la risposta e segnala problemi comuni (es. directory indexing, file di debug, script obsoleti, header deboli, ecc.).

Output:

```
- Nikto v2.1.5
-----
+ Target IP:      172.17.0.2
+ Target Hostname: 172.17.0.2
+ Target Port:    3000
+ Start Time:     2025-07-14 11:44:53 (GMT2)
-----
+ Server: No banner retrieved
+ Server leaks inodes via ETags, header found with file /, fields: 0xW/138f5 0x198083f0de5
+ Uncommon header 'x-recruiting' found, with contents: /#jobs
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'feature-policy' found, with contents: payment 'self'
+ Uncommon header 'access-control-allow-origin' found, with contents: *
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
```

```
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ File/dir '/ftp/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Uncommon header 'access-control-allow-methods' found, with contents:
GET,HEAD,PUT,PATCH,POST,DELETE
+ OSVDB-3092: /css: This might be interesting...
+ OSVDB-3092: /ftp/: This might be interesting...
+ OSVDB-3092: /public/: This might be interesting...
+ 6544 items checked: 2 error(s) and 12 item(s) reported on remote host
+ End Time:      2025-07-14 11:47:07 (GMT2) (134 seconds)
-----
+ 1 host(s) tested
```

Strumenti

<https://dnschecker.org/>

Scopo: confermare che il dominio Juice Shop sia risolvibile da tutto il mondo; verificare la propagazione globale DNS e l'affidabilità del dominio in ottica CTF o esercitazione distribuita.

Funzionamento: il sito effettua richieste DNS da vari nodi nel mondo (Google DNS, OpenDNS, ecc.) per vedere quale IP viene restituito dal dominio. È utile per vedere eventuali problemi di propagazione o cache DNS.

Output:



Scopo: recuperare informazioni OSINT pubblicamente disponibili su IP pubblici, come quelli della demo Juice Shop; verificare le porte aperte, i certificati SSL, il sistema operativo, il provider cloud, eventuali vulnerabilità note.

Funzionamento: Shodan esegue scansioni periodiche su tutto Internet su svariate porte, archivia le “banner response” (es. header HTTP, certificati SSL, info dei servizi) e le mette a disposizione via web (è come un motore di ricerca per host).

Output:

The screenshot displays the Shodan search results for the IP address 46.137.15.86. The interface is divided into several sections:

- Open Ports:** Shows two open ports: 80 and 443.
- 80 / TCP:** Displays the HTTP response for port 80, indicating "No such app" and providing details like "HTTP/1.1 404 Not Found", "Content-Length: 548", "Cache-Control: no-cache, no-store", "Content-Type: text/html; charset=utf-8", "Date: 2025-07-18 03:25:13.035788762 +0000 UTC", and "Server: heroku-router".
- 443 / TCP:** Displays the SSL certificate for port 443, indicating "No such app" and providing details like "HTTP/1.1 404 Not Found", "Content-Length: 548", "Cache-Control: no-cache, no-store", "Content-Type: text/html; charset=utf-8", "Date: 2025-07-18 03:25:13.437062377 +0000 UTC", and "Server: heroku-router".
- General Information:** Provides a summary of the host's details, including Hostnames, Domains, Cloud Provider, Cloud Region, Cloud Service, Country, City, Organization, ISP, and ASN.

The "General Information" section details the following information:

- Hostnames:** ec2-46-137-15-86.eu-west-1.compute.amazonaws.com
- Domains:** amazonaws.com
- Cloud Provider:** Amazon
- Cloud Region:** eu-west-1
- Cloud Service:** EC2
- Country:** Ireland
- City:** Dublin
- Organization:** Amazon Web Services, Elastic Compute Cloud, EC2, EU
- ISP:** Amazon.com, Inc.
- ASN:** AS16509

Scopo: ottenere informazioni su IP, ASN, e blocchi CIDR usati da AWS per Juice Shop; capire a quale rete appartiene un certo IP e se ci sono host “vicini” o simili nello stesso intervallo.

Funzionamento: fornisce informazioni BGP (routing su Internet), e WHOIS, mostrando proprietà, reti, provider, e dettagli di routing IP grazie ai database pubblici.

Output:

[46.137.15.86](https://bgp.he.net/46.137.15.86) (ec2-46-137-15-86.eu-west-1.compute.amazonaws.com)

Announced By		
Origin AS	Announcement	Description
AS16509	46.137.0.0/16	
AS16509	46.137.0.0/17	

Address has 57 hosts associated with it.

Scopo: verifica di JSON Web Tokens per testare meccanismi di autenticazione; decodifica e manipolazione di token JWT per bypassare controlli di accesso, controllo della firma e test di vulnerabilità come “none algorithm” o chiavi deboli.

Funzionamento: decodifica, verifica e genera JWT (token usati per autenticazione e autorizzazione), mostra header, payload e firma del token, testa la sicurezza dei token, verifica la validità e identifica vulnerabilità come JWT malformati o firmati con chiavi deboli.

Output:

The screenshot displays the JWT Debugger application. On the left, the 'JSON WEB TOKEN (JWT)' section shows a 'Valid JWT' status with a message: 'Fix public key input errors to verify signature.' Below this is a long, base64-encoded JWT token. On the right, the 'CLAIMS TABLE' section shows the decoded payload in JSON format:

```
{
  "typ": "JWT",
  "alg": "RS256"
}
```

Below the claims table, the 'DECODED PAYLOAD' section shows the decoded payload in JSON format:

```
{
  "status": "success",
  "data": {
    "id": 3,
    "username": "",
    "email": "bender@juice-sh.op",
    "password": "0c36e517e3fa95aabf1bbffc6744a4ef",
    "role": "customer",
    "deluxeToken": "",
    "lastLoginIp": "",
    "profileImage": "assets/public/images/uploads/default.svg",
    "totpSecret": "",
    "isActive": true,
    "createdAt": "2025-07-26 12:46:11.094 +00:00",
    "updatedAt": "2025-07-26 12:46:11.094 +00:00",
    "deletedAt": null
  },
  "iat": 1753535559
}
```

<https://webhook.site>

Scopo: verificare vulnerabilità di tipo Server-Side Request Forgery (SSRF); dimostrare che il server Juice Shop fa effettivamente richieste HTTP su URL arbitrari controllati dall'utente.

Funzionamento: fornisce un endpoint pubblico temporaneo che registra qualsiasi richiesta HTTP in arrivo. Se un'applicazione target effettua richieste verso quel l'URL, viene riportato tutto nel log: metodo, IP, header, payload.

Output:

The screenshot shows the Webhook.site interface. On the left, there's a search bar and a list of requests. The selected request is a GET request to `https://webhook.site/916b6cb1-f587-4411-b629-6010966a2d84` from IP `137.204.150.21` at `17/07/2025 10:35:00`. The right panel shows the request details and headers.

Request Details & Headers	
Method	GET
URL	<code>https://webhook.site/916b6cb1-f587-4411-b629-6010966a2d84</code>
Host	<code>137.204.150.21</code> Whois Shodan Netify Censys VirusTotal
Date	<code>17/07/2025 10:35:00</code> (alcuni secondi fa)
Size	0 bytes
Time	0.000 sec
ID	<code>786cba2b-6163-4d1f-9a3c-1abfca93c68d</code>
Note	Add Note
accept-encoding	<code>br, gzip, deflate</code>
user-agent	<code>node</code>
sec-fetch-mode	<code>cors</code>
accept-language	<code>*</code>
accept	<code>*/*</code>
host	<code>webhook.site</code>

htmledit.squarefree.com

Scopo: editor HTML/JS in tempo reale per testare codice client-side; crafting di payload XSS persistenti o riflessivi; simulazione di attacchi phishing con interfacce HTML personalizzate; debug e test di codice malevolo in ambienti isolati.

Funzionamento: permette di scrivere e visualizzare codice HTML/CSS/JS direttamente nel browser. Testa payload XSS, crafting di pagine malevole o simulazioni di attacchi client-side.

Output:

The screenshot shows the htmledit.squarefree.com editor. The left pane contains HTML and JavaScript code. The right pane shows the rendered output, which is a button labeled "Carica Prodotti" and a JSON response.

```
<!DOCTYPE html>
<html>
<head>
<title>API Test Juice Shop</title>
</head>
<body>
<button onclick="getProducts()">Carica Prodotti</button>
<pre id="output"></pre>

<script>
async function getProducts() {
  try {
    const response = await fetch('http://localhost:3000/api/Products', {
      method: 'GET',
      headers: {
        'Content-Type': 'application/json'
      }
    });
  } catch (error) {
    throw new Error('Errore nella richiesta: ' + response.status);
  }

  const data = await response.json();
  document.getElementById('output').textContent = JSON.stringify(data, null, 2);
} catch (error) {
  document.getElementById('output').textContent = 'Errore: ' + error.message;
}
}
</script>
```

The rendered output shows a button labeled "Carica Prodotti" and a JSON response:

```
{
  "status": "success",
  "data": [
    {
      "id": 1,
      "name": "Apple Juice (1000ml)",
      "description": "The all-time classic.",
      "price": 1.99,
      "deluxePrice": 0.99,
      "image": "apple_juice.jpg",
      "createdAt": "2025-07-17T08:27:32.658Z",
      "updatedAt": "2025-07-17T08:27:32.658Z",
      "deletedAt": null
    },
    {
      "id": 2,
      "name": "Orange Juice (1000ml)",
      "description": "Made from oranges hand-picked by Uncle Dittmeyer.",
      "price": 2.99,
      "deluxePrice": 2.49,
      "image": "orange_juice.jpg",
      "createdAt": "2025-07-17T08:27:32.659Z",
      "updatedAt": "2025-07-17T08:27:32.659Z",
      "deletedAt": null
    }
  ]
}
```


Postman - http://localhost:3000/api/Users (enumerazione utenti)

Scopo: identificare account attivi, raccogliere informazioni utili per attacchi di social engineering o brute force, verificare se l'endpoint è protetto da autenticazione.

Funzionamento: utilizza un metodo GET per recuperare tutti gli utenti registrati nel sistema.

Output:

```
{
  "status": "success",
  "data": [
    {
      "id": 1,
      "username": "",
      "email": "admin@juice-sh.op",
      "role": "admin",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/defaultAdmin.png",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.094Z",
      "updatedAt": "2025-07-26T12:46:11.094Z",
      "deletedAt": null
    },
    {
      "id": 2,
      "username": "",
      "email": "jim@juice-sh.op",
      "role": "customer",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/default.svg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.094Z",
      "updatedAt": "2025-07-26T12:46:11.094Z",
      "deletedAt": null
    },
    {
      "id": 3,
      "username": "",
      "email": "bender@juice-sh.op",
      "role": "customer",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/default.svg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.094Z",
      "updatedAt": "2025-07-26T12:46:11.094Z",
      "deletedAt": null
    },
    {
      "id": 4,
      "username": "bkimminich",
      "email": "bjoern.kimminich@gmail.com",
      "role": "admin",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/defaultAdmin.png",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.094Z",
      "updatedAt": "2025-07-26T12:46:11.094Z",
      "deletedAt": null
    },
    {
      "id": 5,
      "username": "",
      "email": "ciso@juice-sh.op",
      "role": "deluxe",
      "deluxeToken": "d715c2c75d4a42d3825a050e0a163c1959b51165373f17bd8eed7b1e05b20d",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/default.svg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.096Z",
      "updatedAt": "2025-07-26T12:46:11.096Z",
      "deletedAt": null
    },
    {
      "id": 6,
      "username": "",
      "email": "support@juice-sh.op",
      "role": "admin",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/defaultAdmin.png",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.096Z",
      "updatedAt": "2025-07-26T12:46:11.096Z",
      "deletedAt": null
    },
    {
      "id": 7,
      "username": "",
      "email": "morty@juice-sh.op",
      "role": "customer",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/default.svg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.096Z",
      "deletedAt": null
    },
    {
      "id": 8,
      "username": "",
      "email": "mc.safesearch@juice-sh.op",
      "role": "customer",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/default.svg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.096Z",
      "updatedAt": "2025-07-26T12:46:11.096Z",
      "deletedAt": null
    },
    {
      "id": 9,
      "username": "",
      "email": "J12934@juice-sh.op",
      "role": "admin",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/defaultAdmin.png",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.097Z",
      "updatedAt": "2025-07-26T12:46:11.097Z",
      "deletedAt": null
    },
    {
      "id": 10,
      "username": "wurstbrot",
      "email": "wurstbrot@juice-sh.op",
      "role": "admin",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/defaultAdmin.png",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.097Z",
      "updatedAt": "2025-07-26T12:46:11.097Z",
      "deletedAt": null
    },
    {
      "id": 11,
      "username": "",
      "email": "amy@juice-sh.op",
      "role": "customer",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/default.svg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.097Z",
      "updatedAt": "2025-07-26T12:46:11.097Z",
      "deletedAt": null
    },
    {
      "id": 12,
      "username": "",
      "email": "bjoern@juice-sh.op",
      "role": "admin",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/12.png",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.097Z",
      "updatedAt": "2025-07-26T12:46:11.097Z",
      "deletedAt": null
    },
    {
      "id": 13,
      "username": "",
      "email": "bjoern@owasp.org",
      "role": "deluxe",
      "deluxeToken": "efc2f1599ce2d93440d523a1fa1f5a413b70cf3ac97156bd6fab9b5ddfcb0e4",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/13.jpg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.097Z",
      "updatedAt": "2025-07-26T12:46:11.097Z",
      "deletedAt": null
    },
    {
      "id": 15,
      "username": "",
      "email": "accountant@juice-sh.op",
      "role": "accounting",
      "deluxeToken": "",
      "lastLoginIp": "123.456.789",
      "profileImage": "assets/public/images/uploads/default.svg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.097Z",
      "updatedAt": "2025-07-26T12:46:11.097Z",
      "deletedAt": null
    },
    {
      "id": 16,
      "username": "",
      "email": "uvogin@juice-sh.op",
      "role": "customer",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/default.svg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.097Z",
      "updatedAt": "2025-07-26T12:46:11.097Z",
      "deletedAt": null
    },
    {
      "id": 17,
      "username": "",
      "email": "demo",
      "role": "customer",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/default.svg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.097Z",
      "updatedAt": "2025-07-26T12:46:11.097Z",
      "deletedAt": null
    },
    {
      "id": 18,
      "username": "jOhNny",
      "email": "john@juice-sh.op",
      "role": "customer",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/default.svg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.097Z",
      "updatedAt": "2025-07-26T12:46:11.097Z",
      "deletedAt": null
    },
    {
      "id": 19,
      "username": "E=ma",
      "email": "emma@juice-sh.op",
      "role": "customer",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/default.svg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.097Z",
      "updatedAt": "2025-07-26T12:46:11.097Z",
      "deletedAt": null
    },
    {
      "id": 20,
      "username": "SmilinStan",
      "email": "stan@juice-sh.op",
      "role": "deluxe",
      "deluxeToken": "8f70e0f4b05685eff1ab979e8f5d7c39850369309bb206c2ad3f7d51a1f4c39",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/20.jpg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.097Z",
      "updatedAt": "2025-07-26T12:46:11.097Z",
      "deletedAt": null
    },
    {
      "id": 21,
      "username": "evmrox",
      "email": "ethereum@juice-sh.op",
      "role": "deluxe",
      "deluxeToken": "b49b30b294d8c76f5a34fc243b9b9cccb057b3f675b07a5782276a547957f8f",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/default.svg",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.098Z",
      "updatedAt": "2025-07-26T12:46:11.098Z",
      "deletedAt": null
    },
    {
      "id": 22,
      "username": "",
      "email": "testing@juice-sh.op",
      "role": "admin",
      "deluxeToken": "",
      "lastLoginIp": "",
      "profileImage": "assets/public/images/uploads/defaultAdmin.png",
      "isActive": true,
      "createdAt": "2025-07-26T12:46:11.098Z",
      "updatedAt": "2025-07-26T12:46:11.098Z",
      "deletedAt": null
    }
  ]
}
```

Postman - <http://localhost:3000/rest/products/search> (enumerazione prodotti)

Scopo: identificare la struttura dei dati esposti, analizzare i parametri accettati (es. query, filtri), cercare vulnerabilità come SQL injection, IDOR (Insecure Direct Object Reference), o accessi non autorizzati.

Funzionamento: usa un metodo GET per restituire un elenco di prodotti preso dal database.

Output:

```
{
  "status": "success",
  "data": [
    {
      "id": 1,
      "name": "Apple Juice (1000ml)",
      "description": "The all-time classic.",
      "price": 1.99,
      "deluxePrice": 0.99,
      "image": "apple_juice.jpg",
      "createdAt": "2025-07-26 12:46:19.820 +00:00",
      "updatedAt": "2025-07-26 12:46:19.820 +00:00",
      "deletedAt": null
    },
    {
      "id": 24,
      "name": "Apple Pomace",
      "description": "Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href='\"#recycle\"'>sent back to us</a> for recycling.",
      "price": 0.89,
      "deluxePrice": 0.89,
      "image": "apple_pressings.jpg",
      "createdAt": "2025-07-26 12:46:19.824 +00:00",
      "updatedAt": "2025-07-26 12:46:19.824 +00:00",
      "deletedAt": null
    },
    {
      "id": 6,
      "name": "Banana Juice (1000ml)",
      "description": "Monkeys love it the most.",
      "price": 1.99,
      "deluxePrice": 1.99,
      "image": "banana_juice.jpg",
      "createdAt": "2025-07-26 12:46:19.820 +00:00",
      "updatedAt": "2025-07-26 12:46:19.820 +00:00",
      "deletedAt": null
    },
    {
      "id": 42,
      "name": "Best Juice Shop Salesman Artwork",
      "description": "Unique digital painting depicting Stan, our most qualified and almost profitable salesman. He made a successful career in selling used ships, coffins, krypts, crosses, real estate, life insurance, restaurant supplies, voodoo enhanced asbestos and courtroom souvenirs before <em>finally</em> adding his expertise to the Juice Shop marketing team.",
      "price": 5000,
      "deluxePrice": 5000,
      "image": "artwork42.jpg",
      "createdAt": "2025-07-26 12:46:19.826 +00:00",
      "updatedAt": "2025-07-26 12:46:19.826 +00:00",
      "deletedAt": null
    },
    {
      "id": 30,
      "name": "Carrot Juice (1000ml)",
      "description": "As the old German saying goes: 'Carrots are good for the eyes. Or has anyone ever seen a rabbit with glasses?'",
      "price": 2.99,
      "deluxePrice": 2.99,
      "image": "carrot_juice.jpg",
      "createdAt": "2025-07-26 12:46:19.825 +00:00",
      "updatedAt": "2025-07-26 12:46:19.825 +00:00",
      "deletedAt": null
    },
    {
      "id": 3,
      "name": "Eggfruit Juice (500ml)",
      "description": "Now with even more exotic flavour.",
      "price": 8.99,
      "deluxePrice": 8.99,
      "image": "eggfruit_juice.jpg",
      "createdAt": "2025-07-26 12:46:19.820 +00:00",
      "updatedAt": "2025-07-26 12:46:19.820 +00:00",
      "deletedAt": null
    },
    {
      "id": 25,
      "name": "Fruit Press",
      "description": "Fruits go in. Juice comes out. Pomace you can send back to us for recycling purposes.",
      "price": 89.99,
      "deluxePrice": 89.99,
      "image": "fruit_press.jpg",
      "createdAt": "2025-07-26 12:46:19.824 +00:00",
      "updatedAt": "2025-07-26 12:46:19.824 +00:00",
      "deletedAt": null
    },
    {
      "id": 22,
      "name": "Green Smoothie",
      "description": "Looks poisonous but is actually very good for your health! Made from green cabbage, spinach, kiwi and grass.",
      "price": 1.99,
      "deluxePrice": 1.99,
      "image": "green_smoothie.jpg",
      "createdAt": "2025-07-26 12:46:19.823 +00:00",
      "updatedAt": "2025-07-26 12:46:19.823 +00:00",
      "deletedAt": null
    },
    {
      "id": 41,
      "name": "Juice Shop 'Permafrost' 2020 Edition",
      "description": "Exact version of <a href='\"https://github.com/juice-shop/releases/tag/v9.3.1-PERMAFROST\"'>OWASP Juice Shop</a> that was archived on 02/02/2020<a href='\"https://github.com/juice-shop/releases/tag/v9.3.1-PERMAFROST\"'> by the GitHub Archive Program</a> and ultimately went into the <a href='\"https://github.blog/2020-07-16-github-archive-program-the-journey-of-the-w-oids-open-source-code-to-the-arc\"'>Arctic Code Vault</a> on July 8, 2020 where it will be safely stored for at least 1000 years.",
      "price": 9999.99,
      "deluxePrice": 9999.99,
      "image": "permafrost.jpg",
      "createdAt": "2025-07-26 12:46:19.826 +00:00",
      "updatedAt": "2025-07-26 12:46:19.826 +00:00",
      "deletedAt": null
    },
    {
      "id": 5,
      "name": "Lemon Juice (500ml)",
      "description": "Sour but full of vitamins.",
      "price": 2.99,
      "deluxePrice": 1.99,
      "image": "lemon_juice.jpg",
      "createdAt": "2025-07-26 12:46:19.820 +00:00",
      "updatedAt": "2025-07-26 12:46:19.820 +00:00",
      "deletedAt": null
    },
    {
      "deletedAt": null
    },
    {
      "id": 33,
      "name": "Melon Bike (Comeback-Product 2018 Edition)",
      "description": "The wheels of this bicycle are made from real water melons. You might not want to ride it up/down the curb too hard.",
      "price": 2999,
      "deluxePrice": 2999,
      "image": "melon_bike.jpeg",
      "createdAt": "2025-07-26 12:46:19.825 +00:00",
      "updatedAt": "2025-07-26 12:46:19.825 +00:00",
      "deletedAt": null
    },
    {
      "id": 38,
      "name": "OWASP Juice Shop 'King of the Hill' Facemask",
      "description": "Facemask with compartment for filter from 50% cotton and 50% polyester.",
      "price": 13.49,
      "deluxePrice": 13.49,
      "image": "fan_facemask.jpg",
      "createdAt": "2025-07-26 12:46:19.825 +00:00",
      "updatedAt": "2025-07-26 12:46:19.825 +00:00",
      "deletedAt": null
    },
    {
      "id": 8,
      "name": "OWASP Juice Shop CTF Girlie-Shirt",
      "description": "For serious Capture-the-Flag heroines only!",
      "price": 22.49,
      "deluxePrice": 22.49,
      "image": "fan_girlie.jpg",
      "createdAt": "2025-07-26 12:46:19.820 +00:00",
      "updatedAt": "2025-07-26 12:46:19.820 +00:00",
      "deletedAt": null
    },
    {
      "id": 43,
      "name": "OWASP Juice Shop Card (non-foil)",
      "description": "Mythic rare <em>(obviously...)</em> card 'OWASP Juice Shop' with three distinctly useful abilities. Alpha printing, mint condition. A true collectors piece to own!",
      "price": 1000,
      "deluxePrice": 1000,
      "image": "card_alpha.jpg",
      "createdAt": "2025-07-26 12:46:19.826 +00:00",
      "updatedAt": "2025-07-26 12:46:19.826 +00:00",
      "deletedAt": null
    },
    {
      "id": 34,
      "name": "OWASP Juice Shop Coaster (10pcs)",
      "description": "Our 95mm circle coasters are printed in full color and made from thick, premium coaster board.",
      "price": 19.99,
      "deluxePrice": 19.99,
      "image": "coaster.jpg",
      "createdAt": "2025-07-26 12:46:19.825 +00:00",
      "updatedAt": "2025-07-26 12:46:19.825 +00:00",
      "deletedAt": null
    },
    {
      "id": 37,
      "name": "OWASP Juice Shop Holographic Sticker",
      "description": "Die-cut holographic sticker. Stand out from those 08/15-sticker-covered laptops with this shiny beacon of 80's coolness!",
      "price": 2,
      "deluxePrice": 2,
      "image": "holo_sticker.png",
      "createdAt": "2025-07-26 12:46:19.825 +00:00",
      "updatedAt": "2025-07-26 12:46:19.825 +00:00",
      "deletedAt": null
    },
    {
      "id": 19,
      "name": "OWASP Juice Shop Hoodie",
      "description": "Mr. Robot-style apparel. But in black. And with logo.",
      "price": 49.99,
      "deluxePrice": 49.99,
      "image": "fan_hoodie.jpg",
      "createdAt": "2025-07-26 12:46:19.823 +00:00",
      "updatedAt": "2025-07-26 12:46:19.823 +00:00",
      "deletedAt": null
    },
    {
      "id": 13,
      "name": "OWASP Juice Shop Iron-Ons (16pcs)",
      "description": "Upgrade your clothes with washer safe <a href='\"https://www.stickeryou.com/products/owasp-juice-shop-794\"'>target='\"_blank\"'>iron-ons</a> of the OWASP Juice Shop or CTF Extension logo!",
      "price": 14.99,
      "deluxePrice": 14.99,
      "image": "iron-on.jpg",
      "createdAt": "2025-07-26 12:46:19.822 +00:00",
      "updatedAt": "2025-07-26 12:46:19.822 +00:00",
      "deletedAt": null
    },
    {
      "id": 45,
      "name": "OWASP Juice Shop LEGO™ Tower",
      "description": "Want to host a Juice Shop CTF in style? Build <a href='\"https://github.com/OWASP/owasp-swag/blob/master/projects/juice-shop/lego/OWASP%20JuiceShop%20Pi-server%201.2.pdf\"'>your own LEGO™ tower</a> which holds four Raspberry Pi 4 models with PoE HAT modules <a href='\"https://github.com/juice-shop/multi-juicer/blob/main/guides/raspberry-pi/rasp-berry-pi.md\"'>target='\"_blank\"'>running a MultiJuicer Kubernetes cluster</a>! Wire to a switch and connect to your network to have an out-of-the-box ready CTF up in no time!",
      "price": 799,
      "deluxePrice": 799,
      "image": "lego_case.jpg",
      "createdAt": "2025-07-26 12:46:19.826 +00:00",
      "updatedAt": "2025-07-26 12:46:19.826 +00:00",
      "deletedAt": null
    },
    {
      "id": 26,
      "name": "OWASP Juice Shop Logo (3D-printed)",
      "description": "This rare item was designed and handcrafted in Sweden. This is why it is so incredibly expensive despite its complete lack of purpose.",
      "price": 99.99,
      "deluxePrice": 99.99,
      "image": "3d_keychain.jpg",
      "createdAt": "2025-07-26 12:46:19.824 +00:00",
      "updatedAt": "2025-07-26 12:46:19.824 +00:00",
      "deletedAt": null
    },
    {
      "id": 14,
      "name": "OWASP Juice Shop Magnets (16pcs)",
      "description": "Your fridge will be even cooler with these OWASP Juice Shop or CTF Extension logo <a href='\"https://www.stickeryou.com/products/owasp-juice-shop-794\"'>target='\"_blank\"'>magnets</a>!",
      "price": 15.99,
      "deluxePrice": 15.99,
      "image": "magnets.jpg",
      "createdAt": "2025-07-26 12:46:19.822 +00:00",
      "updatedAt": "2025-07-26 12:46:19.822 +00:00",
      "deletedAt": null
    },
    {
      "id": 18,
      "name": "OWASP Juice Shop Mug",
      "description": "Black mug with regular logo on one side and CTF logo on the other! Your colleagues will envy you!",
      "price": 21.99,
      "deluxePrice": 21.99,
      "image": "fan_mug.jpg",
      "createdAt": "2025-07-26 12:46:19.823 +00:00",
      "updatedAt": "2025-07-26 12:46:19.823 +00:00",
      "deletedAt": null
    },
    {
      "id": 15,
      "name": "OWASP Juice Shop Sticker Page",
      "description": "Massive decoration opportunities with these OWASP Juice Shop or CTF Extension <a href='\"https://www.stickeryou.com/products/owasp-juice-shop-794\"'>target='\"_blank\"'>sticker pages</a>! Each page has 16 stickers on it.",
      "price": 9.99,
      "deluxePrice": 9.99,
      "image": "sticker_page.jpg",
      "createdAt": "2025-07-26 12:46:19.823 +00:00",
      "updatedAt": "2025-07-26 12:46:19.823 +00:00",
      "deletedAt": null
    },
    {
      "id": 16,
      "name": "OWASP Juice Shop Sticker Single",
      "description": "Super high-quality vinyl <a href='\"https://www.stickeryou.com/products/owasp-juice-shop-794\"'>target='\"_blank\"'>sticker single</a> with the OWASP Juice Shop or CTF Extension logo! The ultimate laptop decal!",
      "price": 4.99,
      "deluxePrice": 4.99,
      "image": "sticker_single.jpg",
      "createdAt": "2025-07-26 12:46:19.823 +00:00",
      "updatedAt": "2025-07-26 12:46:19.823 +00:00",
      "deletedAt": null
    },
    {
      "id": 7,
      "name": "OWASP Juice Shop T-Shirt",
      "description": "Real fans wear it 24/7!",
      "price": 22.49,
      "deluxePrice": 22.49,
      "image": "fan_tshirt.jpg",
      "createdAt": "2025-07-26 12:46:19.820 +00:00",
      "updatedAt": "2025-07-26 12:46:19.820 +00:00",
      "deletedAt": null
    },
    {
      "id": 17,
      "name": "OWASP Juice Shop Temporary Tattoos (16pcs)",
      "description": "Get one of these <a href='\"https://www.stickeryou.com/products/owasp-juice-shop-794\"'>target='\"_blank\"'>temporary tattoos</a> to proudly wear the OWASP Juice Shop or CTF Extension logo on your skin! If you tweet a photo of yourself with the tattoo, you get a couple of our stickers for free! Please mention <a href='\"https://twitter.com/owasp_juiceshop\"'>target='\"_blank\"'>code</a>@owasp_juiceshop<code></code> in your tweet!",
      "price": 14.99,
      "deluxePrice": 14.99,
      "image": "tattoo.jpg",
      "createdAt": "2025-07-26 12:46:19.823 +00:00",
      "updatedAt": "2025-07-26 12:46:19.823 +00:00",
      "deletedAt": null
    },
    {
      "id": 20,
      "name": "OWASP Juice Shop-CTF Velcro Patch",
      "description": "4x3.5" embroidered patch with velcro backside. The ultimate decal for every tactical bag or backpack!",
      "price": 2.92,
      "deluxePrice": 2.92,
      "image": "velcro-patch.jpg",
      "createdAt": "2025-07-26 12:46:19.823 +00:00",
      "updatedAt": "2025-07-26 12:46:19.823 +00:00",
      "deletedAt": null
    },
    {
      "id": 9,
      "name": "OWASP SSL Advanced Forensic Tool (O-Saft)",
      "description": "O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. <a href='\"https://www.owasp.org/index.php/O-Saft\"'>target='\"_blank\"'>More...</a>.",
      "price": 0.01,
      "deluxePrice": 0.01,
      "image": "orange_juice.jpg",
      "createdAt": "2025-07-26 12:46:19.821 +00:00",
      "updatedAt": "2025-07-26 12:46:19.821 +00:00",
      "deletedAt": null
    },
    {
      "id": 36,
      "name": "OWASP Snakes and Ladders - Mobile Apps",
      "description": "This amazing mobile app security awareness board game is <a href='\"https://steamcommunity.com/sharedfiles/filedetails/?id=1970691216\"'>available for Tabletop Simulator on Steam Workshop</a> now!",
      "price": 0.01,
      "deluxePrice": 0.01,
      "image": "snakes_ladders_m.jpg",
      "createdAt": "2025-07-26 12:46:19.825 +00:00",
      "deletedAt": null
    }
  ]
}
```

is

10