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;

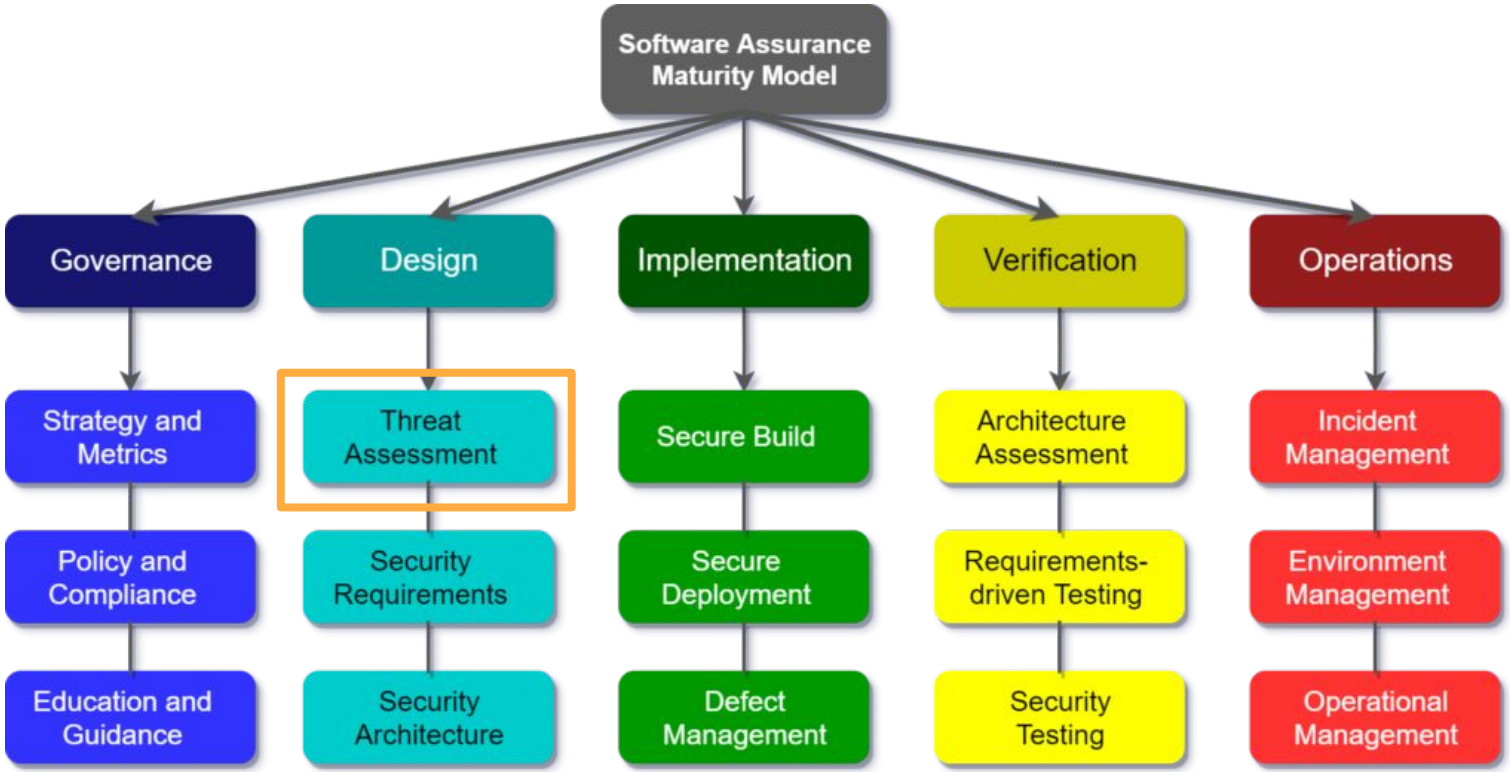
Agenda

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

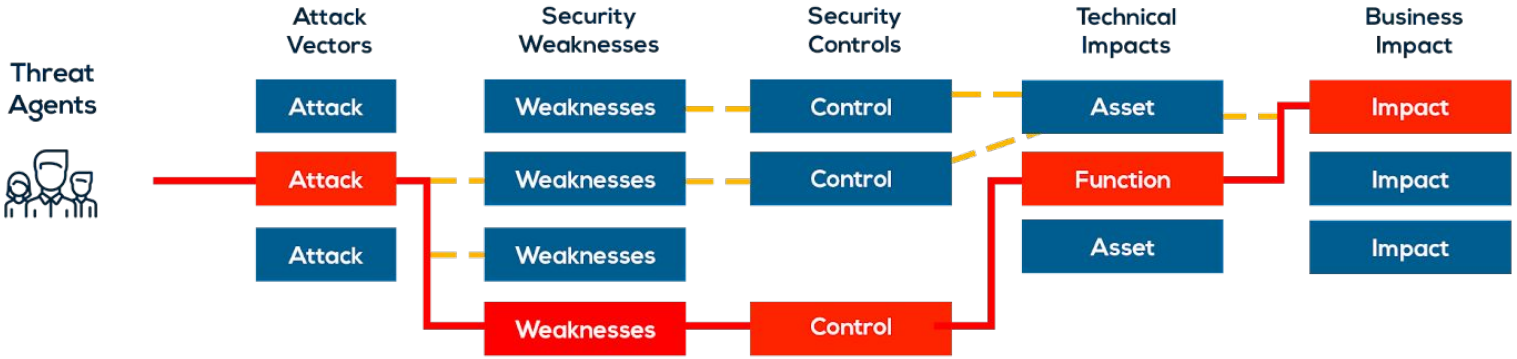
O que é modelagem de ameaças?

"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

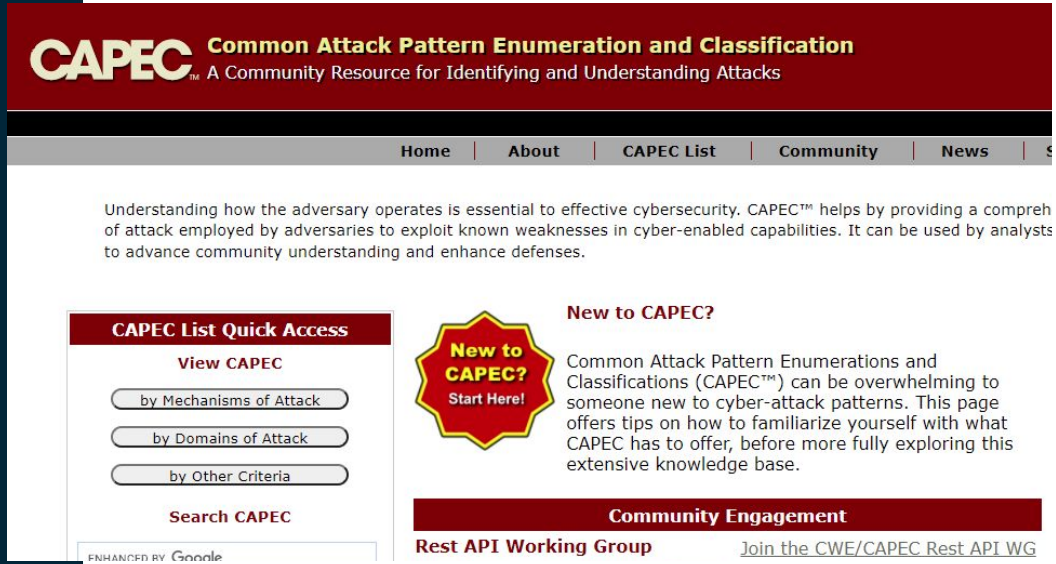

Software Assurance Maturity Model
Governance
Design
Implementation
Verification
Operations
Strategy and Metrics
Policy and Compliance
Education and Guidance
Threat Assessment
Security Requirements
Security Architecture
Secure Build
Secure Deployment
Defect Management
Architecture Assessment
Requirements-driven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

Por que realizar Modelagem de ameaças?



CAPEC™

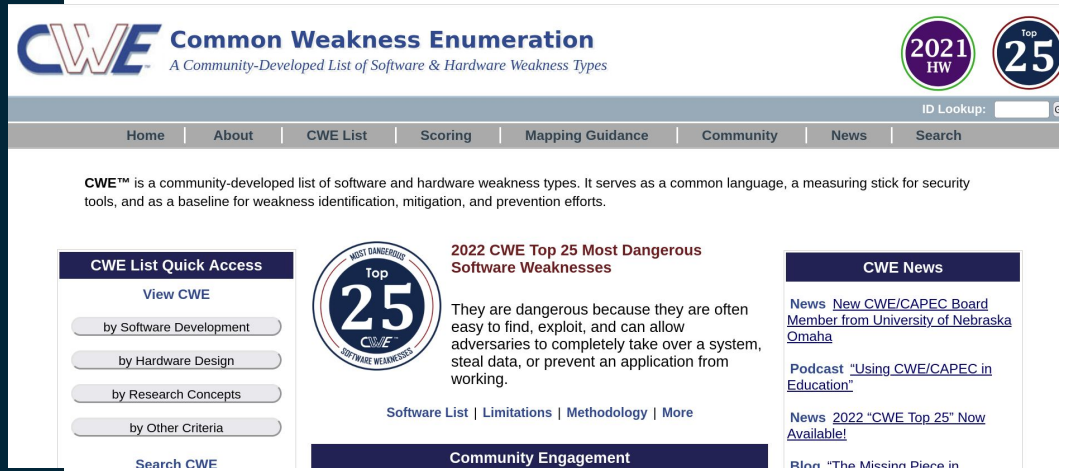
O **Common Attack Pattern Enumeration and Classification** (CAPEC™) fornece um catálogo público de **padrões de ataque comuns** que ajuda os usuários a entender como os adversários exploram pontos fracos em aplicativos e outros recursos cibernéticos.



CWE™

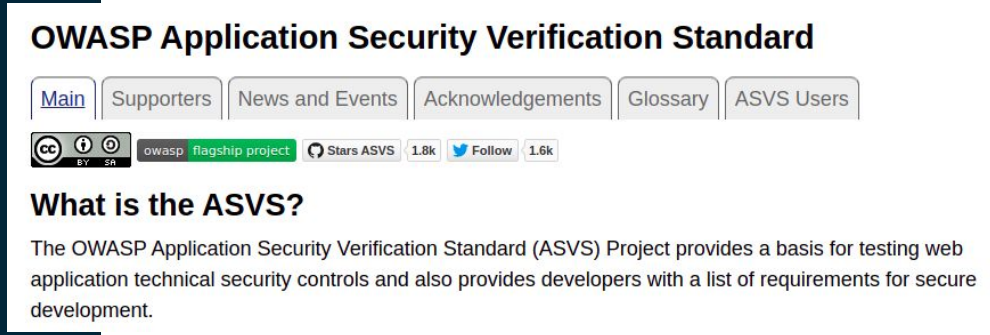
Common Weakness Enumeration (CWE™) é uma lista de tipos de fraquezas de software e hardware, desenvolvida pela comunidade.

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.**



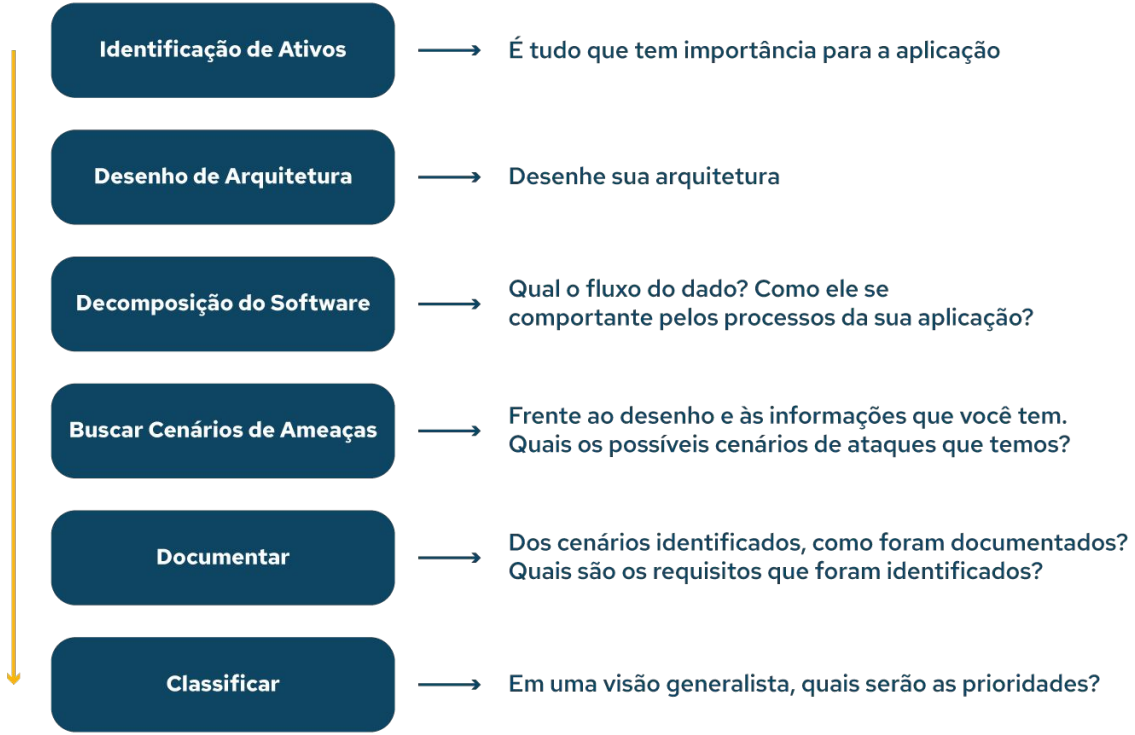
ASVS

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



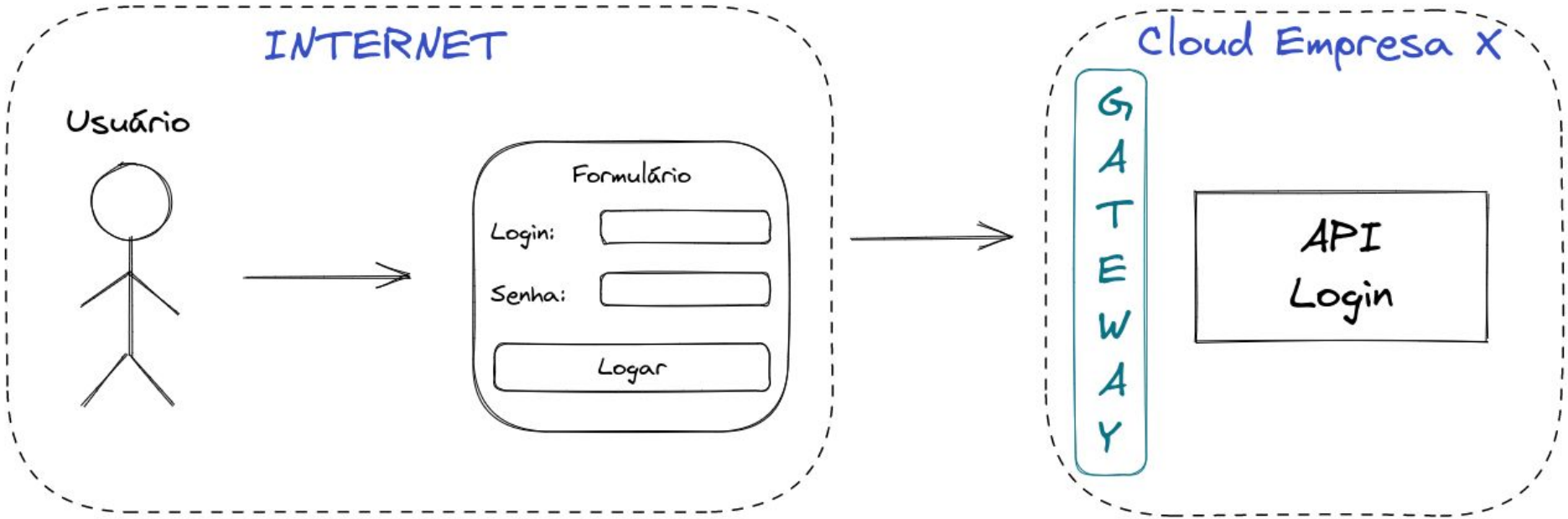
Vamos entender como funciona o processo de **modelagem?**

Processo de Modelagem de ameaças

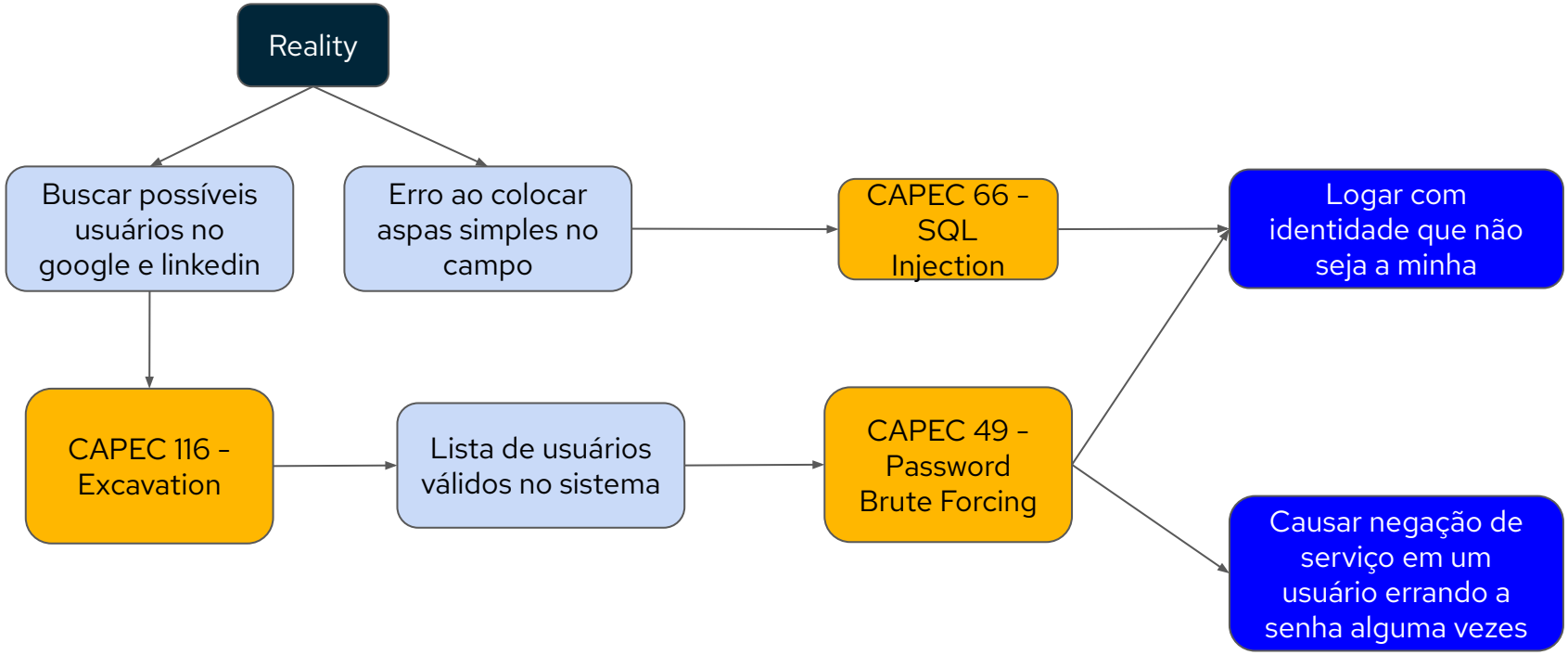


Prática...

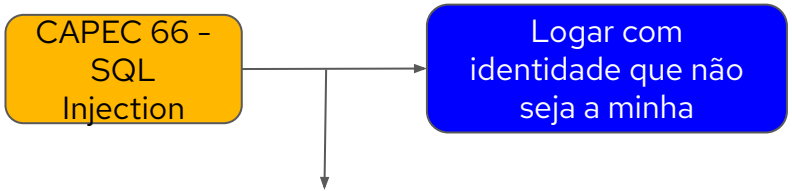
Cenário


INTERNET
Usuário
Formulário
Login:
Senha:
Logar
Cloud Empresa X
GATEWAY
API
Login

Modelagem de Ameaças
Cenários de Ameaça



Modelagem de Ameaças
Requisitos



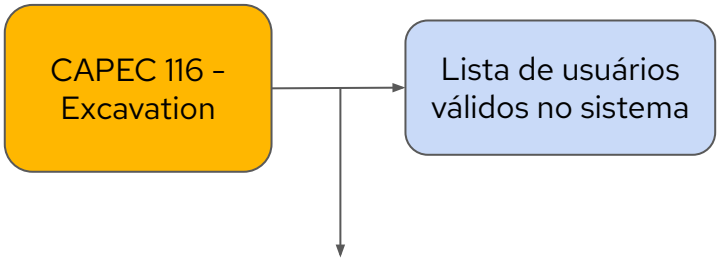
Related Weaknesses

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



Related Weaknesses

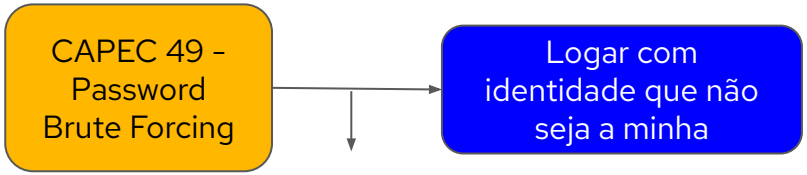
CWE-ID	Weakness Name
200	Exposure of Sensitive Information to an Unauthorized Actor
1243	Sensitive Non-Volatile Information Not Protected During Debug

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