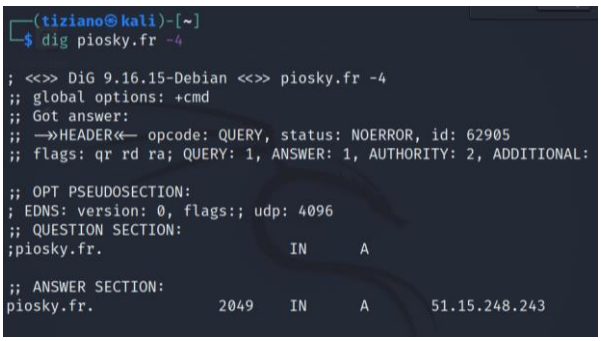
1. DNS

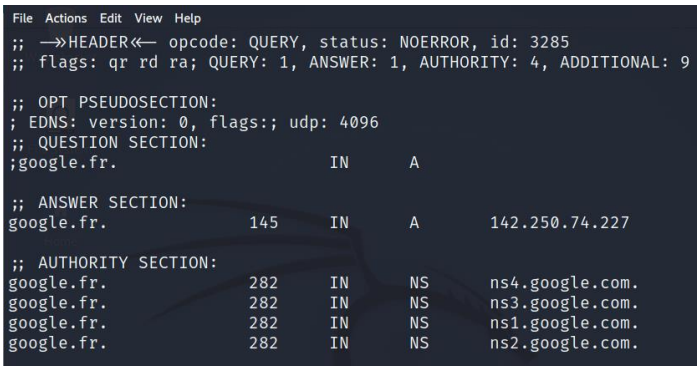
a. ADDR IPV4 of piosky.fr



```
┌──(tiziano㉿kali)-[~]
└─$ dig piosky.fr -4

; <<>> DiG 9.16.15-Debian <<>> piosky.fr -4
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62905
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL:

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;piosky.fr.                     IN      A

;; ANSWER SECTION:
piosky.fr.              2049    IN      A       51.15.248.243
```

*By tapping the command **dig domainName -4** we obtain the IPV4 address of the domain name "piosky.fr" : 51.15.248.243*

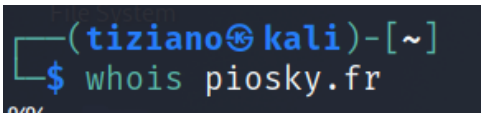
b. ADDR IPV4 of google.fr



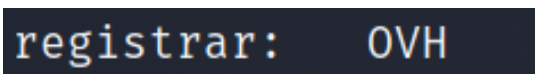
```
File  Actions  Edit  View  Help
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3285
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.fr.                     IN      A

;; ANSWER SECTION:
google.fr.              145     IN      A       142.250.74.227

;; AUTHORITY SECTION:
google.fr.              282     IN      NS      ns4.google.com.
google.fr.              282     IN      NS      ns3.google.com.
google.fr.              282     IN      NS      ns1.google.com.
google.fr.              282     IN      NS      ns2.google.com.
```

*By tapping the command **dig domainName -4** we obtain the IPV4 address of the domain name "google.fr" : 142.250.74.727*

c. Registrar of piosky.fr



```
┌──(tiziano㉿kali)-[~]
└─$ whois piosky.fr
```



```
registrar:    OVH
```

*The command **whois domainName** prints the registrar name of the domainName*

d. Host company of piosky.fr

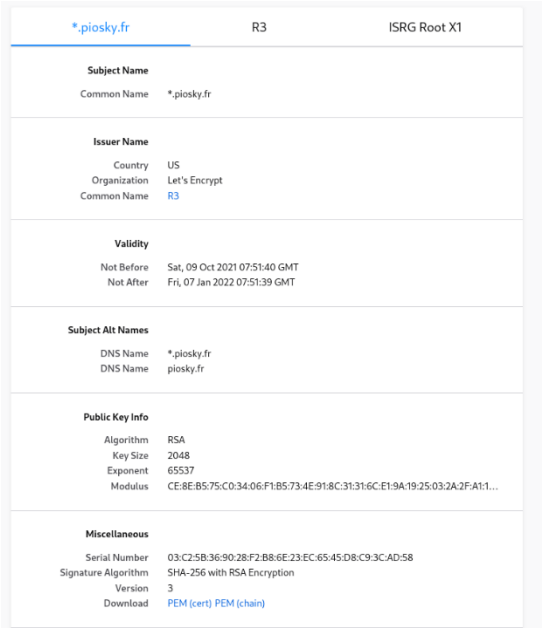
```
┌──(retina㉿kali)-[~]
└─$ dmitry piosky.fr | grep descr
descr:          Dedicated Servers and cloud assignment, abuse reports : http://abuse.online.net
descr:          SCALEWAY
descr:          Paris, France
```

*To find the host company of the domain name "piosky.fr" we can use the following command : **dmitry domainName | grep descry***

And we discover that Scaleway is actual company which host the domain name piosky.fr

2. OSINT

a. Certificate Authority



*.piosky.fr | R3 | ISRG Root X1

Subject Name
Common Name: *.piosky.fr

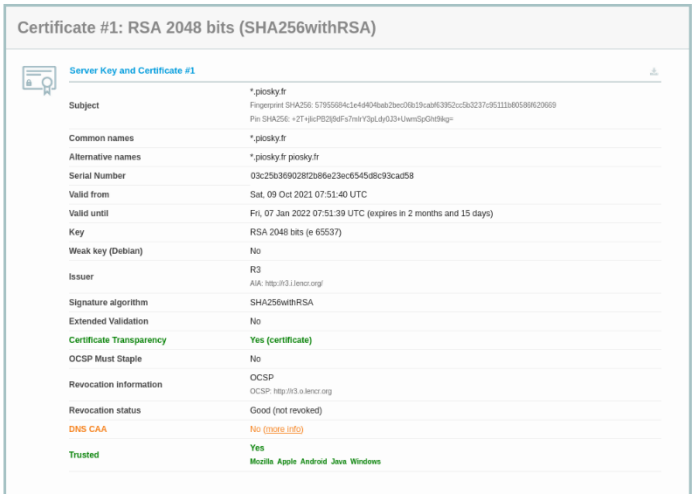
Issuer Name
Country: US
Organization: Let's Encrypt
Common Name: R3

Validity
Not Before: Sat, 09 Oct 2021 07:51:40 GMT
Not After: Fri, 07 Jan 2022 07:51:39 GMT

Subject Alt Names
DNS Name: *.piosky.fr
DNS Name: piosky.fr

Public Key Info
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus: CE:8E:B5:75:C0:34:06:F1:B5:73:4E:91:8C:31:31:6C:E1:9A:19:25:03:2A:2F:A1:1...

Miscellaneous
Serial Number: 03:C2:5B:36:90:28:F2:B8:6E:23:EC:65:45:D8:C9:3C:AD:58
Signature Algorithm: SHA-256 with RSA Encryption
Version: 3
Download: PEM (cert) PEM (chain)



Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

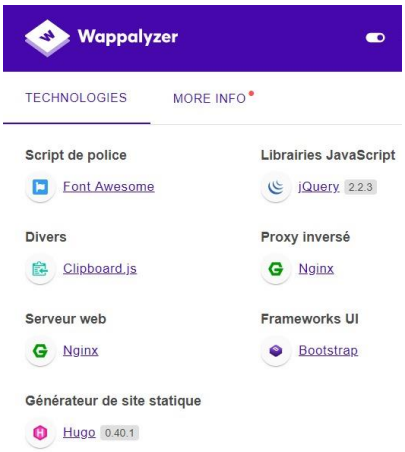
Subject	*.piosky.fr Fingerprint SHA256: 57955884c1e4d404beab2bec08b19cabf63952cc5b3237c95111b80586f620669 Pin SHA256: +2T+jkcPB2j8dFs7mlrY3pLdy0J3+UwmSpGht9Hg=
Common names	*.piosky.fr
Alternative names	*.piosky.fr piosky.fr
Serial Number	03c25b369028f2b86e23ec6545d8c93cad58
Valid from	Sat, 09 Oct 2021 07:51:40 UTC
Valid until	Fri, 07 Jan 2022 07:51:39 UTC (expires in 2 months and 15 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Let'sEncrypt is the Authority which delivered the certificate

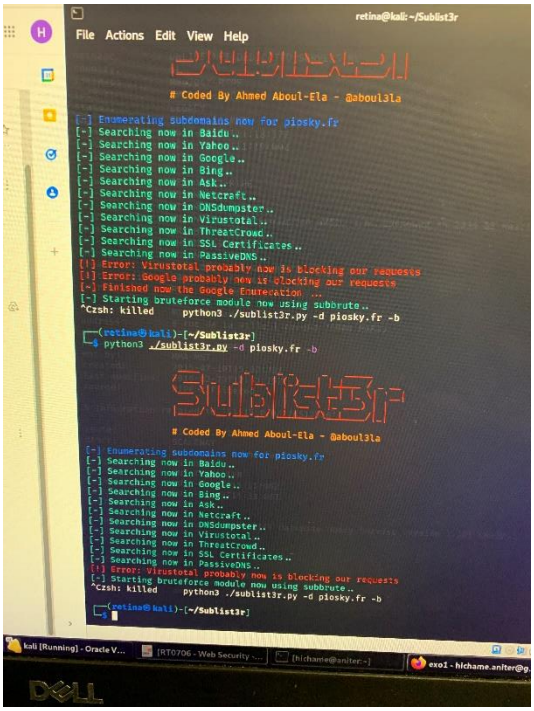
b. Vulnerabilities about the certificate

There is no vulnerabilities because SHA-256 with RSA-2048 Encryption is not a certificate hashing algorithm

c. Web Framework

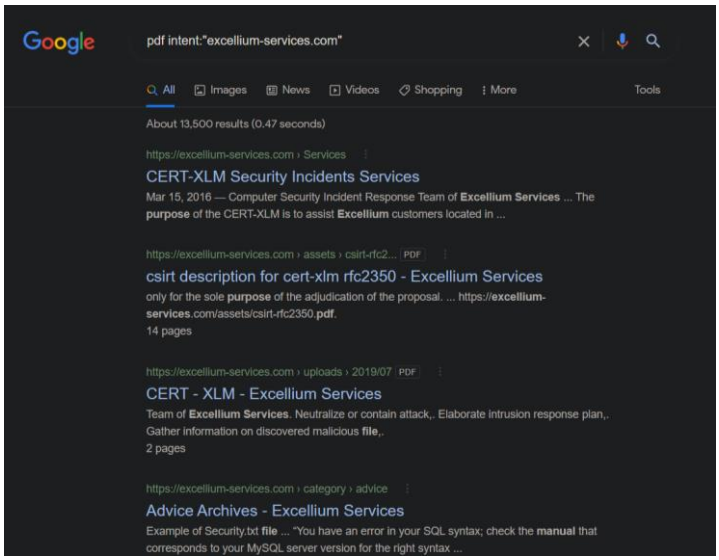


d. Sub domains



The search took more than 30 minutes because of a network problem

e. Google search with Google Dork



pdf intent:"excellium-services.com"

f. Email address

anthony.maia.pro@gmail.com (found on Microsoft teams)

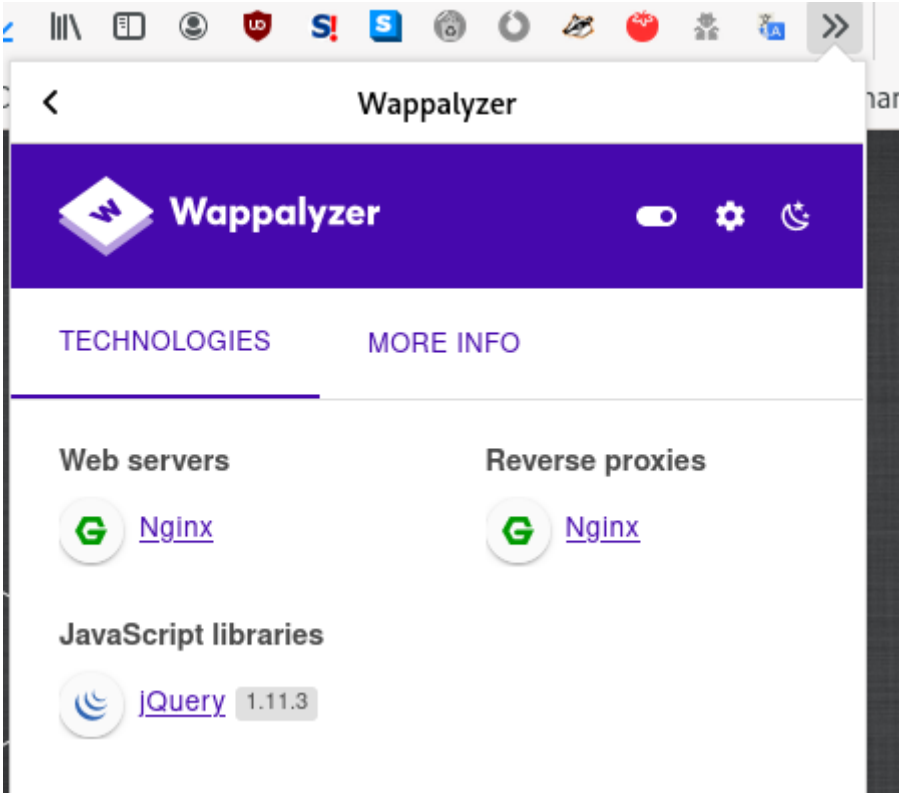
3. MAPPING

a. Services exposed by piosky.fr

```
┌──(retina㉿kali)-[~]
└─$ sudo nmap -sV -O 51.15.248.243
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-22 11:54 CDT
Nmap scan report for 243-248-15-51.instances.scw.cloud (51.15.248.243)
Host is up (0.028s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE    VERSION
21/tcp   open  tcpwrapped
22/tcp   open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http       nginx
82/tcp   open  tcpwrapped
84/tcp   open  tcpwrapped
443/tcp  open  ssl/http   nginx
554/tcp  open  rtsp?
1723/tcp open  tcpwrapped
5060/tcp open  sip?
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=10/22%OT=22%CT=1%CU=36744%PV=N%DS=2%DC=I%G=Y%TM=6172ED
OS:80%P=x86_64-pc-linux-gnu)SEQ(SP=11%GCD=FA00%ISR=9C%TI=I%CI=RD%II=I%SS=S%
OS:TS=U)OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=FFFF%W2=
OS:FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=N%T=41%W=FFFF%O=M5B4%CC=
OS:N%Q=)T1(R=Y%DF=N%T=41%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=N%T=100%W=0%S=Z%A=
OS:S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=N%T=100%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T4(R=Y%
OS:DF=N%T=100%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=100%W=0%S=Z%A=S+%F=A
OS:R%O=%RD=0%Q=)T6(R=Y%DF=N%T=100%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=
OS:100%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=3D%IPL=148%UN=0%RIPL=G%RID
OS:=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=25%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 165.16 seconds
```

*With the command **nmap -sV -O IPADRR** we can see all services used by piosky.fr*

b. Web server's technology used on piosky.fr



To gather information about the technology used on the web server, we can use the plugin Wappalyzer, thus the technology used is Nginx

c. Operating system behind piosky.fr

*To know which OS is behind piosky.fr, we still can use the **nmap** command as above, thus we understand that the OS is Ubuntu*

4. ROOTME

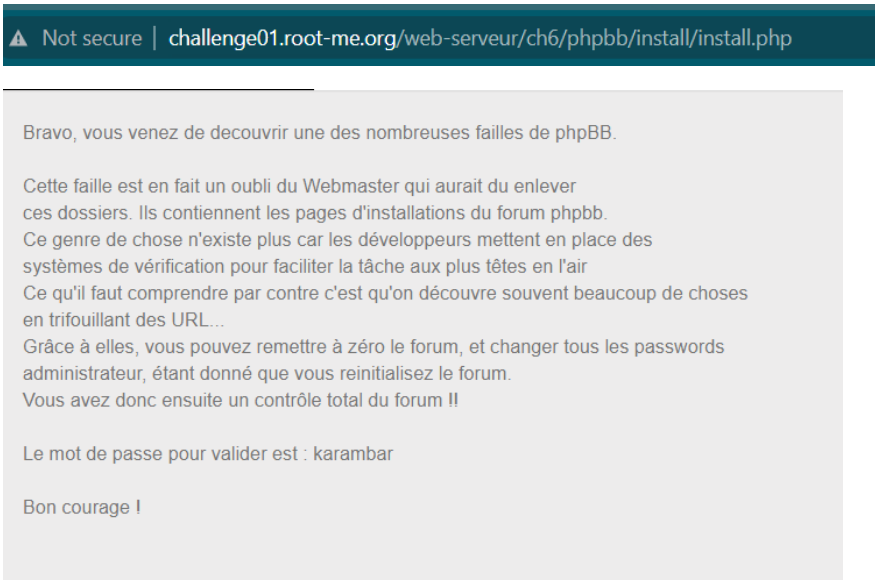
a. Weak password challenge

Bien joué, vous pouvez utiliser ce mot de passe pour valider le challenge

Well done, you can use this password to validate the challenge

The solution was to fill the form by tapping "admin" as username and "admin" as password

b. Install phpBB



To solve this challenge, you must change the URI with the following one : /web-serveur/ch6/phpbb/install/install.php