A5 - Broken Access Control

globo.com

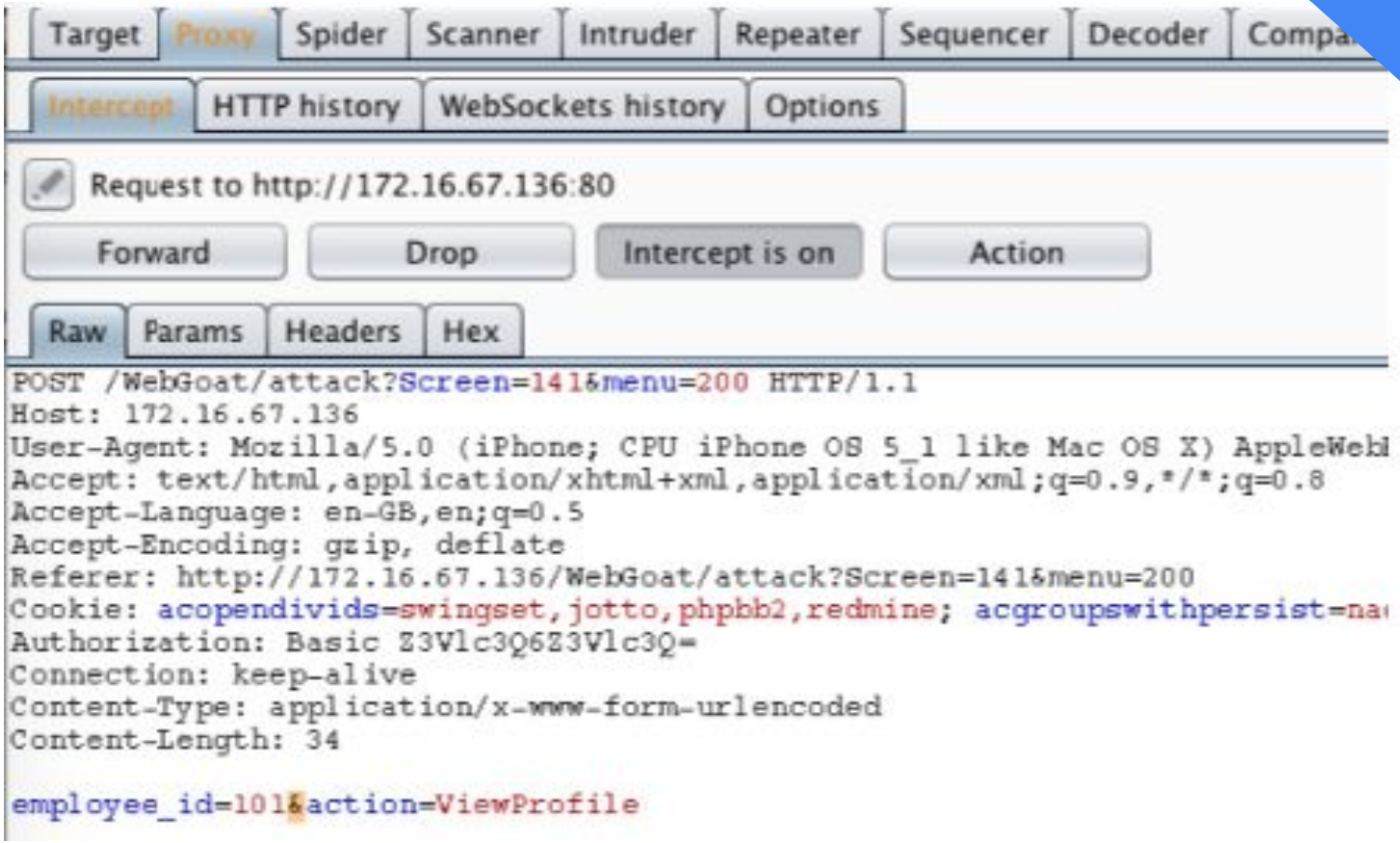
GTS 33 | PA 05/2019

Agenda - A5 - Quebra de Controle de Acesso

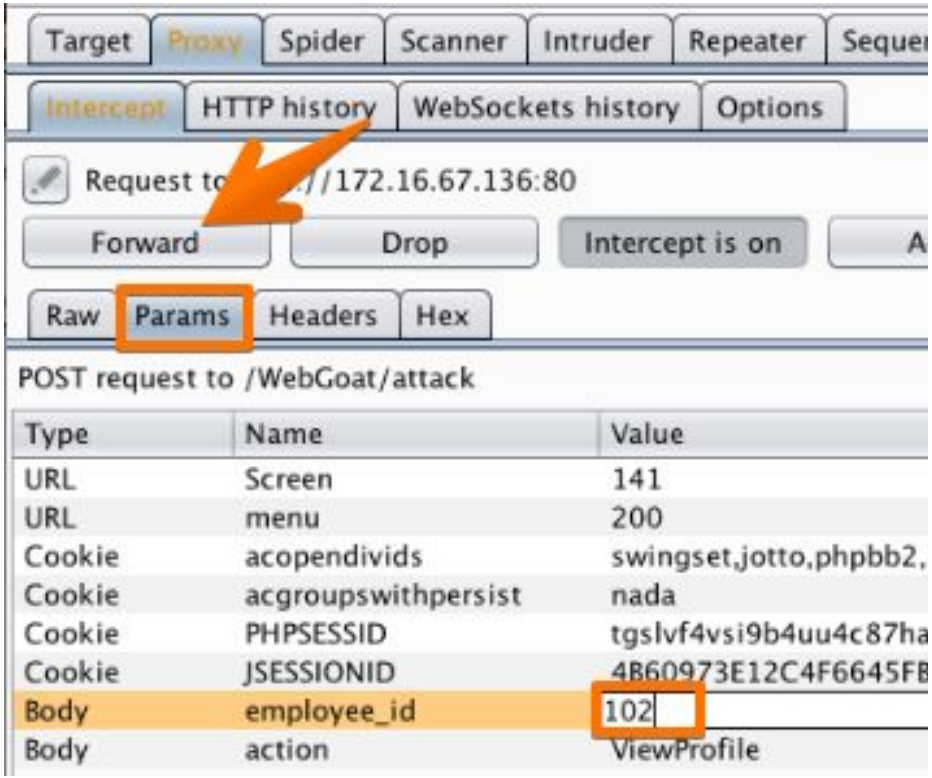
1. Do que se trata?
2. Manipulação de parâmetros
3. Client-side
4. Função administrativa
5. Como se proteger?
6. Ecommerce API

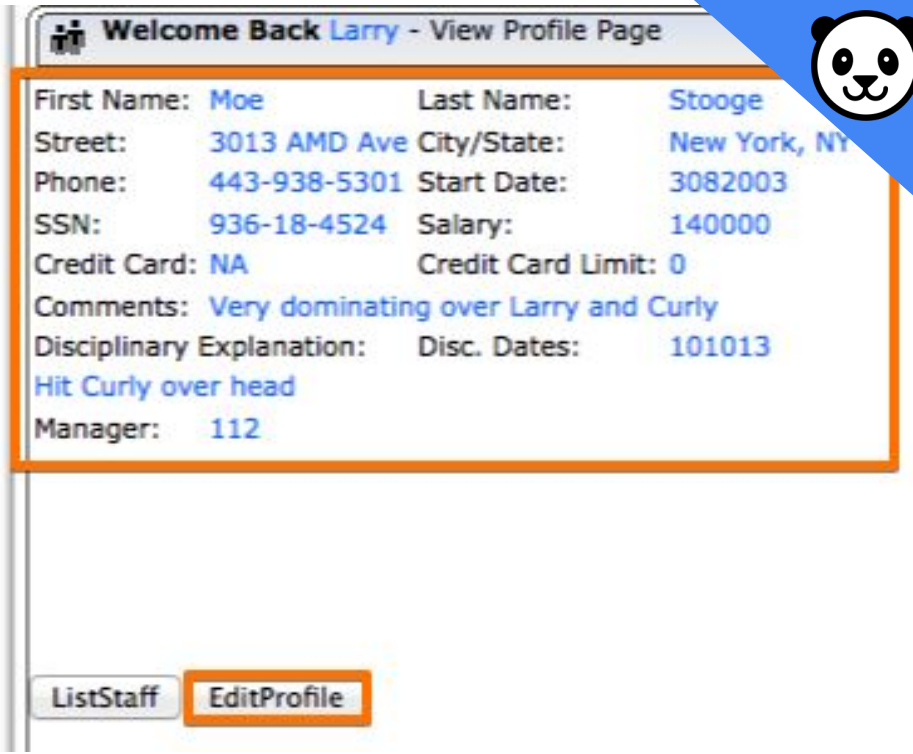
Do que se trata?

Quebra de controle de acesso se dá quando ocorrem falhas no processo de determinar quais elementos (usuários, sistemas, dispositivos) devem ter ou não acesso a determinados objetos.

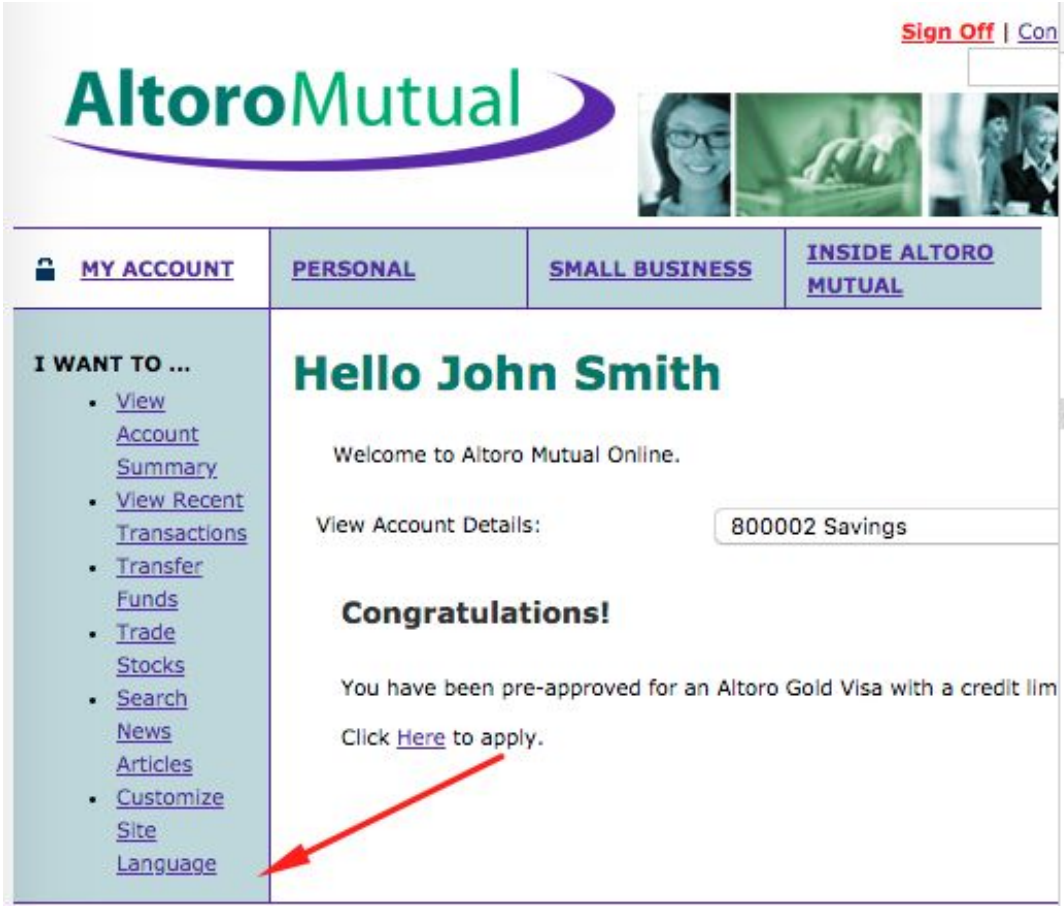


Manipulação de parâmetros





Manipulação de parâmetros


Sign Off | Con
AltoroMutual
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Trade Stocks
Search News Articles
Customize Site Language
Hello John Smith
Welcome to Altoro Mutual Online.
View Account Details:
800002 Savings
Congratulations!
You have been pre-approved for an Altoro Gold Visa with a credit lim
Click Here to apply.


Elements
Console
<a id="MenuHyperLink3"

<a id="MenuHyperLink4" href="/b
Articles

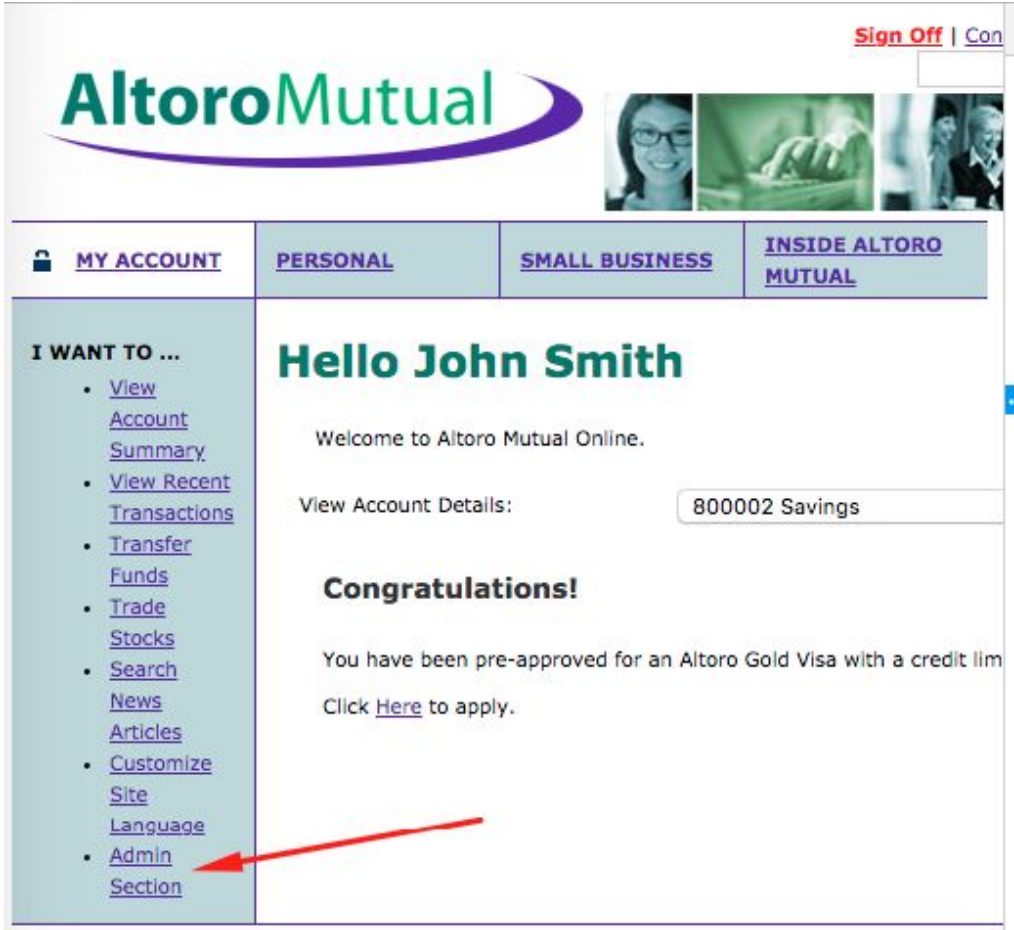
<a id="MenuHyperLink5" href="/bank/cu
Language

<li style="display: none;"> == $0
<a id="MenuHyperLink6" href="/bank/ad

</td>
<!-- MEMBER TOC END -->
<td valign="top" colspan="3" class="bb">…</
<!-- BEGIN FOOTER -->
</tr>
</tbody>
</table>

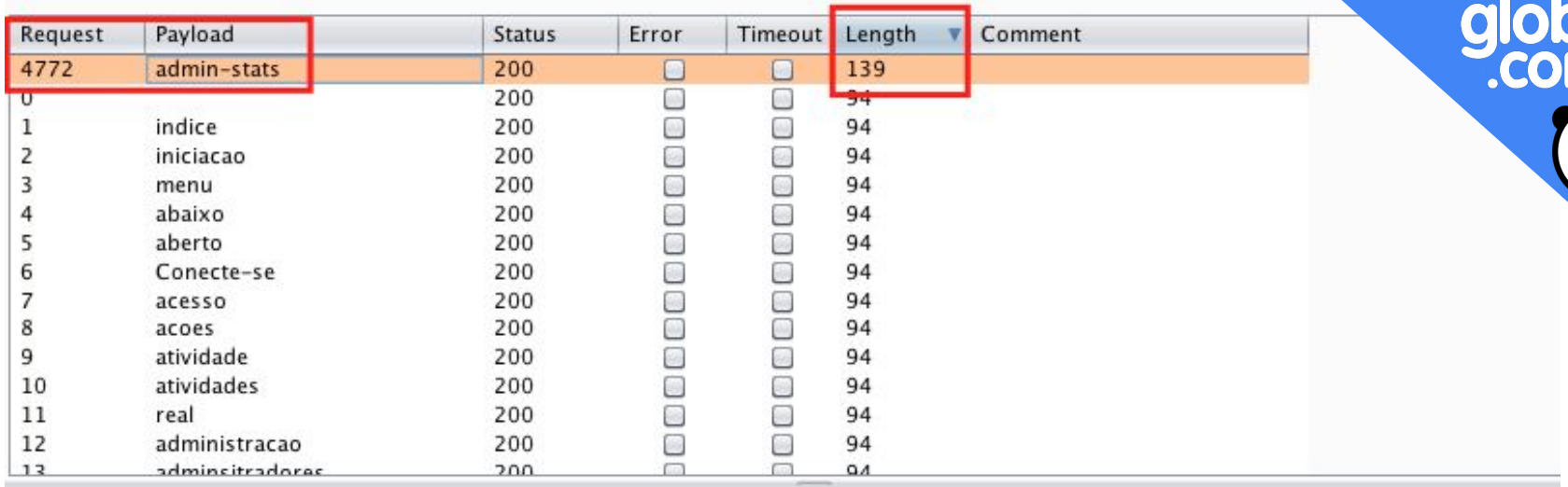
<a id="HyperLink5" href="/index.jsp?content=pr
"
  |
"

Client-side



globo.com

Client-side



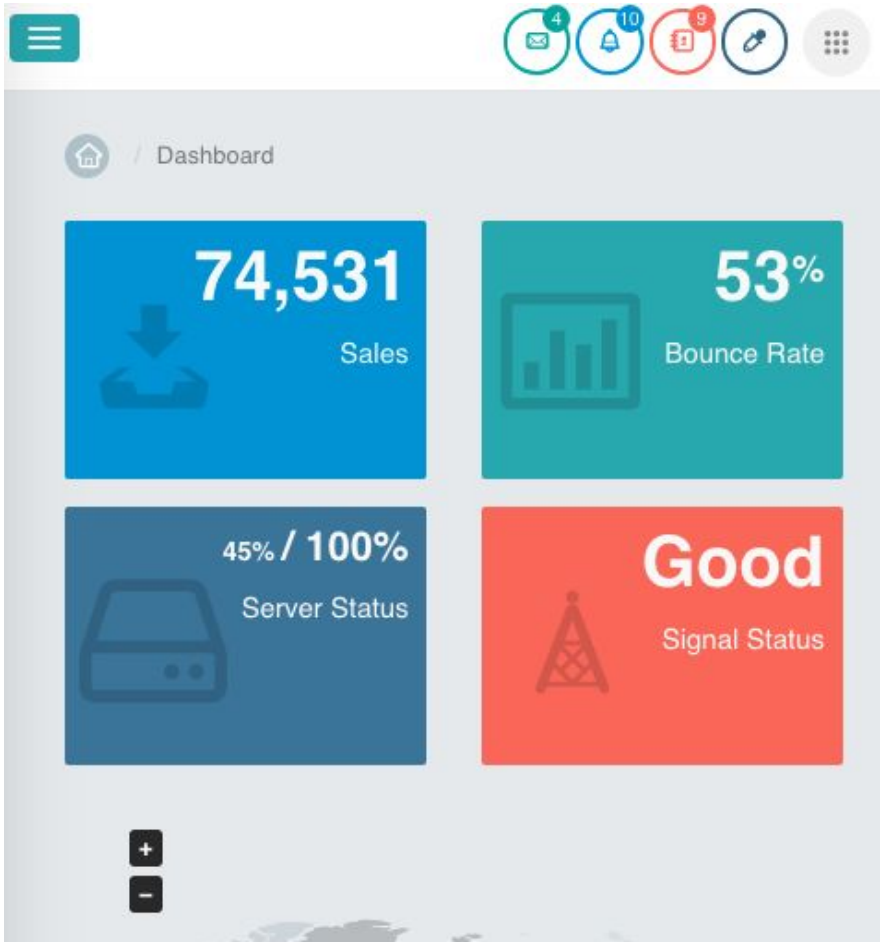
Request	Payload	Status	Error	Timeout	Length	Comment
4772	admin-stats	200	☐	☐	139	
0		200	☐	☐	94	
1	indice	200	☐	☐	94	
2	iniciacao	200	☐	☐	94	
3	menu	200	☐	☐	94	
4	abaixo	200	☐	☐	94	
5	aberto	200	☐	☐	94	
6	Conecte-se	200	☐	☐	94	
7	acesso	200	☐	☐	94	
8	acoes	200	☐	☐	94	
9	atividade	200	☐	☐	94	
10	atividades	200	☐	☐	94	
11	real	200	☐	☐	94	
12	administracao	200	☐	☐	94	
13	administradores	200	☐	☐	94	

Request | Response

Raw | Headers | Hex

```
GET /admin-stats HTTP/1.1
Host: localhost:1232
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

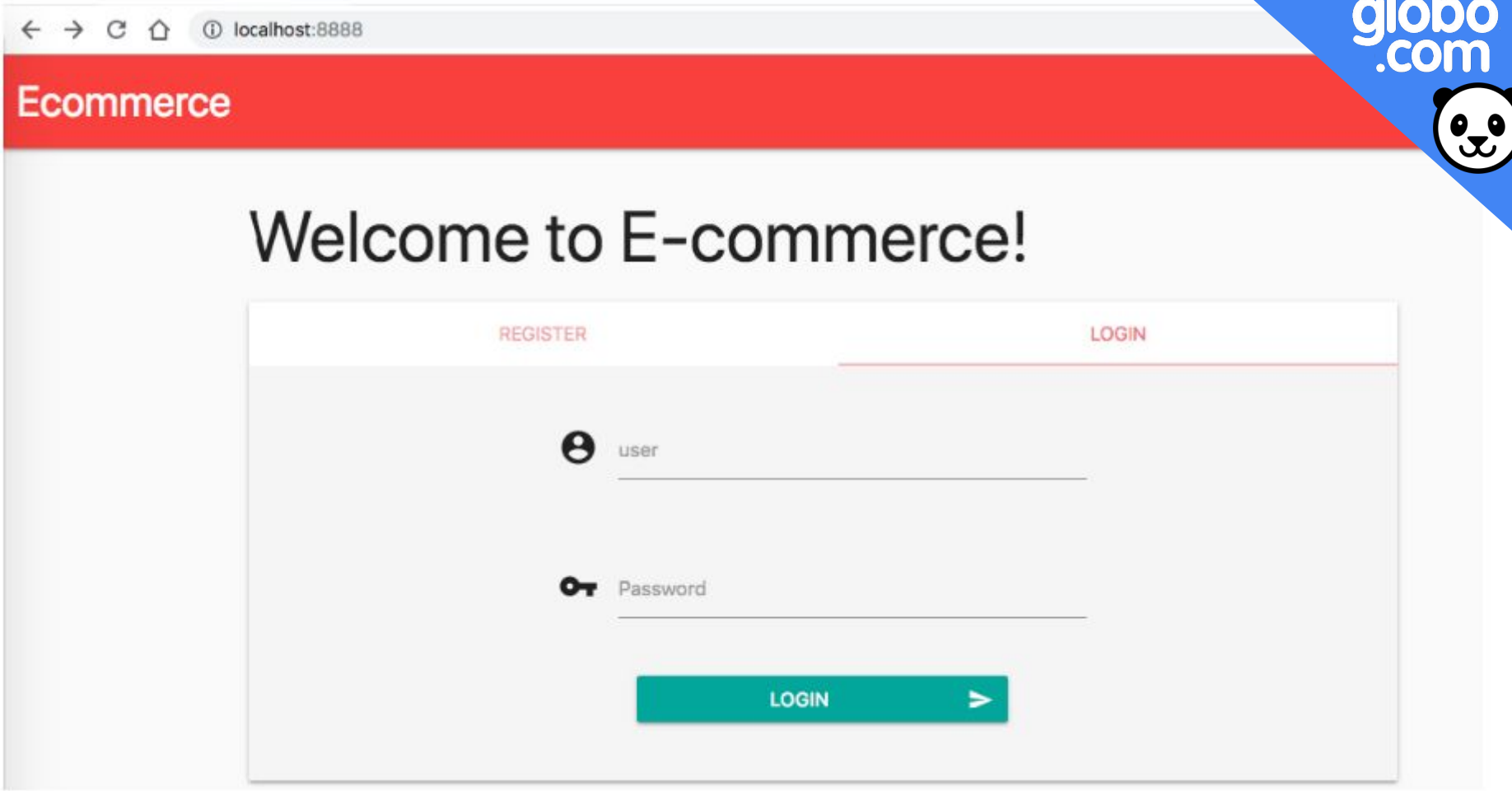
Função administrativa



Função administrativa

Como se proteger?

1. Desenvolver um documento com as **políticas de acesso da aplicação**, mapeando e clarificando todos os objetivos que devem ser atingidos. 📄
2. Evitar que simples **mudanças de parâmetros** (IDs, por exemplo) permitam que um usuário autenticado passe a referenciar um outro usuário.🔀
3. Garantir que URLs destinadas a **usuários privilegiados** não possam ser acessadas pelos demais usuários.🚷
4. Garantir que páginas que contenham informações sensíveis **não sejam cacheadas** no browser do usuário.📲


localhost:8888
Ecommerce
Welcome to E-commerce!
REGISTER
LOGIN
user
Password
LOGIN

Narrativa do ataque

Hands on!

1. Entrar na pasta da app

```
$ cd owasp-top10-2017-apps/a5/ecommerce-api/
```

2. Inicializar o container

```
$ make install
```

3. Acessar a página

```
localhost:8888
```

globo.com

A5 - Broken Access Control