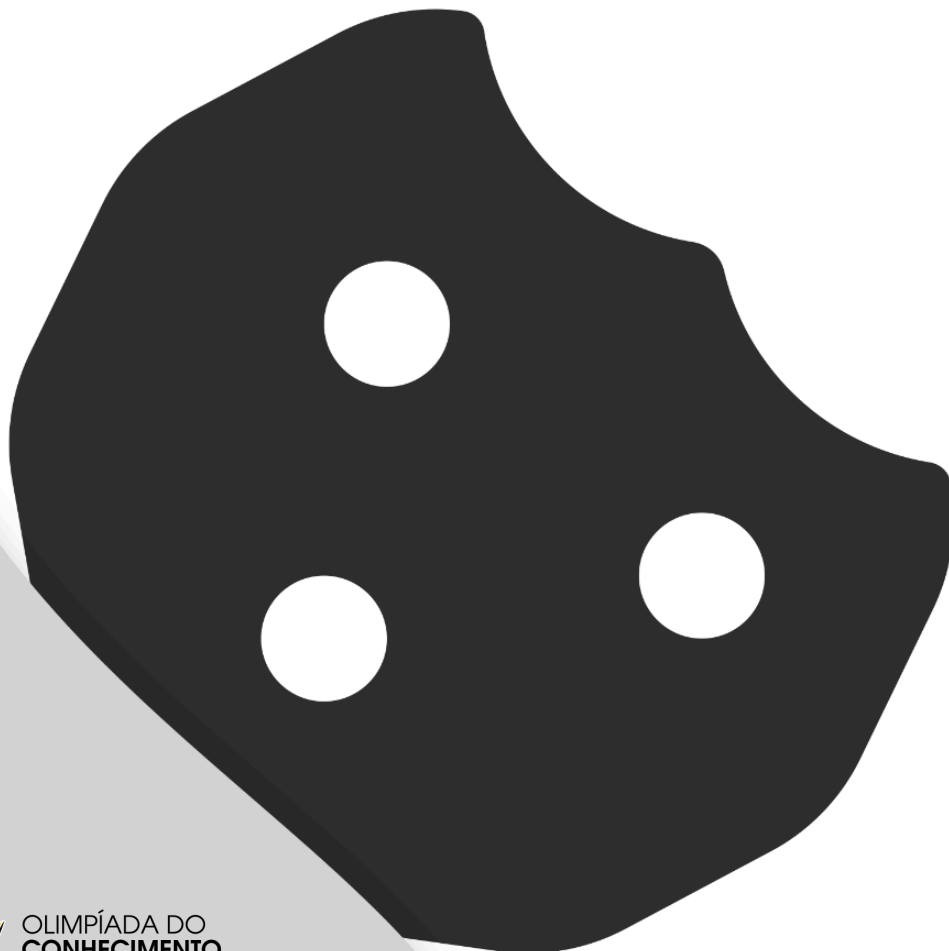


Writeup

cookie easy

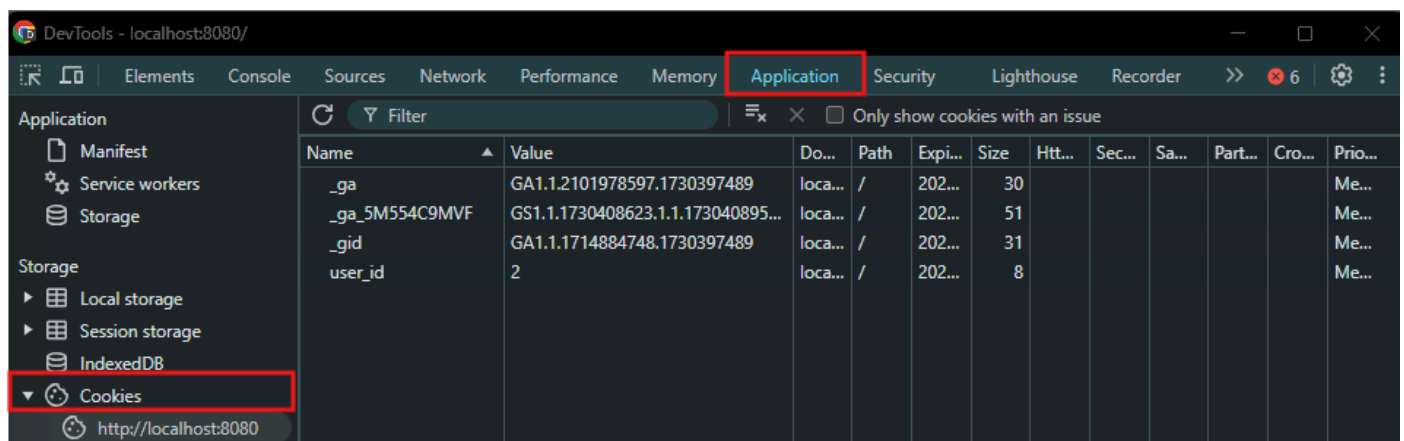
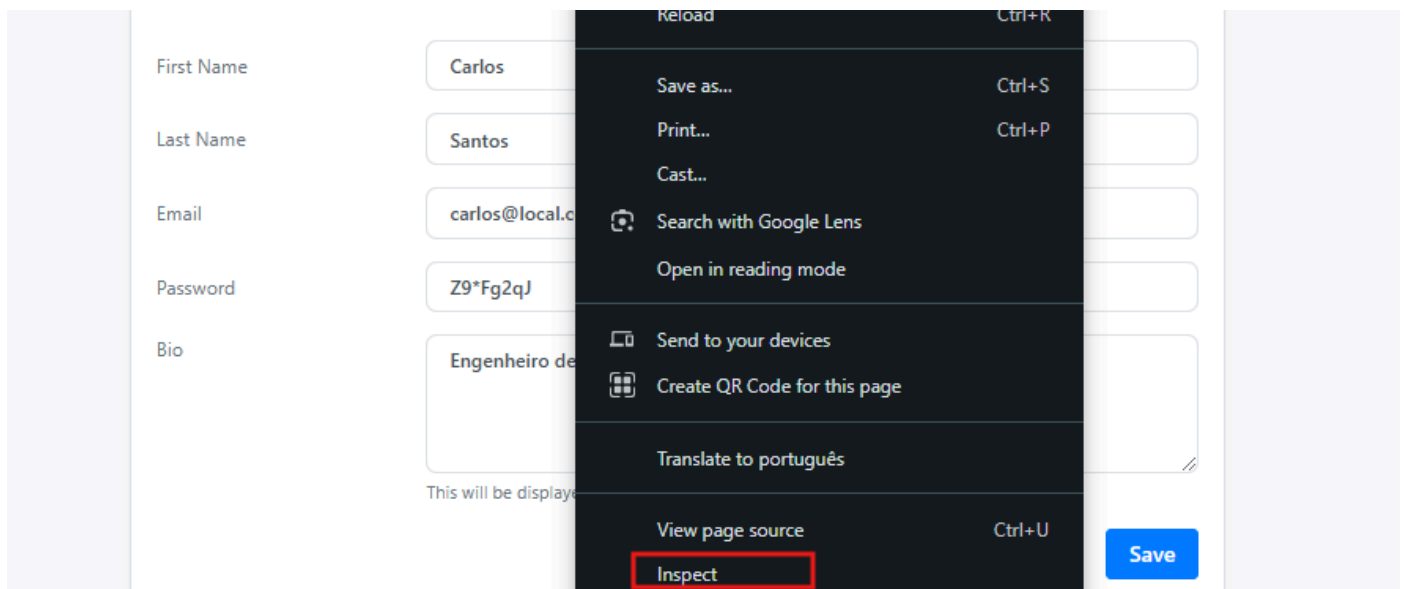
Conseitos de segurança na web.



Cookies

Utilização de cookies

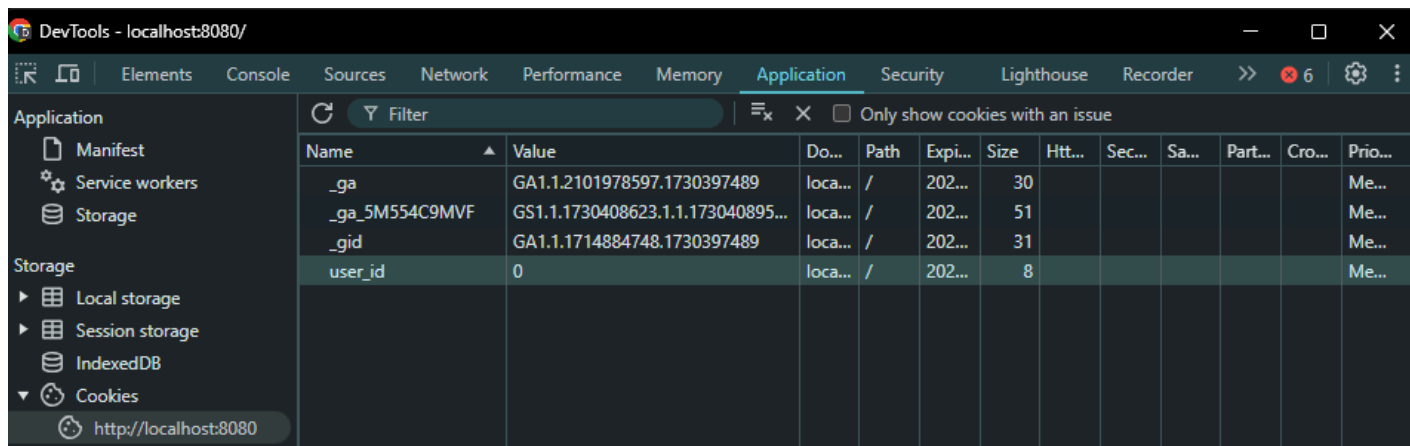
Cookies de uma forma geral, são informações de sites que duram o tempo determinado na sua criação, sendo assim mesmo que o navegador seja fechado, o cookie permanece salvo. Podemos ver os cookies salvos ao clicar com o botão direito do mouse e ir na aba **Inspect > Application > Cookies**.



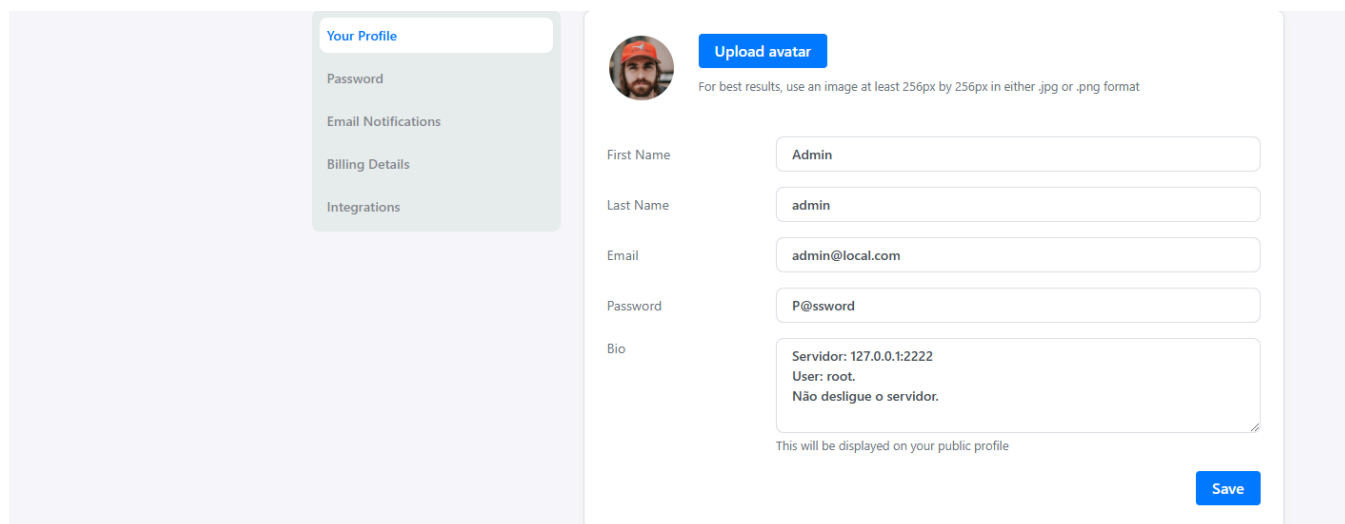
Aqui podemos ver um cookie com o nome interessante chamado “**user_id**”, podemos modificá-lo para ver sua aplicação na página.

Modificando

Ao mudarmos e recarregarmos a página, podemos ver que mudamos nossas informações para as informações de outros usuários. Podemos ir mudando até achar um usuário que nos interesse.



Name	Value	Do...	Path	Expi...	Size	Http...	Sec...	Sa...	Part...	Cro...	Prio...
_ga	GA1.1.2101978597.1730397489	loca...	/	202...	30						Me...
_ga_5M554C9MVF	GS1.1.1730408623.1.1.173040895...	loca...	/	202...	51						Me...
_gid	GA1.1.1714884748.1730397489	loca...	/	202...	31						Me...
user_id	0	loca...	/	202...	8						Me...




Your Profile

Password

Email Notifications

Billing Details

Integrations

 [Upload avatar](#)

For best results, use an image at least 256px by 256px in either .jpg or .png format

First Name:

Last Name:

Email:

Password:

Bio:

Servidor: 127.0.0.1:2222
User: root.
Não desligue o servidor.

This will be displayed on your public profile

[Save](#)

Com o **user_id 0** achamos um usuário bem interessante chamado “**Admin**”, e também podemos ver suas credenciais de acesso ao servidor.

Servidor

Acesso indevido

Ao tentarmos acessar o servidor via **SSH(Secure Shell)**, conseguimos acesso com um usuário com privilégio alto, nesse caso o **root**, o que é uma falha grave, pois o acesso remoto não deve ser disponibilizado ao usuário **root**.

Podemos usar "**ssh root@127.0.0.1 -p 2222**" onde "**-p**" indica a porta.

```
PS C:\Users\nicol\docker\ctf-2> ssh root@127.0.0.1 -p 2222
root@127.0.0.1's password:
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@2ca4da36541a:~#
```

Pegando a flag

Agora devemos procurar nossa flag, como somos usuário **root**, não temos restrições, então podemos acessar qualquer arquivo. Vamos então fazer uma procura usando o comando **find**, que precisa de apenas dois parâmetros, onde ele vai procurar e o nome do arquivo (**-name** especifica o nome).

Podemos usar "**find / -name flag.txt**" onde "/" é o caminho inicial e "**flag.txt**" é o arquivo.

```
root@2ca4da36541a:~# find / -name "flag.txt"
/var/www/flag.txt
```

Agora para ver o conteúdo da nossa flag podemos usar o comando "**cat**", que para mostrar o conteúdo do arquivo precisa apenas do caminho do arquivo.

Podemos usar “**cat /var/www/flag.txt**”.

```
root@2ca4da36541a:~# cat /var/www/flag.txt  
FLAG{SENAI-fbfueblj045hd8}
```

Produzido por Nycolas Ramos dos Santos