

Modelagem de Ameaças

Nunca vi nem comi, só ouço falar.

Who I am...

Tiago Zaniquelli:

- Pai da Bia e Marido da Gabriela;
- De 2003 à 2021 atuei como desenvolvedor;
- Desde 2021 atuando com AppSec na Conviso Application Security;
- Apaixonado por Segurança, Agilidade e Desenvolvimento;

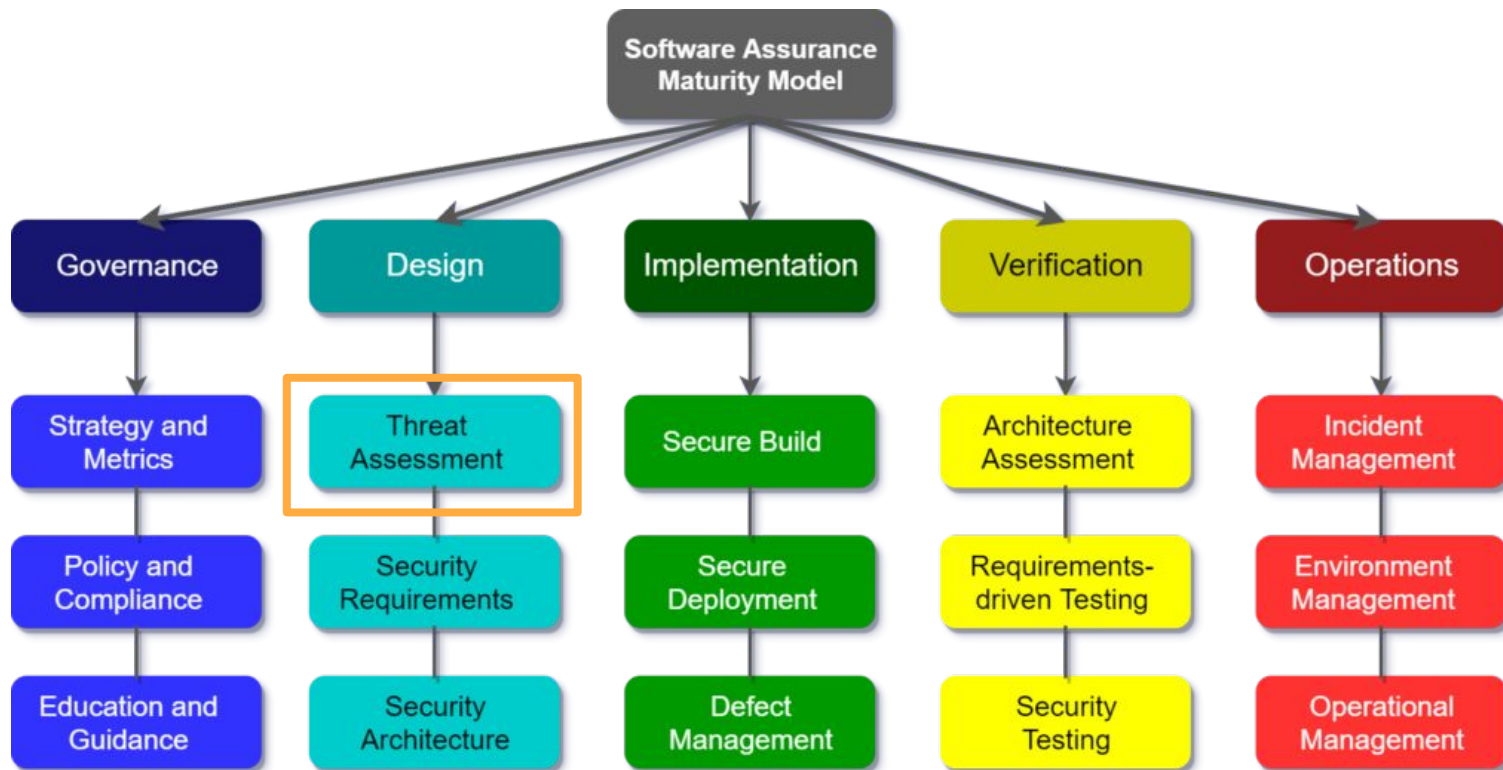
Agenda

- Modelagem de ameaças;
- CAPEC;
- CWE;
- ASVS;
- Processo de Modelagem de Ameaças;
- Prática.

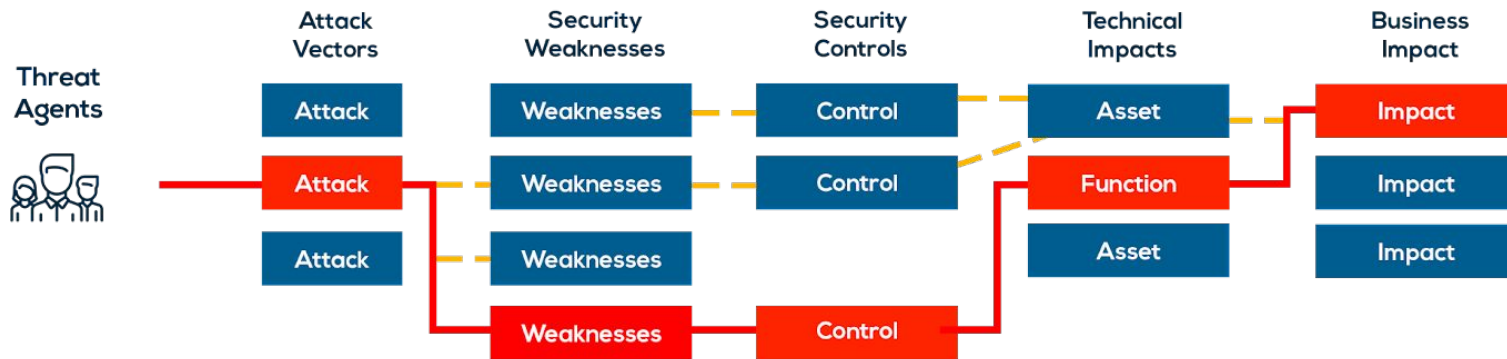
O que é **modelagem de ameaças**?

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

OWASP SAMM



Por que realizar Modelagem de ameaças?



○ 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. The header is dark red with the CAPEC logo and the title "Common Attack Pattern Enumeration and Classification". Below the header is a navigation bar with links: Home, About, CAPEC List, Community, News, and a partially visible "S". The main content area has a white background. It starts with a paragraph explaining the purpose of CAPEC. Below this is a "CAPEC List Quick Access" section with buttons for "View CAPEC" (which has three sub-buttons: "by Mechanisms of Attack", "by Domains of Attack", and "by Other Criteria") and "Search CAPEC". To the right of this section is a red starburst graphic that says "New to CAPEC? Start Here!". Below the starburst is a section titled "New to CAPEC?" with a paragraph of text. At the bottom of the page, there is a "Community Engagement" section with a "Rest API Working Group" link and a "Join the CWE/CAPEC Rest API WG" link. A small "ENHANCED BY Google" logo is visible at the bottom left of the page.

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

New to CAPEC?

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](#)

ENHANCED BY Google

Common Weakness Enumeration

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

Ela serve como uma linguagem comum, uma medida para ferramentas de segurança e como uma linha de base para os esforços **de identificação, mitigação e prevenção de fraquezas**.

The screenshot shows the homepage of the CWE Common Weakness Enumeration website. The header features the CWE logo and the title "Common Weakness Enumeration" with the subtitle "A Community-Developed List of Software & Hardware Weakness Types". Navigation links include Home, About, CWE List, Scoring, Mapping Guidance, Community, News, and Search. A search bar is located on the right. The main content area highlights the "2021 HW" and "Top 25" most dangerous software weaknesses. A sidebar on the left provides quick access to the CWE list by category: Software Development, Hardware Design, Research Concepts, and Other Criteria. The right sidebar contains news and podcast links related to CWE/CAPEC.

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

Home | About | CWE List | Scoring | Mapping Guidance | Community | News | Search

ID Lookup:

CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

CWE List Quick Access

View CWE

- by Software Development
- by Hardware Design
- by Research Concepts
- by Other Criteria

Search CWE

2022 CWE Top 25 Most Dangerous Software Weaknesses

They are dangerous because they are often easy to find, exploit, and can allow adversaries to completely take over a system, steal data, or prevent an application from working.

Software List | Limitations | Methodology | More

Community Engagement

CWE News

News [New CWE/CAPEC Board Member from University of Nebraska Omaha](#)

Podcast ["Using CWE/CAPEC in Education"](#)

News [2022 "CWE Top 25" Now Available!](#)

Blog ["The Missing Piece in](#)

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

[Main](#) | [Supporters](#) | [News and Events](#) | [Acknowledgements](#) | [Glossary](#) | [ASVS Users](#)



owasp **flagship project**

Stars ASVS

1.8k

Follow

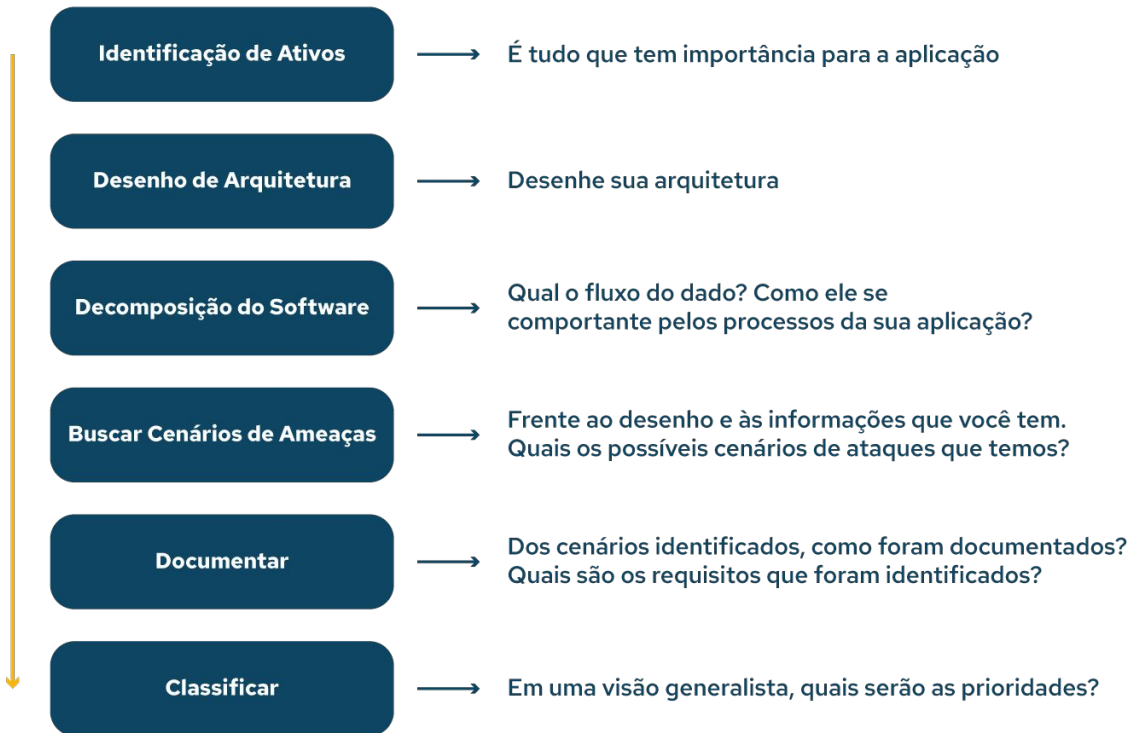
1.6k

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.

**Vamos entender como
funciona o processo de
modelagem?**

Processo de Modelagem de ameaças

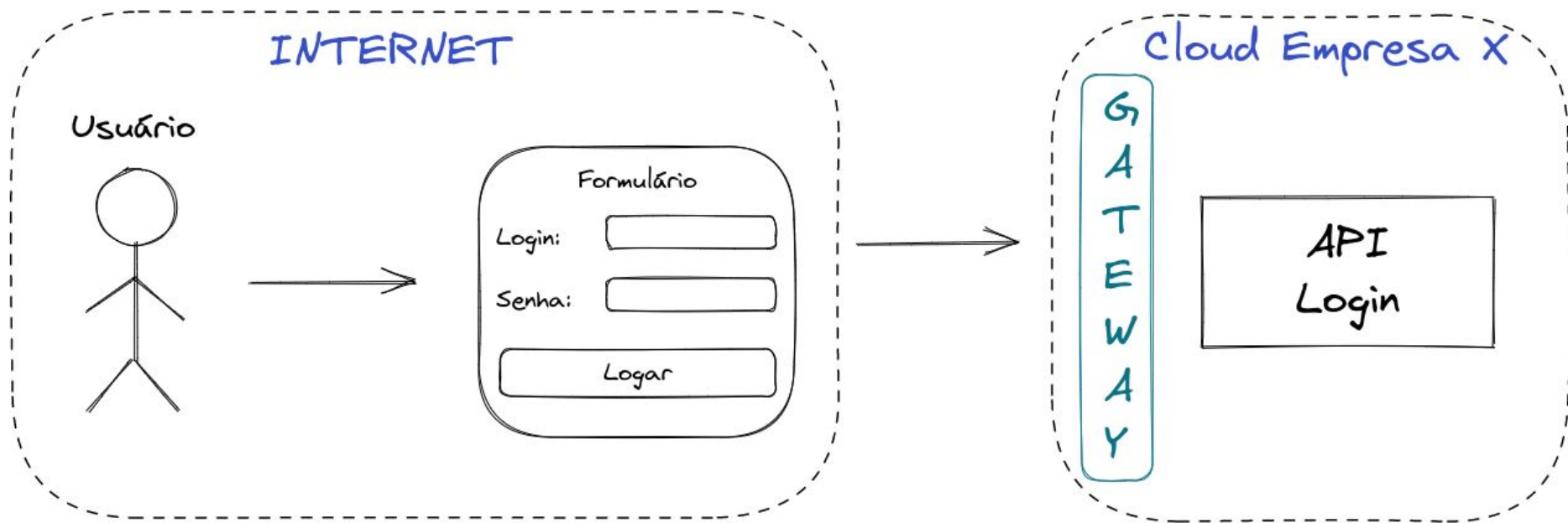




Prática...

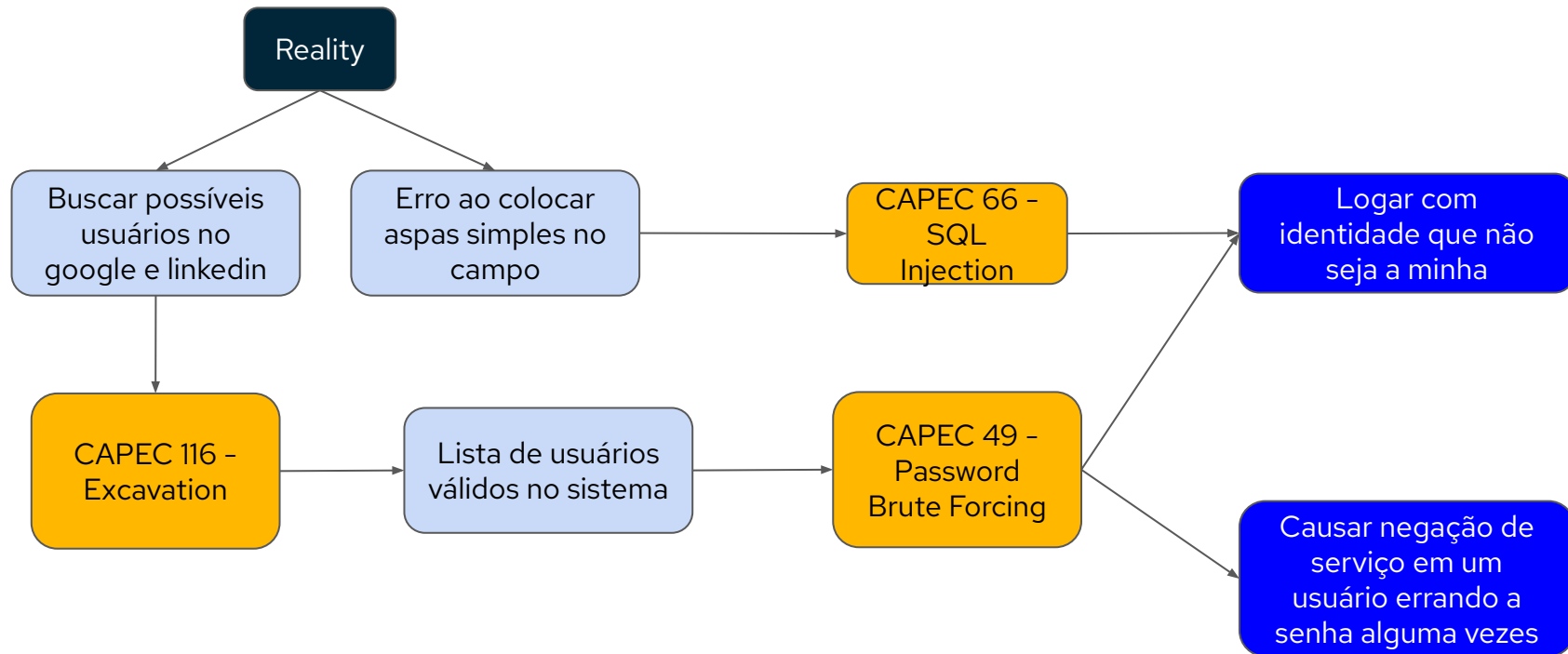


Cenário



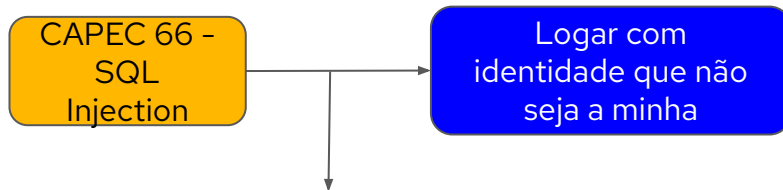
Modelagem de Ameaças

Cenários de Ameaça



Modelagem de Ameaças

Requisitos



▼ Related Weaknesses



CWE-ID

Weakness Name

89

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

1286

Improper Validation of Syntactic Correctness of Input

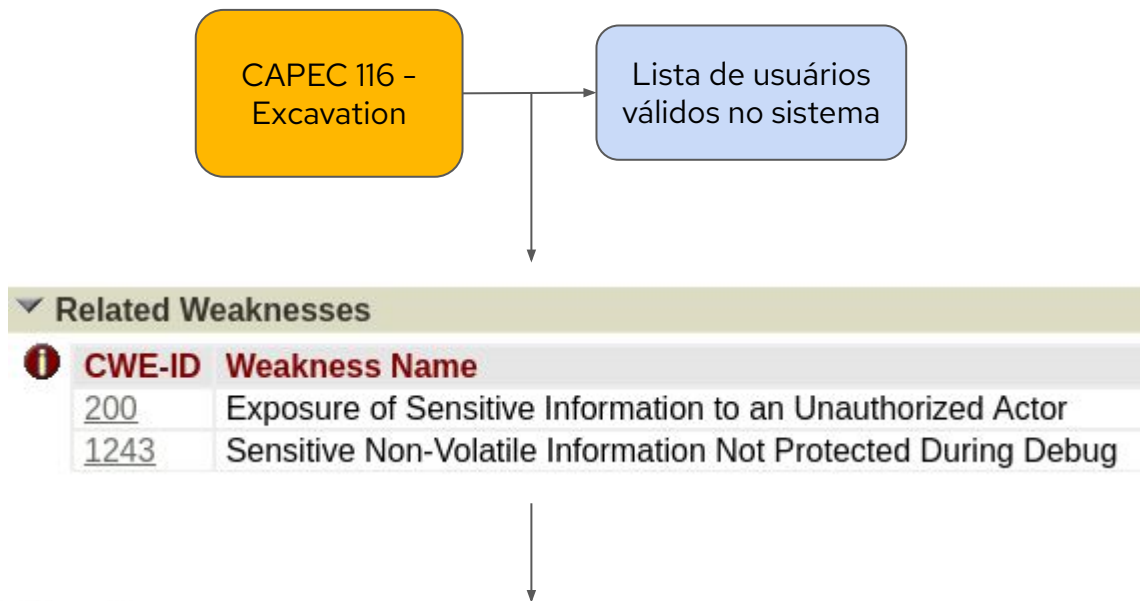


#	Description	L1	L2	L3	CWE
5.3.5	Verify that where parameterized or safer mechanisms are not present, context-specific output encoding is used to protect against injection attacks, such as the use of SQL escaping to protect against SQL injection. (C3 , C4)	✓	✓	✓	89

talk is cheap
show me the code

Modelagem de Ameaças

Requisitos



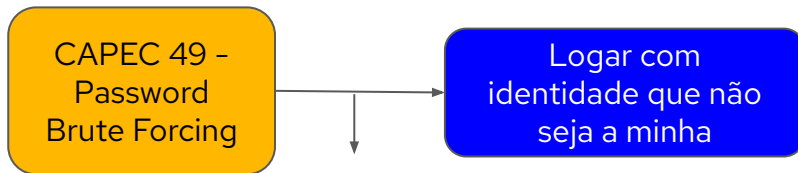
Authentication Responses

Using any of the authentication mechanisms (login, password reset or password recovery), an application must respond with a generic error message regardless of whether:

talk is cheap
show me the code

Modelagem de Ameaças

Requisitos



Related Weaknesses



CWE-ID Weakness Name

521	Weak Password Requirements
262	Not Using Password Aging
263	Password Aging with Long Expiration
257	Storing Passwords in a Recoverable Format
654	Reliance on a Single Factor in a Security Decision
307	Improper Restriction of Excessive Authentication Attempts
308	Use of Single-factor Authentication
309	Use of Password System for Primary Authentication

#	Description	L1	L2	L3	CWE	NIST §
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	5.2.2 / 5.1.1.2 / 5.1.4.2 / 5.1.5.2

talk is cheap
show me the code

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



Tiago Zaniquelli

Security Analyst

tiago.zaniquelli@owasp.org