cais Inteligência em Cibersegurança

RNP

Introdução aos Testes de Intrusão (Pentest)

Leonardo Dias

$cat bio.txt

Leonardo Dias

Analista do Red Team no CAIS/RNP

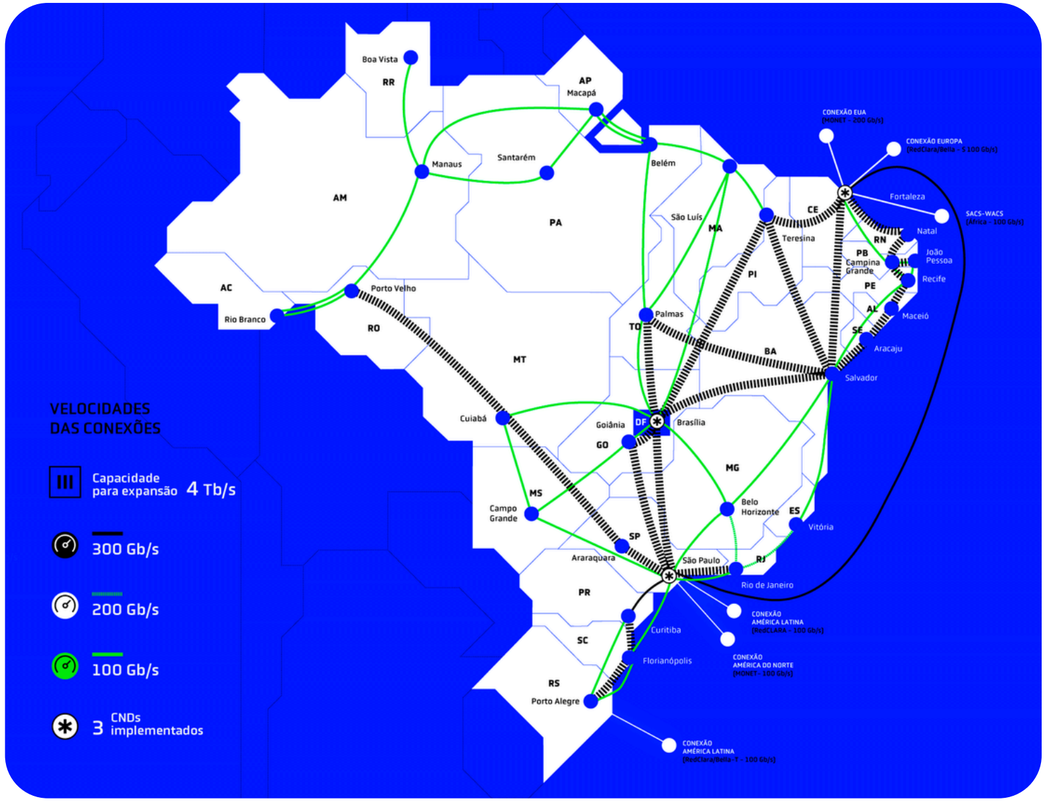
- ⩥ Graduado em Gestão da Tecnologia da Informação;
- ⩥ Especialização em Defesa Cibernética;
- ⩥ Atuando na RNP desde 2017;
- ⩥ Atuo na área de Segurança da Informação desde 2019;
- ⩥ Certificações:

Linux Professional Institute LPIC-1 Linux Administrator
CompTIA Linux+ Powered by LPI Certified
eJPT
CompTIA PenTest+
eWPT
EXIN Information Security Management ISO/IEC 27001 Foundation Certified by EXIN
Cisco Certified CCENT Network
ITIL Foundation V3
tenable

RNP

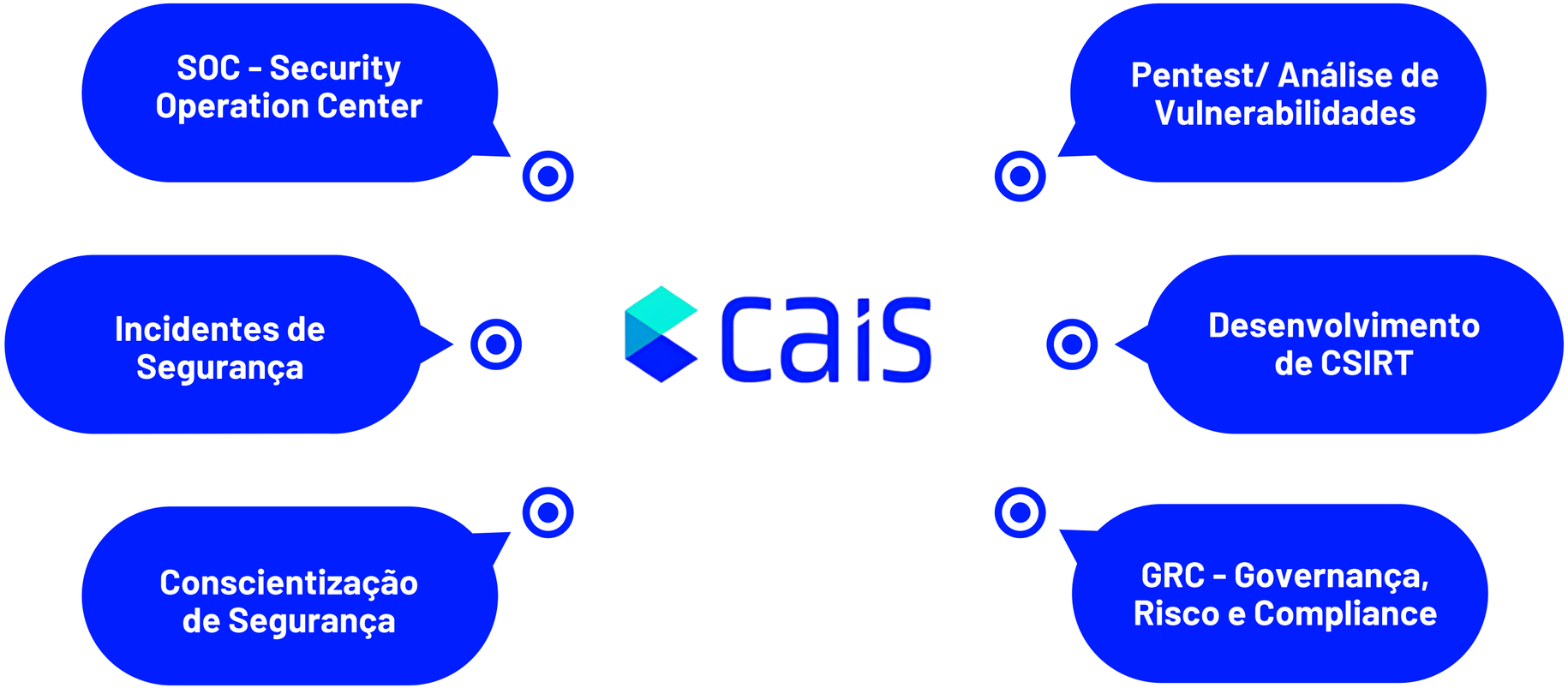
RNP – Rede Nacional de Ensino e Pesquisa

- Internet de alta capacidade, serviços personalizados e incentivo a projetos de inovação.
- Conectamos mais de 4 milhões de alunos, professores e pesquisadores, integrando universidades, institutos, hospitais e polos tecnológicos em todo o Brasil.
- Somos pioneiros ao trazer a internet para o Brasil, em 2005, inauguramos a primeira rede de fibra ótica na América Latina.
- Apoiamos com tecnologia e serviços mais de 1500 universidades, institutos educacionais e culturais, agências de pesquisa, hospitais de ensino, parques e polos tecnológicos.



https://www.rnp.br/

CAIS – Inteligência em Cibersegurança

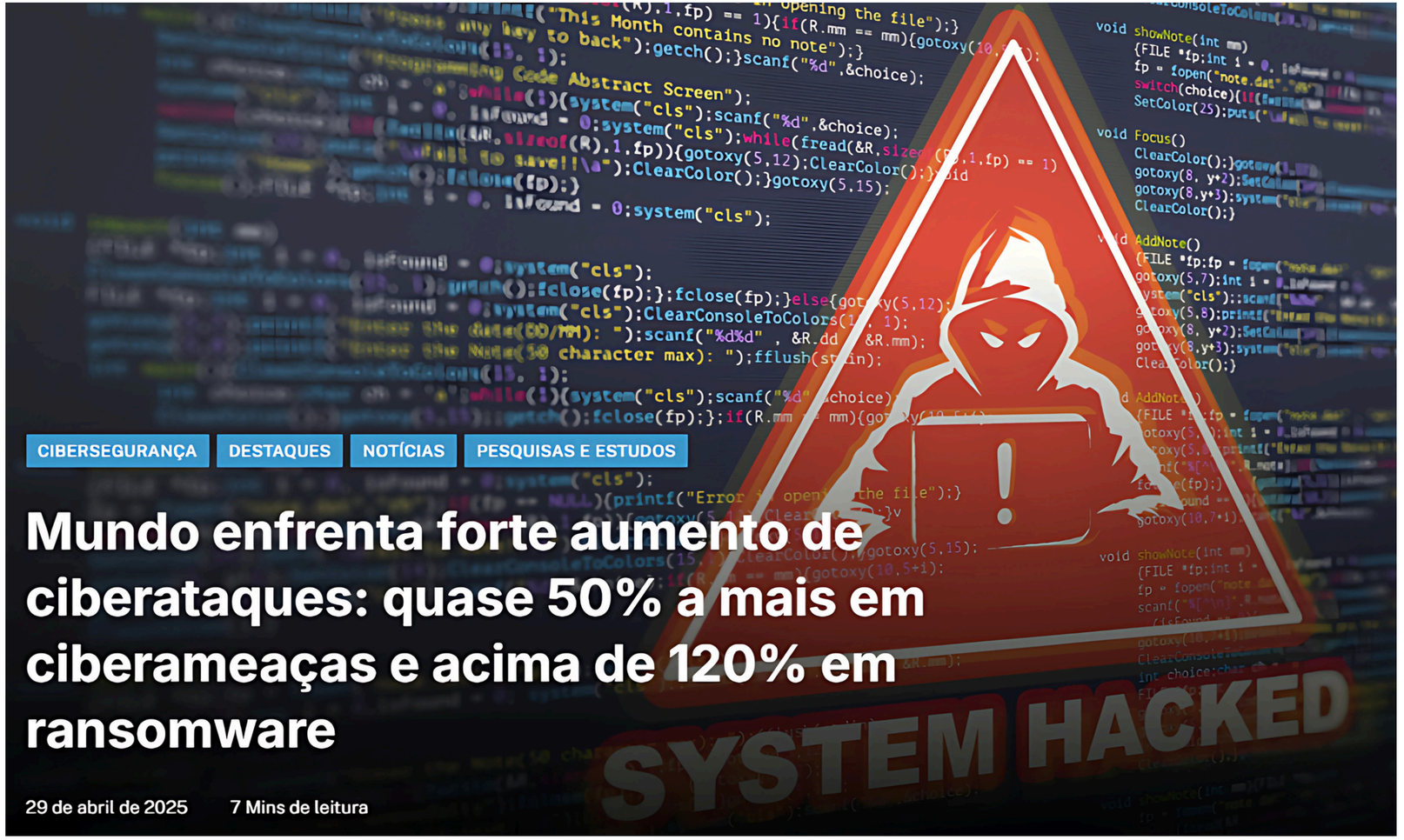


https://www.rnp.br/cais/

RNP

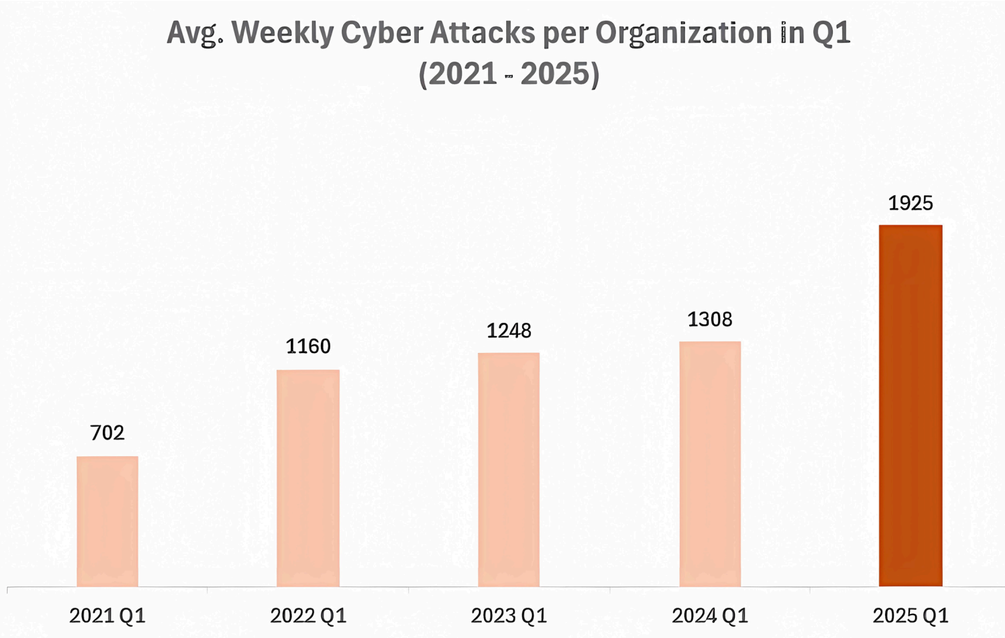
Cenários Atuais

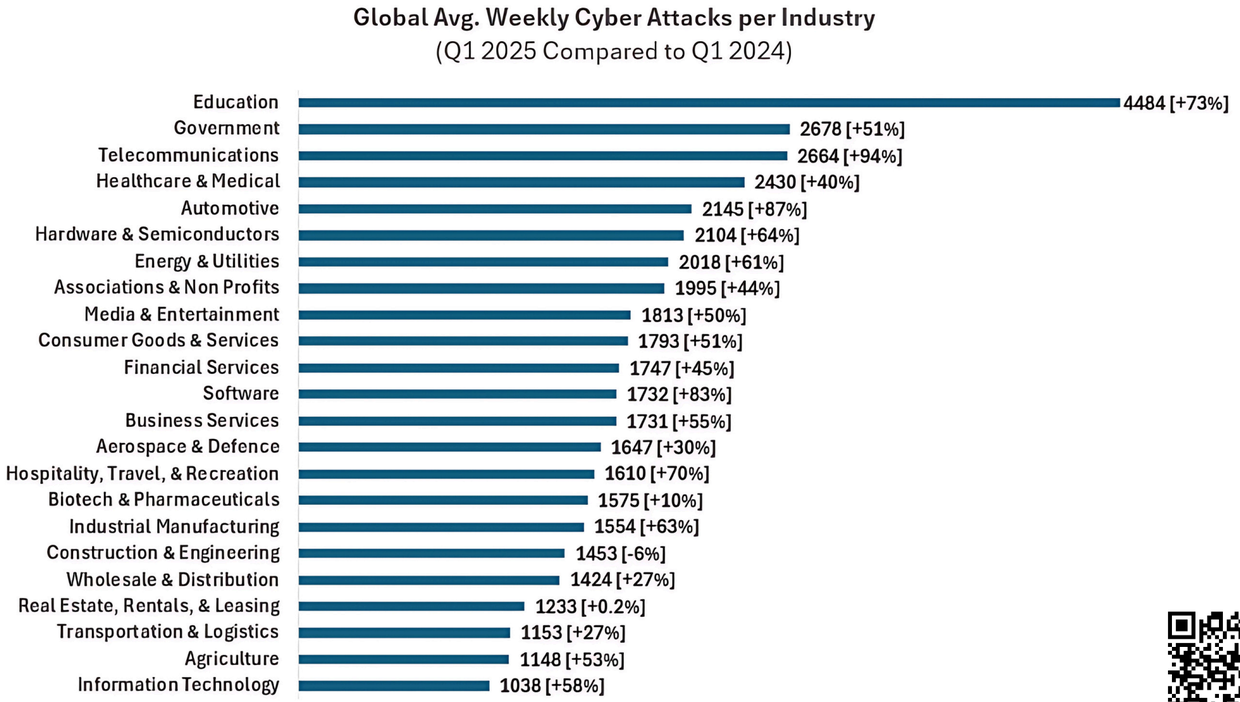
Cenário Atual



Fonte

Cenário Atual





Fonte

Cenário Atual

Recomendações preventivas:

- Reforçar a Postura de Segurança
- Treinamento e Conscientização de Funcionários
- Prevenção Avançada de Ameaças
- Adotar Arquitetura Zero Trust
- Backups Regulares e Planejamento de Resposta a Incidentes
- Segmentação de Rede
- **Gestão de Vulnerabilidades**

Fonte

Qual é o objetivo do treinamento?

Objetivos do treinamento

Apresentar os fundamentos dos testes de intrusão em aplicações web por meio de uma abordagem teórico-prática. O foco será:

- Demonstrar técnicas de ataque e exploração controlada em ambientes simulados
- Utilizar ferramentas amplamente aplicadas em pentests reais
- Identificar vulnerabilidades comuns em aplicações web
- Compreender boas práticas de segurança após os testes

Objetivos do treinamento

Ao final do treinamento, o participante será capaz de:

- Compreender as fases de um pentest web
- Utilizar ferramentas de reconhecimento e exploração
- Identificar vulnerabilidades comuns como XSS, SQLi, Upload Inseguro, entre outras.
- Compreender boas práticas de mitigação de falhas de segurança

Vamos começar!

O que é Segurança Ofensiva?

Segurança ofensiva, ou "OffSec", refere-se a uma variedade de estratégias de segurança proativas que usam as mesmas táticas que os agentes maliciosos usam em ataques do mundo real para fortalecer a segurança da rede em vez de prejudicá-la. Entre os métodos de segurança ofensivos comuns estão: formação de red team, testes de intrusão e avaliação de vulnerabilidade.

Fonte

Principais atividades

- Realização de testes de intrusão
- Análise de vulnerabilidades
- Desenvolvimento de relatórios detalhados
- Recomendação de medidas de mitigação

O que é pentest?

Penetration Testing é um método de avaliar a segurança de um sistema ou aplicação simulando ataques de fontes mal-intencionadas. O objetivo é identificar e explorar vulnerabilidades de segurança, determinar o impacto potencial e validar os controles de segurança existentes.
Fonte: OWASP Testing Guide

Penetration Testing é um teste no qual avaliadores tentam ativamente encontrar e explorar vulnerabilidades em um sistema ou aplicação. O objetivo é determinar a viabilidade de um invasor conseguir comprometer funções específicas ou dados críticos.
Fonte: NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment

Análise de Vulnerabilidades vs Pentest

Aspecto	Avaliação de Vulnerabilidades	Pentest
Objetivo	Identificar, classificar e priorizar vulnerabilidades	Simular ataque real e demonstrar impacto
Método	Semi-automatizado + análise humana	Manual com apoio de ferramentas
Exploração?	❌ Não	✅ Sim
Profundidade	Média	Alta
Ferramentas comuns	Nessus, Qualys, OpenVAS	Burp Suite, Metasploit, Hydra
Relatório	Riscos priorizados e recomendações	Caminhos de ataque e impacto real demonstrado

Tipos de pentest: caixa branca, cinza e preta

White Box

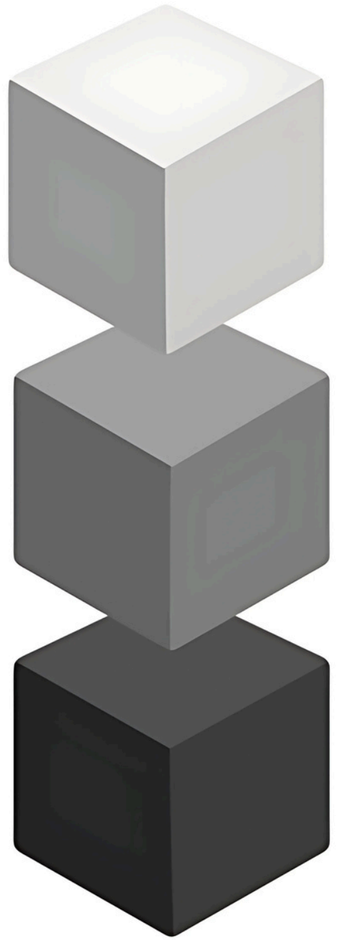
Teste executado com total acesso às informações do sistema e infraestrutura, incluindo bancos de dados, servidores e outros.

Gray Box

Teste executado em áreas específicas do ativo, com informações limitadas fornecidas pelo cliente sobre o sistema e infraestrutura.

Black Box

Teste externo, executado sem nenhuma informação fornecida pelo cliente sobre o sistema e infraestrutura.



Metodologias de Pentest

- **OWASP – Web Security Testing Guide (WSTG):**
  Conjunto de testes focados em segurança de aplicações web. Baseado em práticas ofensivas e vulnerabilidades como XSS, SQLi, CSRF e outras da OWASP Top 10.
- **PTES – Penetration Testing Execution Standard:**
  Guia técnico que define todas as etapas de um pentest — desde o planejamento até o pós-exploração. Ideal para estruturar projetos profissionais.
- **NIST – SP 800-115:**
  Metodologia do governo americano que padroniza a execução de testes de segurança em sistemas. Foca em testes técnicos, validação e relatórios formais.

Fonte

Etapas do Pentest

Planejamento

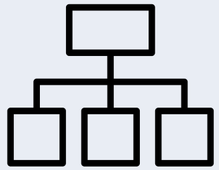
Definição do escopo do teste, estabelecimento de objetivos e regras de engajamento, formalização de autorizações e comunicações.

Reconhecimento (Coleta de Informações)

Passivo: WHOIS, Google Hacking, redes sociais
Ativo: Nmap, DNS, enumeração de serviços

Análise de Vulnerabilidades

Varreduras com scanners como: Nessus, OpenVAS, Burp Suite).
Identificação e priorização de vulnerabilidades conhecidas



Mapeamento e Enumeração

Identificação de sistemas, tecnologias e superfícies de ataque.

Enumeração de diretórios, APIs, usuários e portas.

Exploração (Exploitation)

Testes manuais e automáticos para comprovar vulnerabilidades.

Uso de ferramentas como Metasploit, SQLMap, Hydra

Pós-Exploração

Elevação de privilégios;

Movimentação lateral;

Coleta de provas;

Avaliação do impacto real

Análise e Relatório

Análise dos testes executados.

Compilação de relatório técnico e executivo.

Inclusão de evidências, recomendações de correção e plano de ação.

OWASP Top 10

Código	Categoria	Descrição resumida
A01:2021	Broken Access Control	Falhas no controle de acesso que permitem ações não autorizadas por usuários.
A02:2021	Cryptographic Failures	Problemas com criptografia, como dados sensíveis expostos ou mal protegidos.
A03:2021	Injection	Injeção de código malicioso (ex: SQL, OS, LDAP) via entradas não validadas.
A04:2021	Insecure Design	Falta de princípios de segurança na fase de projeto de sistemas e aplicações.
A05:2021	Security Misconfiguration	Configurações inseguras em servidores, aplicações, permissões, headers etc.
A06:2021	Vulnerable and Outdated Components	Uso de bibliotecas, plugins ou sistemas desatualizados com falhas conhecidas.
A07:2021	Identification and Authentication Failures	Falhas na autenticação, como senhas fracas, brute force e má gestão de sessões.
A08:2021	Software and Data Integrity Failures	Falta de verificação na integridade de atualizações, repositórios e código.
A09:2021	Security Logging and Monitoring Failures	Ausência de logs ou monitoramento eficaz, dificultando detecção de ataques.
A10:2021	Server-Side Request Forgery (SSRF)	Servidores são enganados a fazer requisições para destinos internos ou externos.

RNP

Vulnerabilidades Abordadas

Vulnerabilidade	Descrição rápida
HTML/iframe Injection	Injeção de código HTML/iframe em campos de entrada, podendo manipular o layout da página ou redirecionar o usuário.
Command Injection (RCE)	Execução de comandos do sistema operacional através de entradas mal validadas.
SQL Injection (SQLi)	Injeção de comandos SQL maliciosos para acesso, modificação ou exclusão de dados.
XSS – Reflected e Stored	Injeção de scripts maliciosos para execução no navegador da vítima.
Broken Authentication	Exploração de falhas no processo de login, como senhas fracas ou sem proteção contra força bruta.
Insecure FTP	Serviços FTP sem autenticação segura, permitindo acesso não autorizado ou anônimo.
Unrestricted File Upload	Envio de arquivos sem validação adequada, podendo levar à execução de código malicioso.

Ferramentas utilizadas

Nmap

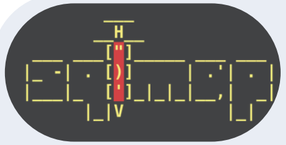
Scanner de rede para identificar hosts, serviços e portas abertas.

WhatWeb

Identifica tecnologias e frameworks usados em websites.

Nikto

Scanner de vulnerabilidades em servidores web, buscando falhas conhecidas.



SQLMap

Automatiza ataques de SQL Injection e extração de dados de bancos.

BurpSuite

Plataforma para análise e exploração de aplicações web (proxy, scanner, intruder).

Hydra

Ferramenta de força bruta para senhas em diversos serviços (FTP, SSH, etc).

Ferramentas utilizadas

Gobuster

Enumeração de diretórios/arquivos ocultos via brute-force.

Metasploit

Framework para desenvolvimento e execução de exploits.

Enum4linux

Enumeração de informações SMB em sistemas Windows/Linux.

Dirb

Ferramenta simples de força bruta para descobrir diretórios/arquivos web.

Hora de Praticar

Hora de praticar

Boas práticas

1. **Validação de Entrada**
   Use listas brancas, filtre dados e evite concatenar comandos.
2. **Prevenção de Injeções e XSS**
   Use prepared statements, output encoding e CSP.
3. **Gerenciamento de Sessão**
   Adote MFA, tokens únicos e cookies seguros (HttpOnly, Secure).
4. **Controle de Acesso**
   Verifique permissões no backend e não confie apenas em parâmetros.
5. **Upload Seguro de Arquivos**
   Valide MIME, armazene fora do diretório público, bloqueie execução.
6. **Monitoramento e Atualizações**
   Mantenha sistemas atualizados, monitore e rode varreduras.

Carreira em cibersegurança

Pesquisa aponta gestão e falta de profissionais qualificados entre os principais desafios da segurança digital

Por **Bruno Lauterjung** - 3 de março de 2025 0

Fonte

Fonte

Recomendação de cursos

Plataformas de Ensino

- https://deseccecurity.com/
- https://gohacking.com.br/
- https://wbeduca.com.br/pr
- https://www.hackingnaweb.com/
- https://adint.com.br/
- https://acaditi.com.brar/
- https://hackershive.io/
- https://www.alura.com/
- https://www.udemy.com.bro/
- https://admnistratives.io/
- https://tryhackme.com/
- https://www.ev.org.br/
- https://academioforensesdigitaal.com.br/
- https://academia.tcm.sec.com/
- https://www.pensarcuroos.com/
- https://bsontreinamentos.cominta.br/

Conclusão

- Conhecemos os fundamentos dos testes de intrusão aplicados a aplicações web.
- Exploramos na prática como identificar e explorar vulnerabilidades comuns.
- Entendemos a importância de pensar como atacante para proteger como defensor.
- Além de explorarmos falhas, também discutimos boas práticas para prevenilas.
- Segurança é um processo contínuo, baseado em aprendizado, atualização e colaboração.

O primeiro passo para fortalecer a segurança é conhecer as próprias vulnerabilidades.

RNP

OBRIGADO (A)!

Leonardo Dias
E-mail: leonardo.silva@rnp.br

Linked in

cais RNP MINISTÉRIO DA CULTURA MINISTÉRIO DA DEFESA MINISTÉRIO DA SAÚDE MINISTÉRIO DAS COMUNICAÇÕES MINISTÉRIO DA EDUCAÇÃO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO