



# Broken Access Control

# Riscos para o Setor Financeiro

Como evitá-los com modelagem de ameaças e outras medidas

Danilo Costa  
Pedro Vargas



# Visão geral

# Visão geral

- CVE x CWE;
- Quebra de Controle de acesso
- CVE-2020-15939
- Outros CVEs
- Riscos de controle de acesso para o setor financeiro
- Boas práticas
- Modelagem de ameaças na prática

**CVE x CWE**

# CVE

Uma lista de nomes padronizados para identificar vulnerabilidades de segurança.



## CVE-ID

**CVE-2020-15939** [Learn more at National Vulnerability Database \(NVD\)](#)


• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

## Description

An improper access control vulnerability (CWE-284) in FortiSandbox versions 3.2.1 and below and 3.1.4 and below may allow an authenticated, unprivileged attacker to download the device configuration file via the recovery URL.

# CWE

(CWE™) é uma lista desenvolvida pela comunidade de tipos de pontos fracos de software e hardware.



**Common Weakness Enumeration**  
*A Community-Developed List of Software & Hardware Weakness Types*

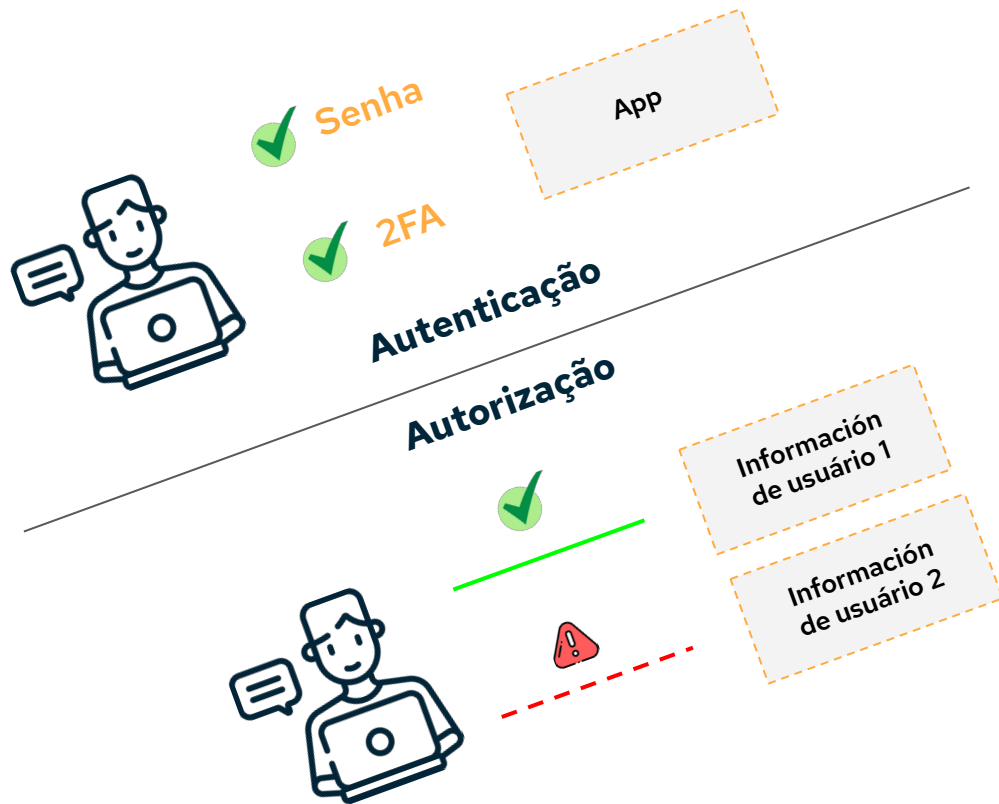
Home > CWE List > CWE- Individual Dictionary Definition (4.7)

[Home](#) | [About](#) | [CWE List](#) | [Scoring](#) |

## CWE-284: Improper Access Control

# Broken Access Control

# Conceito





# OWASP

## TOP 10:2021

A01:2021-Quebra de Controle de acesso

A02:2021-Falhas criptográficas

A03:2021-Injeção

A04:2021-Design inseguro

A05:2021-Segurança mal configurada

A06:2021-Componentes vulneráveis e obsoletos

A07:2021-Falhas de identificação e autenticação

A08:2021-Falhas de integridade de dados e software

A09:2021-Monitoramento de segurança e falhas de registro

A10:2021-Falsificação de solicitação do lado do servidor

# **A01:2021-Broken Access Control**

## **34 CWEs**

### **Mapeados**

#### List of Mapped CWEs

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

CWE-219 Storage of File with Sensitive Data Under Web Root

CWE-275 Permission Issues

CWE-276 Incorrect Default Permissions

CWE-284 Improper Access Control

# Escalação de privilégios Horizontal

<http://vulnerableapp.com/user/account?accountId=7800001>

<http://vulnerableapp.com/user/account?accountId=7800002>

# Escalação de privilégios Vertical

<http://vulnerableapp.com/user/account>

<http://vulnerableapp.com/admin/panel>

**CVE-2020-15939**

# Pesquisa CVE-2020-15939

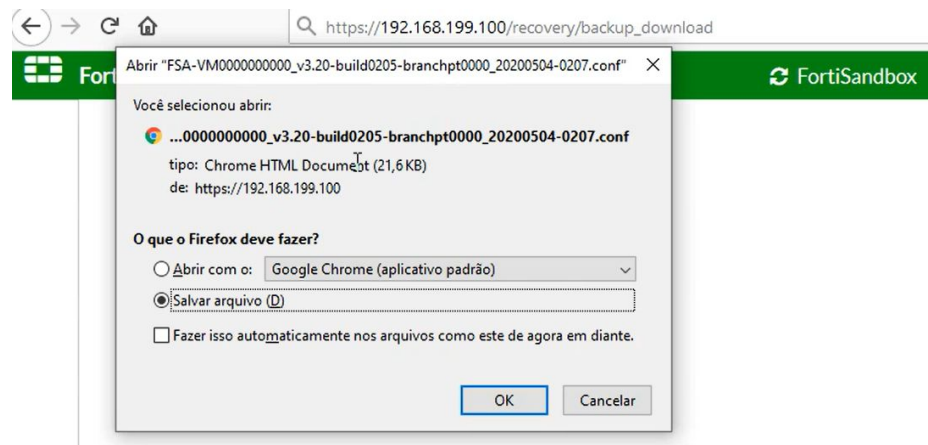
- Produto FortiSandbox
- Pesquisa realizada em 2020
- Informe o fabricante com detalhes do problema.
- Correção feita em 2021

**FortiSandbox VM**

Administrator:	<input type="text" value="none"/>
Password:	<input type="password" value="....."/> <small>Must be 6 - 64 characters long and may contain upper-case letters, lower-case letters, numbers, and special characters.</small>
Confirm Password:	<input type="password" value="....."/> <small>Enter the same password as above, for verification.</small>
Email Address:	<input type="text"/>
Phone Number:	<input type="text"/> <small>Phone number must start with +</small>
Admin Profile:	<input type="text" value="none"/>

# Pesquisa CVE-2020-15939

- Produto FortiSandbox
- Pesquisa realizada em 2020
- Informe o fabricante com detalhes do problema.
- Correção feita em 2021



# Outros CVEs



# CVE-2020-9286 - FortiADC does not verify user's permissions

The image displays a web browser window with an HTTP request and response, and a terminal window showing a command execution.

**Request:**

```
GET /api/platform/reboot HTTP/1.1
Host: 192.168.200.200
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=UTF-8
Authorization: Bearer 380da709b666713bbf6f8af93fe4f558
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://192.168.200.200/ui/?vdom=
Cookie: last_access_time=1579902491
```

**Response:**

```
HTTP/1.1 200 OK
Date: Fri, 24 Jan 2020 21:50:59 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 13
Connection: close
Set-Cookie: last_access_time=1579902654; Path=/; HttpOnly
X-frame-options: SAMEORIGIN

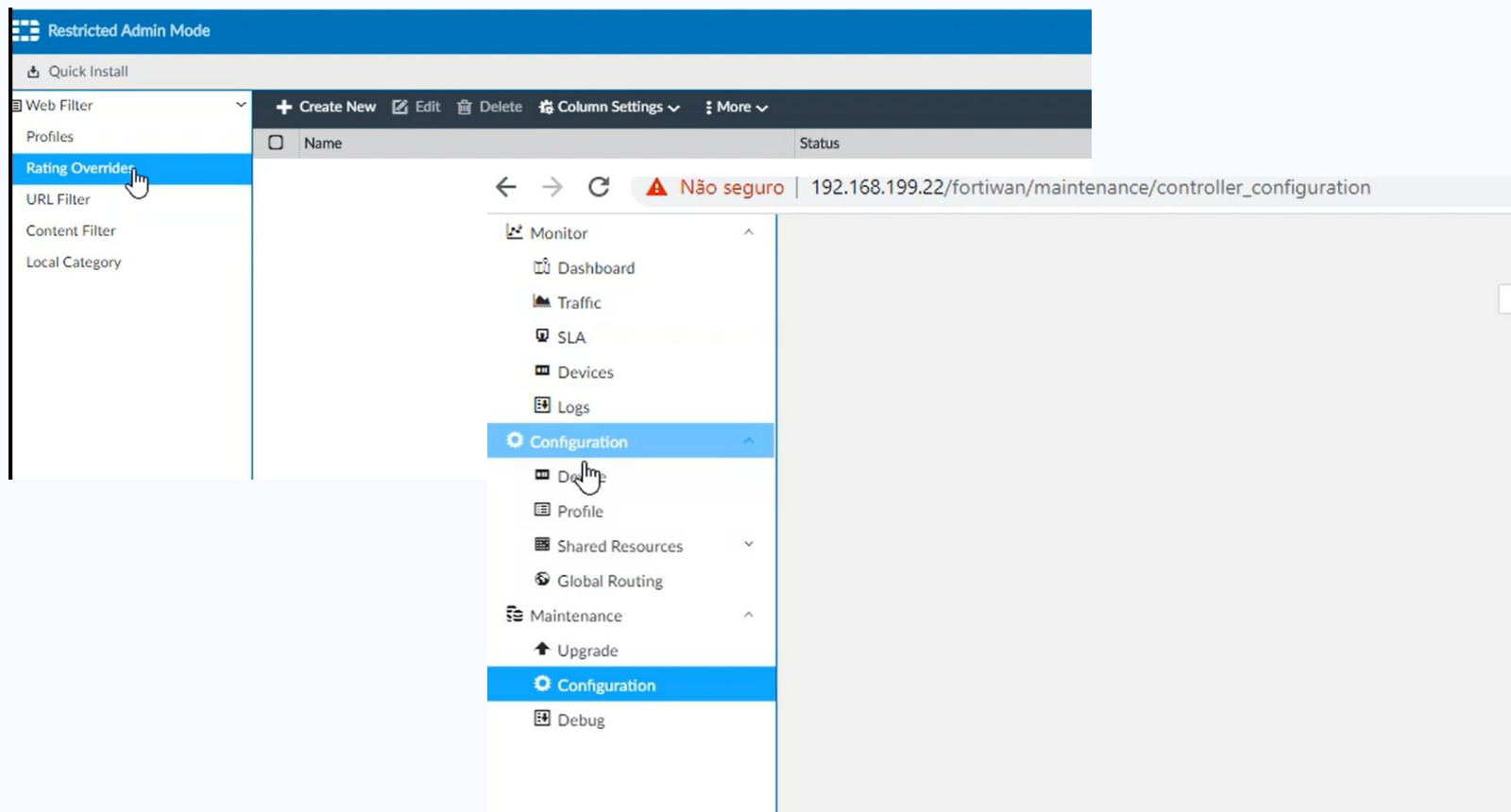
{"payload":0}
```

**Terminal Output:**

```
Player ▾ || ▾ ⏏ ⏏ ⏏
edit portio
set vdom root
config ha-node-ip-list
end
next
end
FortiADC-UM #
The system is going down NOW !!
Please stand by while rebooting the system.
```

A red box highlights the Authorization header in the request and the terminal output. A red arrow points to the Authorization header in the request.

# CVE-2021-24006 - A restricted admin can access SD-WAN ORCHESTRATOR panel



# Artigo no Blog Conviso - Pesquisa CVE-2021-43076



# CVE-2021-43076 e os Riscos causados pelo Insecure Design

- Acesso com usuário restrito;
- Acesso Web console do equipamento;
- Execução do comando `fnsysctl`;
- Execução do comando `fnsysctl ls /` , para listar os arquivos do sistema.
- Execução do comando `fnsysctl ftp client`, para realizar upload dos arquivos maliciosos com o mesmo nome dos arquivos de sistema.
- Upload de arquivos maliciosos na pasta `tmp`.
- Execução do `fnsysctl mv Source > destination` para movimentação dos arquivos dentro do FortiADC.

# CVE-2019-16157 /CWE-200 - Plaintext Password in Debug Commands

```
attr force-password-change(378) => [default]
0: config system admin








0: edit admin

admin_api.c:59: gui local(admin)
0: set password passwordplaintext

0: next

0: end
```

# CVE-2021-24019/CWE- 22 - Session not expire after logout e Path Directory Traversal

Quarantine Management	>	SERVER	 6.2.6  6.2.6	<input type="checkbox"/>	<a href="https://192.168.0.15:10443/installers/SERVER">https://192.168.0.15:10443/installers/SERVER</a>
Software Inventory	>	NEW-PACKAGE	 6.2.6  6.2.6	<input checked="" type="checkbox"/>	<a href="https://192.168.0.15:10443/installers/NEW-PACKAGE">https://192.168.0.15:10443/installers/NEW-PACKAGE</a>
Endpoint Policy	>	./dir/	 6.2.6  6.2.6	<input type="checkbox"/>	<a href="https://192.168.0.15:10443/installers/./dir/">https://192.168.0.15:10443/installers/./dir/</a>
Endpoint Profiles	>	./dir/file bin	 6.2.6  6.2.6	<input type="checkbox"/>	<a href="https://192.168.0.15:10443/installers/./dir/file bin">https://192.168.0.15:10443/installers/./dir/file bin</a>
Manage Installers	▼	./dir/file pcap	 6.2.6  6.2.6	<input type="checkbox"/>	<a href="https://192.168.0.15:10443/installers/./dir/file pcap">https://192.168.0.15:10443/installers/./dir/file pcap</a>
Deployment Packages		./dir/file bat	 6.2.6  6.2.6	<input type="checkbox"/>	<a href="https://192.168.0.15:10443/installers/./dir/file bat">https://192.168.0.15:10443/installers/./dir/file bat</a>
FortiClient Installers					
Policy Components	>				
Telemetry Gateway Lists	>				

# CVE - Em contexto de IA

```
> [CVE Impact Other]
> CWE-285: Improper Authorization
>
> -----
>
> [Attack Vectors]
> The lack of proper authorization checks on the `/users` endpoint can lead to unauthorized access
>
> -----
>
> [Reference]
> https://github.com/0x00sec/0x00sec GPT
>
> -----
>
> [Discoverer]
> cnetsec
```

Use CVE-2024-390

# **Broken Access Control**

## **Riscos para o Setor Financeiro**



# Riscos para o Setor Financeiro

Falha que permite acesso indevido a dados e funções.

Relevância: O setor financeiro lida com dados sensíveis (transações, clientes).

Exemplos: vazamentos de dados e incidentes de fraude.

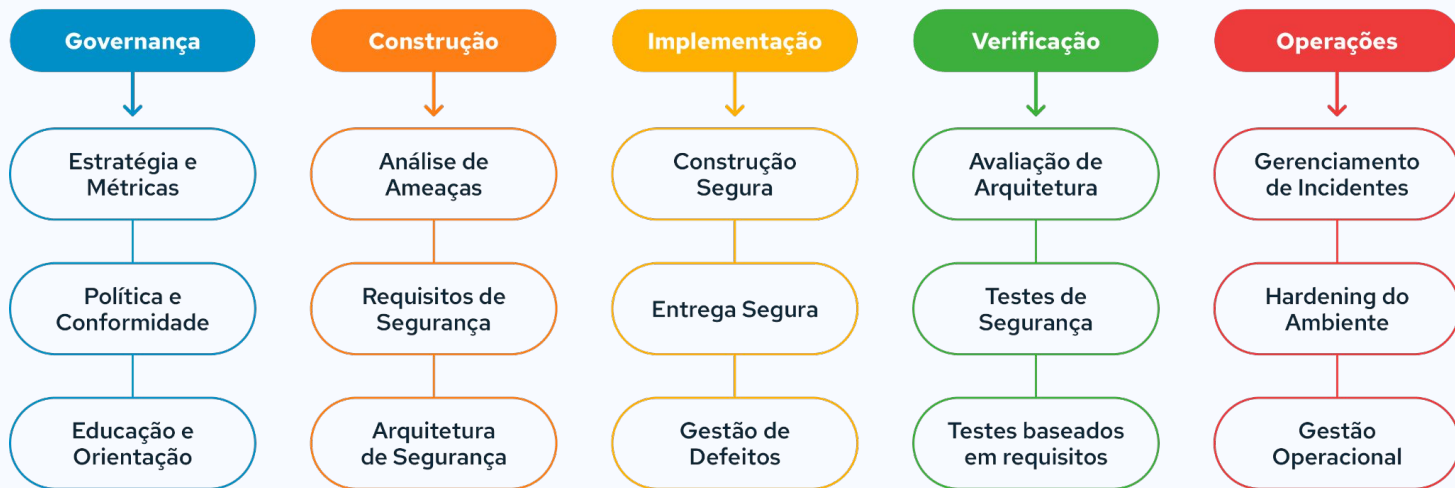
# Impactos do controle de acesso quebrado nas regulamentações do PCI DSS

- Requisito 7 do PCI DSS: Acesso restrito a dados confidenciais.
- Requisito 8 do PCI DSS: Identificação e autenticação fortes.
- Consequências: Multas, perda de certificação e danos à reputação

# Boas Práticas

# Boas práticas para criar aplicações seguras

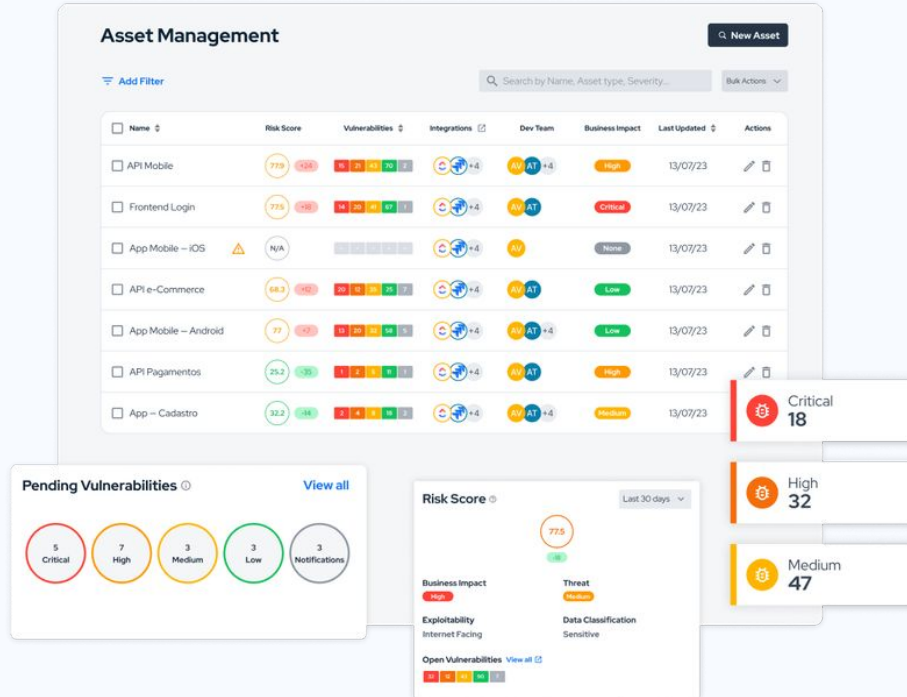
Appsec é o nome dado ao processo de construção, lançamento e manutenção de aplicações seguras, sempre através das melhores práticas aplicadas ao desenvolvimento.



# ASPM –Application Security Posture Management

- Gerencie a postura de segurança do App
- Construa e monitore o programa AppSec
- Gerencie vulnerabilidades orientadas a riscos
- Incorpore segurança no início do desenvolvimento

# Gerencie os riscos associados aos seus ativos



# PCI-DSS

- RBAC: Implementar controle de acesso baseado em função.
- Auditorias e monitoramento: Revisões constantes de segurança.
- Ferramentas: IAM, gateways de API seguros, logs centralizados, WAF
- Conformidade: Garanta a conformidade com PCI

# Exemplo de controle

```
users_data = {
    "user_A": {"balance": 1000, "transactions": ["deposit", "read"]},
    "user_B": {"balance": 500, "transactions": ["deposit", "read"]},
}

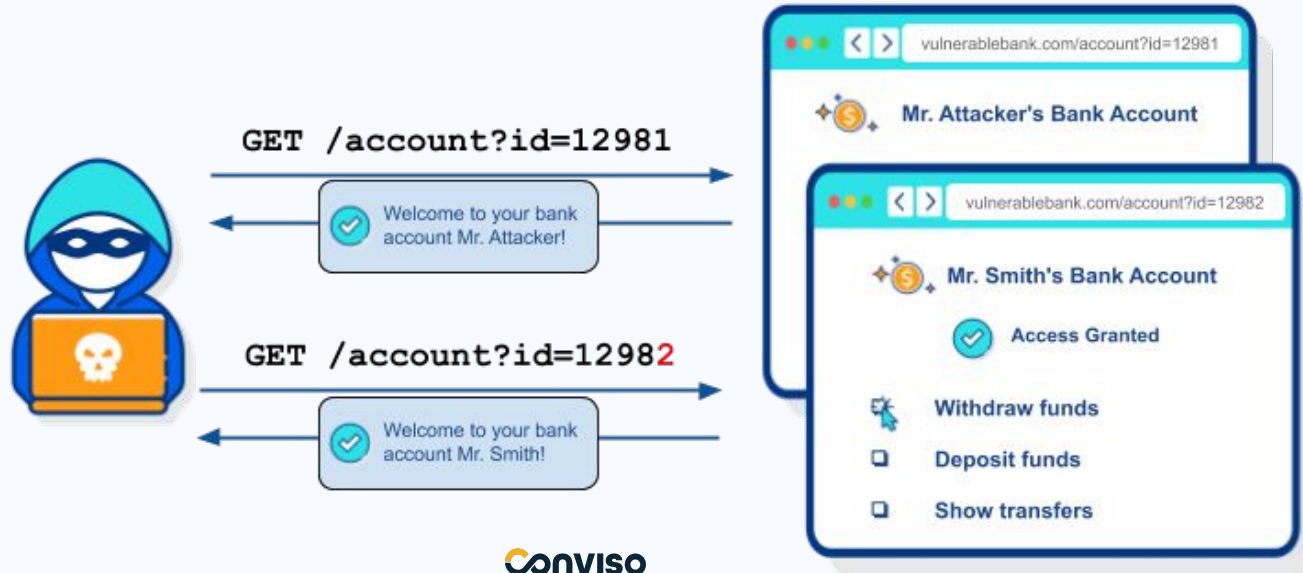
# Función para acceder al estado de cuenta bancario
def access_statement(authenticated_user, authorized_user):
    if authenticated_user == authorized_user:
        return users_data.get(authenticated_user, "Información no encontrada.")
    return "Acceso denegado."

# Ejemplo de uso
print(access_statement("user_A", "user_A")) # Acceso permitido
print(access_statement("user_A", "user_B")) # Acceso denegado
```



## Outras boas práticas

- Aplicar privilégios mínimos
- Revise a lógica de autorização
- Certifique-se de que os identificadores de pesquisa não estejam acessíveis mesmo quando forem adivinhados ou não puderem ser alterados

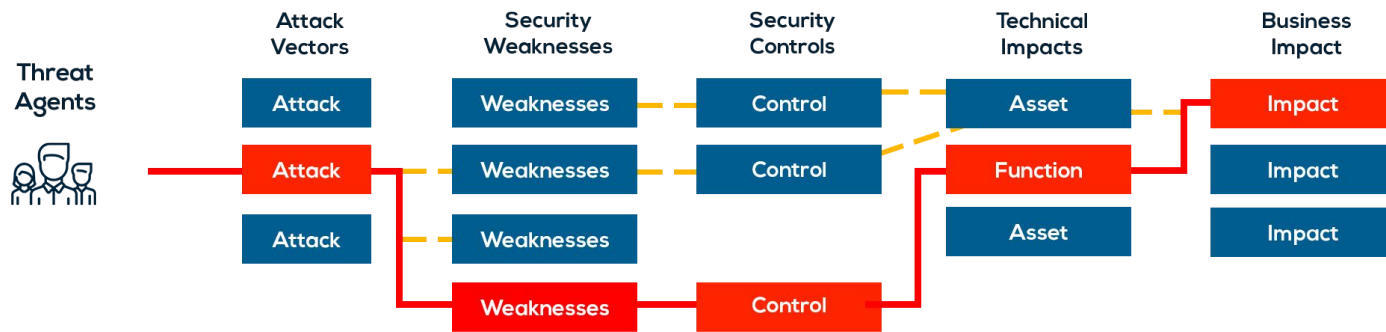


# Modelagem de ameaças na prática

# O que é modelagem de ameaças?

É uma **técnica efetiva** que ajuda a construir aplicações, sistemas, redes e serviços de **maneira segura**. De forma que **identifica ameaças potenciais** e **reduz riscos** estratégicos logo no início do ciclo de desenvolvimento.

# Por que realizar Modelagem de ameaças?




# Testes orientados a requisitos

Governance	Design	Implementation	Verification	Operations
Strategy and Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Policy and Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Education and Guidance	Security Architecture	Defect Management	Security Testing	Operational Management

## ○ Common Attack Pattern Enumeration and Classification

(CAPEC™) fornece um catálogo público de **padrões de ataque comuns** que ajuda os usuários a entender como os adversários exploram pontos fracos em aplicativos e outros recursos cibernéticos.



The screenshot shows the CAPEC website homepage. At the top is a dark red header with the CAPEC logo and the text "Common Attack Pattern Enumeration and Classification" and "A Community Resource for Identifying and Understanding Attacks". Below the header is a navigation bar with links: Home, About, CAPEC List, Community, News, and a partially visible link. The main content area has a paragraph explaining the purpose of CAPEC. Below this, there are two main sections: "CAPEC List Quick Access" and "New to CAPEC?". The "Quick Access" section includes buttons for "View CAPEC" (with sub-options: "by Mechanisms of Attack", "by Domains of Attack", "by Other Criteria") and "Search CAPEC". The "New to CAPEC?" section features a red starburst graphic with the text "New to CAPEC? Start Here!" and a paragraph of introductory text. At the bottom, there is a "Community Engagement" section with links for "Rest API Working Group" and "Join the CWE/CAPEC Rest API WG".

**CAPEC** Common Attack Pattern Enumeration and Classification  
A Community Resource for Identifying and Understanding Attacks

Home | About | CAPEC List | Community | News | S

Understanding how the adversary operates is essential to effective cybersecurity. CAPEC™ helps by providing a comprehensive catalog of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities. It can be used by analysts to advance community understanding and enhance defenses.

**CAPEC List Quick Access**

**View CAPEC**

- by Mechanisms of Attack
- by Domains of Attack
- by Other Criteria

**Search CAPEC**

ENHANCED BY Google

**New to CAPEC?**

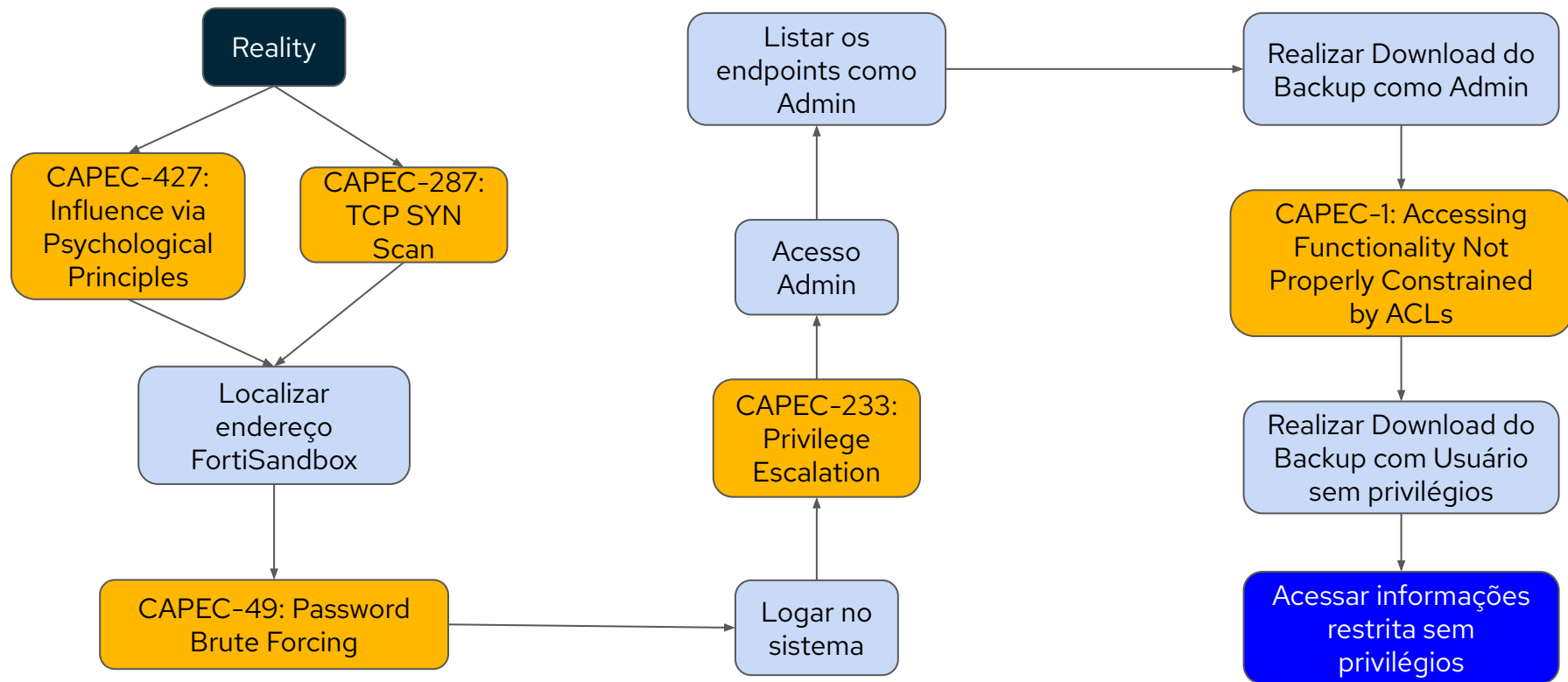
**New to CAPEC? Start Here!**

Common Attack Pattern Enumerations and Classifications (CAPEC™) can be overwhelming to someone new to cyber-attack patterns. This page offers tips on how to familiarize yourself with what CAPEC has to offer, before more fully exploring this extensive knowledge base.

**Community Engagement**

**Rest API Working Group** [Join the CWE/CAPEC Rest API WG](#)

# Modelagem de ameaças visão atacante



O projeto OWASP Application Security Verification Standard (**ASVS**), provê uma base para testar **controles básicos** em suas aplicações web e também provê para os desenvolvedores uma **lista de requisitos de segurança** para desenvolvimento seguro.

## OWASP Application Security Verification Standard



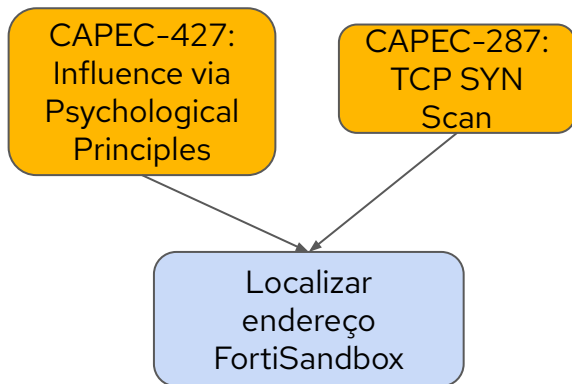
### What is the ASVS?

The OWASP Application Security Verification Standard (ASVS) Project provides a basis for testing web application technical security controls and also provides developers with a list of requirements for secure development.



# Modelagem de ameaças visão defesa

## Ataque



## Controle

OWASP ASVS					
V8.3 Sensitive Private Data					
#	Description	L1	L2	L3	CWE
8.3.4	Verify that all sensitive data created and processed by the application has been identified, and ensure that a policy is in place on how to deal with sensitive data. (C8)	✓	✓	✓	200
14.3.3	Verify that the HTTP headers or any part of the HTTP response do not expose detailed version information of system components.	✓	✓	✓	200

# Modelagem de ameaças visão defesa

## Ataque

CAPEC-49: Password  
Brute Forcing

Logar no  
sistema

## Controle

### OWASP ASVS

#### V2.1 Password Security

#	Description	L1	L2	L3	CWE
2.1.1	Verify that user set passwords are at least 12 characters in length (after multiple spaces are combined). (C6)	✓	✓	✓	521

#### V2.2 General Authenticator Security

2.2.1	Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls include blocking the most common breached passwords, soft lockouts, rate limiting, CAPTCHA, ever increasing delays between attempts, IP address restrictions, or risk-based restrictions such as location, first login on a device, recent attempts to unlock the account, or similar. Verify that no more than 100 failed attempts per hour is possible on a single account.	✓	✓	✓	307
-------	---	---	---	---	-----

# Modelagem de ameaças visão defesa

## Ataque

CAPEC-1: Accessing  
Functionality Not  
Properly Constrained  
by ACLs

Realizar Download do  
Backup com Usuário  
sem privilégios

Acessar informações  
restrita sem  
privilégios

## Controle

### OWASP ASVS

#### V4.1 General Access Control Design

#	Description	L1	L2	L3	CWE
2.1.1	Verify that the principle of least privilege exists - users should only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization. This implies protection against spoofing and elevation of privilege. (C7)	✓	✓	✓	285
4.1.5	Verify that access controls fail securely including when an exception occurs.(C10)	✓	✓	✓	307

## Riesgos

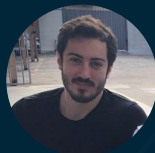
“Há muitas maneiras de mitigar esses riscos! Então você está pronto para o desafio? Vamos começar!”



# Let's **empower developers** to build secure applications?



**Danilo Costa**  
Squad Leader  
[dcosta@convisoappsec.com](mailto:dcosta@convisoappsec.com)



**Pedro Vargas**  
Analista de segurança de aplicações  
[pvargas@convisoappsec.com](mailto:pvargas@convisoappsec.com)