

MAIS UM EVENTO



REALIZAÇÃO



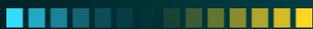
# ROADSEC 15 2023

O MAIOR FESTIVAL HACKER DA AMÉRICA LATINA



15.07.23

ROADSEC  
2023 15.07.23



# Ataque mais comuns em aplicações web

Os ataques mais comuns em aplicações web referem-se a técnicas utilizadas por indivíduos mal-intencionados para explorar vulnerabilidades e comprometer a segurança de websites.

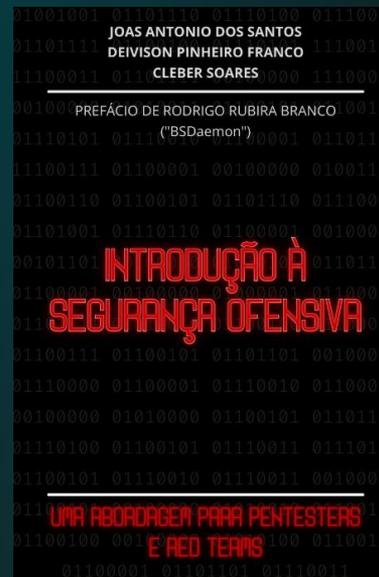


ROADSEC  
2023 15.07.23



## Whoami

- Red Team Leader na HackerSec
- Instrutor de cursos na HackerSec
- Especialista em Segurança Ofensiva
- Autor e Palestrante
- Pesquisador e Contribuidor de TTPs pelo Mitre



ROAD  
SEC  
2023

O MAIOR FESTIVAL HACKER DA AMÉRICA LATINA



# WEB PENTEST 101



# Terminologias de Segurança

**Ameaça:** Uma ação ou um evento que tem o potencial de comprometer e/ou violar a segurança

**Exploração:** Uma forma definida de violar a segurança de um sistema de TI por meio da vulnerabilidade

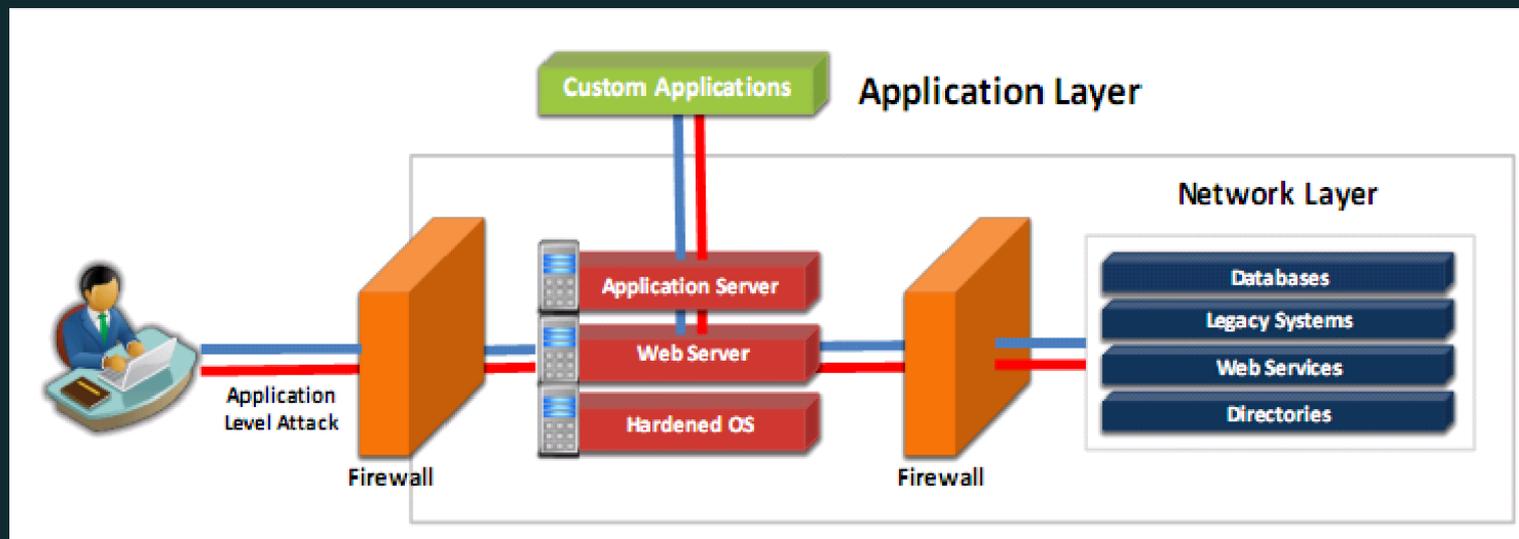
**Vulnerabilidade:** A existência de uma fraqueza, bug ou um erro de design ou implementação que pode levar a um evento inesperável e indesejável que comprometa a segurança do sistema

**Ataque:** Qualquer ação derivada de ameaças inteligentes que podem violar a segurança do sistema

# Vulnerabilidades comuns

- **XSS (Cross Site Scripting):** Permite que um invasor injete códigos maliciosos que executam no navegador da vítima realizando uma ação específica. Existem pelo menos 3 tipos (Refletido, Armazenado e DOM);
- **CSRF (Cross Site Request Forgery):** O invasor faz com que um usuário execute ações na aplicação sem o consentimento do alvo, enviando para formulários de autenticação ou uma ação específica;
- **Arbitrary File Upload:** O invasor envia um arquivo malicioso para um servidor, permitindo outros vetores de ataques também;
- **Subdomain Takeover:** O invasor assume o controle de um subdomínio que não foi removido do seu mapeamento de domínio (CNAME);
- **Account Takeover:** O atacante obtém acesso à conta de um usuário específico e toma o controle da mesma acessando informações confidenciais;
- **JWT Ataques:** O atacante pode comprometer um token JWT para alterar seu conteúdo e obter acessos não autorizados;

# Necessidade de Segurança em Aplicações Web



FONT: CASE JAVA - ECCOUNCIL

“Exemplo de uma simples arquitetura de segurança de aplicação”

# Necessidade de Segurança em Aplicações Web #2

**Proteção dos dados sensíveis:** As aplicações web frequentemente lidam com informações sensíveis dos usuários, como dados pessoais, informações financeiras, senhas e outras informações confidenciais. A falta de segurança adequada pode levar ao roubo de dados e à violação da privacidade dos usuários.

**Prevenção de ataques cibernéticos:** Aplicações web estão constantemente sob ameaça de ataques cibernéticos, como injeção de SQL, cross-site scripting (XSS), cross-site request forgery (CSRF) e outros ataques comuns. Uma aplicação vulnerável pode ser explorada por invasores maliciosos para obter acesso não autorizado, executar ações indesejadas ou causar danos.

**Continuidade do negócio:** Para muitas empresas e organizações, a aplicação web é um componente crítico para a continuidade do negócio. Um ataque bem-sucedido pode resultar em tempo de inatividade, perda de receita e danos à reputação da empresa.

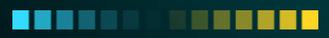
**Conformidade legal:** Dependendo do tipo de dados que a aplicação web lida e da região em que está operando, pode haver requisitos legais e regulatórios relacionados à segurança e proteção de dados. A conformidade é essencial para evitar penalidades legais e danos à reputação.

**Confiança dos usuários:** Os usuários esperam que as aplicações web sejam seguras e confiáveis. Uma aplicação comprometida pode afetar a confiança do usuário, levando a uma redução no número de usuários e potencialmente impactando negativamente o sucesso do negócio.

**Prevenção de vazamentos de informações:** A segurança adequada é necessária para evitar vazamentos acidentais ou intencionais de informações, o que pode causar danos significativos à organização e aos usuários envolvidos.

ROAD  
SEC  
2023

O MAIOR FESTIVAL HACKER DA AMÉRICA LATINA



# NA PRÁTICA



# Ferramentas de Reconhecimento

- Levantar arquivos de configuração;
- Dados sensíveis expostos;
- Subdomínios vulneráveis;
- Diretórios e arquivos expostos;
- Chaves e Secrets no código fonte;
- Portas de serviços abertas;

## Recon Tools

- Assetfinder, Findomain and Subfinder - Subdomain Enum
- Amass - Attack Surface
- Ffuf and Turbosearch - Content Discovery
- Gospider - Web Spider
- HTTPX - HTTP Toolkit
- Axiom - Complete Framework to Recon
- Nuclei - Vulnerabilities Scan
- Gotator - Permutation DNS
- JSubfinder - Javascript and Webpages Scan
- Naabu - Portscanner
- Paramspider - Finds parameters in domain
- Chaos - Subdomain Finder
- Waybackurls - Web Page Snapshots
- SecretFinder - Find apikeys and tokens
- Github Search - Searches Github
- Aquatone - Inspection website
- Katana - Web Crawling
- Dalfox - Scan XSS
- Seclist - General Wordlists

Joas A Santos

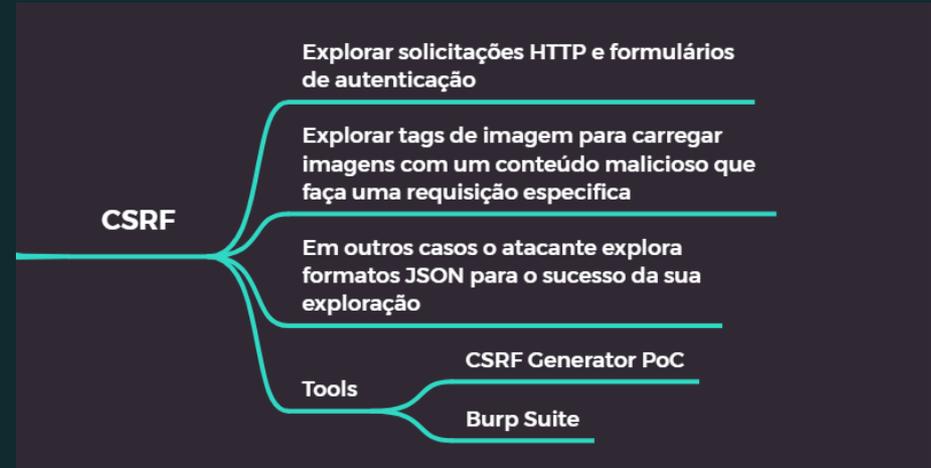
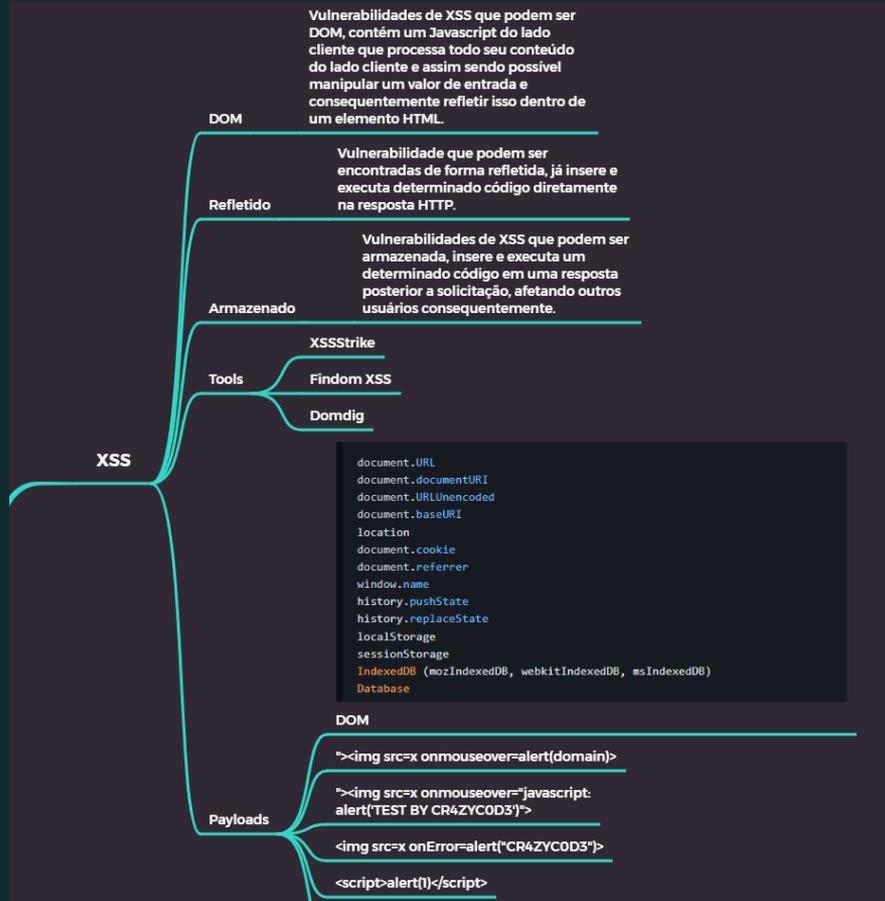
Repositórios interessantes:

<https://github.com/KingOfBugbounty/KingOfBugBountyTips>

<https://cheatsheet.haax.fr/web-pentest/tools/nuclei/>

<https://github.com/six2dez/reconf>  
[tw](#)

# XSS e CSRF



# Subdomain Takeover e Account Takeover

## Subdomain Takeover

**CNAME Subdomain Takeover:** Nesse tipo de subdomain takeover, um invasor identifica um subdomínio que tem um registro CNAME (Canonical Name) apontando para um serviço externo. O invasor pode registrar uma conta nesse serviço externo e reivindicar o subdomínio, assumindo o controle sobre ele.

**NS Subdomain Takeover:** Nesse caso, o invasor identifica um subdomínio que tem registros NS (Name Server) apontando para um serviço de terceiros. Se o invasor conseguir controlar o servidor de nomes, ele poderá redirecionar o tráfego do subdomínio para um servidor sob seu controle.

**MX Subdomain Takeover:** Aqui, o invasor encontra um subdomínio que possui registros MX (Mail Exchanger) apontando para um serviço de e-mail externo. Se o invasor conseguir controlar o serviço de e-mail, ele poderá interceptar e manipular as comunicações de e-mail do subdomínio.

**Sublist3r:** Uma ferramenta de enumeração de subdomínio que pode ajudar a descobrir subdomínios associados a um domínio.

**Amass:** Outra ferramenta de enumeração de subdomínio que pode ajudar a descobrir subdomínios e identificar vulnerabilidades de subdomain takeover.

### Tools

**SubOver:** Uma ferramenta específica para subdomain takeover que verifica subdomínios em busca de vulnerabilidades de CNAME, NS e MX.

**Nuclei:** Uma ferramenta de scanner de segurança que suporta uma ampla variedade de templates para testar várias vulnerabilidades em um aplicativo web. Isso inclui a detecção de possíveis vulnerabilidades de subdomain takeover.

Tentar cadastrar o mesmo e-mail com uma nova senha, explorando erros de design

Vulnerabilidades em OAuth

Crie um PoC para capturar requisição de autenticação

CSRF

Técnicas

Mudar o ID de uma conta para uma com privilégios maiores

IDOR

## Account Takeover

**Password-based Account Takeover:** Nesse tipo de ataque, um invasor tenta obter as credenciais de login de um usuário legítimo, seja por meio de técnicas como phishing, keylogging, força bruta ou reutilização de senhas comprometidas.

**Credential Stuffing:** Nessa técnica, os invasores utilizam credenciais de login roubadas ou vazadas de um serviço online para tentar acessar outras contas do mesmo usuário em diferentes serviços. Como muitos usuários tendem a reutilizar senhas, os invasores podem ter sucesso em acessar várias contas.

**Session Hijacking:** Também conhecido como sessão ou token hijacking, nesse tipo de ataque, os invasores interceptam a sessão ativa de um usuário legítimo para obter acesso não autorizado. Isso pode ser realizado por meio de ataques de Man-in-the-Middle (MITM) ou roubo de cookies de sessão.

**Email-based Account Takeover:** Nesse caso, os invasores obtêm acesso à conta de e-mail de um usuário e, em seguida, utilizam o controle dessa conta para redefinir senhas em outros serviços vinculados ao endereço de e-mail comprometido.

# Arbitrary File Upload e JWT Ataques

**Execução de Código Remoto:** Nesse tipo de ataque, o invasor faz o upload de um arquivo malicioso contendo código que pode ser executado no servidor. Isso permite ao invasor assumir o controle do servidor e executar comandos ou operações indesejadas.

**Inclusão de Arquivo:** Nesse ataque, o invasor faz o upload de um arquivo malicioso que é incluído em outros arquivos ou processos do aplicativo. Isso pode levar à execução posterior de código arbitrário ou à divulgação não autorizada de informações sensíveis.

## Arbitrary File Upload

Utilização de Técnicas de Obfuscação

Exploração de Validação Insuficiente

Bypass de Verificação de Tipo de Arquivo

Manipulação de Extensão de Arquivo

Técnicas

BurpSuite

Tools

**Manipulação do Payload:** Os invasores podem tentar modificar o payload do token JWT para alterar os dados autorizados, como o nível de privilégios, a identidade do usuário ou outros atributos relevantes.

**JWT Injection:** É um ataque em que um invasor tenta inserir ou modificar os dados dentro do token JWT, geralmente manipulando o payload do token. O objetivo é alterar as informações autorizadas ou obter privilégios indevidos.

**JWT Brute-Force:** Nesse tipo de ataque, um invasor tenta adivinhar a chave secreta usada para assinar e verificar a integridade do token JWT. Por meio de força bruta ou dicionários de chaves possíveis, o invasor tenta encontrar a chave correta e, assim, comprometer a autenticidade do token.

**Interceptação e Reprodução:** Os invasores podem interceptar tokens JWT válidos durante a transmissão ou armazenamento e reutilizá-los posteriormente para obter acesso não autorizado.

**JWT Replay:** Nesse ataque, um invasor intercepta um token JWT válido e o reenvia posteriormente para obter acesso não autorizado. O invasor explora a falta de controle de expiração ou mecanismos de proteção de repetição de tokens para realizar o ataque.

**Modificação de Assinatura:** Em alguns casos, um invasor pode tentar manipular a assinatura do token JWT para que pareça válida, mesmo após modificar o payload ou outros elementos do token.

**JWT Key Confusion:** Esse tipo de ataque ocorre quando uma implementação incorreta gera e valida tokens JWT usando chaves diferentes. O invasor pode explorar essa inconsistência para criar ou manipular tokens com uma chave diferente daquela esperada, resultando em autenticação bem-sucedida e acesso indevido.

JWT Ataques

JWT.IO

JWT-Hack

JWT\_Tool

Tools

# Mitigando vulnerabilidades

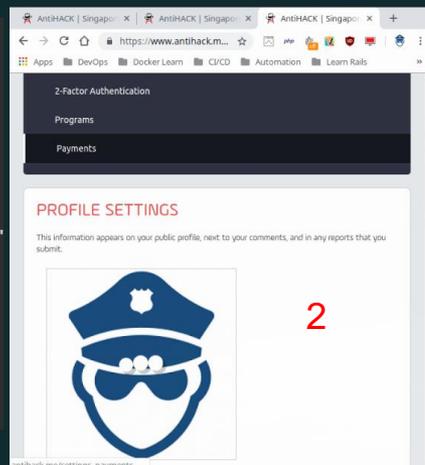
- Validação e Sanitização de Dados, processando qualquer dado e validando antes de processá-los e exibi-los;
- Escape de Saída, garantindo que os dados inseridos sejam tratados corretamente;
- Autenticação Robusta, usando mecanismos de armazenamento de senha segura com HASH + SALT;
- Proteção CSRF, usando tokens anti-csrf e implementações de cabeçalhos HTTP
- Controle de Acesso restritivos;
- Configuração de Arquivos de Upload, limitando uploads por extensão e tamanho de arquivo;
- Gerenciamento de Subdomínio e monitoramento;
- Implementação Segura de JWT, sem armazenamento em LocalStorage e totalmente rotativo;



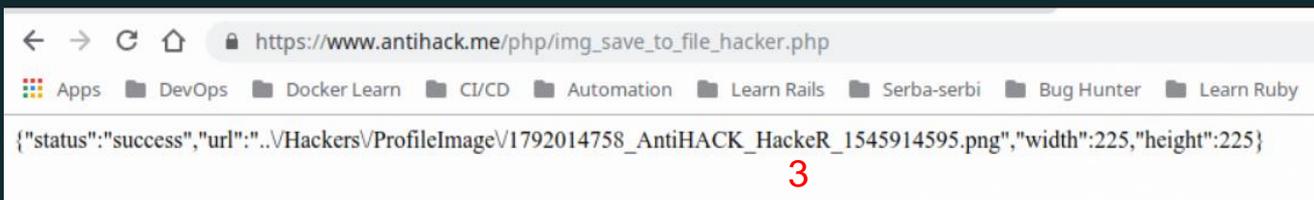
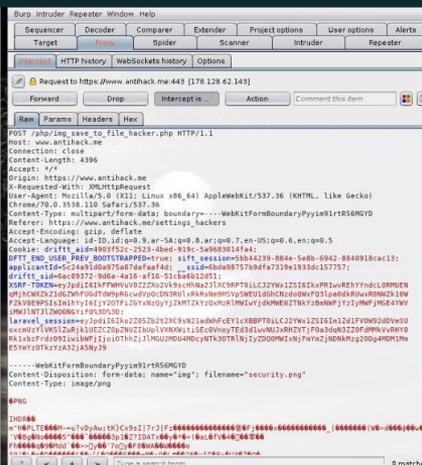
# Exemplos de exploração – CSRF e Arbitrary File Upload

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>CSRF File Upload</title>
</head>
<body>
  <form action="https://www.antihack.me/php/img_save_to_file_hacker.php" method="POST" name="csrf">
    <input type="file" name="img">
    <input name="HOST" value="AntiHACK">
    <input type="submit" value="Kirim">
  </form>
</body>
</html>
```

1



2



3



# Exemplos de exploração – Subdomain Takeover

```
← → ↻ 🔒 [redacted].amazonaws.com

Este arquivo XML não parece ter qualquer informação de estilo associado a ele. A estrutura do documento é mostrada at

<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>NoSuchBucket</Code>
  <Message>The specified bucket does not exist</Message>
  <BucketName>[redacted]</BucketName>
  <RequestId>2A2PVXEX0SS7EH7D</RequestId>
</Error>
<HostId>
  VRLQoh8iOWMO5QqhyaiuKTr06b6sAdeS7rsoi2eRV7AjNuoPWHV2zAD4smm5iI9NDdJ/GkeS126zTcU0cYX
</HostId>
</Error>
```

[Alt+S] Global JoasA

Bloqueio de objeto  
Desabilitado

No momento, o Amazon S3 não oferece suporte à habilitação do bloqueio de objetos após a criação de um bucket. Para habilitar o bloqueio de objetos deste bucket, entre em contato com o [suporte ao cliente](#)

**Pagamento pelo solicitante** Edit  
Quando habilitado, o solicitante paga os custos de solicitações e transferências de dados, e o acesso anônimo a este bucket é desabilitado. [Saiba mais](#)

Pagamento pelo solicitante  
Desabilitado

**Hospedagem de site estático** Edit  
Use este bucket para hospedar um site ou redirecionar solicitações. [Saiba mais](#)

Hospedagem de site estático  
Habilitado

Tipo de hospedagem  
Hospedagem de buckets

Endpoint de site de bucket  
Quando você configura seu bucket como um site estático, o site fica disponível no endpoint de site específico da região da AWS do bucket. [Saiba mais](#)

[http://\[redacted\].us-east-2.amazonaws.com](http://[redacted].us-east-2.amazonaws.com)

← → ↻ ⚠ Não seguro [redacted].website.us-east-2.amazonaws.com

# HACKERSEC PENTEST

# Exemplos de exploração – XSS DOM

Dispositivo ou navegador não suportado

Para garantir a melhor experiência, utilize o navegador Google Chrome (no desktop) ou o navegador de seu smartphone. Para isso, abra o link no botão "COPIAR LINK":

``

OK

Transferindo dados de credenciais homolog.acesso.io...

Inspetor Debugger Console Editor de estilos Rede Desempenho Memória Armazenamento Acessibilidade Aplicação

```
var i = new URLSearchParams(window.location.search)
URLSearchParams(3) { os -> "generic", id -> "xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx", url -> "https://www.google.com?id=xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx" }
url: getAppPartURL('Capture/SMS/BrowserNotSupported.aspx/GenerateQRCode')
">","undefined" />
i != null ? (t = i.url, $('#qrCodeWrapper').append('')) : ($('#txtMessage').html('Ops, alguma coisa deu errado!'))
Object { 0: div#qrCodeWrapper.row, length: 1 }
url: getAppPartURL('Capture/SMS/BrowserNotSupported.aspx/GenerateQRCode'),
i != null ? (t = i.url, $('#qrCodeWrapper').append('')) : ($('#txtMessage').html('Ops, alguma coisa deu err
Object { 0: div#qrCodeWrapper.row, length: 1 }
url: getAppPartURL('Capture/SMS/BrowserNotSupported.aspx/GenerateQRCode'),
i != null ? (t = i.url, $('#qrCodeWrapper').append('<img src=x onerror=alert(document.domain)>', ' + i.qrCode + '" />')) : ($('#txtMessage').html('Ops, alguma
Object { 0: div#qrCodeWrapper.row, length: 1 }
```



MAIS UM EVENTO



REALIZAÇÃO



# ROADSEC 15 2023

O MAIOR FESTIVAL HACKER DA AMÉRICA LATINA



15.07.23

## JOAS SANTOS

RED TEAM LEADER - HACKERSEC  
[in/joas-antonio-dos-santos](https://www.linkedin.com/in/joas-antonio-dos-santos/)



[linkedin/joas-antonio-dos-santos/](https://www.linkedin.com/in/joas-antonio-dos-santos/)