

A5 - Broken Access Control



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.



Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Compa

Intercept HTTP history WebSockets history Options

Request to http://172.16.67.136:80

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
POST /WebGoat/attack?Screen=141&menu=200 HTTP/1.1
Host: 172.16.67.136
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.67.136/WebGoat/attack?Screen=141&menu=200
Cookie: acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=na
Authorization: Basic Z3Vlc3Q6Z3Vlc3Q=
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 34

employee_id=101&action=ViewProfile
```

Manipulação de parâmetros



Target Proxy Spider Scanner Intruder Repeater Sequer

Intercept HTTP history WebSockets history Options

Request to //172.16.67.136:80

Forward Drop Intercept is on A

Raw **Params** Headers Hex

POST request to /WebGoat/attack

Type	Name	Value
URL	Screen	141
URL	menu	200
Cookie	acopendivids	swingset,jotto,phpbb2,
Cookie	acgroupswithpersist	nada
Cookie	PHPSESSID	tgslvf4vsi9b4uu4c87ha
Cookie	JSESSIONID	4B60973E12C4F6645FB
Body	employee_id	102
Body	action	ViewProfile

Welcome Back Larry - View Profile Page

First Name: Moe Last Name: Stooze
Street: 3013 AMD Ave City/State: New York, NY
Phone: 443-938-5301 Start Date: 3082003
SSN: 936-18-4524 Salary: 140000
Credit Card: NA Credit Card Limit: 0
Comments: Very dominating over Larry and Curly
Disciplinary Explanation: Disc. Dates: 101013
Hit Curly over head
Manager: 112

ListStaff **EditProfile**

Manipulação de parâmetros



MY ACCOUNT	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<p>I WANT TO ...</p> <ul style="list-style-type: none"> • View Account Summary • View Recent Transactions • Transfer Funds • Trade Stocks • Search News Articles • Customize Site Language 	<h2 style="text-align: center;">Hello John Smith</h2> <p style="text-align: center;">Welcome to Altoro Mutual Online.</p> <p>View Account Details: 800002 Savings</p> <h3 style="text-align: center;">Congratulations!</h3> <p style="text-align: center;">You have been pre-approved for an Altoro Gold Visa with a credit lim</p> <p style="text-align: center;">Click Here to apply.</p>		

```

Sign Off | Con
Elements Console
<li>
  <a id="MenuHyperLink3" href="#">
</li>
<li>
  <a id="MenuHyperLink4" href="/bank/Articles">
    Articles</a>
</li>
<li>
  <a id="MenuHyperLink5" href="/bank/cuLanguage">
    Language</a>
</li>
<li style="display: none;" == $0
  <a id="MenuHyperLink6" href="/bank/ad
  </li>
</ul>
</td>
<!-- MEMBER TOC END -->
<td valign="top" colspan="3" class="bb">...</td>
<!-- BEGIN FOOTER -->
</tr>
</tbody>
</table>
<div id="footer" style="width: 99%;">
  <a id="HyperLink5" href="/index.jsp?content=pr
  "
  &nbsp;&nbsp;&nbsp;|&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;
  "

```



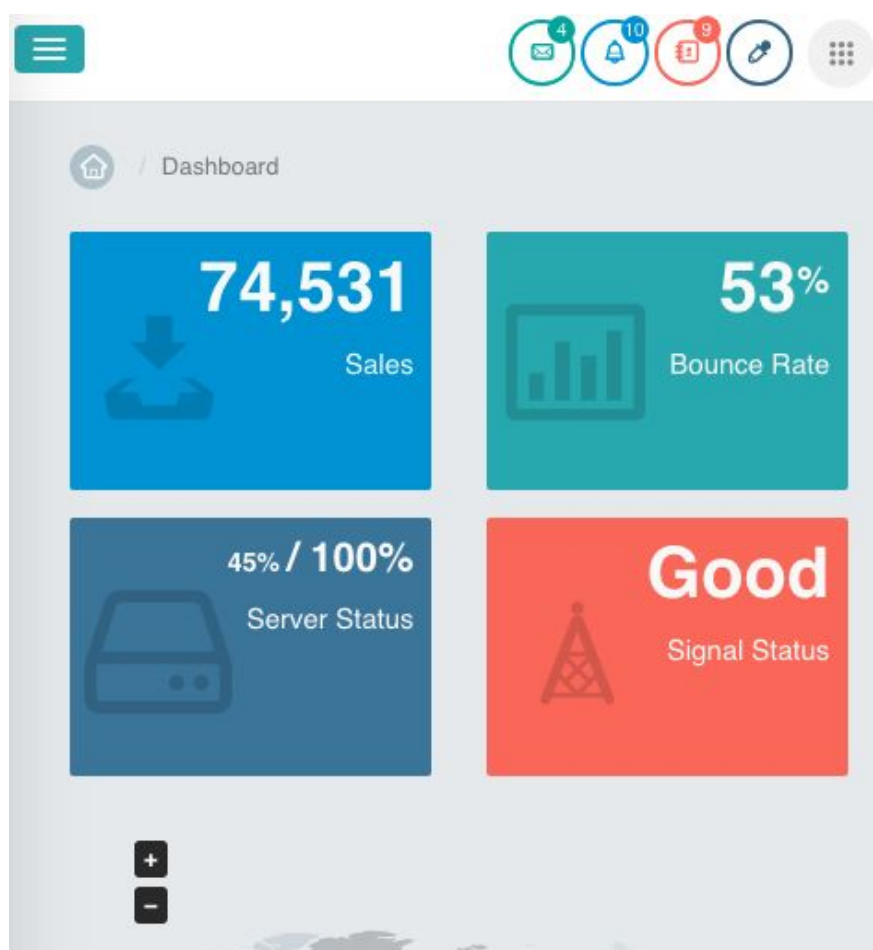

Request	Payload	Status	Error	Timeout	Length	Comment
4772	admin-stats	200	<input type="checkbox"/>	<input type="checkbox"/>	139	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	94	
1	indice	200	<input type="checkbox"/>	<input type="checkbox"/>	94	
2	iniciacao	200	<input type="checkbox"/>	<input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



Ecommerce

Welcome to E-commerce!

REGISTER

LOGIN



user



Password

LOGIN





Narrativa do ataque



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
```



A5 - Broken Access Control

