Tempest

# Cross-Site Script Inclusion

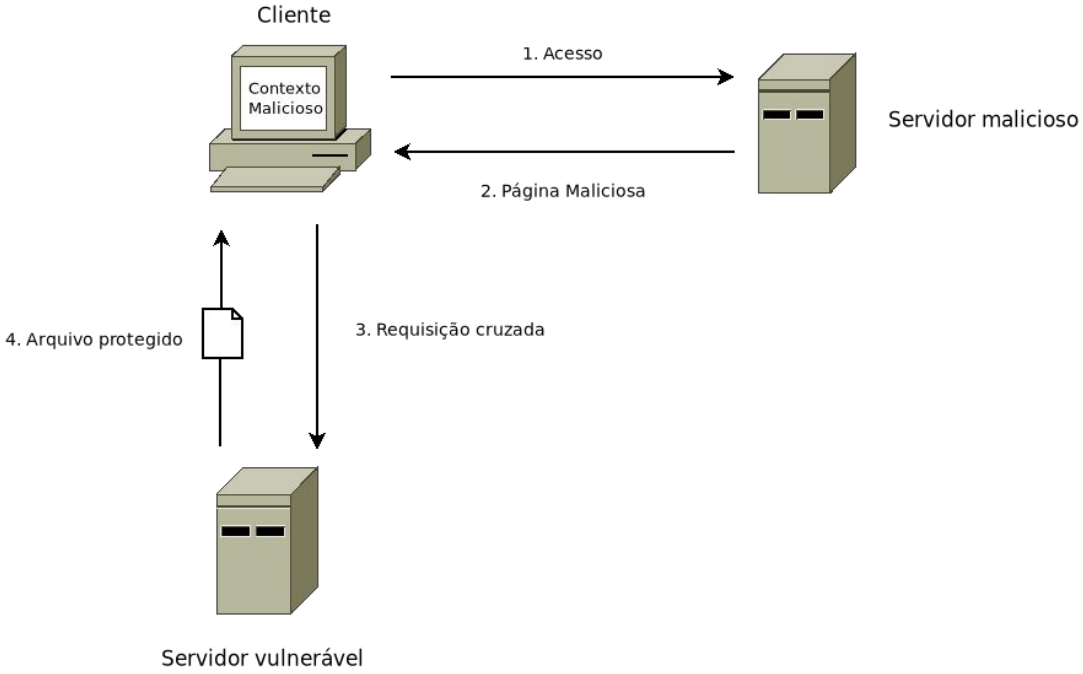
Um estudo das estratégias de mitigação e atual prevalência da vulnerabilidade em navegadores

Henrique Curi de Miranda (Tempest / UFLA)
Henrique Arcoverde (Tempest)
Renan Villela Oliveira (UFLA)
Luiz H. A. Correia (UFLA)

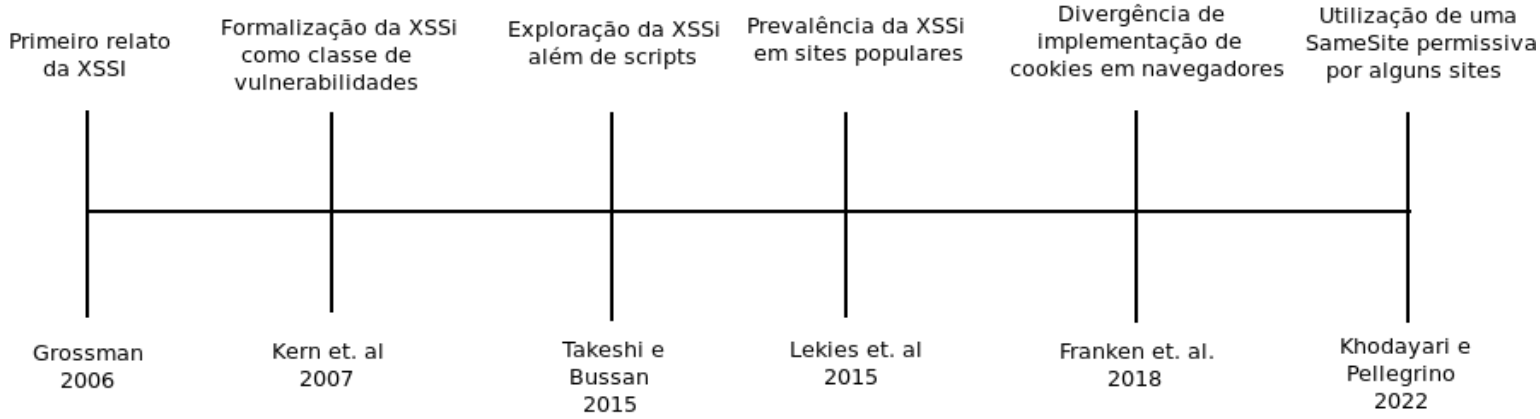
Tempest

# Introdução

# Cross-Site Script Inclusion (XSSi)



# Trabalhos relacionados



# • Objetivos

- Estudar o impacto da SameSite na exploração da XSSi
- Observar a vulnerabilidade em navegadores atualizados

Tempest

Tempest

# Ambiente de Testes

# • Servidor vulnerável

- Autenticação e controle de permissão: 200 / 403
- Samesite: None, Lax, sem declaração
- 3 arquivos vulneráveis: JSONP, Javascript, Imagem

Tempest

# • Servidor malicioso

- Exploração de cada caso implementado

Tempest

# • Cliente

- Navegadores atualizados (Jan/2024)

- Chromium, Chrome, OperaGX, Opera, Edge, Vivaldi, Avast Secure Browser, Firefox, Brave, Tor, Librewolf

Tempest

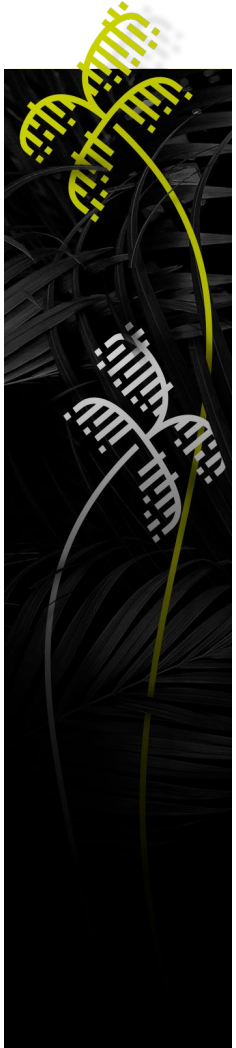
Tempest

# Resultados e Discussão


- Mudança de comportamento a partir da 102.1esr

Tempest

Tempest



GET https://tccxssi.duckdns.org/tcc.jsonp

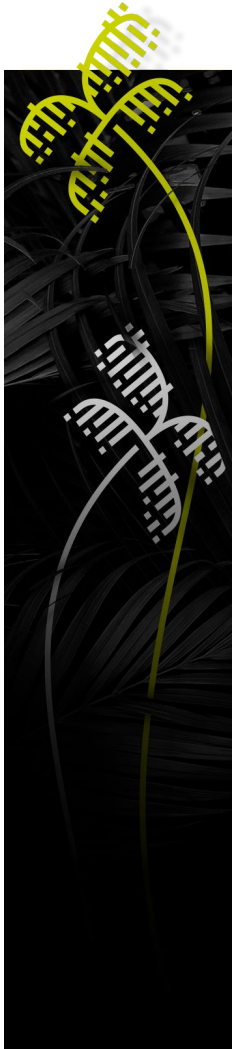
| | |
|---|---|
| Status | 200 OK |
| Versão | HTTP/1.1 |
| Transferido | 75 B (tamanho 75 B) |
| Referrer Policy | strict-origin-when-cross-origin |

Cabeçalhos da resposta (258 B)

Cabeçalhos da requisição (422 B)

- Accept: */*
- Accept-Encoding: gzip, deflate, br
- Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
- Connection: keep-alive
- Cookie: authenticated=true
- Host: tccxssi.duckdns.org
- Referer: *http://tccatacante.duckdns.org/*
- Sec-Fetch-Dest: script
- Sec-Fetch-Mode: no-cors
- Sec-Fetch-Site: cross-site
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0

Tempest



GET https://tccxssi.duckdns.org/tcc.jsonp

| | |
|---|---|
| Status | 403 Forbidden |
| Versão | HTTP/1.1 |
| Transferido | 502 B (tamanho 285 B) |
| Referrer Policy | strict-origin-when-cross-origin |

Cabeçalhos da resposta (217 B)

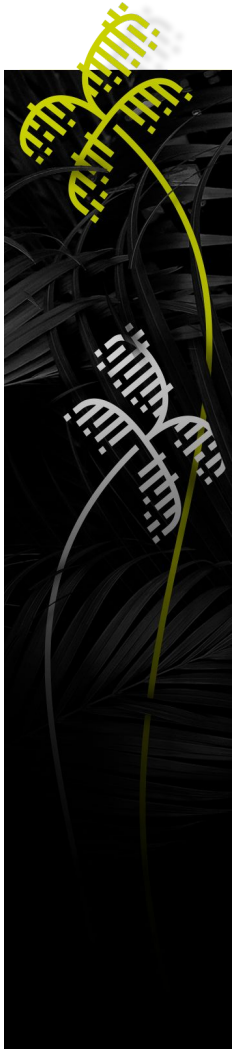
Cabeçalhos da requisição (394 B)

- Accept: */*
- Accept-Encoding: gzip, deflate, br
- Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
- Connection: keep-alive
- Host: tccxssi.duckdns.org
- Referer: *http://tccatacante.duckdns.org/*
- Sec-Fetch-Dest: script
- Sec-Fetch-Mode: no-cors
- Sec-Fetch-Site: cross-site
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0


- Exploração para SameSite=None em 7 navegadores

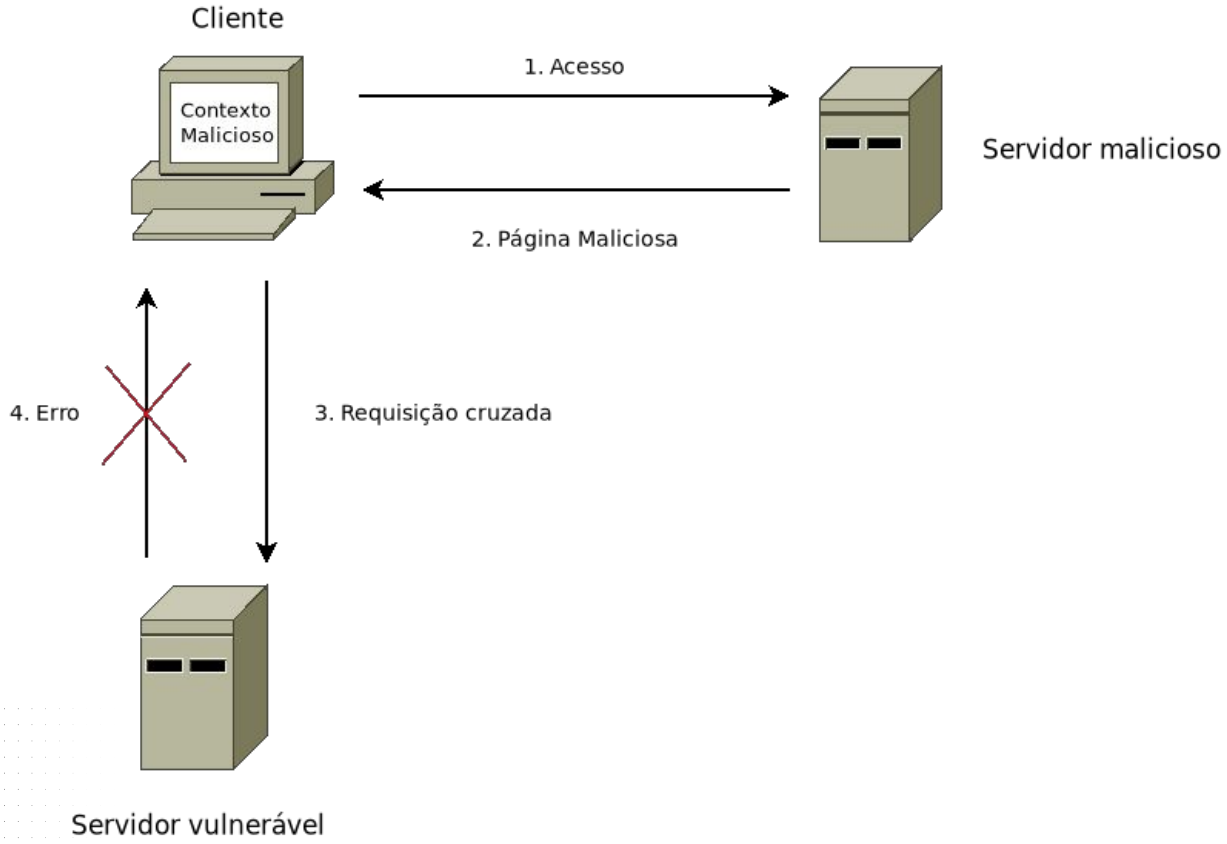
Tempest

| | *None* | *Lax* | Sem declaração |
|---|---|---|---|
| **Casos explorados** | 3 | 0 | 0 |
| **Navegadores explorados** | 7 | 0 | 0 |
| **Navegadores não explorados** | 4 | 11 | 11 |



Tempest

| Navegador | Versão | Ocorreu exploração? | Base | Lançamento |
|---|---|---|---|---|
| Chromium | 120.0.6099.224 | Sim | Própria | 12/01/2024 |
| Chrome | 121.0.6167.86 | Sim | Chromium | 25/01/2024 |
| OperaGX | 106.0.4998.61 | Sim | Chromium | 25/01/2024 |
| Opera | 106.0.4998.52 | Sim | Chromium | 18/01/2024 |
| Edge | 120.0.2210.144 | Sim | Chromium | 17/01/2024 |
| Vivaldi | 6.5.3206.57 | Sim | Chromium | 24/01/2024 |
| Avast Secure Browser | 120.0.23647.224 | Sim | Chromium | 19/01/2024 |
| Firefox | 122.0 | Não | Própria | 23/01/2024 |
| Brave | 1.61.120 | Não | Chromium | 17/01/2024 |
| Tor | 13.0.9 | Não | Firefox | 22/01/2024 |
| LibreWolf | 122.0-1 | Não | Firefox | 24/01/2024 |


Cliente
Contexto Malicioso
1. Acesso
Servidor malicioso
2. Página Maliciosa
4. Erro
3. Requisição cruzada
Servidor vulnerável

Tempest

# Conclusões e Trabalhos futuros

# • Conclusões

- Estratégia de mitigação baseada na SameSite
- Divergência de padronização de implementação da SameSite e SOP

Tempest

# • Trabalhos futuros

- Estudo de outras vulnerabilidades
- Análise de código fonte
- Impacto em imagens

Tempest

Tempest

# Obrigado!